UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

Tesi di Dottorato in Ingegneria Informatica e Automatica

XXVII Ciclo

Methods and Techniques for Enhancing Physical Security of Critical Infrastructures

---

Author:

Dr. Annarita DRAGO

Supervisors:

Prof. Valeria VITTORINI

Dr. Concetta PRAGLIOLA

Coordinator:

Prof. Franco GAROFALO

A thesis submitted in fulfillment of the requirements
for the degree of Doctor of Philosophy

Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione

March 2015

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

Bruce Schneier

UNIVERSITY OF NAPLES *"FEDERICO II"*

Abstract

Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione

Doctor of Philosophy

Methods and Techniques for Enhancing Physical Security of Critical Infrastructures

by Annarita Drago

In the last years, research on Critical Infrastructure Protection (CIP) has become one of the primary matters for the development of modern societies. Water, power, banking, transportation and communication systems are only a few examples of essential infrastructures to daily human activities and their protection is a concept relating to the preparedness and response to serious incidents that could threaten them. The term protection is a broader concept in which three main aspects can be individuated: safety, security, and emergency. The safety aspects are out of the scope of this thesis, indeed, the focus is on security. In particular, this investigation will address the concerns of security tied to physical and human factors without considering those related to the cyber ones. This is because the present work is born in the railway context, where the attention is usually oriented to the physical aspects of security since, until now, a common practice has been to realize dedicated connections and isolated networks. With respect to the emergency aspects, only the advantages that a security solution can induce will considered. Physical security is one of the most fundamental aspect of the protection. It concerns the use of physical controls for protecting premises, sites, facilities, buildings or other physical assets belonging to the critical sectors. The application of physical security is the process of using layers of physical protective measures to prevent unauthorized access or harm. This harm can involve terrorism, theft, destruction, sabotage, vandalism, espionage, and similar. A crucial element which contributes to improve the protection of critical infrastructures seamlessly is the technology. Thanks to fast technological progress, it is possible to build complex surveillance systems able to integrate heterogeneous sources which can monitor environments potentially at risk. In this way, resilience may be accomplished, for example, through hardening the system by adding redundancy and robustness. However, for enhancing significantly the protection level, integration of different technologies is not enough, but a collaborative approach is essential. A strong protection calls for interoperability not only among ICT systems, but also among different operators, organizations, companies, and any other entity belonging to the public security sector. Nevertheless, the security designer must determine how best to combine elements like fences, barriers, sensors, procedures, security systems, and security personnel into a Physical Security System (PPS) that can achieve the protection objectives. For this reason, another important element is to conduct a systematic evaluation in which quantitative and/or qualitative techniques are

used to predict overall system effectiveness, by identifying exploitable weaknesses in asset protection for a given threat. The original contribution of this thesis is to provide methods for enhancing effectiveness and reliability of integrated security systems in order to guarantee an adequate protection level. To achieve the desired level of protection, a two phase approach is proposed combining proactive and reactive strategies. The first one involves the vulnerability assessment based on quantitative methods and the second one introduces an interoperability framework. Specifically, this thesis is the result of research funded by Ansaldo STS, a leader company in railway industry, and carried out also thanks to involvement in research projects about security theme (such as SECUR-ED and METRIP).

Contents

List of Figures

List of Tables

Acronym

ACS	**A**ccess **C**ontrol **S**ystem
ASSESS	**A**nalytic **S**ystem and **S**oftware for **E**valuating **S**afeguards and **S**ecurity
ATL	**A**TLAS **T**ransformation **L**anguage
BN	**B**ayesian **N**etwork
CBRNE	**C**hemical, **B**iological, **R**adiological, **N**uclear and high-yield **E**xplosives
CAP	**C**ommon **A**lerting **P**rotocol
CCTV	**C**losed **C**ircuit **T**ele**V**ision
CI	**C**ritical **I**nfrastructure
CIP	**C**ritical **I**nfrastructure **P**rotection
CMS	**C**risis **M**anagement **S**ystem
CPT	**C**onditional **P**robability **T**able
DoD	**D**epartment **o**f **D**efense
DSML	**D**omain **S**pecific **M**odeling **L**anguage
EASI	**E**stimated of **A**dversary **S**equence **I**nterruption
EDA	**E**vent **D**riven **A**rchitecture
FP	**F**ramework **P**rogramme
ICT	**I**nformation & **C**ommunication **T**echnology
IDS	**I**ntrusion **D**etection **S**ystem
ISEM	**I**nsider **S**afeguards **E**ffectiveness **M**odel
MDE	**M**odel **D**riven **E**ngineering
METRIP	**ME**thodological **T**ool for **R**ailway **I**nfrastructure **P**rotection

OASIS	**O**rganization for the **A**dvancement of **S**tructured **I**nformation **S**tandard
PPS	**P**rotection **P**hysical **S**ystem
PSIM	**P**hysical **S**ecurity **I**nformation **M**anagement
PTZ	**P**an **T**ilt **Z**oom
RIS	**R**ailway **I**nfrastructure **S**ystem
SAPE	**S**ystematic **A**nalysis of Physical **P**rotection **E**ffectiveness
SAVI	**S**ystematic **A**nalysis of **V**ulnerability to **I**ntrusion
SECUR-ED	**SEC**ured **U**rban **T**ransportation - **E**uropean **D**emonstration
SIEM	**S**ecurity **I**nformation and **E**vent **M**anagement
SMS	**S**ecurity **M**anagement **S**ystem
SOA	**S**ervice **O**riented **A**rchitecture
SOAP	**S**imple **O**bject **A**ccess **P**rotocol
VMS	**V**ideo **M**anagement **S**ystem
UML	**U**nified **M**odeling **L**anguage
UMT	**U**rban **M**ass **T**ransportation
URN	**U**niform **R**esource **N**ame
VA	**V**ulnerability **A**ssessment
VAM	**V**ulnerability **A**nalysis and **M**odeling
VCA	**V**ideo **C**ontent **A**nalysis
WS	**W**eb **S**ervice
WSDL	**W**eb **S**ervice **D**escription **L**anguage
XML	e**X**tensible **M**arkup **L**anguage

Introduction

Security of contemporary society is a primary concern broadly discussed in recent years, especially in connection with the spread of international terrorism which still represents a complicated issue to contain or, at least, to mitigate. This has contributed to generate a considerable feeling of being unsafe among the population, since their lives are strictly dependent on the use of complex infrastructures defined as "critical". They allow to simplify and accelerate the main human activities and, for this reason, they are often the target of criminal, vandalistic and terroristic actions. At this aim, the European Union has established legislative instruments (e.g. the directive 2008/114/EC [3] establishes a procedure for identifying and designating European Critical Infrastructures and a common approach for assessing the need to improve their protection) and financial ones (e.g the "Secure Societies-Protecting freedom and security of Europe and its citizens" programme in HORIZON 2020) in order to protect critical infrastructures. In particular, the European Parliament defines a critical infrastructure as *an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.* From this definition, the key role and the importance that these infrastructures have in the current society comes to light, and consequently the need for enhancing their security is felt. Even if the responsibility to define objectives is a task of the Institutions, the fulfillment of measures for reducing vulnerability of strategic assets depends mainly on the effort and actions of the different authorities and organizations involved, belonging to both public and private sectors. It is clear that, in order to meet this need, a multidisciplinary research is necessary to develop and

implement new technological solutions able to provide a proper reaction against the main threats for citizens' global security, respecting the people's basic rights. The work described in this thesis takes up the challenge of deal with the issues described above, trying to combine research and technology as a result of joint support of University and Company in order to encourage innovation, also through technology transfer processes between academic and manufacturing community. Specifically, this thesis is the result of research funded by Ansaldo STS, an international railway transportation leader in the field of signaling and integrated transport systems for passenger traffic and freight operation, and carried out also thanks to involvement in research projects about security theme (such as SECURED[1] and METRIP[2]). In this perspective, the area of interest of this work is the critical infrastructure protection, focusing on physical security.
The physical protection of CIs requires the development of innovative approaches for identification, detection and mitigation of threats, vulnerabilities and risks. Hence, it represents an area in which practical needs (e.g., coming from end-users), technological resources (e.g., belonging to physical security market) and scientific research (e.g., evaluation of effectiveness of physical protection system) converge all together. In such context, the thesis concerns two aspects of the protection that together can contribute to enhance the effectiveness of the protection: i) an architectural approach which enables the interoperability of security systems and involved organizations; and ii) an analytical approach for evaluating the effectiveness of the overall protection system. At this aim, this thesis is structured as follows:

- Chapter 1 provides an overview of the physical security and the main open issues. In particular, it addresses the aspects consisting of the architecture and analysis of the Physical Protection Systems. The chapter also describes the railway domain, the application field of this work.

- Chapter 2 presents a methodology for the vulnerability assessment of a PPS that has been partially supported by the METRIP project. It concerns a MDE approach in which an UML profile, a vulnerability model, and the model transformations have been defined.

[1] http://www.secur-ed.eu/
[2] http://metrip.unicampus.it/

- Chapter 3 reports the experience with the concrete application of a System-of-Systems conducted in the SECUR-ED project. In particular, an innovative interoperability framework, which represents a technological approach for improving physical protection, will be presented.

- Chapter 4 deals with a case study, performed on a real metro system, where both the approaches included in the previous chapters will be applied, in order to show that vulnerability analysis and security management are the two sides of the same coin.

Chapter 1

Physical Protection

In the last years, research on Critical Infrastructure Protection (CIP) has become one of the primary matters for the development of modern societies. Water, power, banking, transportation and communication systems are only a few examples of essential infrastructures to daily human activities and their protection is a concept relating to the preparedness and response to serious incidents that could threaten them. Moreover, the last traumatic events have given still more prominence to protection of CIs. A recent work [4] presents a comprehensive literature review of significant extreme events that occurred in the past two decades which exposes an insufficient preparedness and maturity in case of serious events.

The Council of the European Union states, *"protection" means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralize a threat, risk or vulnerability* [3].

As reflected in this definition, the term protection is a broader concept in which three main aspects can be individuate: safety, security, and emergency. *Safety* involves the safeguard or protection against events or situations generally unintentional such as malfunctioning or faults of systems, accidents caused by human carelessness, inattentiveness, lack of training, and so on. Instead, *security* refers to the safeguard or protection of people and assets against attacks, assaults, and damages carried out voluntarily by individual or organizations in order to harm. This includes civil disturbances, sabotage, theft of critical property or information, pilferage, extortion or other intentional attacks on assets by a human. *Emergency*

refers to all those activities which have to be undertaken when safety and/or security fail and consequently require intervention of rescue teams such as first responders, civil protection, fire brigade, and so on. Thus, it regards the containment of hazard and minimization of damages. The relationships between these aspects are depicted in figure 1.1.

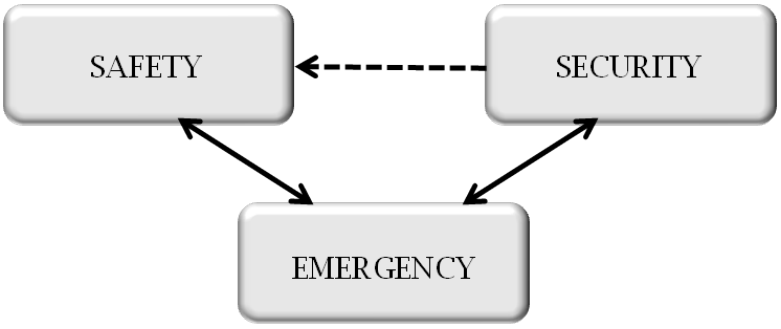


FIGURE 1.1: Aspects of protection

Often the binomial safety-security is used indiscriminately, but, as highlighted, the two terms differ in the triggering events of a disaster. For in-depth analysis, in [5] the authors explain how to avoid ambiguities in the terms "security" and "safety". On the contrary, the emergency does not focus on the origin of crisis, but manages its consequences. Furthermore, security can affect safety; for example, a disgruntled employee can sabotage critical equipment causing a disaster which can appear at a first glance like a lack of safety measures.

The safety aspects are out of the scope of this thesis, indeed, the focus is on the security. Nevertheless, this investigation will address the concerns of security tied to physical and human factors without considering those related to the cyber ones. This is because the present work is born in the railway context, where the attention is usually oriented to the physical aspects of security since, until now, a common practice has been to realize dedicated connections and isolated networks. With respect to the emergency aspects, only the advantages that a security solution can induce will considered.

A security threat is always attributable to a location (within a bus, a station platform, etc.) at a given moment (when there is a crowd, after a football game, etc.) and involves someone (criminal, bomber, suicidal person, etc.) and/or something harmful (bomb, gun, toxic gas, fire, knife, etc.). In order to face such critical

situations the security strategies that can be adopted are fundamentally three: proactive (stop the event before it occurs), reactive (act to limit the impact of the event, if the previous strategy fails), and forensic (get information to put the system back in operation). Obviously, from a security perspective, the best is to be as proactive as possible (stopping terrorists before they burst their bomb is preferable than finding the culprits), but it is very hard to meet this objective from a technological point of view. Using disparate technologies surely will help to have a reactive behavior to threats, while the proactive effect will be strictly limited to the motivations inciting an attacker. Generally, a proactive approach involves assessment methodologies, more or less detailed and complex, able to analyze or prove the protection levels of an infrastructure. Eventually, the forensic strategies can help to understand the dynamics of a successful attack in order to discover where and why the system failed. In addition, they allow to gather important information useful for facing future threats.

1.1 Physical Security

Physical security is one of the most fundamental aspect of the protection. It concerns the use of physical controls for protecting premises, sites, facilities, buildings or other physical assets belonging to the critical sectors. The application of physical security is the process of using layers of physical protective measures to prevent unauthorized access or harm. This harm can involve terrorism, theft, destruction, sabotage, vandalism, espionage, and similar.

The choice among the physical security measures to be adopted depends greatly on what assets need to be protected, where they are located, and what threats, vulnerabilities, and risks pertain to them. Thus, applying an appropriate level of protection requires a specific understanding of environment under consideration as well as the threats to which is exposed. In order to accomplish this, it is clear that an effective design have to be carried out. So, an effective design involves the use of multiple layers of interdependent systems and covers all the means and technologies for perimeter, external and internal protection such as barrier, lighting, different kinds of sensors, closed-circuit television, access control, and people. In this phase the choice of technological security systems and the adoption of

architectures for integrating such systems play an important role, since they are effective means that contribute to increase resilience of a CI, providing early warning of threats and improving the response to eventual disasters.
However, the activities tied to security design are very difficult considered the complexity and interconnectedness of current infrastructures, the lack of standards in physical security matters, the diversity of threats, and the different local regulations. Furthermore, the cost of physical security is not insignificant. Reaching an appropriate balance between adequate levels of protection and the cost of the systems enabling physical protection can be hard. Too little security leaves vulnerabilities in place, increasing risks. Too much security may mitigate threats and vulnerabilities and reduce risks, but leads to unnecessary expenditures. Inefficient application of security controls (spending more than you need for a physical security service or product) may use scarce resources that otherwise would be available for additional protective measures [6]. Consequently, a trade-off between costs and effective protection based on their contributions to risk reduction is necessary.
Translating strategic security objectives into wise choices is a challenging design problem both when designing a new physical security system and when upgrading to an existing system. In the context of infrastructure resilience and protection some considerations have been made for guaranteeing a certain risk level.
A crucial element which contributes to improve the protection of critical infrastructures seamlessly is the technology. Thanks to the fast technological progress, it is possible to build complex surveillance systems able to integrate heterogeneous sources which can monitor environments potentially at risk. In this way, resilience may be accomplished, for example, through hardening the system by adding redundancy and robustness. However, for enhancing significantly the protection level, integration of different technologies is not enough, but a collaborative approach is essential. A strong protection calls for interoperability not only among ICT systems, but also among different operators, organizations, companies, and any other entity belonging to the public security sector. This lead to look into System-of-Systems approaches, whose issues are still subject matter for discussion, since they are systems evolving continuously and quickly [7]. All this makes up the tools for managing the complexity of the protection and for reducing the intervention times lending support to crisis management with a better promptness. Nevertheless, the designer must determine how best to combine elements like

fences, barriers, sensors, procedures, security systems, and security personnel into a Physical Security System (PPS) that can achieve the protection objectives. For this reason, another important element is to conduct a systematic evaluation in which quantitative and/or qualitative techniques are used to predict overall system effectiveness, by identifying exploitable weaknesses in asset protection for a defined threat. A typical weakness of the PPS is quite the lack of a global and integrated vulnerability evaluation. Traditionally, their effectiveness evaluation was due to judgments of experts because of the lack of scientific methods able to provide systematic and objective estimates. On the contrary, an accurate vulnerability assessment can produce results for establishing the requirements during the design of the PPS and, in addition, it can also support the decisions regarding protection system upgrades. [8].

1.2 The Vulnerability Problem

Effective protection demands the availability of proper methodologies and tools to evaluate the vulnerability of the assets, and the ability of the adopted protection systems to meet its objectives.

The vulnerability is a very complex concept which has more interpretations in research literature. An accurate disquisition about the term "vulnerability" can be found in [9], where the author exposes the meaning of the concept in different scientific research communities. Some interesting definitions for the context of this work are "*Vulnerability is emerging as a multi-dimensional concept involving at least exposure - the degree to which a human group or ecosystem comes into contact with particular stresses; sensitivity - the degree to which an exposure unit is affected by exposure to any set of stresses; and resilience - the ability of the exposure unit to resist or recover from the damage associated with the convergence of multiple stresses*" or "*vulnerability is an incapacity to anticipate, cope with, resist to, adapt to and recover from hazards*". In [10], vulnerability is defined as the *susceptibility* to physical injury or threat. For Haims[11], "*vulnerability is the manifestation of the inherent states of the system (e.g. physical, technical, organizational, cultural) that can be exploited by an adversary to harm or damage the*

system". Therefore, the vulnerability concept implies the possibility that a traumatic event causes probable harms.
Several protective factors exist for preventing, limiting and modulating the risk that such vulnerabilities can induce. The term vulnerability is sometime confused with risk. In general terms, the risk can be considered as a cumulative index which expresses the likelihood of the occurrence of an undesirable event and of the potential damages to the environment, permanent or long-term. Actually, the vulnerability can be considered as an internal risk factor of a system or a subject that is exposed to a threat and it corresponds to its intrinsic predisposition to be affected to damage[12]. Then, reducing vulnerability can reduce risk and consequently increase resilience which in turn may reduce the consequences of a disaster.

1.2.1 Vulnerability Assessment

The Vulnerability Assessment (VA) is a proactive strategy for improving infrastructure security and it is able to provide essential information that may be used in the Risk Assessment process. Risk Assessment requires a suitable understanding of both threats and vulnerabilities. Both of them should be identified, but generally the threats often remain out of control, while vulnerabilities may be corrected through security countermeasures. This means it is very hard to stop the efforts of an international terrorist group in advance, but it is possible to strengthen the security in the weak points of an infrastructure.
One of the most delicate task is to evaluate risk and vulnerability. In this perspective the analysis can be both *quantitative* and *qualitative*. In a quantitative analysis, an adequate quantity of numerical data is necessary for calculating the risk of an attack in terms of probability. Very often such data are not available and thus a qualitative analysis may be better suited. These kinds of methods require generally less effort and, in certain cases, can be also used in support of quantitative methods.
Given the broad spectrum of existing critical infrastructures, some methodologies either quantitative or qualitative have emerged in academic literature but, in practice, the most used methods are qualitative. [13] provides a state of the art of risk

methodologies; certain methods include both risk analysis and vulnerability analysis, while others are more suited to specific systems or a specific need. Generally, existing quantitative methodologies focus on one kind of critical infrastructure such as telecommunications (in [14] is possible to find an overview of approaches for evaluating network vulnerabilities), critical information systems ([15] proposes a methodology for a supervisory control and data acquisition (SCADA) system), water system (in [16] a parametric-system method based on background value is used for the quantitative assessment of each subsystem and of the integrated water resources system), and so on. Finally, in [17], Ezell et al. provide a description of the probabilistic techniques widely used to carry out risk and vulnerability analysis.
A well-known formula used in risk analysis field is the following[18]:

$$Risk = Threat \cdot Vulnerability \cdot Consequence \tag{1.1}$$

that is, risk represents the expected consequences of attacks, taking into account the likelihood that attacks occur and that they are successful, if attempted. In spite of its simplicity, this formula needs the evaluation of three parameters whose value is hard to compute especially in quantitative terms.
A quantitative definition of the vulnerability is given by Lewis [19], who defines it as "a conditional probability", that is the probability that an asset suffers damages if an attack occurs or, in probabilistic terms:

$$Vulnerability = P(attack\ results\ in\ damage | attack\ occurs) \tag{1.2}$$

Note that the measure specified above does not include magnitude of the damage. This measure assumes a representation of vulnerability in which there is either a successful attack with damage or no success with no damage [18].

Traditionally, the literature exhibits two distinct research branches for addressing vulnerability evaluation: threat-driven and asset-driven.
The threat-driven approaches are suitable for analyzing the initiating events that are well understood and whose rate of occurrence can be reliably deducted from historical data. The main disadvantage of these approach is that they ultimately

fail to consider emerging or unrecognized threats devised by an innovative adversary [20]. A recent threat-driven approach can be found in [21]. This paper presents an asset vulnerability model based on his earlier work in game theory and designed to provide a strategic risk measure which is predicated on the probability of failure of an attacker.

Asset-driven approaches search for sensitive points that attackers can exploit to kill a lot of people and damage environmental assets. Thus, they focus on finding and mitigating vulnerabilities regardless of whether a specific kind of event has occurred. In other word, these methods estimate the consequences and probability of success of an attacker for an exhaustive set of plausible scenarios, without considering their occurrence probability [22].

Other approaches that does not belong to these two categories exist and they can be found in [21].

Up to now, a little attention has been devoted to approaches which integrate more aspects. In [8], Garcia considers both of them, but the attacks are considered form an high level of detail. An interesting work moving towards this direction is [23], where the authors present a novel attack tree paradigm, called attack countermeasure tree, which takes into account attacks as well as countermeasures (in the form of detection and mitigation events). Again, [24] provides an intuitive and visual representation of interactions between an attacker and a defender of a system, as well as the evolution of the security mechanisms and vulnerabilities of a system.

Finally, many studies on vulnerability assessment focus on modelling of the CIs' interdependencies. In these works, typically, the adopted approaches aim to understand structural vulnerabilities through "what-if" analysis and simulations in order to asses and mitigate the risk of domino effects and multiple disruptions, and to provide a support to decision-makers. For example, a popular work is [25], where the authors explore the challenges and complexities of the interdependencies making an analysis with respect to different dimensions.

1.2.2 Evaluating Physical Protection Systems

A Physical Protection System (PPS) involves systems, procedures and people for the protection of assets and facilities from malevolent human attacks [26]. The

capability of a PPS to withstand a possible attack and prevent an attacker from achieving his objectives is generally specified as PPS effectiveness. Thus, with respect to the protection measures, assessing the vulnerability corresponds to evaluate the effectiveness of the protection systems. The PPS can be considered to be effective only when it contributes to decrease the risk to an acceptable level. Quantitative techniques are recommended for facilities with high-consequence loss assets [8]. In this perspective, Hennessey et al. [27] express the vulnerability term as

$$V = 1 - P_E \quad P_E = P_D \cdot (P_I \cdot P_N) \quad P_D = P_S \cdot P_A \tag{1.3}$$

where:

- P_E (Probability of effectiveness) is the probability that the physical protection system is effective;
- P_D (Probability of detection) is calculated through the P_S and P_A values and it represents the probability that an attacker has been detected;
- P_S (Probability of sensing) is the probability that a sensing system detects the attack;
- P_A (Probability of assessment) is the probability that a security operator at the control room correctly assess the situation and react accordingly;
- P_I (Probability of interruption) is the probability that the reaction to the attack takes place in time in order to neutralize it;
- P_N (Probability of neutralization) is the probability that the reaction successfully neutralizes the threat.

There are many quantitative tools that can help the analyst to evaluate the effectiveness of a PPS. For giving an idea, in the following an overview of the most frequently used techniques for a quantitative evaluation of the effectiveness of a PPS [28] [26] will be briefly described. Furthermore, other approaches concerning the evaluation of a PPS face the problem from a point of view of optimization for optimally locating the physical protection components in order to balance cost and performance (e.g. see [29] and [30]).

1.2.2.1 EASI

The Estimated of Adversary Sequence Interruption (EASI) is an easy-to-use method developed to evaluate PPS performance at nuclear facilities under conditions of threat and system operation [31]. It is a pathway analysis combined with computer modeling techniques. The method consists of a probabilistic analysis of the interactions of detection, assessment, communications, delay, and response time. The results of the analysis are expressed in terms of the probability that the PPS can respond in time to stop specific action sequences of an attacker. The basic principle of this method is that attacks on nuclear facilities can only be averted after the prompt notification and response of the guard force which is presumed to be adequate. This involves the proper use of alarm systems to be considered in the evaluation.

1.2.2.2 SAVI

The Systematic Analysis of Vulnerability to Intrusion (SAVI) method evaluates the vulnerability of a PPS. Features of this method include analysis of all adversary paths, a safeguards-component catalog with a detection/delay performance database, results in graphic form, and path-upgrade recommendations [32]. Thus, the method enables to analyze all the possible paths of an attack and evaluate the most vulnerable paths including the position of a critical detection point along each path. It uses a multi-path model, called Adversary Sequence Diagram (ASD), where the facilities and the paths connecting them are represented. Since this ASD model is too simple, often it causes inaccuracies (i.e the distance needed to cross an area is considered equal when using the ASD, regardless of the particular route).

1.2.2.3 ASSESS

Developed under the sponsorship of the Department of Energy, the Analytic System and Software for Evaluating Safeguards and Security (ASSESS) is an analytical tool with the aim to conduct an integrated evaluation of safeguards systems at facilities handling facilities. This method is a standard procedure in the USA for

evaluating the PPS of nuclear facilities, airports and other important buildings. In particular, it focuses on the threat of theft/diversion of special nuclear material by insiders, outsiders, and a special form of insider/outsider collusion [**?**]. As the previous method, it uses a multi-path model, and, substantially, it is an enhanced version of SAVI with additional insider attack analysis and neutralization modules.

1.2.2.4 ISEM

The Insider Safeguards Effectiveness Model [33] is a stochastic, discrete event, monte-carlo simulation model which simulates the interaction of a group of insiders (guards or other employees who have authorized access to the facility) with the facility's safeguards system. The methodology provides a structure through which an analyst may choose guard tactics to complement the other portions of the safeguards system in combating the perceived threat. It is not dependent on the specific effectiveness model employed nor on the assumption that the adversary is an insider. The effectiveness of guard tactics is demonstrated by computing the effectiveness measure of a range of guard tactics employed in spite of a number of distinct insider paths through the facility.

1.2.2.5 SAPE

Systematic Analysis of Physical Protection Effectiveness [34] is the most recent method that presents an intuitive technique for the VA of a PPS. As the previous techniques, it deals with a pathway analysis in order to determine the ordered series of a potential adversary's actions (called an adversary path) and to calculate the probability that a response force will stop this adversary before his/her task is completed. Nevertheless, unlike the previous ones, the use of a two dimensional (2D) map of a facility as a model for a PPS is suggested as an alternative approach to the adversary sequence diagram. Compared to an ASD it has two advantages: providing an intuitive bird's eye views of a PPS, and representing relative positions between protection elements in a realistic way.

1.3 Technological Tools for Physical Security

In the past decade, the security landscape has dramatically changed with the introduction of several new security technologies to deter, detect and react to more disparate attacks. Organizations are constantly introducing new technologies and upgrading existing ones in order to ensure the security of their most valuable assets such as people, infrastructure, and property. Typical systems include access control systems, CCTV systems, intrusion detection systems, firefighting systems, CBRNe sensors, content video analytics, intelligent sound detection, perimeter intruder detection, and so on [35].

Redundancy and diversity of sensing technology is essential to build effective surveillance systems, but this increases the number of sensing devices and, consequently, of the alarms to be managed. So, the integration of such security systems has been one of the primary requirements in the scenario of the physical security. However, regarding the information integration and management, the industry is still underdeveloped. In fact, potential capabilities of traditional systems are limited by their low abilities in data analysis and interpretation, resulting in an inadequate prevention and real-time reaction.

In practical applications, each monitoring system is managed by means of an ad-hoc software platform. The traditional surveillance solutions include, for example, VMS (Video Management System), ACS (Access Control System), etc. They provide an overview of the installed devices (with a related report of diagnostic, warning, and alert messages) and a set of basic functionalities (e.g. for data acquisition, control, configuration, and rules setting). In this way, each event is handled separately without an effective information sharing, resulting in a very fragmented approach to the physical security [1]. Furthermore, the separated use of multiple systems can even complicate the security management. For example, take a human operator at the control center: in case of attack he may be inundated of alert messages, coming from multiple separated interfaces, one for each management system of the single technology. Hence, industrial needs require supporting platforms capable of integrating monitoring components with data processing subsystems, with also final consumers of produced warnings.

A well-designed integrated security system allows the full control of a CI, unifying alarm signaling, management and control procedures, optimizing the human

resource necessary. The general architecture (Figure 1.2) is composed by three fundamental components: field subsystems, communication network, and supervision and control system [36].

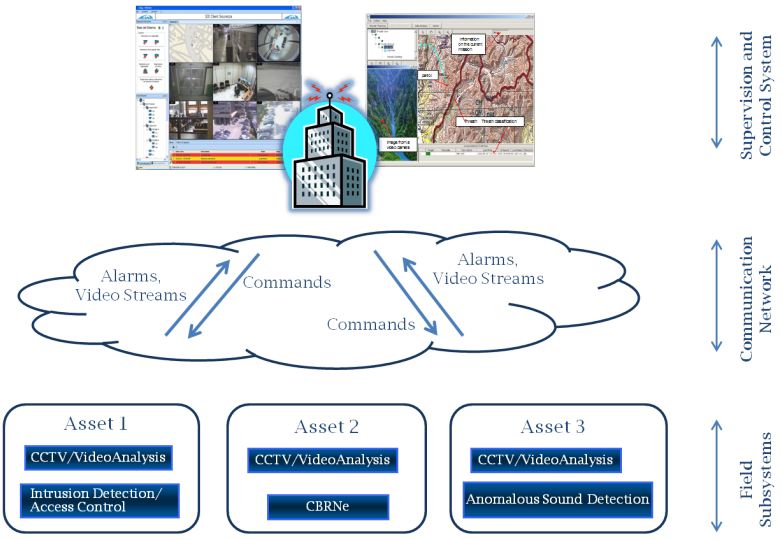


FIGURE 1.2: General architecture of an integrated security system

The different subsystems are distributed within the infrastructure and are able to send alarms and video streams to the supervision and control system through the communication network. The supervision and control system is in charge of analyzing and possibly elaborating data in order to support the decision making. In addition, if anything it can send commands to field subsystems still through the communication network.

When the emergencies occur, one of the fundamental task is to get the right information in order to allocate the right resources. Quick collaboration between local, state, and, in some instances, federal agencies is critical to saving lives and critical assets. Therefore, security systems must be tightly integrated with policies, procedures, and protocols to empower decision makers to quickly make the proper decision [37]. Security officials need a solution that overcomes the technology integration, multiple involved operators, and real-time collaboration challenges, so that all sorts of data are translated to relevant information that may be shared promptly to support organizations in detecting, analyzing, diagnosing, and resolving situations. New management technologies, like physical security information management (PSIM), are enabling these requirements.

1.3.1 Security Monitoring

Investments in security monitoring are likely to increase. Even if the human observers theoretically offer the greatest security, they are not enough since it is necessary to take account the drawbacks of human inattention and limited senses. The ability to continuously monitor the environment, to detect abnormal conditions, and to capture information of interest, all in real-time, gives the opportunity to reduce inspection costs while providing for increased security to the public.
Generally, security monitoring requires several sensor devices that are based on more or less sophisticated technologies, basically according to the application need. The strong need to have surveillance systems more and more intelligent has resulted in a new generation of sensors, “smart sensors”.
The fundamental difference between a traditional sensor and smart sensor is the latter’s flexible communication and information processing capability. Each sensor has an on-board microprocessor that can be used for digital signal processing, self-identification, self-adaptation and self-diagnostics functions. Furthermore, all smart sensor platforms use wireless communication technology [38]. Actually, in the last years, the scientific community distinguishes between the concepts of "smart" and "intelligent", pointing out that the former is related to technological aspects while the latter to functional ones [39].
Thanks to the technological progress in the miniaturization techniques, the size of sensors has decreased over time as well as their costs. This allowed to build more complex systems for disparate applications able to implement effective protection strategies. Thus, modern surveillance systems integrate heterogeneous security systems equipped with smart sensors. In the following, the most relevant systems in security field are presented.

1.3.1.1 Video Surveillance

Cameras are the most widespread devices in the surveillance field and their level of maturity is getting higher both in indoor and outdoor applications. Monitoring through video streams of a Closed-Circuit Television (CCTV) system allows a quick recognition of a situation in order to prevent or detect possible malevolent intents, as well as to conduct post incident analysis. The main characteristics of a

camera are type of acquisition (color, thermal or infrared), resolution (standard or megapixel), field of view (fixed or variable), physical transmission interface (wired or wireless), and signal processing technology (analog or digital).
Video surveillance is a field whose development keeps abreast of technology evolution. Indeed, cameras are equipped more and more with special features and often the CCTV system is combined with a Video Content Analysis (VCA) system. VCA is the capability of automatically analyzing video to detect and determine temporal and spatial events. This technical capability is used in a wide range of domains including transport, safety, security, health-care, retail, automotive, home automation and entertainment. Many different functionalities, more or less complex, can be implemented in VCA. Relating to the complexity of the algorithm, it can be hosted on the camera (using on board processing units) or on a dedicated server. Table 1.1 lists some features of interest for security.

Functionality	Description
Motion detection	It allows to detect the motion of an object within a video stream
Object Tracking	The feature allows to follow the path of an object within one or more video streams
Facial recognition	It is a biometric application for automatically identifying or verifying a person from a video source
Line crossing	It allows to define sensible areas (also virtual) and generates an alarm when something is crossing boundaries
Unattended object	The objective is to warn in case of unattended objects like baggage in order to prevent bomb attacks
Overcrowding	It determines the people density in a given area that is a key parameter in the decisions process related to crisis situations

TABLE 1.1: VCA features for security

Despite the continuous enhancement in this field, VCA still presents several limits. Their effectiveness may be reduced by multiple factors such as the difficulty of modeling complex behaviors (i.e. isolating individual people in crowds is hard [40]), the sensitivity to changes of lighting conditions, the presence of reflective surfaces in the scene, etc. In addition, VCA is often topic of debate for ethical issues (e.g. facial recognition in public transportation is not allowed in all countries).

1.3.1.2 Intrusion Detection and Access Control

Intrusion detection and access control belong to two diverse typology of systems but are closely connected between them.
Intrusion Detection System (IDS) groups several devices able to detect unauthorized access of people into sensible areas. It involves magnetic contacts, volumetric sensors, glass break detectors, etc. However, in order to differentiate the accesses unauthorized from the authorized ones an Access Control System (ACS) is required. ACS is based on three main concepts: possess (e.g. a card), knowledge (e.g a pin) and biometric feature (e.g fingerprint).
According to the required protection level or the permit level assigned, ACS can manage more combinations of entry to or exit from secured areas. ACS is constantly incorporating improvements in communications and security technologies; nevertheless, each technology has a certain level of vulnerability to be considered. For this reason, hybrid approaches which combine technologies based on the three concepts above are preferred.

1.3.1.3 Audio Surveillance

An emergent security solution is the audio surveillance. By combining audio sensors with advanced algorithms, this kind of technological tool is able to recognize automatically abnormal or unexpected noises such as scream, glass breaks, explosions, and shots.
This security system is particularly useful in situations of inadequate or absent visibility; in this case, the sound constitutes an essential information source for discriminating between suspicious events. In addition, this approach is especially advantageous if compared to other systems (e.g VCA systems) since it is independent from lighting conditions and it has low computational needs.
In contrast, their effectiveness decreases in areas where the noise is very high. Despite of this, adopting adaptive frameworks is possible to detect atypical situations under adverse conditions containing highly nonstationary background noise (e.g see [41]).

1.3.1.4 CBRNe Sensors

CBRNe systems are a good security solution for environmental monitoring and are very specific technologies for particular threats. CBRNe is the term for protective measures taken against chemical, biological, radiological, nuclear and explosive attacks. So, it is clear they constitute a powerful countermeasure against attacks where weapons of mass destruction are expected.
This technology allows an effective identification of bombs, drugs, metallic and nonmetallic weapons and explosives at long distance. Actually, unlike to radiological and explosive sensors, chemical ones have still some problems about the coverage range. For overcoming this restriction, often these tools dedicated to explosive detection are combined with the deployment of dog patrols [42]. Unfortunately, the cost of this technology is rather high so it is essential to balance the security needs with budgetary constraints. In practice, this limits the number of checkpoints for dangerous substances detection; thus, their locations must be evaluated accurately. Furthermore, the current solutions for CBRNE for people scanning are not directly suitable to all situation due to their excessive processing time (let consider the mass-transit system where this is not compatible with the crowd flows) [43].

1.3.2 PSIM Systems

Given the proliferation of the variety of interconnected systems, the willingness to develop an "open" system architecture with the backdrop of interoperability, and driven from needs to include other value-added functionality, PSIM solutions have been developed. Born initially as a physical security integration enhancement, PSIM is rapidly evolving to encompass information management systems insomuch as it draws the attention of government agencies and businesses from a wide range of markets [44].
It is a software platform that collects, correlates and manages information from disparate security devices and information systems into one common situation picture in order to empower personnel to identify and proactively resolve situations. The key element is its ability to integrate different complex subsystems easily, as

well as its interoperability with third-party applications and legacy security systems without being "locked-in" to any specific vendor. Many security benefits hail from adoption of PSIM solutions, like better situation awareness, decrease of reaction times to events, driven management of the procedural actions in case of crisis situations, support to post event analysis, etc. For this reason, they are assuming a strategic role for properly responding to any kind of emergency and are essential to respond and deal with the wide range of potential security risks. In detail, in order to provide a complete Situation Assessment and Situation Management this new generation of systems should fulfill five key capabilities [45] shown in figure 1.3:

FIGURE 1.3: Key capabilities of a PSIM system [1]

1. Gathering: the system gathers data from a wide range of disparate devices and subsystems;

2. Analysis: the gathered data should be analyzed in order to recognize the situation and to give the right priority to a possible emergency;

3. Confirmation: the system shows the situation to the security operator in a clear and concise way enabling an accurate and quick confirmation of the appeared alarms;

4. Resolution: the PSIM system should clearly present to the security operator the steps of the procedure to carry out for managing the situation in real time;

5. Reporting: all activities should be recorded for supporting the post-event investigative analysis.

PSIM is analogous to SIEM (Security Information and Event Management) software. Basically, it does for physical security what SIEM does for cyber security, simplifying the surveillance activities, while improving security and reducing time, cost and effort that physical security requires [46].

1.4 Railway Domain

Railroads and mass-transit systems are critical transportation assets and are integral to the economy and welfare of the nations. They are able to connect different cities or different areas of a city providing not only the passenger transport but also the freight transport.
Passenger rail service, especially the commuter and underground ones, concentrates large numbers of people on trains and their location in the urban environment offers the attacker easy access to the train to launch an attack, with multiple escape routes that allow them to blend into the surrounding population after the attack has been completed. In addition, the railroads also carefully serve the movement of hazardous freight daily. Movement of hazardous materials not only represents a potential for significant negative consequences to the community and environments through which they are moved, but can cause serious economic damages to the railroads in case of accidental or deliberate release. In particular, railroad infrastructure is grown in the course of time in term of sizes, capabilities and service offering. Just to give an idea, Figure 1.4 shows the Istat data (kilometers of railway network per 100 km^2 of area) related to the overall railway and the electrified double-track network in the EU member states in 2014. On one hand this has contributed to the onset of new and unexpected vulnerabilities and on the other hand this has made the consequences potentially more serious in case of attacks. At the same time, they are often the target of criminal and vandalistic actions.

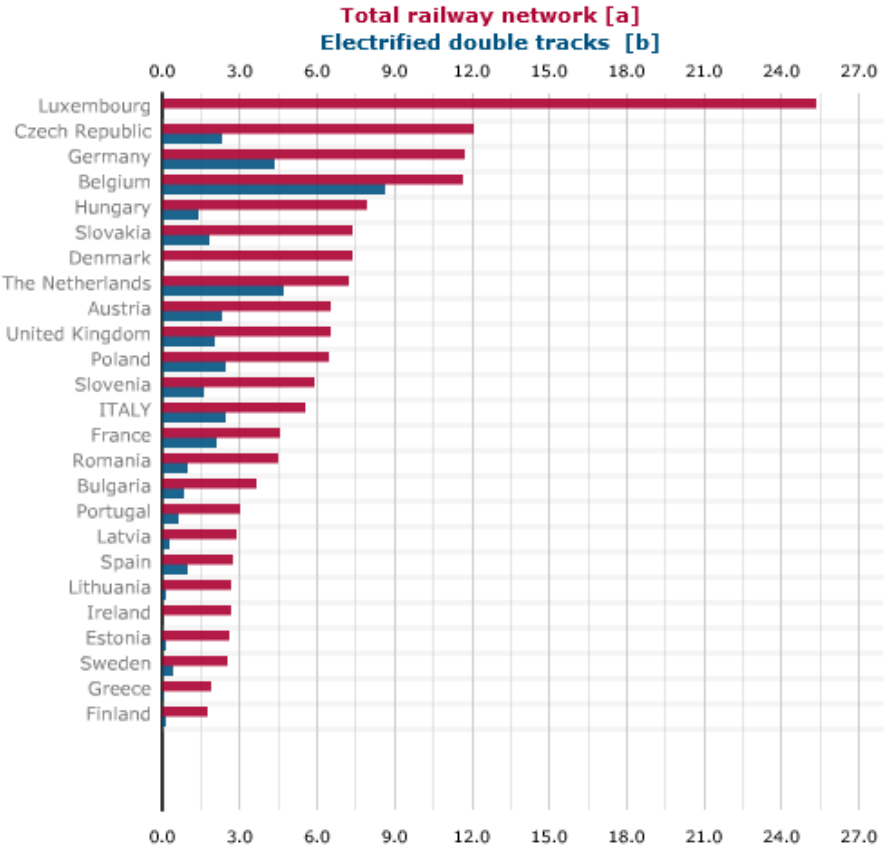


FIGURE 1.4: Railway network in EU countries in 2014 [2].

Following September 11th, 2001 and the Madrid (March 11th, 2004) and London (July 7th and 21st, 2005) terrorist attacks, the authorities operating in the transportation sector have increasingly intensified the efforts for improving security and an increasing number of studies and research work have been performed in this domain. Several EU Research actions have already been carried out or are in progress allowing clarifying the background and potential proposals for actions in the area of transportation security. The following are examples of FP7 projects:

- The **COUNTERACT** project [47], completed in March 2009, was set up to improve security against terrorist attacks aimed at public passenger transport, inter-modal freight transport, production of energy and transmission infrastructure. This project focused on the protection of critical transport infrastructures, public transport passengers and goods.
- The **MODSAFE** project [48], completed at in August 2012, has addressed the harmonization of safety requirements, models, roles and certification

schemes in the European Urban Guided Transport sector. It have also addressed security requirements in their relations to the global safety objective of the project, like ensuring the protection of persons and the system from criminal acts.

- The **DEMASST** project [49], ended in May 2010, aimed to provide a roadmap for the development and integration of System-of-Systems solutions. It provided a structured approach on identifying the main security gaps and the most promising integrated solutions, using sufficiently mature technologies, for filling them.
- The **PROTECTRAIL** project [50] ended in May 2014, whose objective was to integrate the growing influx of security technologies into rail operations and make them interoperable to improve security.
- The **SecureStation** project [51] ran from June 2011 until May 2014, dealt with the passenger station and terminal resilience to terrorist attacks and safety incidents through technologies and methodologies enabling design to reduce the impact of blast, fire and the dispersion of toxic agents on passengers, staff and infrastructure.

Although the rail industry and government have taken significant steps to enhance rail network security further improvements are still necessary. In this scenario, all the actors in charge of such infrastructures share a common mission: to guarantee an accessible and flexible service which is reliable and secure at the same time. At this aim, adopting adequate methodologies of analysis, design strategies, and technologies is the cornerstone of the protection.
The railway system needs to be equipped with complex and integrated protection systems, to avoid criminal attacks and/or to reduce their impact. Innovative systems in security surveillance integrate heterogeneous sensors [52, 53]; the events should be correlated [54] in order to increase the reliability of these technologies, avoiding the generation of unnecessary warnings and better supporting decisions [55].
Also such protection systems need to be adequately designed since the preliminary phases of the life cycle in order to obtain the best trade-off between costs and effective protection. This implies an accurate assessment through apposite

methodologies able to evaluate the effectiveness of protection systems. In this perspective, both quantitative and qualitative methodologies can be used. For example, in [56] a qualitative methods are used for assessing terrorism risk in railway domain. The method is based on threat that is how terrorists have attacked in the past and the many different ways in which they might attack in the future. On the contrary, Sapori at al. [57] proposes the implementation of risk-based methodologies in use by process engineering to achieve a quantitative assessment of security management systems and applies it to railway context. The first steps show how to analyze the system and how to integrate technological, human and procedural aspects by flow charts. The next steps describe how to manage threats, vulnerability and criticality of CI subsystems and how to identify causes and consequences through fault trees and event trees, and finally how to calculate the residual risk for security management system.

1.5 Thesis Contribution

The original contribution of this thesis is to provide methods for enhancing effectiveness and reliability of integrated security systems in order to guarantee an adequate protection level. To achieve the desired level of protection, a two phase approach is proposed combining proactive and reactive strategies. The first involves a vulnerability assessment of a PPS based on quantitative methods while the second introduces an interoperability framework for improving reaction to attacks. The overall approach will be applicable to the design phase of a PPS as well as to the evaluation phase of an existing PPS in order to determine the changes to be made for achieving the desired level of security. The pivotal points on which this thesis is founded are mainly two:

- defining and developing an interoperability framework for improving effectiveness and flexibility of a PSIM system;
- defining a methodology for evaluating vulnerabilities of a PPS system.

These are two complementary approaches that converge towards the same objective. The first approach provides a tool for integrating and making interoperable

different security systems and security management systems in order to counteract the attacks. However, hardening of all potential targets against all possible forms of attack is cost prohibitive. For this reason, the second approach aims to assign confidence levels to protection of assets derived from an accurate quantitative evaluation of vulnerability of the PPS.

Chapter 2

A Model-Driven Approach to Vulnerability Evaluation

As said in the section 1.2.2, a PPS involves systems, procedures and people for protecting assets and facilities from malevolent human attacks. The need to have an interoperability context interconnecting heterogeneous monitoring systems, security systems and security operators, has conducted towards the adoption of new category of management systems known as PSIM. Such systems collect and correlate events from security devices and information systems enabling situation awareness and management reporting. Nevertheless, effective protection calls for the availability of proper methodologies and tools to evaluate the vulnerability of critical assets and the ability of the adopted protection system to meet its objectives. In the context of security information management, the vulnerability is often defined as a weakness that can be exploited by a threat. This definition is widely used in risk assessment methodologies designed to be *qualitative* and based on the work of skilled security analysts. In fact, vulnerability is commonly qualitatively evaluated, also relying on the availability of historical data related to past threat events. On the contrary, effective protection needs to an accurate quantitative evaluation of vulnerability able to produce scientific and rigorous measures. In the field of physical security few efforts have been made to the development of approaches for the quantitative analysis of vulnerability. The objective of this chapter is to propose a model-driven approach in order to evaluate quantitatively

the vulnerability of CIs through the effectiveness evaluation of the whole PPS. In particular, the proposed methodology is based on a MDE approach that considers the three aspects of the matter of interest: infrastructure, attack, and protection. Hence, this modeling approach evaluates the vulnerability of an asset with respect to the threats and specific protection systems applied. The approach defines a UML profile for Vulnerability Analysis and Modeling for Critical Infrastructure Protection (CIP_VAM) and the automated generation of quantitative vulnerability models from UML annotated artifacts.

2.1 Aims, Scope and Hypotheses

This work contemplates security aspects of CIs considering situations where the perpetrators exploit vulnerable elements of the civilian infrastructure for the purpose of indiscriminate murder or criminal activities.

Vulnerabilities may be associated with physical (e.g., a broken fence), cyber (e.g., lack of a firewall), or human (e.g., untrained guards) factors. For this reason, security of critical infrastructures is often considered a multi-faceted and multi-disciplinary problem that requires an integrated approach [58–60]. Nevertheless, as outlined in the chapter 1, this work considers the concerns of security tied to physical and human factors without considering those related to the cyber ones. In the physical security field, the vulnerabilities identification and evaluation are necessary activities in order to restrict as possible as the consequences originating from voluntary actions. Nevertheless, these are difficult tasks that must be adapted to the application domain and the current needs of the organizations. The environment of the critical infrastructures is strongly distributed in the space and the effect of this is to have likely weaknesses distributed along the whole system[1]. In effect, a vulnerability is a weak spot that might be exploited to launch an attack and accordingly it is strictly related to the capacity of counteract threats that take place in that moment. Furthermore, not all weakness affect the system's vulnerability equally and so each of them contributes to it in a different measure. This measure reflects the likelihood of the weakness of being exploited during attacks.

[1] when we refer to 'system' we tend to mean the infrastructure with the protection systems

To be more precise we can consider the vulnerability as *specific to an asset* due to the its attractiveness from an attacker's point of view, *physically distributed and affected* by circumstances also seemingly independent, and *variable* because it changes and spreads in the course of the time according to what happens. In particular, for a given asset the variability of vulnerability is due not only to the typology of attack and the set of protection systems used, but also to the actions undertaken to contain propagation of the effects. Vulnerabilities to a specific attack are indications of the practicality of an attack, assuming security measures are in place.

There have been few attempts to combine more factors that contribute to vulnerability. This investigation aims at propose a comprehensive approach that includes environmental, physical, human, and organizational variables in addition to operational measurements of protection components which can help to enhance the understanding of vulnerability regarding to the main threats. The assessment of overall vulnerability requires the consideration of all protective interventions, both active and passive.

Specifically, the focus is on quantitative methods since they allow to obtain a measure for evaluating the protection of an asset in a more rigorous way and then how notable is the risk in case of attacks considering the applied choices. Hence, here the definition introduced by Lewis in [19] is adopted, where vulnerability is "the conditional probability that the asset is damaged, given that an attack or incident occurs"(see the formula 1.2 in the section 1.2.1).

2.2 Background

2.2.1 The METRIP project

METRIP[2] was an European project under the Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks"

[2] http://metrip.unicampus.it/

coordinated by AnsaldoSTS. Its general objective was the development of methodological tools for increasing the physical protection of railway infrastructure systems with a focus on urban mass transportation. At this aim, METRIP defined a decision making system for supporting the design and evaluation of physical protection systems. The decision making system is intended to: (i) suggest the types and disposition of devices that maximize protection effectiveness; and (ii) help evaluate the effectiveness of a given PPS against attacks. The approach adopted within the METRIP project combines Model-Driven Engineering (MDE) techniques, optimization models and formal quantitative models to carry out a vulnerability analysis of the critical assets of a Railway Infrastructure System (RIS) against various classes of attacks, and evaluate different solutions in the design of protection systems.

2.2.2 Model-Driven Engineering

Model-driven engineering (MDE) is a software development methodology which focuses on creating and exploiting domain models (they are representations of knowledge and activities that govern a particular application domain), rather than on the computing (i.e. algorithmic) concepts. MDE is a promising approach to address platform complexity and the inability of third-generation languages to alleviate this complexity and express domain concepts effectively combining the following [61]:

- Domain Specific Modeling Languages (DSML)s whose type systems formalize the application structure, behavior, and requirements within particular domains. DSMLs are described using metamodels, which define the relationships among concepts in a given domain, specifying the key semantics and constraints associated with these domain concepts. In this way, for building applications, developers use the elements captured by metamodels and express design intent declaratively rather than imperatively.

- Transformation engines and generators that analyze certain aspects of models and then synthesize various types of artifacts, such as source code, simulation inputs, XML deployment descriptions or alternative model representations. The ability to synthesize artifacts from models helps ensure the consistency between application and analysis information associated with functional requirements captured by models.

So, MDE focuses on developing domain models and it is very appealing in industrial settings. It allows for a high level of abstraction as well as the definition of modeling paradigms that are effective from the modeller's point of view, since they are based on the domain knowledge.

DSML and UML profiles

DSMLs are small and well focused on domain scope, they simplify the design process, tracing recurring design patterns in the application domain, and promote communication by standardizing the terminology and the best practices to be used in the specific application domain. A key category of support for domain-specific modeling is represented by UML profiles. UML profiling is actually a lightweight meta-modeling technique to extend UML [62]. It is a powerful mean to define DSMLs [63] which exploits two main advantages within a Model-Driven Engineering context with respect to the development of ad-hoc DSMLs: i) a UML profile is effective from the modeler's perspective, as it captures and easily replicates the modeler's architectural knowledge of a specific domain at different levels; ii) a UML profile allows for the adoption of available and standard techniques and tools which maybe easily integrated into existing production systems. In addition, the usage of a modeling language based on few and well specified domain-related concepts supports the definition of model transformations so allowing the development of a complete model-driven design methodology. A UML Profile is just an extension of the UML, defined in terms of *stereotypes* or concepts in the target domain that will be added to UML and *tags*, the attributes of the stereotypes.

Transformation

The transformational approach is based on: a) definition of a set of proper transformation rules to map the high level conceptual languages to the formal languages used for quantitative modeling or to the input data format of solving tools; b) implementation of the transformations which translate the conceptual models into quantitative models or other artifacts needed for decision support. The transformations can be classified in Model-to-Model (M2M) and Model-to-Text (M2T) transformations. The first category aims at transforming the model in an other model, expressed for example in a different formalism. The main reason of their usage is that the new model may enable analysis that are not feasible in the previous formalism. This approach are widely used in this thesis. The second category is typically performed by queries in order to obtain from the model some textual information. For example, this can be useful when structured data must be extracted to perform the processing with other software tools.

2.2.3 Bayesian Networks

Bayesian Networks (BNs) [64, 65], also known as belief networks, provide a graphical representation of a joint probability distribution over a set of random variables with a possible mutual causal relationship. The network is a directed acyclic graph (DAG) whose nodes represent random variables and arcs represent casual influences between pair of nodes (i.e., an arc stands for a probabilistic dependence between two random variables). In addition to the DAG structure, which is often considered as the "qualitative" part of the model, one needs to specify the "quantitative" parameters of the model [66]. The parameters are described through a conditional probability distribution which is defined for each node in the network. For discrete random variables, this conditional probability is often represented by a table (conditional probability table, CPT). Hence, the CPT gives the probability of each value of a child node given every possible combination of values for its parents. A prior probability should be provided for the source nodes of the DAG as they have no parents. Founded on the Bayes theorem, a BN provides a means to evaluate all possible inference queries, where the probabilities does not understand

as frequencies but rather as confidence levels in the case an event occurs. In this way, it is possible to provide a *predictive support* for a node, based on evidence nodes connected to it through its parent nodes.

2.3 Vulnerability Evaluation Process

According to MDE principles, the vulnerability evaluation process encompasses three main directions: models, automation and quantitative analysis.

Models are used at different points of the design and evaluation approach, and they play different roles in the assessment process according to the two phase in which they are used:

- UML models are used to represent the critical assets, protection measures and attack scenarios. These models contain the information needed to specify the target system, the components of the integrated security systems and the steps of the adversary's attack. They are the inputs for the vulnerability analysis phase.
- Quantitative (probabilistic) models are used to evaluate the vulnerability of a critical asset equipped with protection facilities against a specified attack. This modeling phase is automated on the basis of the structure and the information contained in the UML specification (including a representation of the attack scenario).

Automation consists in automated generation of the quantitative models for the vulnerability analysis. This is accomplished thanks to the model transformation which represents the heart of the model-driven process; an useful taxonomy may be found in [67]. Several approaches are developed in the last decade and the major categories are described in [68] and [69]. Although in literature many works address automatic model transformation in order to achieve different investigation (some of these concern the railway domain, e.g. for safety analysis and verification of a railway interlocking system [70] and for verification of train control system specification [71]), comparable approaches having as target model those

for vulnerability analysis seem not to be there. In the physical security field, the vulnerability analysis is a necessary activity concerning with the problem of identifying weaknesses in order to restrict as possible as the consequences originating from voluntary actions. As discussed in the paragraph 1.2 either quantitative or qualitative methods can be used for vulnerability analysis. This work focuses on quantitative methods since they allow to obtain a measure for evaluating the protection of an asset in a more rigorous way and then how notable is the risk in case of attacks considering the applied choices. A quantitative notion of vulnerability is used and commonly defined as the likelihood that an attack is successful, given that it is attempted [19]. In this direction, practical applications for vulnerability analysis use statistical approaches and mathematical modeling (see for example [72] and [73]), stochastic models (e.g. in [74]), Bayesian Networks have been also used, both for cyber-security analysis [75] and for vulnerability evaluation [29] in physical protection applications.

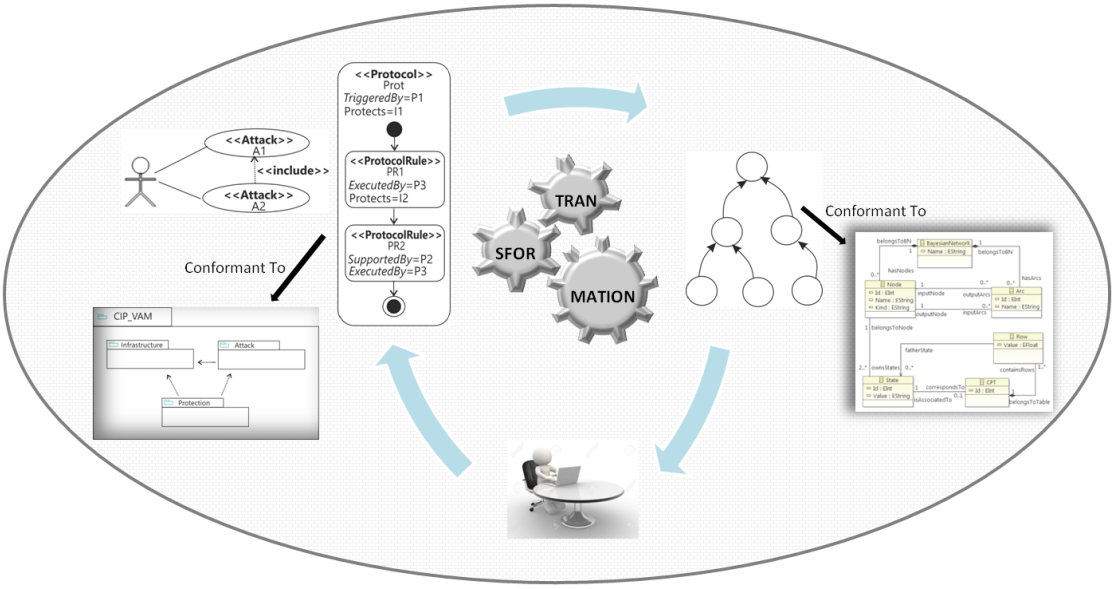


FIGURE 2.1: The vulnerability evaluation process

A schema of the overall approach is showed in Figure 2.1. An user, such as security designer or analyst, builds UML models that are the inputs of the process. This specification is annotated with the stereotypes and tagged values of the CIP_VAM profile and contains all the information needed to analysis (e.g., the concrete values of the parameters required to fully describe a specific infrastructure, or a specific protection device, or a given attack scenario). These models are the inputs for the

transformation that builds the quantitative model automatically. This requires the definition of a Model-to-Model (M2M) transformation which produce target model from UML models. The target model is given back to the user which analyzes it in order to perform the vulnerability evaluation.

2.4 CIP_VAM Language

The CIP_VAM language is a DSML conceived within the European project METRIP to support the design and evaluation activities of physical protection systems. Although born for addressing the issue of the protection of a Railway Infrastructure System (RIS), their concepts are intentionally general so that they are applicable to any critical infrastructure.

CIP_VAM is a light-weight UML extension and may be used to derive a quantitative model for vulnerability evaluation, as well as to generate proper input to decisional tools in order to calculate the optimal location of security devices [76, 77]. The literature supplies a wide selection of papers about using UML profiles like MARTE [78] (Modeling and Analysis of Real-Time and Embedded Systems), UMLsec [79] (allows to specify security information during the development of security-critical systems and provides tool-support for formal security verification), RCDS [80] (a domain specific modeling language for railway and tramway control systems that covers the segments of the rail network, sensors, and control elements like signals and switches), and so on, but it is lacking regarding UML profiles for modeling critical infrastructure protection. In [81] the UML-CI profile is presented that deals with modelling of critical infrastructures. It consider the management aspects of a CI even if, given the publishing year of last reference found, it does not appear carry on.

The ultimate goal of the CIP_VAM language is to offer a comprehensive modelling of physical protection issues during design phases of integrated security systems. Among the found profiles, SecAM [82] is what which mainly comes close to this approach also for a possible integration of the cyber security aspects. It is a recent work that enables the modelling and security specification for critical infrastructures during the early phases (requirements, design) of system development life

cycle. The original contribution of CIP_VAM is to correlate both infrastructure and attack with the protection, applied to defend the assets.

A first definition of this language was given in [83] where the protection was considered in its simplest form, by providing the possibility of representing the presence of protection equipment, including technical features and localization data, and excluding the combined usage of different devices and the effects produced by a real integration which comes from using PSIM systems. For this reason further extensions have been introduced by revisiting the concepts in the Protection package. In this thesis the last version of the CIP_VAM language is presented.

With the aim to provide a clear characterization of the application domain, a conceptual model was defined in order to identify all the needed concepts and relations. Once the conceptual model was completed, it have been mapped into a UML profile, by identifying for each domain concept the most suitable UML notation. The next subsections will describe the domain model and the corresponding profile.

2.4.1 CIP_VAM Domain Model

The CIP_VAM domain model is represented by a set of UML Class Diagrams, structured into three main packages, which provide a comprehensive view of both the system and threats to analyze (Fig. 2.2).

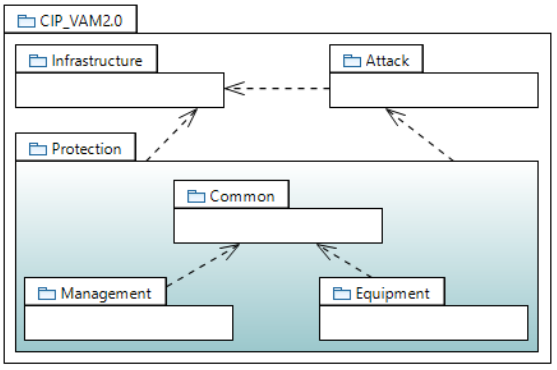


FIGURE 2.2: CIP_VAM domain model

The "system" consists of a physical infrastructure (whose elements may be considered assets to protect) and the protection system to assess or to design. Hence, the three packages included in the CIP_VAM domain model are:

- *Infrastructure*, which includes all the concepts necessary to describe the physical elements of the infrastructure, and contains both asset and environmental related concepts;
- *Attack*, which individuates concepts related to threat and attack events conducted against the assets within the infrastructure;
- *Protection*, which introduces protection related concepts and provides a description of techniques and countermeasures which may be applied to defend the assets. Actually, the protection of a critical infrastructure is an elaborate task requiring the joint set of interoperable systems, procedures and people. For including the combined usage of different devices and the effects produced by a real integration which comes from using PSIM systems, the protection package is in turn organized into three sub-packages:
  - *Common* acts like a bridge between the Protection model and the concepts introduced by the *Infrastructure* and *Attack* packages.
  - *Equipment* introduces different domain classes representing protection items or devices that can be deployed;
  - *Management* contains the concepts related to security procedures and the actions which are undertaken after the occurrence of an event (e.g., an alarm) raised by a protection equipment.

As the target of an attack is always an asset and a protection is used to protect the asset to a specific asset against one or more attacks classes, dependencies exist between the *Attack* package and the *Infrastructure* package, as well as between the *Protection* package and the *Infrastructure* and *Attack* packages. The *Equipment* and *Management* packages are closely dependent (through the *Common* package), these dependencies enable the possibility to model the effective integration of several protection devices as well as devices and procedures.

The remainder of this paragraph will provide a description of the CIP_VAM domain model, describing the elements belonging to three packages.

Infrastructure Package

The main concepts of the *Infrastructure* package are *Site*, *Interface*, *Object* and *Service* (Fig. 2.3). A physical infrastructure consists of a number of *sites* which may contain one or more *subSites* (e.g., corridors, rooms, functional areas, etc.). *Objects* may be located into *Sites* and may be composed by *subObjects*, they may also *provide* or *request* services, which in turn may be implemented through *subServices*. Different *Sites* may share *interfaces* (e.g., windows, doors, gratings, etc.). *Asset* is a concept that may be related to any element whose loss or disruption cause an economic loss. An *Asset* is characterized by its economic *value*, *vulnerability*, occurrence probability of an attack against it (*attackProb*), quantitative and qualitative estimate of potential or unwanted outcome (*risk* and *riskLevel*).

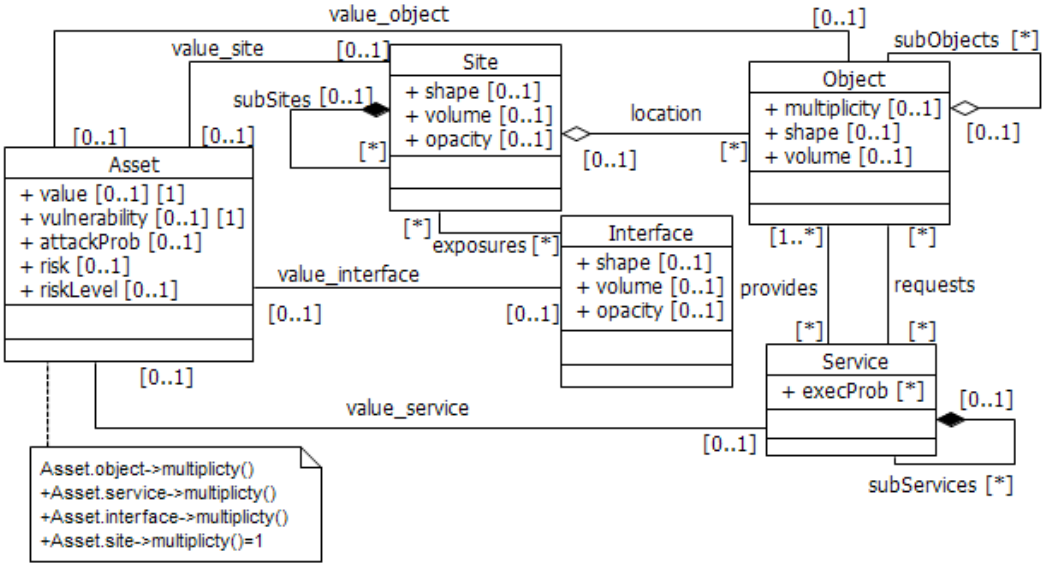


FIGURE 2.3: CIP_VAM domain model: infrastructure

Attack Package

The *Attack* package (Fig. 2.4) models the offensive operation (*Attack*) conducted by an *Attacker* against an asset according to the adopted *tactic* (nature of the attack: kidnapping, armed attack, sabotage, etc.). An *attack* may be be decomposed into a sequence of *steps* (*Actions*). Each *action* of the attack may be performed by using one (or more) *Weapons* and it has a failure probability (*failure*), in addition it may be triggered by a *Trigger* event. The *Threat* association models the effect that the attack wants to cause on the asset. Both attack and action can be characterized over time by a temporal *duration*. The *Impairment* class models the consequence of the attack actions on the asset. When an attack action affects an asset, then the damage may propagate and cause further damages with a given *probability* and under specific *conditions*.

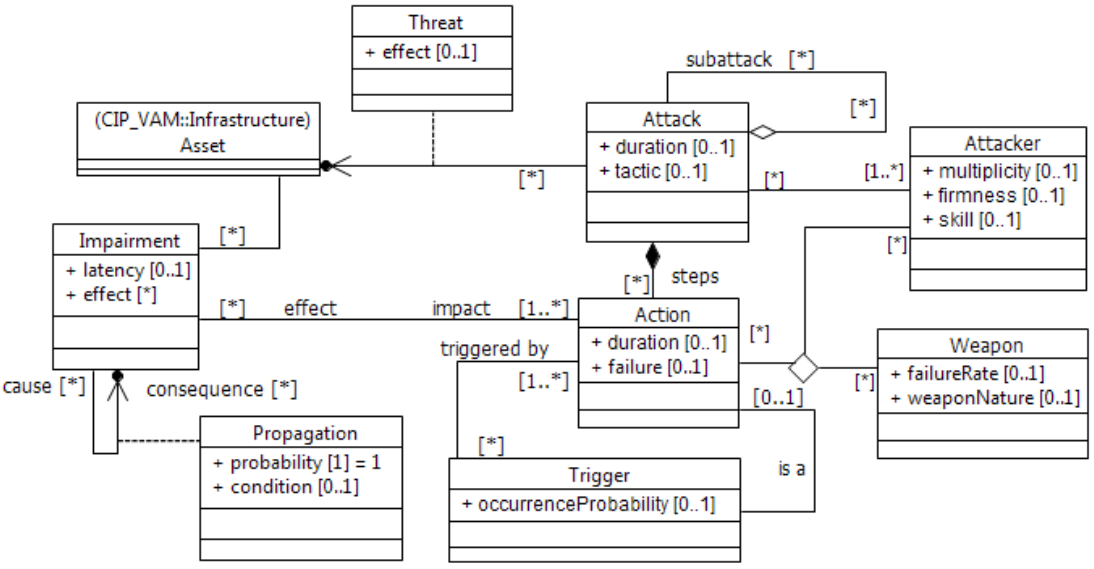


FIGURE 2.4: CIP_VAM domain model: attack

Protection Package

The Protection model (Fig. 2.5) concerns equipment, personnel and procedures involved in defending assets from attacks.

The *Common* package introduces the general concept of protection and the main relationships with *Attack* and *Infrastructure* ones. *Protection* is an abstract class

modelling a generic protection/defence mechanism: it is characterized by a *cost* and by the probability to be effective against an attack (*succesProb*). The association *protection* links a protection to the asset it protects (*Asset* class from the *Infrastructure* package). In addition, the associations *mandatory* and *forbidden* allow for specifying if a protection must/mustn't be applied to an asset (e.g., in some cases the privacy norms may forbid the usage of specific equipments, as cameras or CCTV systems).

From the point of view of the *Equipment* package, the abstract concept *Protection* is specialized by the *Equipment* class, characterized by the attributes *failureRate* (failure probability) and *nature*. In turn *Equipment* is further specialized by several classes representing distinct kinds of security devices, (*Barrier*, *Sensor*, and *Deterrent*) some of which were already present in the model described in Section 2.4, some others have been added with an increased level of detail. *Sensor* will be extensively used in the applications described in this paper. It may represent several kinds of devices such as CBRNe, microphones, bomb sniffer and so on. It adds information about the range of the sensor, its false positive and false negative rates (*fpr* and *fnr* attributes), the sensing *latency* and its data transmission technology (*transData*). Hence, *Sensor* represents a wide spectrum of technology instruments and it is specialized by the *Camera* class in order to meet specific needs. Every camera is characterized by a given *resolution* and *processing* technique (analogical or digital). To take into account the possibility of using cameras capable of remote directional and zoom control, the *Camera* class has been further specialized by the *Ptz* class which allows to set typical technical parameters of a pan-tilt-zoom camera, as angular speed, range and zoom. An *Equipment* may be applied (through an *InstallationPoint*) to a *Site*, an *Interface*, an *Object* or a *Service* in order to defend an asset. *InstallationPoint* also specifies the *position* and the *direction* of the equipment installation.

The *Management* package introduces the concepts related to defense that is the countermeasures triggered by an attack. The abstract class *Protection* is specialized in this package by three classes: *Protocol*, *Operator* and *ManagementSystem*. In particular, the latter represents a management system that integrates multiples and different protection systems. So, an aggregation relation exists between *ManagementSystem* and *Protection*. *Operator* represents a generic operator, human

or mechanical. An *Operator* is not tied to a specific location but may change its position if it is necessary. Finally, *Protocol* allows to combine the effects originating from the integration of subsystems and people when an event is raised by a *Protection* system. In particular, it models a generic procedure that is triggered by a generic *Protection* system and it is composed by a sequence of steps (*ProtocolRule*), each one representing a specific action. The latter describes the actions executed by one or more *Operator*s with the eventual support of a *Protection*.

2.4.2 CIP_VAM Profile

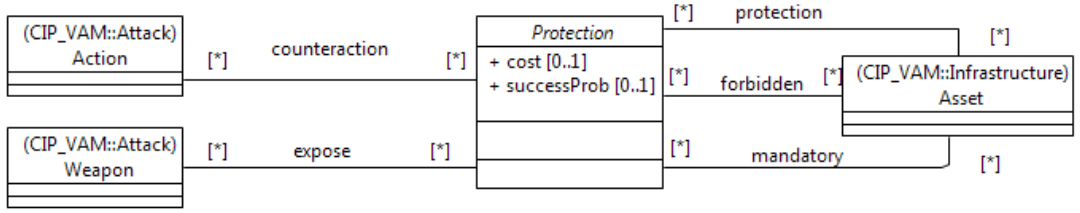
In this section the mapping from the conceptual domain model to a concrete UML profile is described. The CIP_VAM UML profile has been built in a systematic way following rules described in [84]; concepts from the domain model are mapped to stereotypes and tagged-values. Fig. 2.6 shows a general overview of the CIP_VAM profile which includes a set of UML extensions and a Library.

CIP_VAM Library.

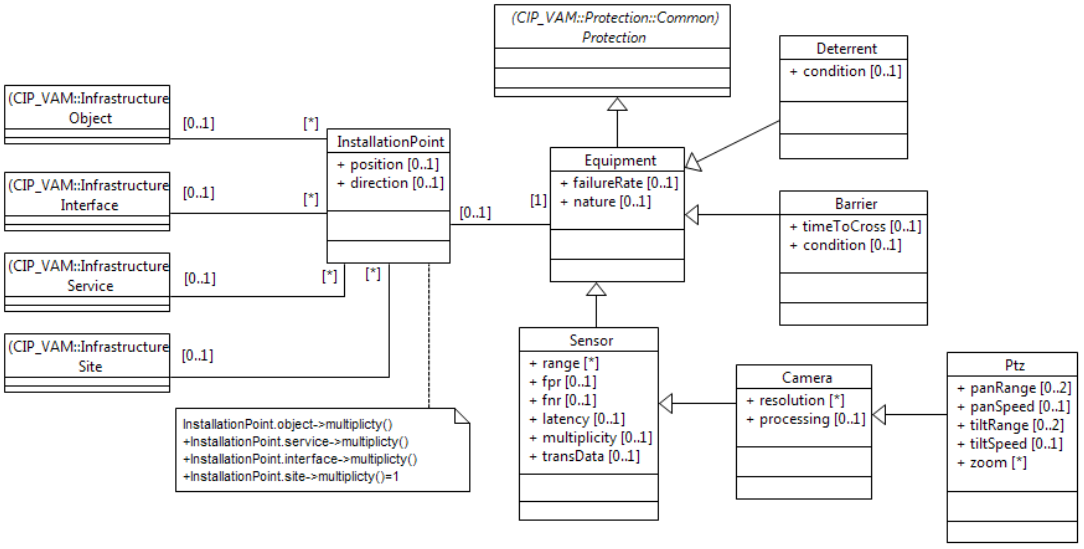
The *CIP_VAM_Library* (detailed in Fig. 2.7) imports some packages of the existing library from the OMG MARTE profile [78] and defines some specific basic, geometric and structured data types. The CIP VAM Library is composed as following: a set of enumerations are defined in BasicDT (Figure 2.7(a)); the geometric data types in GeometricDT are necessary in order to model physical structures and spaces (Figure 2.7(b)); the Structure package defines complex data types by means of aggregation of BasicDT and GeometricDT types (Figure 2.7(c)). Both GeometricDT and StructuredDT use some types defined in the MARTE Library. The meaning of each element of the CIP_VAM Library may be found in Appendix A.

CIP_VAM Extensions.

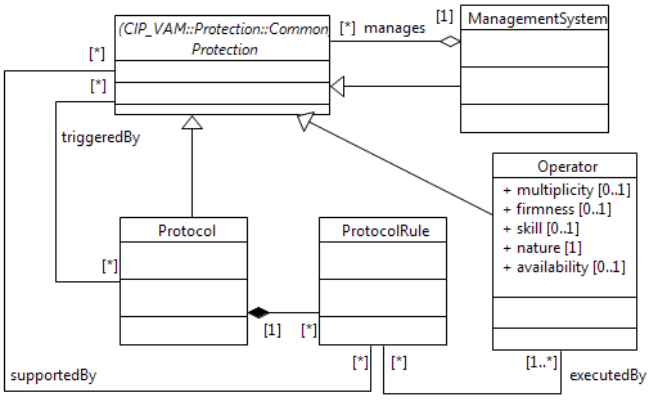
The *CIP_VAM extensions* packages is illustrated in Fig. 2.8. The extensions are organized into three main packages whose structure is the same of the domain



(a) Common



(b) Equipment



(c) Management

FIGURE 2.5: CIP_VAM domain model: protection

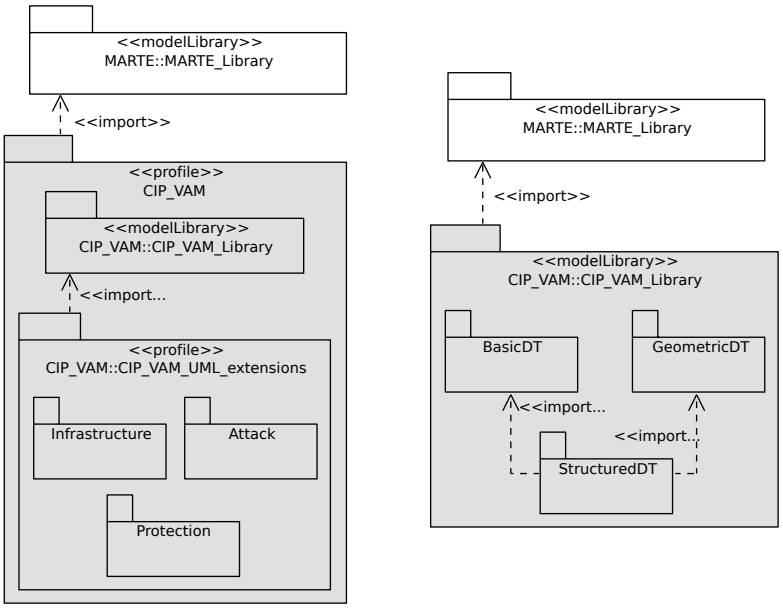


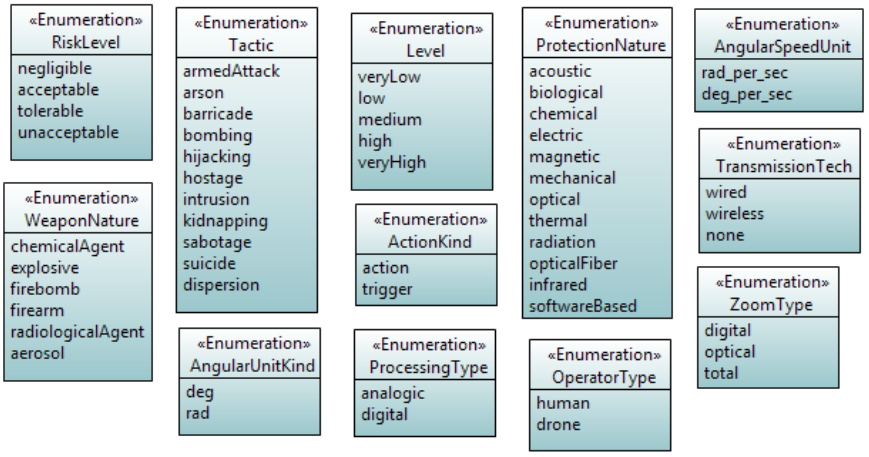
FIGURE 2.6: CIP_VAM UML profile: overview.

model. The relevant stereotypes and tags, to the vulnerability analysis are introduced and described here below.

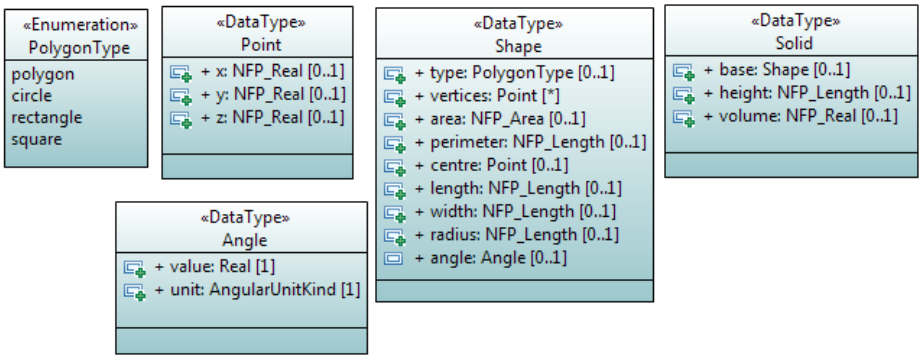
The stereotypes introduced to model the *Infrastructure* have been reported in Figure 2.8(a). The three main stereotypes are: «Site», «Object» and «Interface».

«Site» shall be applied on all modeling elements which represent physical (or logical) areas in which the system under analysis can be decomposed (e.g. control rooms, waiting rooms, platforms, etc.). «Interface»s join more sites, examples are doors, windows, balconies as they join two sites (specified by the *exposures* tag). «Object»s can be located in a site, or it may be considered on its own if no sites are specified (in this case the tag location will not be assigned a value).

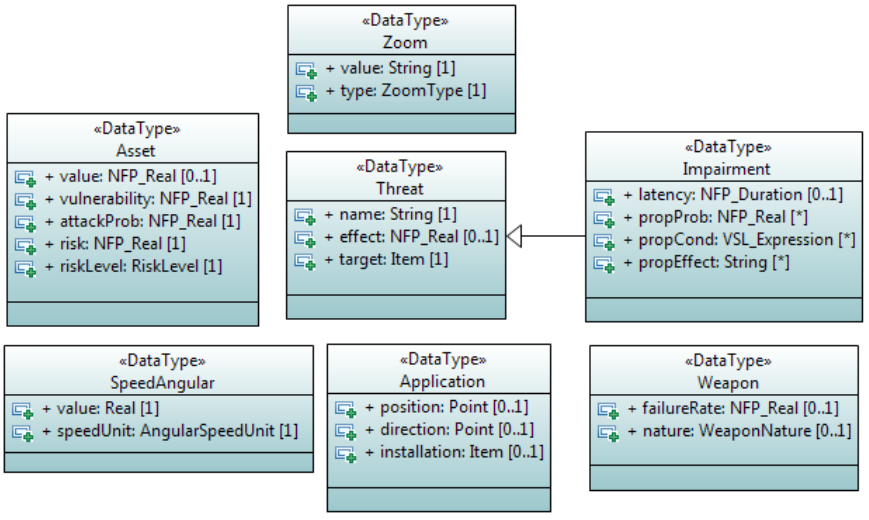
«Site», «Object» and «Interface» are different specifications of «Item» through the «Physical» stereotype. Both «Item» and «Physical» are abstract stereotypes (i.e., they are not directly applicable on modeling elements): they specify some tags which model features shared by «Site»s, «Object»s and «Interface»s. In particular, they all may be assets. This is modeled by specifying a value for the tag *asset* (see «Item») which represents the weight of the asset according to several indexes. Among them, the economic loss in case of destruction, damage or theft of the asset. Hence, by definition, an asset has an economic price.



(a) BasicDT

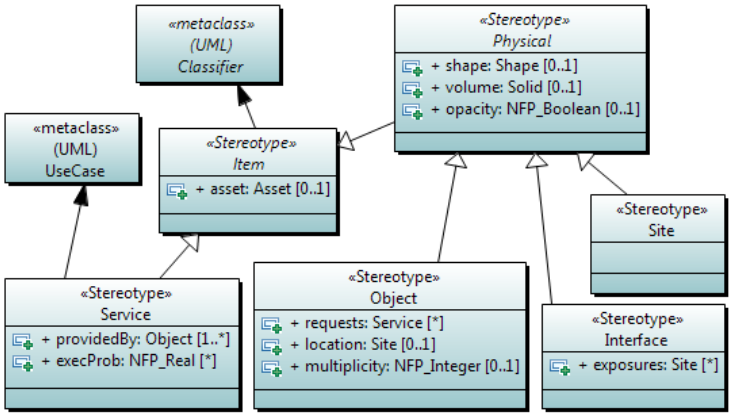


(b) GeometricDT

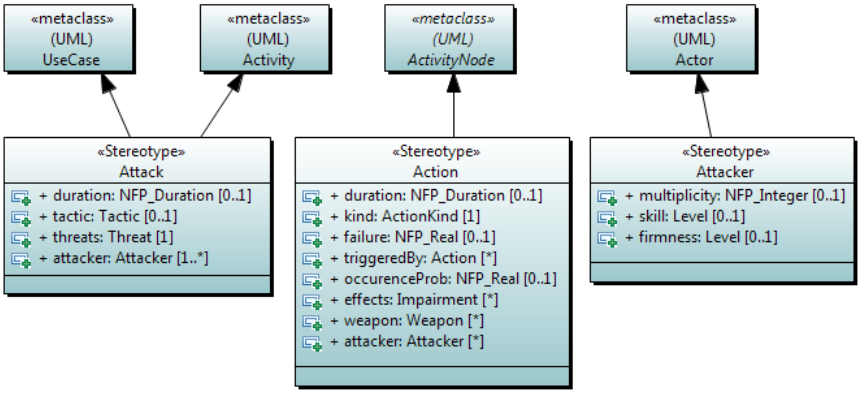


(c) StructuredDT

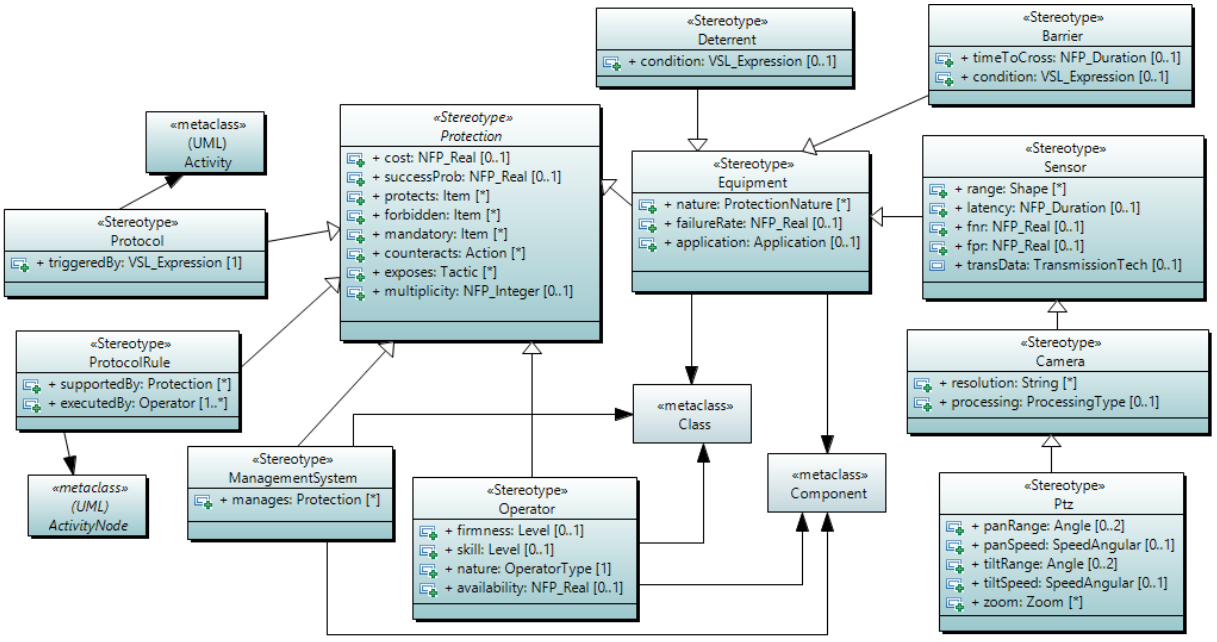
FIGURE 2.7: The CIP_VAM Library



(a) Infrastructure



(b) Attack



(c) Protection

FIGURE 2.8: The CIP_VAM UML extension

As for the «Physical» stereotype, its meaning is that, at the state, the entities we deal with within the *Infrastructure* model are not "virtual" but concrete things. They may have a *shape* and be 3D object (*volume*).

The hierarchy described above extends UML as the root stereotype «Item» extends the UML meta-class *Classifier*. This implies that its specialized stereotypes can be applied on all the UML *Classifier*s (Classes, Associations, Components, etc.) making it possible the usage of all the UML *Classifier* modeling elements. For example, nested sites can be modeled through a Component Diagram in which Components can be nested or, similarly, the *Interface* stereotype could be applied on Association because both Component and Association are UML *Classifier*s. This deep specialization chain between stereotypes also enables future extensions of the profile.

The stereotypes introduced to model *Attacks* have been reported in Figure 2.8(b). The main stereotypes in the Figure are: «Attacker», «Attack» and «Action». The «Attacker» models the person or people which conduct an «Attack» against an asset. It is possible to represent the attacker's capabilities through the *firmness* and *skill* tags, while some features of the attack may be modeled using the tags *duration*, *tactic* and *threats*. The «Action» stereotype is introduced to model the steps of an attack. Details about each action may be expressed through its tags: for example, *weapon* may be used to specify the kind of weapons used during a specific attacker's action; *occurrenceProb* tag is the probability that the action is performed.

«Attacker», «Attack» and «Action» extend the UML meta-class *Classifier*, too. Nevertheless, further extensions could allow to model an attack by using also different UML modeling elements: «Attack» extends the UML meta-class *UseCase* and «Attacker» extends the UML meta-class *Actor* allowing to reuse the UML Use Case Diagram in modeling the structure of an attack. Finally, «Action» and «Attack» extend the UML meta-class *ActivityNode* so enabling the insertion of attack related concepts into the UML Activity Diagram.

Again, the stereotypes used to model *Protection* facilities have been reported in Figure 2.8(c). Similarly to «Item» and «Physical», the «Protection» stereotype enables further extensions of the CIP_VAM profile. Hence, its tags are general

enough: *cost*, *successProb*ability, and others. Again, «Protection» is specialized by the stereotype «Operator», «ManagementSystem», «Equipment», «Protocol» and «ProtocolRule».

The «Equipment» stereotype may be applied on modelling elements which represent protection devices or systems installed in a fixed point (*application*) and it is characterized by their *nature* and *failureRate*. It is specialized by three stereotypes «Sensor», «Deterrent» and «Barrier». Specifically, the «Sensor» stereotype (e.g. cameras, microphones, bomb sniffer, etc.) adds information about the *range* of the sensor, its false positive and false negative rates (*fpr* and *fnr* tags) and the sensing *latency*. In turn, «Sensor» can be further specialized for typology of device (e.g. «Camera»).

The «Equipment», «Operator» and «ManagementSystem» stereotypes extend the *Class* and the *Component* UML metaclasses. The «Protocol» stereotype, instead, extends the *Activity* UML metaclass, while the «ProtocolRule» extends the *ActivityNode* UML metaclass.

2.5 Deriving the Vulnerability Model

This section describes how to derive a vulnerability model based on Bayesian Networks and how to automate its generation from a CIP_VAM annotated UML model.

The transformation from CIP_VAM to BN is able to generate the structure of the BN model which also catches information about the dependency relationships among the three modeling levels (infrastructure, protection and attack). Established the graph, for each node of the BN model a CTP has to be deduced allowing quantitative analysis.

In order to obtain a consistent BN, some rules must be obeyed during the UML modeling phase: a) *attacks* are represented by Use Cases, an Activity is associated to each Use Case if its behavior has to be detailed, in this case the *actions* which realize an *attack* are modeled by ActivityNodes; b) *services* are not considered in this version of the transformations; c) *protocols* (i.e., the protection procedures)

are represented by Activities where *protocol rules* are ActivityNodes; d) a BN is a DAG, for this reason it is necessary that Activity Diagrams, representing both *attacks* and *protocols*, do not contain cycles; e) it will be clear later that some specific tags play an important role in establishing relationships between BN nodes, consequently these tags must be set in the concrete UML models.

2.5.1 BN Structure

Before describing the transformation, the BN model to be built is presented. It reflects the structure of the source UML model, i.e., it is organized into three levels: infrastructure, attack and protection. Fig. 2.9 exemplifies this organization and highlights the levels into which the nodes are divided.

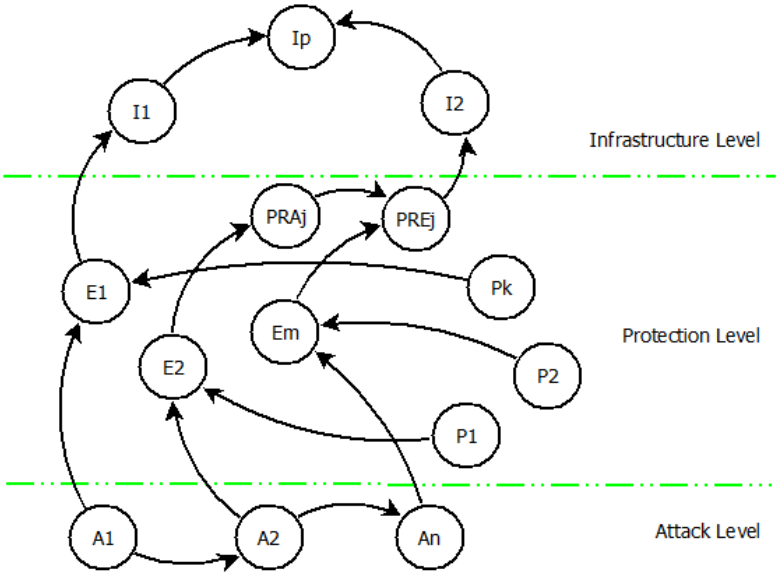


FIGURE 2.9: General structure of BN

On the bottom level attacks are placed; each attack node ($A_1, A_2, \ldots, A_n$ nodes in Fig. 2.9) represents a random variable associated to the occurrence of an attack action, the arcs between these nodes specify the causal influences between attack actions. Let them be node of type A; each A-node represents a random Boolean variable where the value in each node represents the occurrence or the absence of the related attack action.

The protection level includes different kinds of nodes since they model random variables associated to different classes of protection items (protection equipments, operators and protocols). In Fig. 2.9 the generic node P_i represents the availability/unavailability of a protection device (equipments and operators) involved in the protection system. Each P-node is connected to one of the E-nodes: the truth of an E-node says that the protection device successfully detects (infers, recognises, depending on device) an attack action. Hence an E-node is also connected to one or more A-nodes representing attack actions the protection may detect.

Each protection action of a protocol is associated to one pair of BN nodes: a PRA-node and a PRE-node. The PRA-node models the activation of the protection action, the PRE-node represents the execution of the same action. The relationship between activation and execution is realised by an arc from the PRA to PRE nodes. Arcs from the E-nodes to PRE-nodes model the causal influence between on a protection action by both the operator who executes it and the protection device which supports the action (if any). In addition, the PRA-node which is associated to the *first* action performed according to the protection protocol, is connected to all the E-nodes corresponding to the protection devices which may trigger the protocol.

At the top of the BN model of Fig. 2.9, the infrastructure level contains some I-nodes representing a random Boolean variables whose truth means the associated asset is protected by at least a protection item (equipment or protocol). The I-nodes correspond to infrastructural UML elements tagged as `«Asset»`. An arc between two I-nodes models the effect that a successful attack, carried out against a first asset (the source BN node), may have on a second asset (the target BN node). Finally, arcs from E-nodes (resp. PRE-nodes) to I-nodes model the causal influence of a protection device (resp. a protection protocol) on the asset associated to the I-node.

Summarizing, the set of nodes of the BN model are partitioned in the following classes:

- A: nodes modeling actions of an attack;
- P: nodes modeling protection devices;

- E: nodes modeling detection/recognition of attack actions by protection devices;
- PRA: nodes modeling activation of protection actions belonging to a protection protocol;
- PRE: nodes modeling execution of protection actions belonging to a protection protocol;
- I: nodes modeling elements of the infrastructure.

2.5.2 Conditional Probability Table

Given the structure of the BN model, each BN node has a CPT where its structure is related to the type of the node while the parameters are is filled instanced with the tagged values deduced by the model. As showed in Fig. 2.10, we can have two kinds of A-nodes: a root (A_1) that corresponds to the first step of an attack sequence or an inner node (A_2) that corresponds to a succeeding action. The CPTs of the two nodes are reported: both of them are very simple and represent the evidence of an attack step. This comes directly from the definition of the vulnerability reported in the section 2.1. Since A_1 is a root, the related CPT corresponds to a prior probability which is the occurrence probability of the starting event. Instead, the CPT of A_2 describes conditional probability of the node according to the previous step of the attack (in this case A_1).

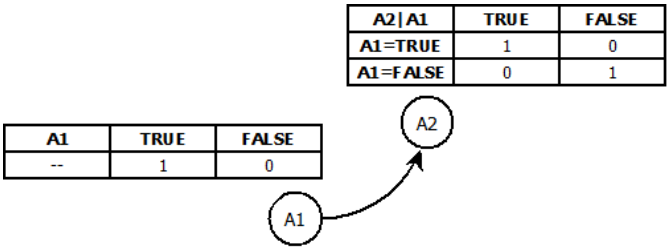


FIGURE 2.10: CPT for attack nodes

P-nodes are always root nodes: the CPT of a P-node considers the failure rate of the device or the operator's availability (Fig. 2.11).

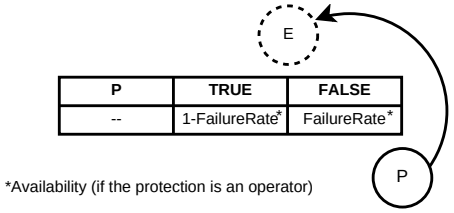


FIGURE 2.11: CPT for protection nodes

The CPT of an E-node takes account of the detection probability of the related protection (P-node) and the event of the attack (A-node) that triggers the detection. As showed in Fig. 2.12, given the attack ($A = TRUE$) the probability of the effect node is equal to *1-fnr* where *fnr* is the false negative rate of the device (a tagged value of the «Sensor» stereotype). To the contrary, if the attack there is not (A=FALSE) we consider the false positive rate (fpr) of the protection. In particular, Fig. 2.13 shows a CPT corresponding to the case where the effect of a protection is also conditioned by the effect of an enabling protection. The first CPT results a special case of the second one when E_2 is always true.

E|A,P	TRUE	FALSE
A,P=TRUE	1-fnr	fnr
A=FALSE P=TRUE	fpr	1-fpr
A=TRUE P=FALSE	0	1
A,P=FALSE	0	1

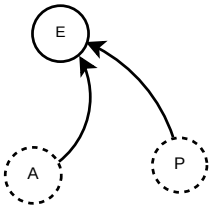


FIGURE 2.12: CPT for effect nodes

E1|A,P,E2	TRUE	FALSE
A,P,E2=TRUE	1-fnr	fnr
A=FALSE P,E2=TRUE	fpr	1-fpr
A,E2=TRUE P=FALSE	0	1
A,P=FALSE E2=TRUE	0	1
E2=FALSE P,A=TRUE	0	1
E2,P=FALSE A=TRUE	0	1
E2,A=FALSE P=TRUE	0	1
A,P,E2=FALSE	0	1

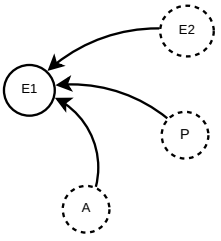


FIGURE 2.13: CPT for effect nodes with dependency by protection

Fig. 2.14 and Fig. 2.15 show the CPTs for the PRA-nodes and PRE-nodes. Let be $E(T)$, $E(S)$ and $E(E)$ the E-nodes representing the protections written respectively in the *triggeredBy*, *supportedBy* and *executedBy* tagged values of the

«Protocol» and «ProtocolRule» stereotypes. The CPTs implement an AND logic resulting true if all the input nodes are true: this means that both the activation and execution of a protocol and a protocol rule are strictly conditioned by the combined effect of the related protection measures. It is important to underline that the *PRA*-node which plays the role of parents to the *PRE*-node is related to the same «ProtocolRule» while the *PRE*-node which plays the role of parents to the *PRA*-node refers to the previous protection procedure step.

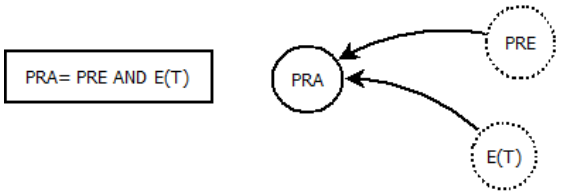


FIGURE 2.14: CPT for activation nodes of a protocol

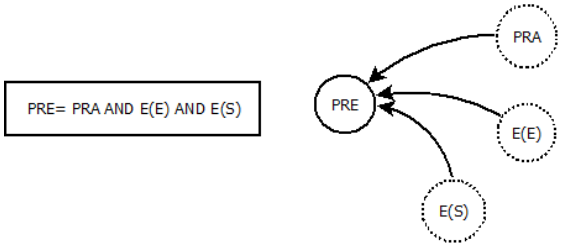


FIGURE 2.15: CPT for execution nodes of a protocol

Finally Fig. 2.16 shows the CPT of an *I*-node which can be affected by the execution of a protocol rule (PRE), the effect of a protection (E) and the contained sites or objects (I_1 and I_2). The CPT is summarised by a Boolean function which combines both the effects of protection measures (PRE and E) and the protection of its subcomponents (I_1 and I_2). These two kinds of contributions are logically in AND since we consider the I protected only if all of its subcomponents are protected and at least one of the protection measures reacts correctly.

2.5.3 Model Transformation

The transformation process is in charge of generating the vulnerability model described above. The UML metamodel extended with CIP_VAM UML profile is used as source metamodel, the BN metamodel shown in Fig. 2.17 is used instead as target metamodel.

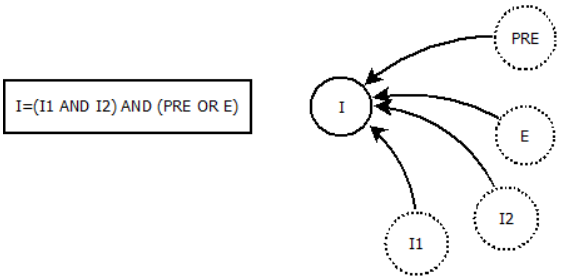


FIGURE 2.16: CPT for infrastructure nodes

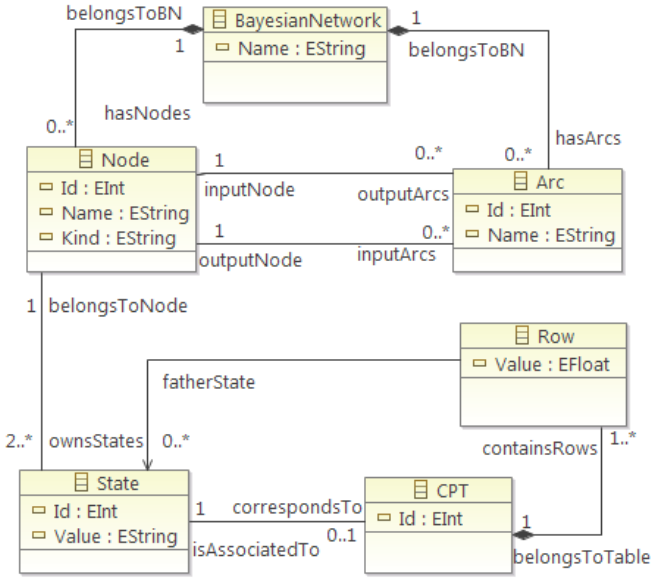


FIGURE 2.17: Metamodel of BN

A high-level description of the most significant parts of the transformation is provided in form of pseudocode. The following naming convention is adopted in the description of the algorithms:

- N_A: a BN A-node;
- N_E: a BN E-node;
- N_I: a BN I-node;
- N_P: a BN P-node;
- N_{PRA}: a BN PRA-node;
- N_{PRE}: a BN PRE-node;

- the names of the UML elements that are sources in a UML relationship are subscripted with "S";
- the names of the UML elements that are target in a UML relationship are subscripted with "T";
- The notation $N_{X(Y)}$ stands for "the BN X-node generated from the UML Element Y";

In addition, the effects of each algorithm is also described graphically to help the reader understand the performed mapping.

Algorithm 1 shows the pseudocode corresponding to the generation of the attack nodes and arcs of the BN structure.

Algorithm 1 shows the pseudocode corresponding to the generation of the attack nodes and arcs of the BN structure. The transformation creates a BN A-node from the Activities modeling the attacks. The transformation also takes into account the Include UML relationships between Use Cases (if any) for creating dependencies between couples of attacks.

The generation of the attack nodes and arcs of the BN structure, according to the algorithm reported above, is exemplified in Fig. 2.18. In this Figure two attacks *A1* and *A2* are considered, and detailed through two Activities. In particular, *A1* includes *A2*. The three actions of the two attacks generate three BN nodes, an arc between nodes B and C is generated according to the existing UML Control Flow between them. An additional arc, between nodes A (last action of *A1*) and B (first action of *A2*) is generated since the attack *A2* includes the attack *A1*.

Algorithm 2 shows the pseudocode corresponding to the generation of the infrastructure nodes (nodes I) and arcs of the BN structure. The transformation creates the infrastructure nodes of the BN model from Classifiers representing physical elements of the infrastructure. In this case, an important condition for obtaining an infrastructure node is to set the *asset* tag of the stereotyped UML Elements; in fact, only the Elements with a valued *asset* tag are considered by the transformation.

Algorithm 1 generateAttackLevelBN

for all *Activity Ac* stereotyped as «Attack» **do**
  for all *ActivityNode An* stereotyped as «Action» in *Ac* **do**
    create a *BN node N_a*;
  end for
  for all *ControlFlow Cf* in *Ac* **do**
    if *Cf* is between two *ActivityNodes A_S, A_T* **then**
      create a *BN arc Ar*;
      inputnode(Ar) ← N_a(A_S);
      outputnode(Ar) ← N_a(A_T);
    end if
  end for
end for
for all *Include In* between two *UseCases UC_S, UC_T* stereotyped as «Attack» **do**
  if (UC_S is specified by the *Activity A_S* stereotyped as «Attack») **and** (UC_T is specified by the *Activity A_T* stereotyped as «Attack») **then**
    create a *BN arc Ar*;
    inputnode(Ar) ← N_a(Al) where Al is the last action of A_S;
    outputnode(Ar) ← N_a(Af) where Af is the first action of A_T;
  end if
end for

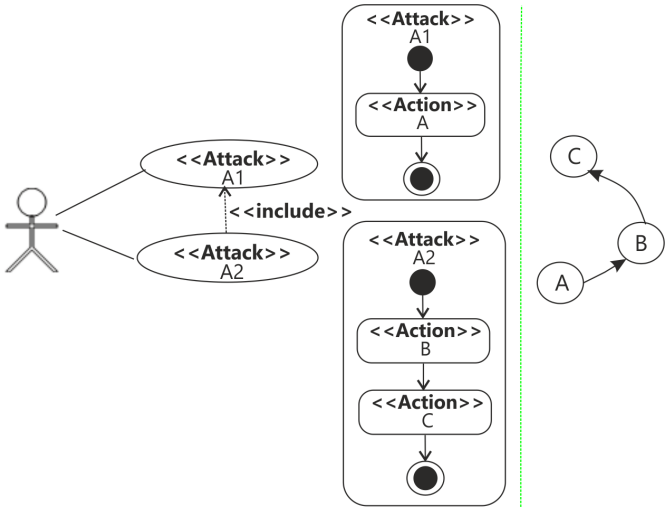


FIGURE 2.18: Transformation for Attack

The generation of the infrastructure nodes and arcs of the BN structure, according to the algorithm reported above, is exemplified in Fig. 2.19. In this Figure three sites A, B and C have been considered; an object Ob is located in A. C is not an

Algorithm 2 generateInfrastructureLevelBN

```
for all Classifier Cs stereotyped as «Site» do
  if asset tag is defined for Cs then
    create a BN node N_i;
    for all Classifier Ci stereotyped as «Site» in Cs do
      if asset tag is defined for Ci then
        create a BN arc Ar;
        inputnode(Ar) ← N_i(Ci);
        outputnode(Ar) ← N_i(Cs);
      end if
    end for
  end if
end for
for all Classifier Co stereotyped as «Object» do
  if asset tag is defined for Co then
    create a BN node N_i;
    if location tag is defined for Co then
      if location tagged value refers to a «Site» Si and
      the asset tag is defined for Si then
        create a BN arc Ar;
        inputnode(Ar) ← N_i(Co);
        outputnode(Ar) ← N_i(Si);
      end if
    end if
  end if
end for
```

asset (the *asset* tag is not defined for it), hence only three BN nodes are generated, corresponding to A, B and Ob. An arc is created from B to A since the former is included into the latter (according to the UML Component Diagram). Another arc connects Ob and A since the former is located into the latter. Note that, in the last case, the arc corresponds to the value of the *location* tag since, extending UML Classifier, the stereotype «Object» can be applied also on Classes or on other elements.

The following four algorithms generate the nodes and arcs of the protection level, they are also in charge of generating the arcs of the BN model which represent dependencies between the adjacent levels (i.e., from nodes belonging to the protection level to nodes belonging to the infrastructure level, and from nodes belonging to the attack level to nodes belonging to the protection level).

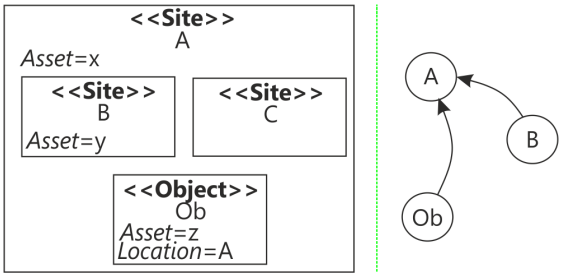


FIGURE 2.19: Transformation for Infrastructure

With respect to the BN structure depicted in Fig.2.9, Algorithm 3 generates:

- the protection nodes P and E corresponding to UML Element stereotyped as «Equipment» and «Operator»;
- the arcs from the protection nodes P to the protection nodes E;
- the arcs from the attack nodes A to the protection nodes E;
- the arcs from the protection nodes E to the infrastructure nodes I.

Starting from UML Classes and Components stereotyped as «Equipment» (as well a other derived stereotypes) or «Operator», this algorithm generates a P-node, an E-node and an arc between them.The arcs from A-nodes and E-nodes are drawn according to the *counteracts* tag of the stereotyped UML Elements.

In addition, the *protects* tag, if defined, creates an arc from the E-node to the I-node of the protected infrastructure; the UML Dependency relationship between two equipments, if any, generates an arc which from the "independent" E-node to the "dependent" one. As an example, in Section 4.2 the detection of an intruder by a thermal camera enables the tracking functionality by a pan-tilt-zoom camera.

The generation of the protection nodes and arcs of the BN structure according to the algorithm reported above is exemplified in Fig. 2.20. Specifically the three equipments *P1*, *P2* and *P3* generate three homonyms nodes of type P, three others of type E and three arcs which connect the node P to the node E. Since each i-th equipment counteracts the i-th activity, then an arc for each couple of them is generated. At last, since *P3* protects the site I, another arc connecting the two corresponding nodes is generated.

Algorithm 3 generateProtectionLevelBN - P and E nodes

for all *Class* or *Component* C stereotyped as «Equipment» or «Operator» **do**
  create a *BN node* N_p;
  create a *BN node* N_e;
  create a *BN arc* Ar;
  inputnode(Ar) $\leftarrow$ N_p(C);
  outputnode(Ar) $\leftarrow$ N_e(C);
  if *counteracts* tag is defined for C **then**
    for all *ActivityNode* AN stereotyped as «Action» referred by the tagged value *counteracts* **do**
      create a *BN arc* Ar;
      inputnode(Ar) $\leftarrow$ N_a(AN);
      outputnode(Ar) $\leftarrow$ N_e(C);
    end for
  end if
  if *protects* tag is defined for C **then**
    for all *Classifier* Cl stereotyped as «Site» or «Object» referred by the tagged value *protects* **do**
      create a *BN arc* Ar;
      inputnode(Ar) $\leftarrow$ N_e(C);
      outputnode(Ar) $\leftarrow$ N_i(Cl);
    end for
  end if
end for
for all *Usage* U between two *Classes* or *Components* U_S, U_T stereotyped as «Equipment» **do**
  CreateNodeFromProtocol(Ac);
  create a *BN arc* Ar;
  inputnode(Ar) $\leftarrow$ N_e(U_T);
  outputnode(Ar) $\leftarrow$ N_e(U_S);
end for

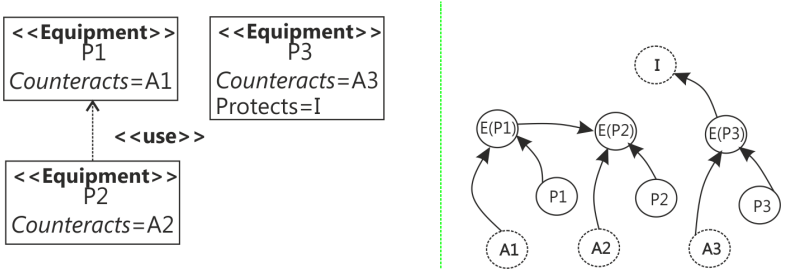


Figure 2.20: Transformation for Protection

With respect to the BN structure depicted in Fig.2.9, the following Algorithm 4 generates the nodes related to the protection protocols. This Algorithm is more complex than the other, for this reason two procedures have been defined and properly invoked in the pseudocode. These two procedure will be described in the following and will generate: (1) nodes and arcs corresponding to the internal activities of a protocol and (2) arcs corresponding to the decision and merge nodes, if used in the description of a protocol.

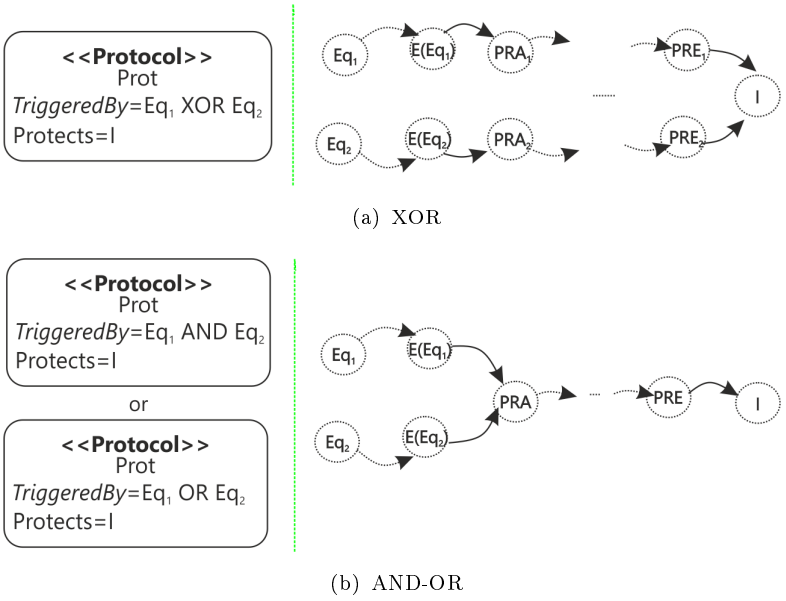
The remaining part of Algorithm 4 is used to manage the activation condition of the protocol itself (specified through the *triggeredBy* tagged value) and the connections with the protected sites. Note that the *triggeredBy* tag is typed as *VSL_Expression*, the transformation algorithm works under the hypothesis that it has been set as a simple logic condition (*AND*, *OR* and *XOR*) between equipments. In detail, if the triggering equipments are in *XOR* relationship, then the nodes and arcs corresponding to the protection protocol shall be replicated many times as the number of triggering equipments in the logical condition. Otherwise, in cases of *AND* and *OR* conditions, the nodes shall not be replicated, and the arcs connect each node generated from a triggering equipment to the node representing the first action of the protocol.

The generation of the protection nodes and arcs of the BN structure according to the algorithm reported above is exemplified in Fig. 2.21. Specifically, in Fig. 2.21(a), a protocol triggered by the *XOR* of two equipments *Eq1* and *Eq2* is showed. The Algorithm just described, generates two different chains of Bayesian nodes, one for each equipment. In both chains the *PRA*-node related to the first equipment is connected to the *E*-node of one of the two triggering devices. The PRE node of the final activity is then connected to the *I*-node related to the site *I*, protected by the protocol.

Fig. 2.21(b) reports the Bayesian network generated in case of *AND* and *OR* boolean operators. In these cases the chain related to the protocol is not replicated, both the *E*-node of the triggering equipments are connected to the *PRA*-node related to the first activity of the protocol. The final *PRE*-node is connected to the *I*-node related to the protected site, as in the previous case.

Algorithm 4 generateProtectionLevelBN - PRA and PRE nodes

```
for all Activity Ac stereotyped as «Protocol» do
  if triggeredBy tagged value for Ac contains XOR then
    for all Class or Component C stereotyped as «Protection» contained in
    the tagged value triggeredBy do
      CreateNodeFromProtocol(Ac);
      if DecisionNodes and MergeNodes exist in Ac then
        CreateArcsForDecisionAndMergeNodes(Ac);
      end if
      create a BN arc Ar;
      inputnode(Ar) ← N_e(C);
      outputnode(Ar) ← N_pra(Af) where Af is the first action of Ac;
    end for
  else
    CreateNodeFromProtocol(Ac);
    if DecisionNodes and MergeNodes exist in Ac then
      CreateArcsForDecisionAndMergeNodes(Ac);
    end if
    for all Class or Component C stereotyped as «Protection» contained in
    the tagged value triggeredBy do
      create a BN arc Ar;
      inputnode(Ar) ← N_e(C);
      outputnode(Ar) ← N_pra(Af) where Af is the first action of Ac;
    end for
  end if
  if protects tag is defined for Ac then
    for all Classifier C stereotyped as «Infrastructure» referred by the tagged
    value protects do
      create a BN arc Ar;
      inputnode(Ar) ← N_pre(Al) where Al is the last action of Ac;
      outputnode(Ar) ← N_i(C);
    end for
  end if
end for
```



(a) XOR

(b) AND-OR

FIGURE 2.21: *triggeredBy* pattern transformation for Protocol

The internal part of the Bayesian network related to the protocol is generated by the Algorithm 5, which generates:

- the protection PRA and PRE nodes, corresponding to UML Elements stereotyped as «ProtocolRule»;
- the arcs from PRA-nodes to PRE-nodes;
- the arcs from E-nodes to PRE-nodes;
- the arcs from PRE-nodes to the I-nodes.

The transformation generates a pair of PRA and PRE nodes for each UML ActivityNode stereotyped as «ProtocolRule» as well as an arc connecting them. The PRA-node represents the starting of an action of a protection protocol, the PRE-node represents the execution of that action. Since an action is executed by an operator and could be supported by other protection systems (according to the tagged values *executedBy* and *supportedBy*), additional arcs are generated from related E-nodes to PRE-node of this action.

The generation of the protection nodes and arcs of the BN structure according to the algorithm reported above is exemplified in Fig. 2.22. The two actions *PR1*

Algorithm 5 CreateNodeFromProtocol procedure

```
CreateNodeFromProtocol(Activity Ac)
for all ActivityNode An stereotyped as «ProtocolRule» in Ac do
  create a BN node N_pra;
  create a BN node N_pre;
  create a BN arc Ar;
  inputnode(Ar) ← N_pra(An);
  outputnode(Ar) ← N_pre(An);
  for all Class or Component C stereotyped as «Operator» referred by the
  tagged value executedBy do
    create BN arc Ar;
    inputnode(Ar) ← N_e(C);
    outputnode(Ar) ← N_pre(An);
  end for
  if supportedBy tag is defined for An then
    for all Class or Component C stereotyped as «Protection» referred by the
    tagged value supportedBy do
      create BN arc Ar;
      inputnode(Ar) ← N_e(C);
      outputnode(Ar) ← N_pre(An);
    end for
  end if
  if protects tag is defined for An then
    for all Classifier C stereotyped as «Infrastructure» referred by the tagged
    value protects do
      create BN arc Ar;
      inputnode(Ar) ← N_pre(An);
      outputnode(Ar) ← N_i(C);
    end for
  end if
end for
for all ControFlow Cf in Ac do
  if Cf is between two ActivityNodes A_S, A_T stereotyped as «ProtocolRule»
  then
    create BN arc Ar;
    inputnode(Ar) ← N_pre(A_S);
    outputnode(Ar) ← N_pra(A_T);
  end if
end for
```

and *PR2*, stereotyped as «ProtocolRule» generates four Bayesian nodes (two for each one of them). Since both *PR1* and *PR2* are executed by *P1*, two arcs from the *E*-node related to *P1* to the *PRE*-node of *PR1* and to the *PRE*-node of *PR2* are generated. An arc from the *PRE*-node of *PR1* to the *I1* node is generated since the action *PR1* protects *I1*, as well as the arc from the *E*-node of *P2* to the *PRE*-node related to *PR2* since this action is supported by *P2*.

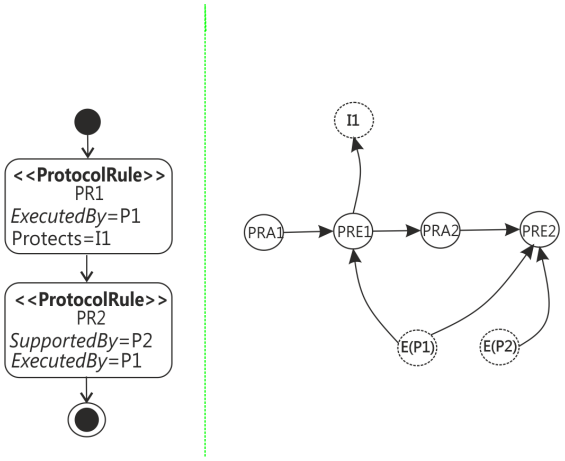


FIGURE 2.22: Transformation for Protocol

Decision and merge nodes require the generation of complex structures, in terms of arcs; for this reason these structures are generated by the Algorithm 6. In detail, the Algorithm connects the predecessor node with the successors nodes and these last together, avoiding the contemporary activation of more than one branch. Obviously the conditions indicated on the exiting branches shall be in mutual exclusions; one *ELSE* condition is also admitted.

The generation of the protection nodes and arcs of the BN structure according to the algorithm reported above is exemplified in Fig. 2.23. In this case a protocol control flow, exiting from the action *A*, can either enters the *B* or the *C* action on the basis of the identification of an attack action by the equipment *Eq*. From this situation, a Bayesian network connecting the *PRE*-node related to *A* is connected to both *PRA*-nodes related to the actions *B* and *C*; another arc, connecting the *E*-node related to *Eq* to the *PRA*-node related to *B*, is also generated. At last the arc from the *PRA*-node related to *B* to the *PRA*-node related to *C* is added, in order to model the mutual exclusion between the two branches.

Algorithm 6 CreateArcsForDecisionAndMergeNodes procedure

```
CreateArcsForDecisionAndMergeNodes(Activity Ac)
for all DecisionNode D in Ac do
  for all ControlFlow Cf where Cf_S is D do
    create BN arc Ar;
    inputnode(Ar) ← N_pre(CfE_S) where CfE is the ControlFlow in which
    D is CfE_T;
    outputnode(Ar) ← N_pra(Cf_T);
    if condition(Cf) contains ELSE then
      for all ControlFlow CfO different from Cf where CfO_S is D do
        create BN arc Ar;
        inputnode(Ar) ← N_pra(CfO_T);
        outputnode(Ar) ← N_pra(Cf_T);
      end for
    else
      for all Class or Component C contained in condition(Cf) do
        create BN arc Ar;
        inputnode(Ar) ← N_e(C);
        outputnode(Ar) ← N_pra(Cf_T);
      end for
    end if
  end for
end for
for all MergeNode M where M_T is not a FinalNode do
  for all ControlFlow Cf where Cf_T is M do
    create BN arc Ar;
    inputnode(Ar) ← N_pre(Cf_S);
    outputnode(Ar) ← N_pra(CfE_T) where CfE is the ControlFlow in which
    M is CfE_S;
  end for
end for
```

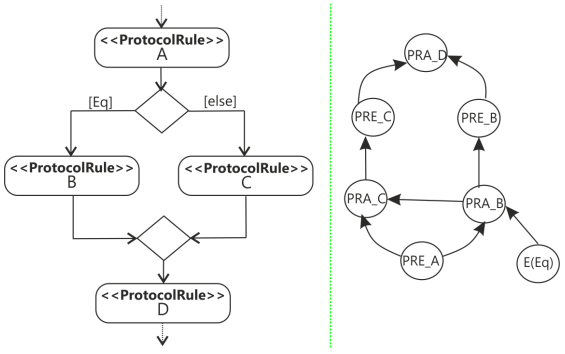


FIGURE 2.23: Transformation for Decision Node

Chapter 3

An Innovative Interoperability Framework for PSIM Systems

As stated in section 1.3, the integration of security systems is one of the primary requirements in the scenario of the physical security. Actually, the companies' application portfolio is still a mosaic founded on several independent systems. In contrast with this, new applications can't operate as stand-alone entity and they need to integrate with existing systems. In addition, a real security improvement can be reached only through the cooperation not only among ICT (Information & Communication Technology) systems but also among operators belonging to the same interest domain, resulting in the adoption of a new class of systems: the Systems of Systems.

The Department of Defense (DoD) defines a SoS *"as a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities"* [85]. The architecture requirements of an integrated security system comply with the five main characteristics of SoS individuated by Mayer [86]: (i) Geographic Distribution (the several systems of an SoS are geographically distributed), (ii) Operational Independence (the SoS is composed of systems which are independent which can often perform their functionalities when not working with other constituent systems), (iii) Managerial Independence (each system of SoS can keep its own managerial sphere that is each of them is separately acquired and integrated and maintains a continuing operational existence

independent of the SoS), (iv) Evolutionary Development (functions and purposes of SoS can dynamically change and systems can be added, removed, and modified with experience), and (v) Emergent Behaviour (SoS are capable to provide new functionalities resulting from cooperation of the constituent systems).
This chapter reports the experience with the concrete application of a SoS architecture to rail mass-transit systems. Specifically, it describes part of the work conducted within the Secur-ED project by Ansaldo STS in the realization of a framework which allows for the interoperability between different security equipments.

3.1 Context: the Secur-ED Project

The complexity of modern security systems, deputed to the protection of mass-transit transportation, reflects the complexity of the transportation systems themselves: a very high number of daily passengers, an high number of access points, an high number of interconnection nodes and neuralgic transport interchanges to economic activities require complex interconnections of existing and newest protection devices, security processes and organizations leading to a System of Systems (SoS), based on networked communication.
Secur-ED was a demonstration EU-funded project aiming at integrating technologies and processes covering all aspects of urban transport security for typical big and mid-sized European cities. Completed in September 2014, the project involved 41 partners (industries, operators, universities and research institutions) with the intent to provide a comprehensive set of organizational, procedural and technical tools addressing the major sources of threats and disruption and validate the provided solutions through the demonstrations in several real contexts[87]. One of main objectives of Secur-ED was to implement an *interoperability framework* in order to tie all security actors into a SoS. The focus was on enabling providers to adapt their solutions with minimal non-recurring costs and proving the maturity of modern technologies by putting them in operation. Integration was demonstrated in four flagship demonstrations which took place in Paris, Milan, Madrid and Berlin as well as in other satellite (smaller-scale) demos. Ansaldo STS played different roles in the project, in particular it was responsible for developing the

interoperable framework and collecting and analyzing results in order to provide guidelines and best practices. The project results are publicly available in[42],[88], [89], [43], and [90].

3.1.1 Design Principles

This Section aims to describe the fundamental technical, technological and functional requirements adopted for the architecture design in the Secur-ED project.

3.1.1.1 Security Technologies and Integration

The security technological panorama has been certainly strengthened in the last decade thanks to the introduction of numerous new technologies to detect and deter more disparate attacks. Nevertheless, many security technologies, which have been developed and deployed in the past, have gone through upgrades in order to adapt themselves to the evolved security measures. Furthermore, in the railway industry, the life cycle of these security technologies extends much longer in comparison to other industries; as a consequence a requirement of the overall architecture is to sustain the existing legacy technologies. So, one of the primary concerns was to integrate legacy and innovative technologies in a single management system.

3.1.1.2 Interoperability

Nowadays, interoperability is a fundamental concern for improving security in the transportation domain. In fact, this is an essential quality for a distributed systems as well as for a SoS. This application domain is characterized by the presence of different public and private companies, and its security involves various kinds of organizations. Then, for counteracting serious threats like terrorist attacks, important requirements are information sharing and collaboration at the occurrence of security accidents. This is possible only through an high interoperability, which can enable the interaction among security systems, different transport operators authorities (e.g. metro, railway, bus) and so on.

3.1.1.3 Open Standard

By now, the benefits arising from the usage of open standards are fully blown. Today, also in the context of railway security, the need to adopt open standards is very strong. Multiple factors drove this trend, such as the growing interest towards the security issues, the market orientation in innovative security technologies, changed current regulations in critical infrastructure protection matters, and so on. Other reasons can be found in the fact that they help to overcome the barriers towards the subsystems integration, reducing the dependencies from specific vendors and simplifying the communication among stakeholders. Furthermore, a recent trend is to go towards a convergence of "safety" and "security" and thus, the adoption of open standards supports this change.

3.1.1.4 Event Orientation

The security operates in an unpredictable and dynamic context where an attack can happen anytime. So, the event-driven approach [91] deals with needs of protection systems perfectly. This approach is built around the idea that events are the most significant elements in the system and that they are produced somewhere in the system and consumed somewhere else in the system. Thus, two concepts are basic in this approach: event and notification. An event can be defined as something that happens somewhere that is of interest for one or more objects; while, the notification is the message sent by an object to the interested parts to inform about the event. In this perspective, when the various security systems (e.g., video analysis, intrusion detection, sound detection, management systems, etc.) detect particular events or situations, they generate a notification and send it to management systems.

3.1.1.5 Scalability, Modularity & Reusability

These requirements are tied directly to one of the most strategic objectives: the definition of an architecture which is applicable in different contexts, like big and mid-sized European cities, and is adoptable to new threat scenarios. Hence, a

modular architecture is necessary in order to be extended or reduced depending on specific security needs. Given the large numbers of different technologies of a complex security system, modularity is a critical aspect of the design and development phase since it allows for decomposing the system into a number of components that may be mixed and matched in a multiple configurations.

3.2 Interoperability Framework

Interoperability is an essential quality for a distributed systems as well as for a SoS and it has been much discussed by the scientific community. According to ISO/IEC 2382-01, Information Technology Vocabulary, Fundamental Terms [92], it is defined as: *"the capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units"*.
Interoperability is the key concept to arrive at systems-of-systems that support security awareness and response in public urban transport. Starting from what stated in[93] which presents a stack with different layers of interoperability, the aim was to make the effort for reaching as more levels as possible. In particular, *technical interoperability* is achieved by means of common standard communication protocols in order to exchange data between the component systems, *syntactic interoperability* is achieved adopting a common data model and eventually, *semantic interoperability* is achieved by defining the content of the information exchanged in the chosen data model. In addition, in order to achieve a higher level of interoperability configurable operative procedures have been used for an efficient management of security incidents[89].

The figure 3.1 shows the general paradigm from an architectural point of view. The overall architecture, shall rely on a dependable and effective communication frameworks which allows events sharing through standard interfaces. In this way, it enables interoperability of security systems (depicted at the bottom) but also of management systems through integration and aggregation of information into one or more control center (depicted in the upper part). The role of a control center is to gather and correlate various event sources into a single platform in order to

show to operator a coherent situation with what is happening. Furthermore, this paradigm allows also to integrate easily other kinds of systems like events correlation systems which are able to reason about heterogeneous data, implementing the concept of "fusion" through event correlation. Such systems can play an important role for an effective enhancing of the situation awareness and for improving the decision making process of human operators [94].

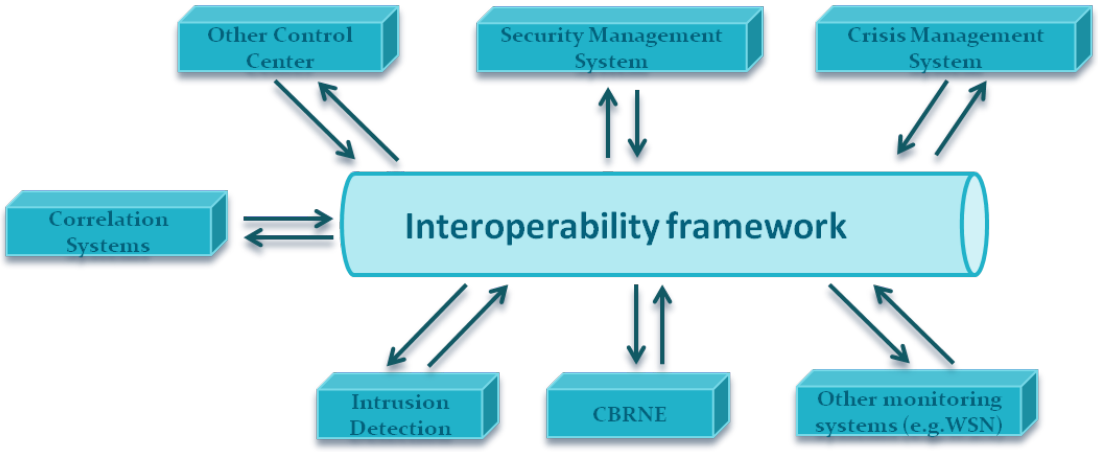


FIGURE 3.1: General paradigm of a security architecture

Examples of event-based communication frameworks can be found in [95], where the authors describes a service based approach which integrate different components in automotive domain. In [96] an innovative event-driven architecture, integrated with web services, is described. [97] proposes a reference architecture for event-driven traffic management systems, which enables the analysis and processing of complex event for decision support in sensor-based traffic management systems.

One of the most essential enabling element of interoperability is the data model for events exchanging. Typical attributes for the event specifications are: an unique identifier, the type of event, the time when the event occurred, the location where the event happened, the device or system that originated the event, etc. At this aim, the Common Alerting Protocol (CAP) [98] standard of the Oasis Consortium has been chosen. Based on best practices identified in academic research and real-world experience, CAP is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. It provides a

XML-based template for effective warning messages, so allowing dissemination of consistent alerts simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. Also, it facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act.

3.2.1 Implementation Principles

The interoperability framework is the key component of the general paradigm presented above (see figure 3.1). It is based on architectural patterns and open standards which are successfully used in other industries; in fact, it combines the intelligence and proactiveness of Event-Driven Architecture (EDA) with the organizational capabilities found in Service-Oriented Architecture (SOA) [99]. Basically, it is an event broker Web Service-based which allows for interchanging of events. It contains also a discovery service which is able to discover new services inside the overall system.

The interaction pattern used to disseminate information among different entities is event-driven, also called notification-based (a review of dissemination protocols can be found in [100]), based on the well-known publish-subscribe scheme. In addition, with the aim of uniquely identifying the resources (e.g. sensors, systems, etc.), the Uniform Resource Identifier (URI) standard, and specifically the Uniform Resource Name (URN) syntax [101], has been adopted.

The event broker has been developed in Java language adopting the following standards: WS-BaseNotification [102] for the service implementation, and the CAP [98] format as events data model. In order to meet different needs (e.g., integration of a CAP alert into a notification message or support to development) some extensions have been made to the WS-BaseNotification standard. Nevertheless, these extensions don't change the behavior of standard functionalities but just help to cover these specific needs.

As shown in Figure 3.2, the event broker interface is composed of two interfaces, one for exchanging the events and another for managing the subscriptions. In this way, the security systems are the producers while the integrated management

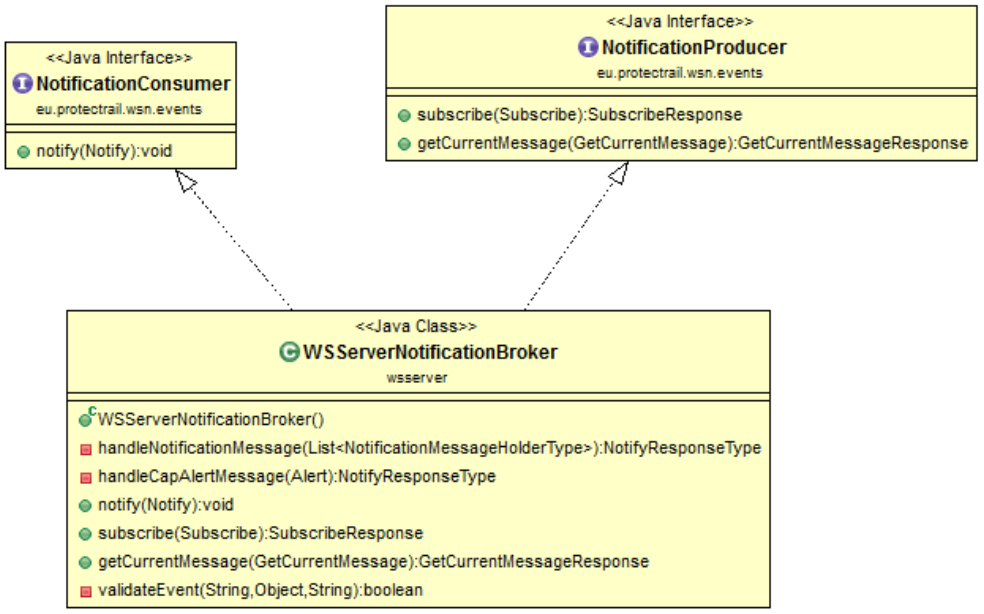


FIGURE 3.2: Class diagram of event broker

systems are consumers. Actually, this is not a strict assignment since a generic system can play both the role of producer and consumer. For example, this is the case of an event correlation system: this kind of system initially plays the role of consumer, as it receives the events, but it use the received events to generate new events and send them to the broker. This peculiarity highlights the flexibility which has been introduced into the architecture.

WS-BaseNotification is a generic event interface that can transport generic XML contents so, in order to wrap an alert into the notification message, two following actions have been performed:

1. the import of the XML schema of the CAP in the wsdl;
2. the extension of the NotificationMessageHolderType, a type defined in the wsdl (Figure 3.3).

The *notify* service scenario is shown in Figure 3.4: the producer invokes the *notify* service exposed by the event broker for sending a notification message, and then the consumer receives messages directly from the broker through the *notify* service that, in turn, it exposes.

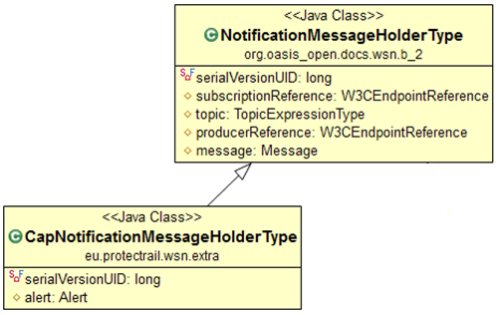


FIGURE 3.3: Extension for alert CAP

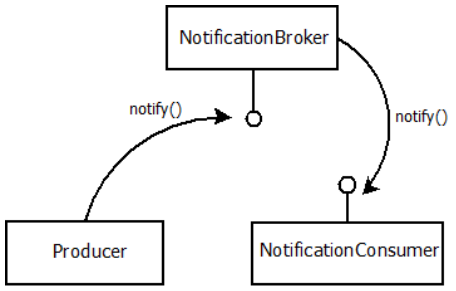


FIGURE 3.4: Interaction for notification message

3.3 Experimentation on Field: Enabling the System-of-Systems

The interoperability framework has been successfully tested in the scope of Secur-ED project on different on mass transit systems of several European cities. In this work the experimentation is referred to Milan demo, carried out on ATM[1] transportation.

Architectures for mass-transit security consist of several distributed and heterogeneous components, enabling the detection of attack actions, and of integrated management systems, able to collect and correlate to a some extent the detected events into a shared situation picture. The security needs of the Secur-ED project asked for an open architecture that shall be adaptable to different environments and that shall address wide spectrum of threats, ranging from low-probability high-impact events (e.g., terrorist attacks) to daily threats (e.g., acts of vandalism).

According to the general paradigm outlined in previous section, the requirements

[1] Azienda Trasporti Milanesi-public transportation company in the Milan metropolitan area

listed in the paragraph 3.1.1, and also in continuity with the previous project PROTECTRAIL[87], the realized architecture for the Secur-ED demos was an Event Driven Service Oriented Architecture (SOA 2.0) whose building blocks are shown in Figure 3.5. The combination of web services and event-driven systems was able to address the interoperability issue in heterogeneous distributed systems, enabling asynchronous interactions.

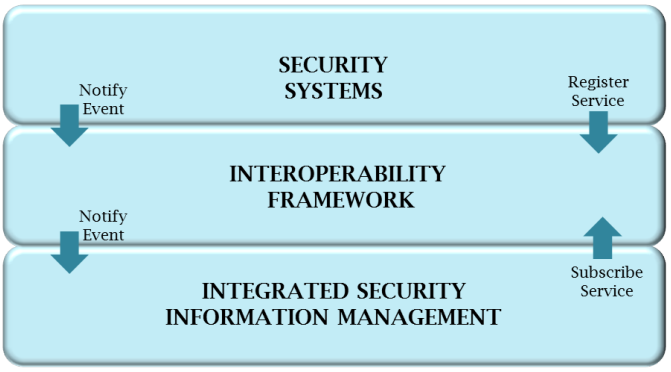


FIGURE 3.5: The Secur-ED Architecture

The experimentation concerned the technical feasibility of the solution and the implementation of actual attack scenarios in order to evaluate the effectiveness of the proposed architecture in mass-transit domain. The main aim was to demonstrate how innovative and legacy security technologies could be used and integrated, in order to improve the protection of critical assets. At the same time, the experimentation goals were to validate technologies and procedures used in the demonstrators and show the versatility, interoperability, and interchangeability of the security systems as well as their integration within existing operational procedures and are appropriate with respect to societal demands.

The interoperability framework has been used for creating the Secur-ED SOCC (Security Operator Control Center), which is a global security control center able to coordinate organizations with authorities, exchange information and integrate systems, also belonging to different public transport operators. Its effectiveness has been proved by the results of three real scenarios aiming at demonstrating the implementation of a local SoS in the Milan Area. In particular, the image 3.6 represents a general map of the hardware architecture for the Milan demonstration, where the following scenarios took place:

- Scenario 1 concerned the identification and tracking of persons presenting a suspicious behavior within the network of public transport managed and owned by different PTOs;
- Scenario 2 was related to the protection of a train in a stabling area and depot yard;
- Scenario 3 dealt with the reaction to an event in case of emergency and the subsequent management of the crisis;

Name and location are reported for each element in the map. At the top level, the technical room situated in ATM's premises of Monte Rosa is depicted in which all the necessary servers to connect all the protection systems with the SECUR-ED Control Centre provided by Ansaldo, composed by the Security Management System (SMS) and the interoperability framework. The result is a true PSIM system able to monitor and manage events detected by new and legacy system (i.e. the ATM's Control Centre (KABA)) providing a decisions support. In particular, SMS manages and controls a hierarchy of subsystem and devices from a central position. So it improves the situations awareness allowing a prompt reaction. In fact, a security operator has a global vision of what happens and he is able to supervise an emergency situation supporting the local operator with valuable information and coordinating the operations. On the contrary, the bottom level describes all the integrated security systems, composed by devices and if anything local servers. In detail, the systems are: CBRNE sensors for detecting radiological and chemical materials, several video analysis systems for tracking and crowding people, and for checking empty train, RFID systems and ticketing systems for tracking people by means of tickets equipped with RFID tags.
On the whole, the three scenarios have involved two operators of public transport (ATM and FNM), different Milan areas (Malpensa airport, 3 metro stations and depot area) and several organizations (police, municipal authority, fire brigades, ect) covering different security needs. In the tracking scenario, a suspicious person is followed through two different metro lines (ATM and FNM[2]) without losing him. In the depot scenario, the integration of different innovative technological systems (CCTVs, perimeter protection, train scanning and monitoring, procedures) has

[2]FNM Group Milano S.p.A.-Lombardy Regions Railway Operator

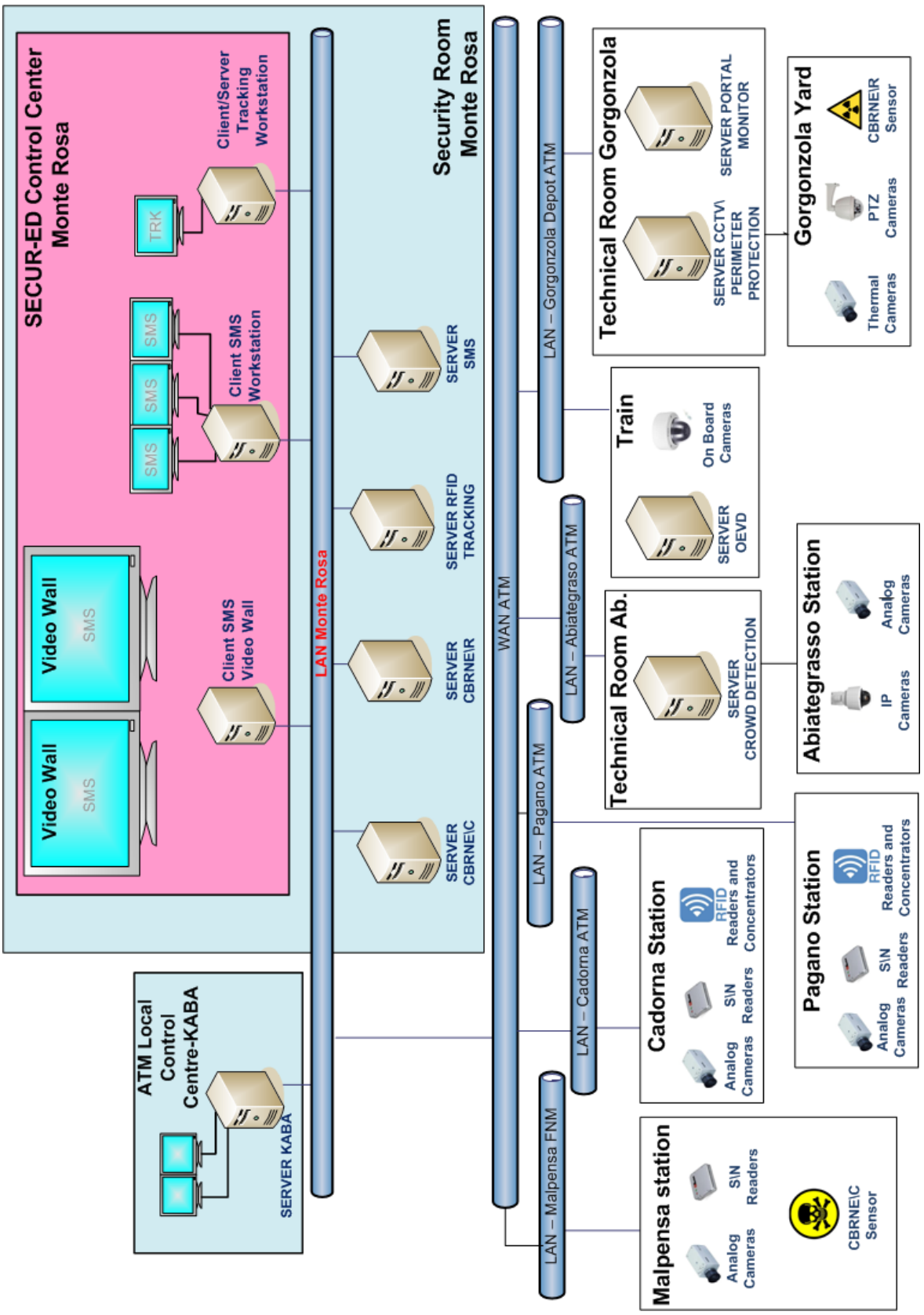


FIGURE 3.6: Hardware architecture in Milan Demonstration

provided a full security of the vehicles in the depot area. Thanks to the interoperability framework all systems worked together, succeeding even if some actions of an attack are partially performed. In the crisis management scenario different actors (Operator staff, Ambulance, Fire brigades, etc.) worked together to face a danger situation and to rescue people in the shortest time. Combining the three scenarios it is possible to deduce how the whole system was able to manage effectively different phases of a critical situation: before, during and after. For better clarify this point, please refer to the table 3.1 where some relevant system capabilities are listed.

Scenario	Before	During	After
1	Identification of suspicious passenger	Tracking of suspicious passenger in a multimodal transit network	
2	Perimeter protection	Tracking of intruder in area depot	
3		Crowding detection	Crisis Management for evacuation procedures

TABLE 3.1: System capabilities related to phases of the scenarios

3.3.1 A Real Usage Scenario

This section describes the tracking scenario in regard to the alarms exchanged through the interoperability framework. In this scenario different security systems have been integrated for tracking a terrorist having a dangerous chemical agent, who goes from Milan center to the Malpensa airport by three metro lines (two operated by ATM and one by FNM):

- the TVCC-based system for tracking people (producer);
- the ticket-based system for tracking people (producer);

- the RFID-based system for tracking people (producer);
- the CBRNe sensor for detecting chemical material (producer);
- the Security Management System (consumer).

The event broker sends all events generated by producers towards the security management system. In this way, the security operator has a global knowledge of what is happening, improving the situation awareness. The figure 3.7 shows a sequence diagram with the main events sent by the producers above.

A man with a briefcase enters in a Milan metro station. His behavior is perceived as suspicious, then the tracking procedure starts. The person is individuated and the first event "suspect tagged" is sent through the event broker. In Figure 3.8 the content of this event is shown, where some value tags are specified. The body of this message is a CAP alert where the tags contain information about the security system (the value, expressed in the URN syntax, represents the tracking people TVCC-based), the specific camera (source tag), the timestamp and the event type. From now on, all the cameras which detect the man are able to send an event of "suspect detected" allowing the tracking through the video flows. The man buys a ticket equipped with RFID, whose serial number is marked. In this way, when the suspect goes toward the turnstiles for validating the ticket (both in entrance and exit) the ticketing system sends an event which allows to follow him when it crosses different stations. Similarly, the RFID system sends an event when detects the ticket in the stations. Thanks to the use of the event broker, combining these three kind of information the probability of losing the man decreases considerably. Furthermore, at Malpensa airport a CBRNe sensor is deployed in the entrance, so the chemical substance in the man's briefcase is detected and thus the security operator alerts the competent authorities promptly.

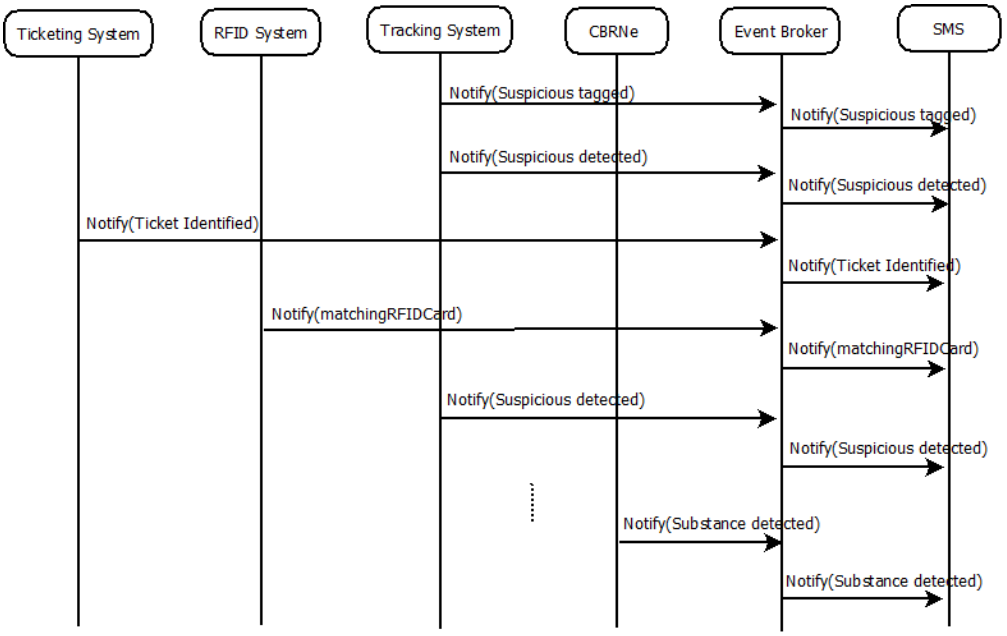


FIGURE 3.7: Events in the tracking scenario

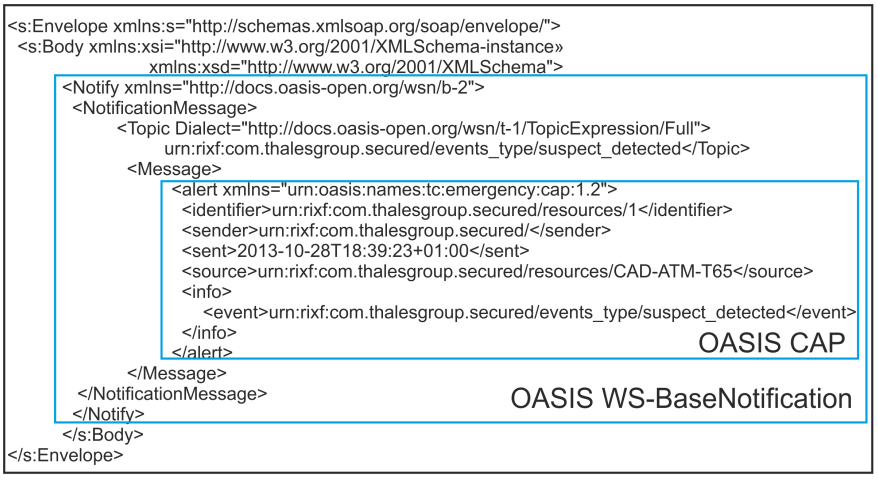


FIGURE 3.8: "Suspicious detected" event

Chapter 4

Application to the Mass-Transit Domain

This Chapter describes the application of the proposed approaches to a real world case study: the ATM's depot located in Gorgonzola, Milan. Two realistic attack scenarios have been considered: these scenarios have been taken from those defined by the SECUR-ED Project. In detail, the selected scenarios have been considered as significant and realistic inside the context of an European project since their realism have been studied through a risk assessment so that they correspond to real concern on security threats. They regarded the execution of physical attacks and were devoted to the demonstration of the effectiveness of integrated protection systems; in fact, these scenarios ended with the blocking of the attacker.
The case study will be presented in relation to the two perspectives given in this thesis: the architectural approach defined in the Secur-ED project and the analysis approach defined in the METRIP project.

4.1 Case Study

As said, the case study consists of two scenarios, both of them concerning the train protection within a stabling area or a depot yard. In particular, the aim is to preserve the integrity of trains both when they enter or leave the depot area and

they come to rest at depot area. It takes place in ATMs Gorgonzola depot since it is potentially exposed to many attacks by graffiti perpetrators and intruders because of its location, very far from the city. The attacks concern an intrusion in depot in order to make graffiti on a train and a radiological attack. The aim of the scenario is double:

1. assuring the capacity to identify any access violation at the depot (by perimeter or by any other entry);
2. demonstrating the capability to detect presence of unauthorized people or dangerous objects, vandalistic acts or sabotages against the trains.

4.2 Architectural Approach

The depot area is showed in Fig. 4.2(a): it is connected to the railway line through a main entrance with two tracks. The total area is around 450 meters long and 100 meters wide, while the internal of the depot is around 250 meters long and 75 meters wide. The protection system comprises different security devices deployed in the depot area. The perimeter of the area is covered by six thermal cameras whose video streams are analyzed by a VCA server which performs motion detection algorithms. In addition, in order to cover the overall depot area PTZ cameras are used exploiting their variability of field view. This is made by an innovative system based on VCA using detections of thermal cameras for activating object tracking algorithms that automatically pilots a PTZ camera. At this aim, thermal cameras are organized in clusters with PTZ cameras. Each cluster is composed by two thermal cameras, which are able to detect a human intrusion, and a PTZ camera, which traces the intruder's movements. Thus, the PTZ camera is automatically activated by the detection of the thermal cameras. Moreover, a CBRNe system is deployed close to the rail exit. It is used to verify the presence of radiological elements on a vehicle which is entering the service. Furthermore, another system VCA-based is used for onboard protection. Using the onbord cameras, an On Board Empty Vehicle Detection (OEVD) system is used to detect the presence of unauthorized people when a vehicle enters the depot. Finally, a Security Guard

(SG) and a Security Operator (SO) are present. The first is at depot area while the second at the control center. The figure 4.1 depicts the hardware architecture for this scenario.

The two considered attack scenarios regards an intrusion and a chemical attack. In the following, showing the pictures taken on the field during the demo, we describe the evolution of the two scenarios.

- **Scenario 1: intrusion inside depot**. In Fig. 4.2(a), a top-view of the area depot and of the deployed protection devices is depicted; the yellow line traces the path followed by the intruder, while the pink one the path followed by the SG. In detail, the intruder enters within the depot area (Fig. 4.2(b)), climbing over the fence at the point indicated by the red star. The thermal camera, placed close to this entry point, detects the intrusion, sends alarms to the Security Control Center, and enables the tracking functionality of the PTZ cameras. The SG, alerted by the SO, goes to the place where the intrusion has been detected. In the meantime the intruder crosses the line of tracks and heads toward the covered area of the depot (Fig. 4.2(c)), where the trains are sheltered, and follows the dirt road near the depot perimeter, on the opposite side from which he entered. Still activated by a thermal camera, a PTZ camera follows the intruder until he passes behind a building where it looses him. Another thermal camera detects him again along the perimeter and the associated PTZ camera follows him; so the SO alerts the SG, who changes direction and moves towards him. Thanks to the tracking algorithm running on the PTZ cameras, the SO is able to support in a more accurate way the SG, who reaches the intruder and stops him(Fig. 4.2(d)).

- **Scenario 2: radiological attack on the train**. A train ends the service and enters into the depot area (Fig. 4.3(a)); the OEVD system checks the presence of unauthorized people on the vehicle (Fig. 4.3(b)). The presence of the intruder is hence individuated and, before the SG reaches the place, the intruder gets off the train (Fig. 4.3(c)) and put a radiological weapon on the external body of the vehicle (Fig. 4.3(d)). Then he runs away, but the SG is able to stop him (Fig. 4.3(e)) thanks to detections performed by

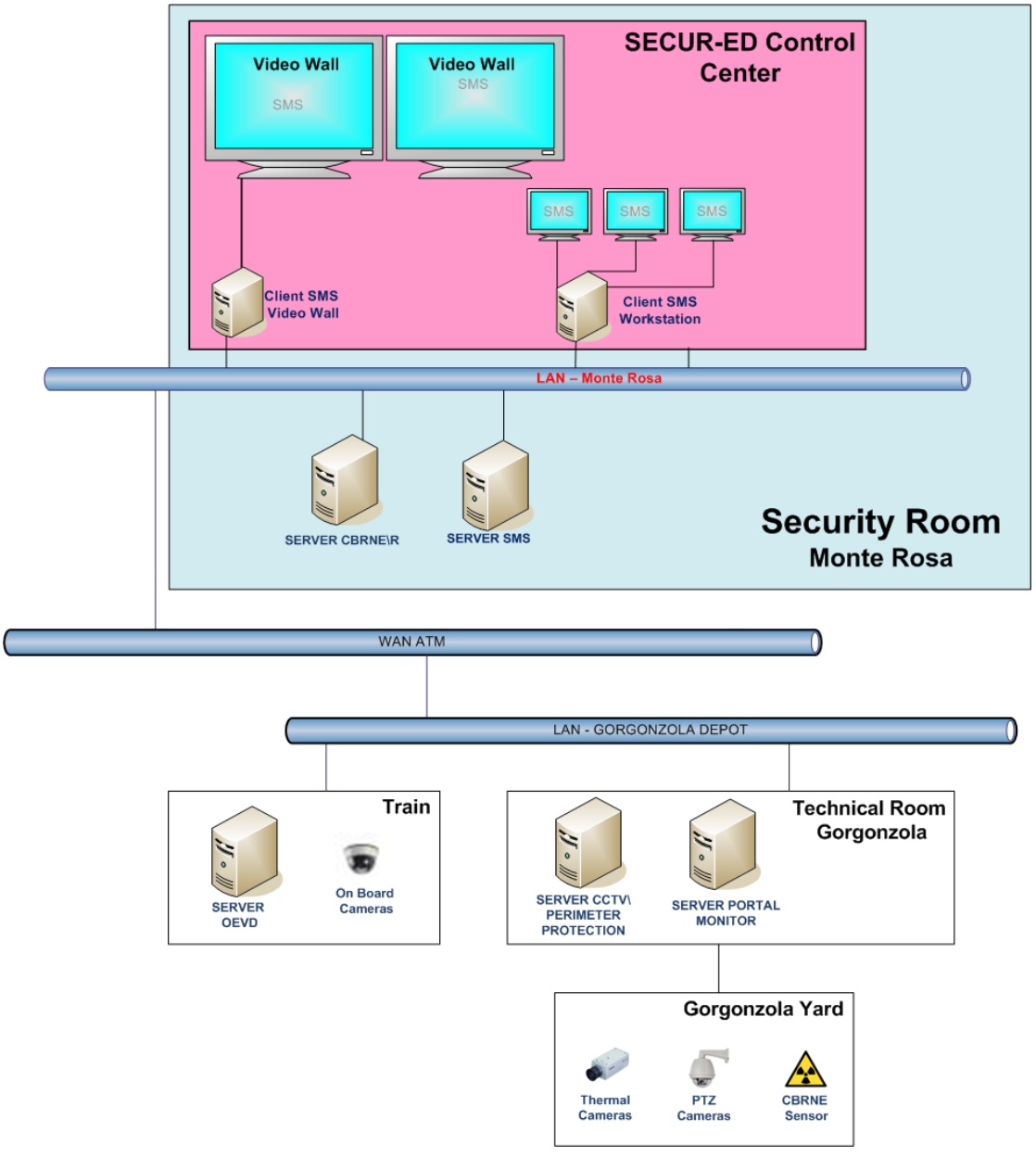
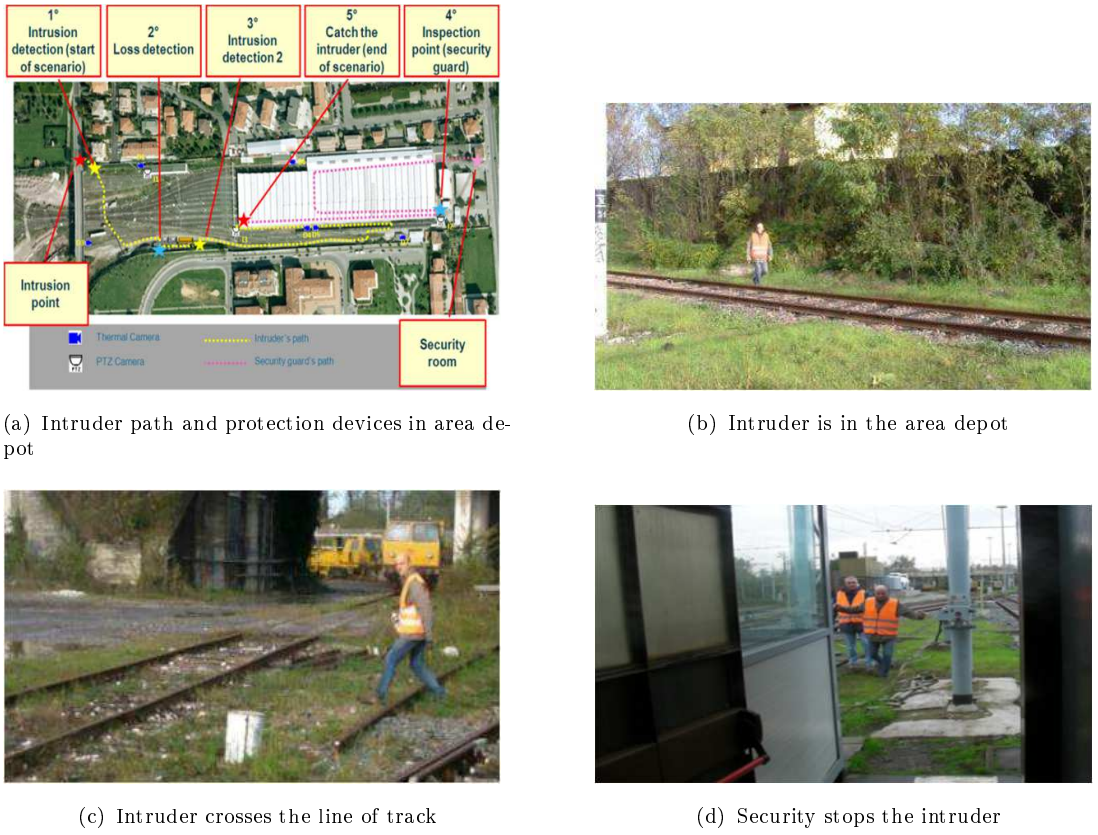


FIGURE 4.1: Hardware architecture for depot scenario

different sensors deployed in the depot. Before the vehicle enters in service (Fig. 4.3(f)), the CBRNe sensor, placed close to the exit of the depot area, detects the radiological agent emitted by the weapon (Fig. 4.3(g)); so the train moves toward a dead track and the necessary emergency procedures are executed (Fig. 4.3(h)).



(a) Intruder path and protection devices in area depot

(b) Intruder is in the area depot

(c) Intruder crosses the line of track

(d) Security stops the intruder

FIGURE 4.2: Intrusion and tracking scenario

4.3 Analysis Approach

The objective of this section is to show how the vulnerability, evaluated as the probability of having a successful attack, varies according to the physical features of the adopted protection system. The nature and the positions of the devices have not been changed with respect to the realistic scenarios since, in the real application inside SECUR-ED, they have been effective against the considered attacks. A quantitative analysis of the vulnerability have been conducted by applying the

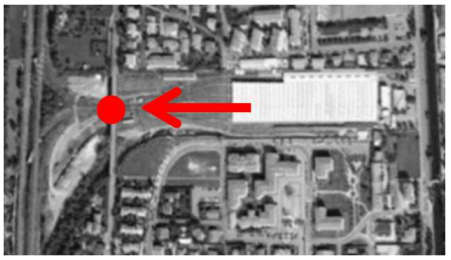
(a) The train enters in depot area and OEVD starts

(b) OEVD checks train

(c) Intruder gets off

(d) Intruder sabotages the train

(e) Security stops the intruder



(f) The train leaves the depot

(g) CBRNe sensor during the train transit

(h) CBRNe unit performs the emergency procedures

FIGURE 4.3: CBRNe and on-board monitoring scenario

METRIP approach, performing lastly a sensitivity analysis on the automatically generated Bayesian Network. In detail, we modelled the system by applying the CIP_VAM UML Profile, representing the interest portions of the system, the critical assets, the attacks and the protection system. Then, taking advantage of the automatic transformation described in paragraph 2.5.3, we evaluate the vulnerability corresponding to the given configuration of protection systems. The generated Bayesian Network has been analysed with the JavaBayes tool[1], while the sensitivity analysis have been conducted by implementing a trivial Java application which automates the execution of the network with the addressed tool. Table 4.1 summarizes the model parameters.

4.3.1 Infrastructure Model

The entire system is modelled through Composite Structure Diagrams. For sake of simplicity here we describe only the portion of the model that we consider necessary to understand better the following analysis: in fact, the set of tagged values modelling the geometrical features of each infrastructural element are here not shown. The Composite Structure Diagram in Fig. 4.4(a) provides a view of the whole area involved in both the scenarios, highlighting on one hand the sub-areas (stereotyped as *Site*) and objects (stereotyped as *Object*) of interest, and, on the other, the nested structure of the various elements.

At highest level of detail, the infrastructure has been modelled as a unique area (**DepotArea**) to whom is applied the video surveillance system. Then, the area under analysis is decomposed into subareas, the internal of the depot (**Depot**) and three external subareas (**Area1**, **Area2** and **Area3**). Specifically, the three external sub-areas have been defined according to the application range of the cluster of cameras belonging to the protection system. Inside each area, a specific set of tracks is present; hence we defined different classes, one for each site (e.g., **Track1** inside **Area1**) and we stereotyped those as *Object*. The tagged value *multiplicity*, not shown in the figure, has been used to model how many tracks are present inside each area. Furthermore, inside the depot, **ServiceTrain**s have been modelled through a class stereotyped as *Object*.

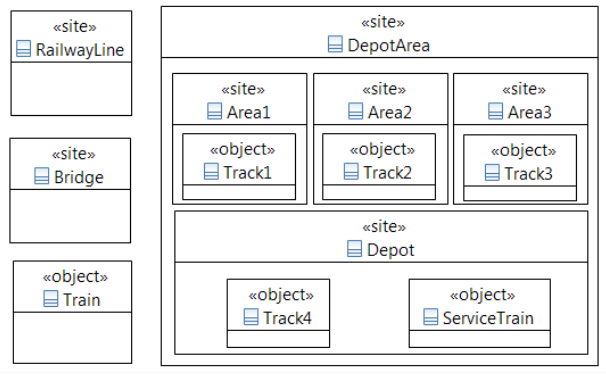
[1] http://www.cs.cmu.edu/~javabayes/

TABLE 4.1: Model parameters

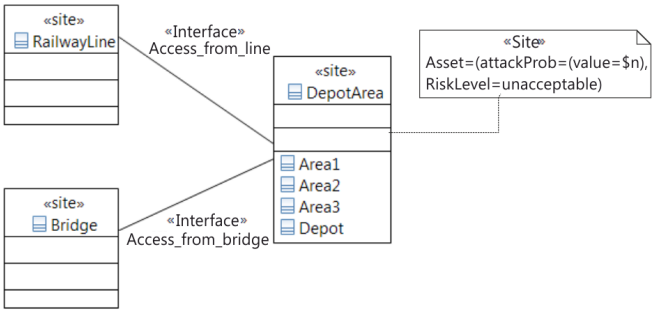
Parameter	Value
Number of attackers	1
Number of Security Guard	1
Availability of Security Guard	0.03
Effectiveness of Security Guard with PTZ support	0.7
Number of Security Operator	1
Availability of Security Operator	0.03
Number of thermal cameras	6
Failure rate of thermal camera	0.0012
Fnr of thermal camera	0.001
Fpr of thermal camera	0.05
Number of PTZ cameras	3
Failure rate of PTZ camera	0.0012
Fnr of PTZ camera	0.05
Fpr of PTZ camera	0.1
Number of OEVD System	1
Failure rate of OEVD System	0.0012
Fnr of OEVD System	0.01
Fpr of OEVD System	0.001
Number of CBRNe	1
Failure rate of CBRNe	0.012
Fnr of CBRNe	0.02
Fpr of CBRNe	0.1
Number of On-Board Camera	1
Failure rate of On-Board Camera	0.0012
Fnr of On-Board Camera	0.01
Fpr of On-Board Camera	0.1
Failure rate of Fence	0.000001

Other two classes model the other interest sites of the attack scenarios: **RailwayLine** represents the external railway which enters the depot; **Bridge** models the bridge outside the depot. At last, **Train** represents an external train that is running along the line and eventually will enter the depot.

The entrances of the depot are stereotyped as *Interface*: the Class Diagram depicted in the Fig. 4.4(b) reports the two accesses, from the line (used by the trains) and from the bridge (used by the attackers).



(a) Composite Diagram



(b) Class Diagram with interfaces

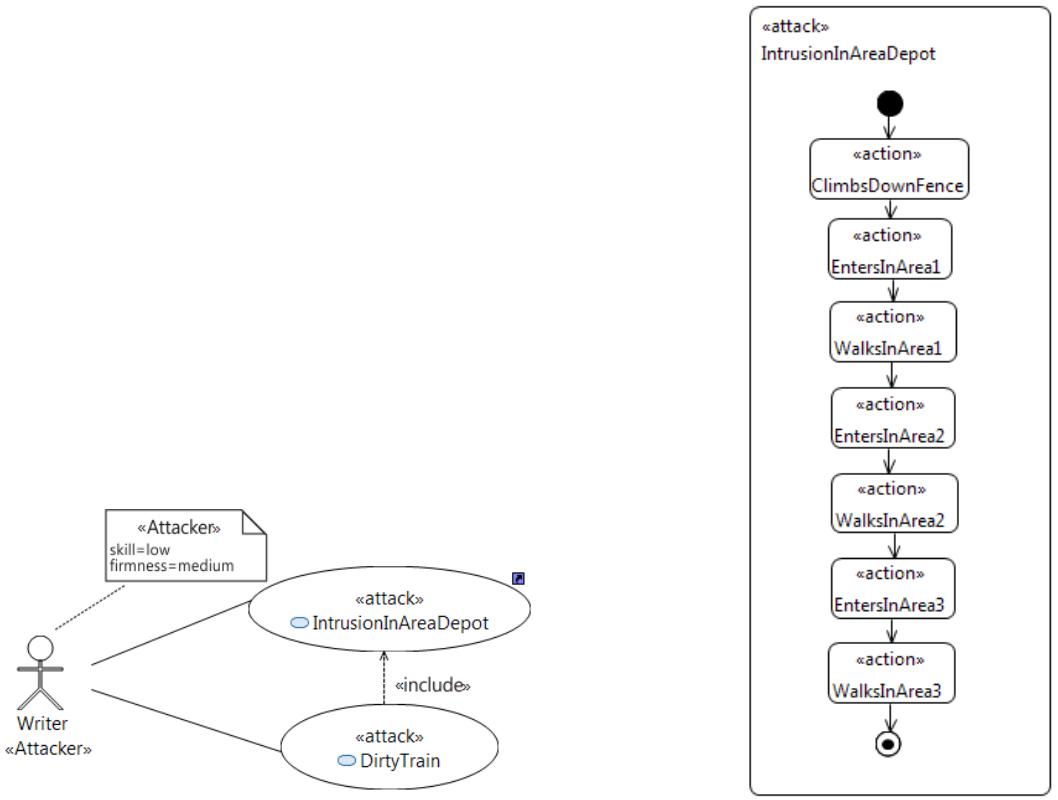
FIGURE 4.4: Infrastructure model

4.3.2 Attack Model

The two attack scenarios have been modelled through Use Case Diagrams and detailed through Activity Diagrams.

As described in Section **??**, in the first scenario a writer intrudes in the depot area in order to find a train on which to draw graffiti. Fig. 4.5 shows the corresponding attack model, where the Use Case Diagram (Fig. 4.5(a)) is composed by the actor **Writer**, stereotyped as *Attacker*, and by two use cases, stereotyped as *Attack*. In particular, there is an inclusion relation between the use cases since the intrusion is necessary to perform the graffiti attack. The Activity Diagram in Fig. 4.5(b) details the use case, previously described, showing the sequence of steps performed by the intruder. Each step has been stereotyped as *Action*.

In the second attack scenario a terrorist performs a radiological attack on a train by placing a radiological element on the external part of the carriage. Before this

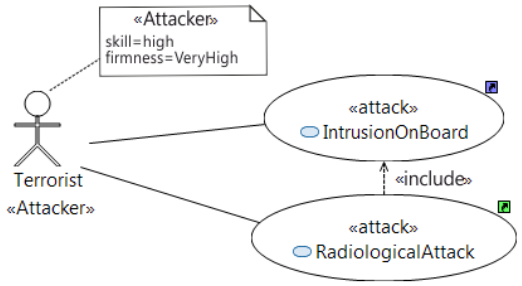


(a) Use case attack

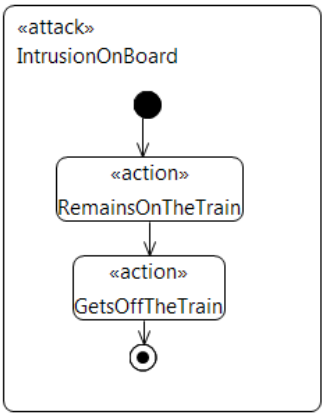
(b) Activity Diagram of intrusion attack

FIGURE 4.5: Scenario 1: Attack model

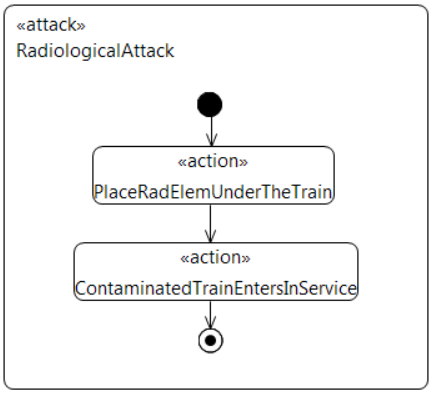
attack, the terrorist shall intrude the depot by remaining on the train at the end of the trip. Hence, the Use Case Diagram related to this attack (Fig. 4.6(a)) reports two use cases in which the one representing the radiological attack that includes the use case representing the intrusion. With respect to the **Writer**, the **Terrorist** is highly determined, patient and adaptive, hence the tagged values *skill* and *firmness* highlight this difference. Fig. 4.6(b) and Fig. 4.6(c) depict the Activity Diagrams which detail respectively the intrusion and the radiological attack use cases (this decomposition allows to consider separately the specific actions related to the two modeling phases of the attack). Hence, it is possible to reuse the intrusion use case in other possible attacks (performed by the terrorist) exploiting the inclusion dependency between use cases.



(a) Use case attack



(b) Activity Diagram of intrusion attack



(c) Activity Diagram of radiological attack

FIGURE 4.6: Scenario 2: Attack model

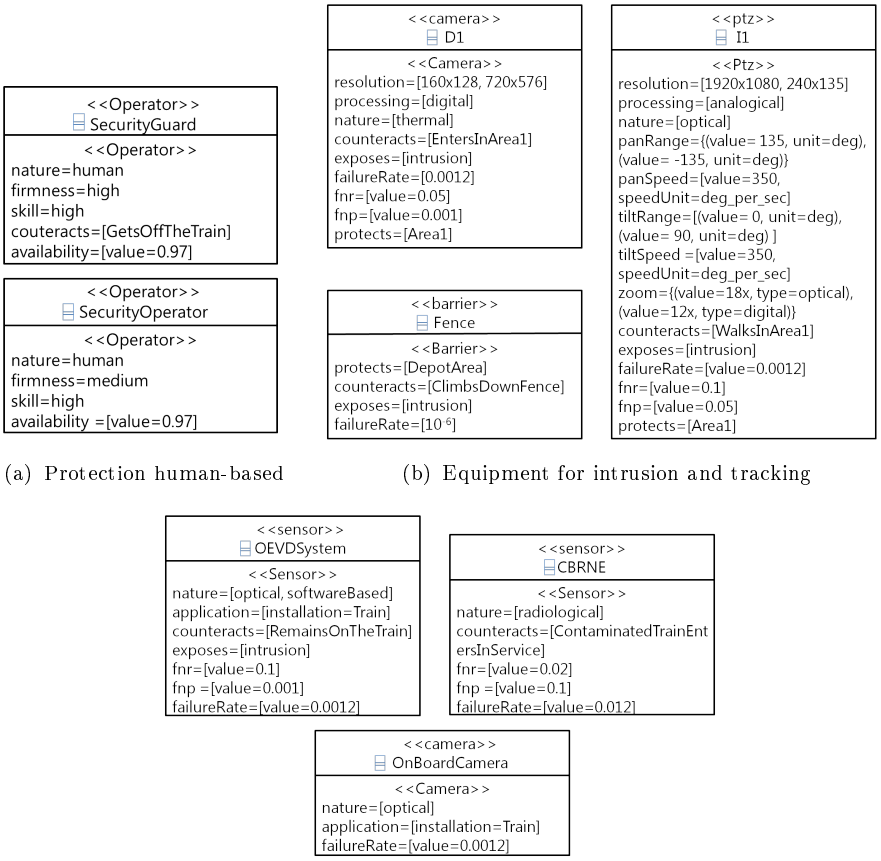
4.3.3 Protection Model

This Section describes the protection model. It consists of a set of protection systems (Fig. 4.7), referred by protocols (Fig. 4.8) and attack models.

Human resources (stereotyped as *Operator*) are employed to defend the asset in both scenarios: **SecurityOperator** and **SecurityGuard**. The first one is in charge of supervise and manage protections, while the second one deals with the physical defence of the area; for this reason, in the model they have different skills, costs, protection objectives and so on (see tagged values in Fig. 4.7(a)).

As described before, the depot perimeter is protected, by a **Fence** (stereotyped as *Barrier*) and by six thermal cameras (**D1,D3-D7**[2]) equipped with motion detection algorithms. As shown in Fig. 4.7(b), the thermal cameras are modelled

[2]for sake of simplicity, Fig. 4.7(b) details only the camera D1.



(a) Protection human-based

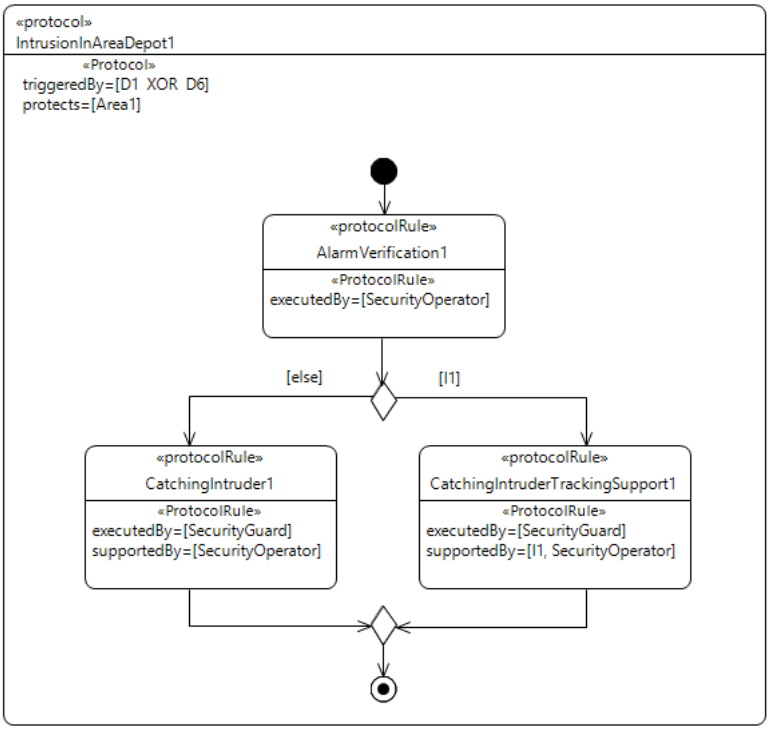
(b) Equipment for intrusion and tracking

(c) Equipment for on-board monitoring and radiological attack

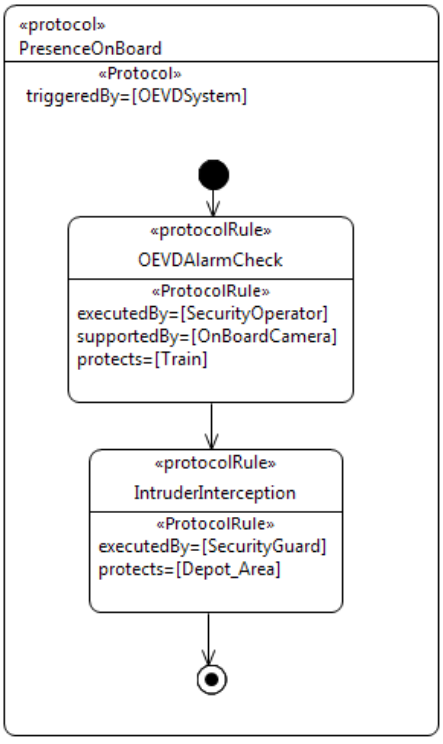
FIGURE 4.7: Protection systems of Protection model

using the *Camera* stereotype and, for each of them, tagged values specify their own features such as *resolution*, *processing*, *nature*, *counteracts* (it gives information about the actions of the attack to whom the protection device reacts). Moreover, there are three PTZ cameras (**I1-I3**[3]) stereotyped as *PTZ*, a specific form of *Camera*; consequently, in addition to tagged values already mentioned for thermal ones, some own features such as pan, tilt e zoom are reported by means of additional tagged values. The PTZ cameras are logically organized in clusters with the thermal cameras in order to improve the security of depot and support the intervention operations: briefly, when the motion detection algorithm of a thermal camera detects an intrusion, the PTZ camera belonging to its own cluster is activated and the object tracking starts. Since the PTZ camera requires

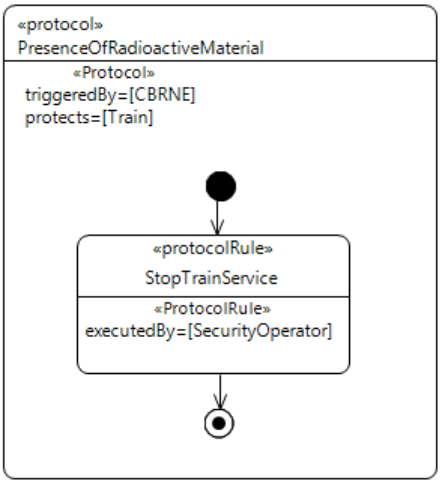
[3]for sake of simplicity, Fig. 4.7(b) details only the camera I1.



(a) Intrusion in area depot



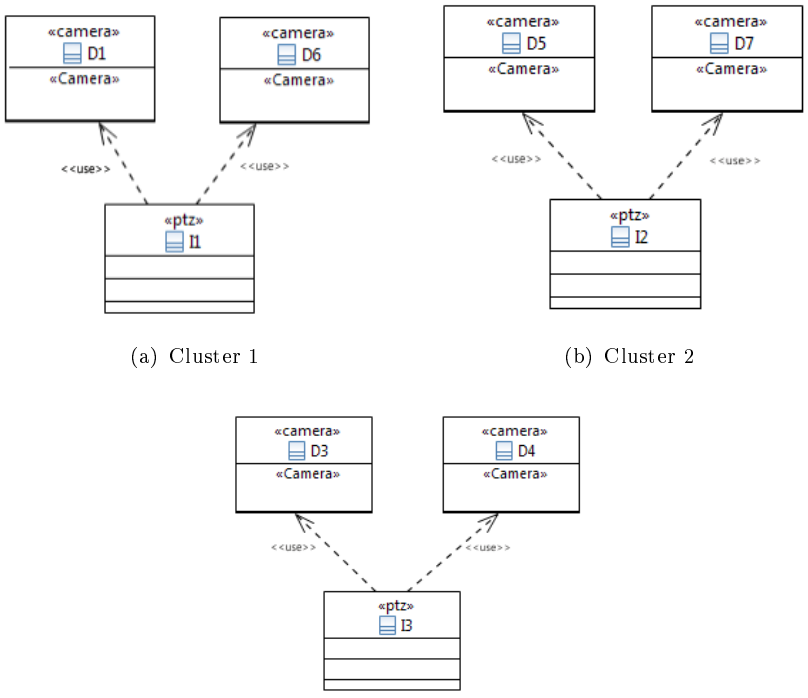
(b) Presence on board



(c) Presence of radioactive material

FIGURE 4.8: Protocols of Protection model

a thermal camera to be activeted, each cluster is modelled by means of the UML dependency << *usage* >>, as depicted in Fig. 4.9.



(a) Cluster 1

(b) Cluster 2

(c) Cluster 3

FIGURE 4.9: Clusters of thermal and PTZ cameras

The behaviours of the operators depend on the detection and tracking performed by the clusters and they obey to precise procedures that are represented by means of three protocols, one of which is showed in Fig. 4.8(a)[4]. Since we have just one intruder, the activation of the protocol is triggered by the XOR of two thermal cameras (*triggeredBy=[D1 XOR D6]*). Basically, the **SecurityOperator** verifies the intruder alarm generated by the thermal camera and then supports the **SecurityGuard** to catch the intruder. If the tracking algorithm correctly starts and pilots the PTZ, the **Security Operator** can watch the video streams and point the exact position of the intruder out to the **Security Guard**. In particular, the possibility to support the **SecurityGuard** with or without the object tracking running on PTZ camera is modelled by the decision node, in which the exit branch is chosen according to the availability of the PTZ camera.

[4]for sake of simplicity, Fig. 4.8(a) reports only one of the protocols, since they are substantially similar.

As for the onboard intrusion, the **OEVDSystem** performs on board monitoring when the train is out of service and enters the depot. This innovative device has been stereotyped as *sensor* as showed in Fig. 4.7(c). When the **OEVDSystem** detects a presence on board (*counteracts=[RemainsOnTheTrain]*) the related protocol (Fig. 4.8(b)) is activated. It involves two steps: after the **OEVDSystem** detection the **SecurityOperator** verifies the alarm using an on board camera (*supportedBy=[OnBoardCamera]*) and calls the **SecurityGuard** to apprise him about the intrusion so that he can catch him when the train comes in depot.

Finally, the **CBRNe** sensor (stereotyped with *sensor*) checks all the trains which leave the depot for resuming transportation service, in order to detect the presence of possible radioactive material (*counteracts= [ContaminedTrainEntersInService]*). In case of detection of radiological material, the simple protocol shown in figure 4.8(c) is performed.

4.3.4 Vulnerability Analysis

4.3.4.1 Scenario 1

This section describes the results obtained by analyzing the Bayesian Network, generated by applying to the first scenario (intrusion in area depot) the transformation. The resulting Bayesian Network is reported in Fig. 4.10, after a necessary graphical reorganization of the layout. According to what described in section 2.5.1, the attack nodes are placed at the bottom of the figure. In the middle of the network, the node related to the protection devices and protocols are depicted (notice that the nodes related to protocols are replicated as many times as for the conditions of the *triggered by* tagged value).

The vulnerability evaluated with the parameters given in Table 4.1 is 6.07%. A sensitivity analysis has been also conducted by implementing and running a trivial Java application which modifies the set of interest parameters. Specifically, three different studies have been performed that are described in the following:

1. *thermal fnr VS PTZ fnr*: the vulnerability is evaluated by varying the fnr of the entire set of thermal cameras and the fnr of the PTZ cameras;

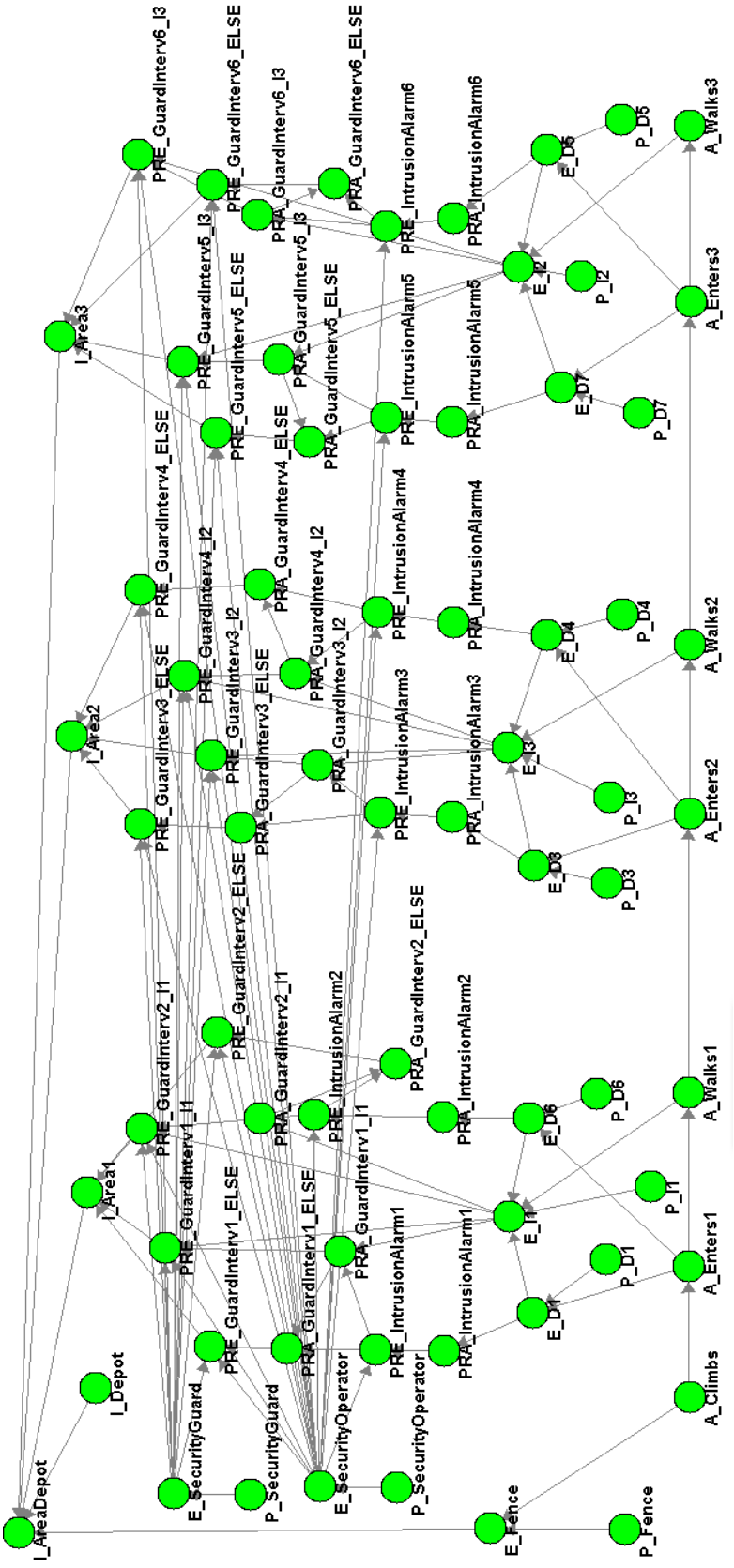


FIGURE 4.10: BN Attack Scenario 1

2. *PTZ availability VS catching success probability*: the vulnerability is analyzed with respect to the availability of the PTZ cameras and the probability of detecting an intrusion, without the support of PTZ cameras and intruder tracking;

3. *SO availability VS SG availability*: the vulnerability is evaluated with respect to the availability of both SO and SG.

The results of the analyses are plotted in the figures 4.11, 4.12, and 4.13 respectively. For each study, 882 evaluations (441 points for each surface, 21 values for each axis) have been conducted on the bayesian model. Each study required about 30 minutes to complete the analysis on a personal computer (Intel Core i5, 4GB of RAM).

Study 1. Fig. 4.11 reports the results for the vulnerability calculated by varying the fnr of the thermal and of the PTZ cameras. Different fnr values can be founded for commercial cameras; for these reasons the fnr values considered in this study varies in the range from 0% to 20% in order to assess the vulnerability in a very large range of possibilities. In fact, with fnr of 0%, the depot vulnerability is around 6%, reaching the maximum (about 24%) corresponding to an fnr of 20%. Furthermore, as showed by the graph, the vulnerability gradient along the axis related to PTZ is, in absolute value, lower than one measured along the other axis. This happens since the thermal cameras enable the intervention protocol; hence, if they don't work properly, the protocol is not executed.

Study 2. Fig. 4.12 depicts the trend of vulnerability with respect to the PTZs availability and the success probability of the catching action, performed by SG without the support of the PTZ cameras. This is because of considering the case in which the tracking algorithm fails and the PTZ does not start. The availability of the PTZ cameras varies from 99.78% to 99.98%, while the success probability goes from 60% to 80%. The graph shows that the vulnerability does not change very much varying these parameters: in fact, the variation from the maximum to the minimum is minor than 0.3%.

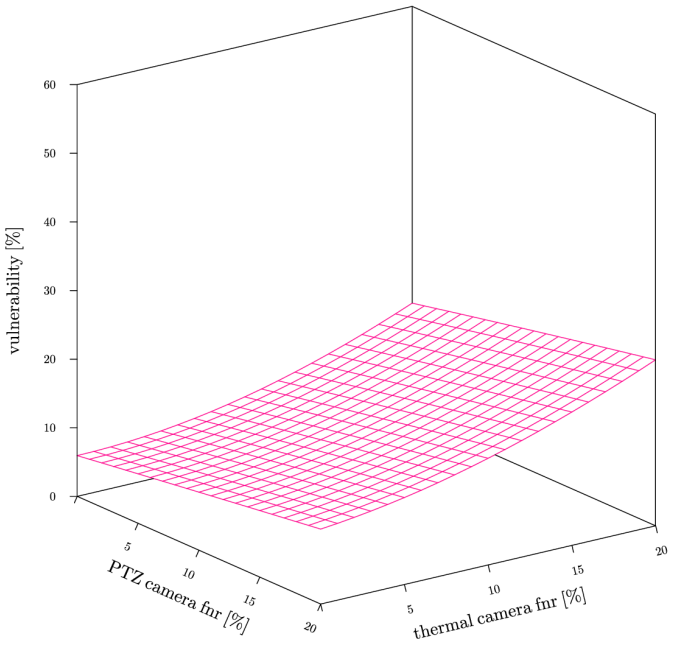


FIGURE 4.11: Study 1: thermal fnr VS PTZ fnr

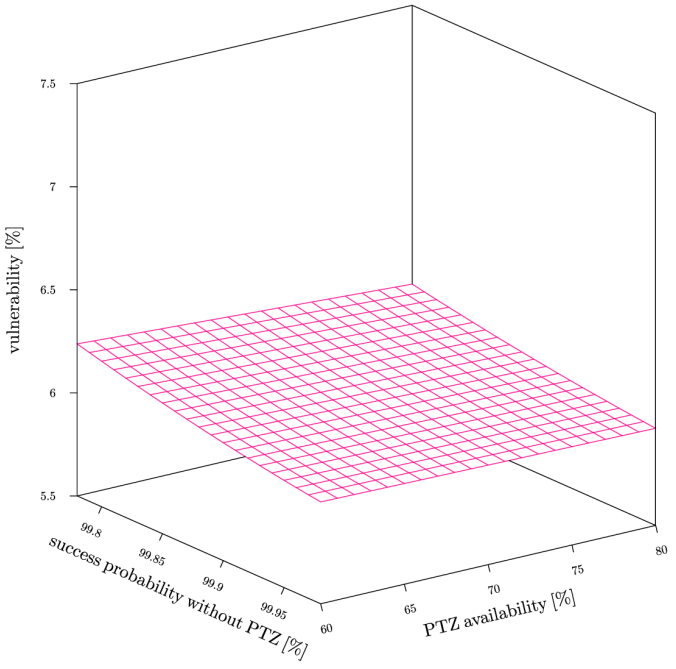


FIGURE 4.12: Study 2: PTZ availability VS catching success probability

Study 3. Fig. 4.13 reports the trend of vulnerability with respect to SO's and SG's availability. These availability varies from 80% to 100% for both operators:as expected, the maximum vulnerability (around 37%) corresponds to the minimum value for availability, while maximum availability leads to the minimum vulnerability of about 1%.

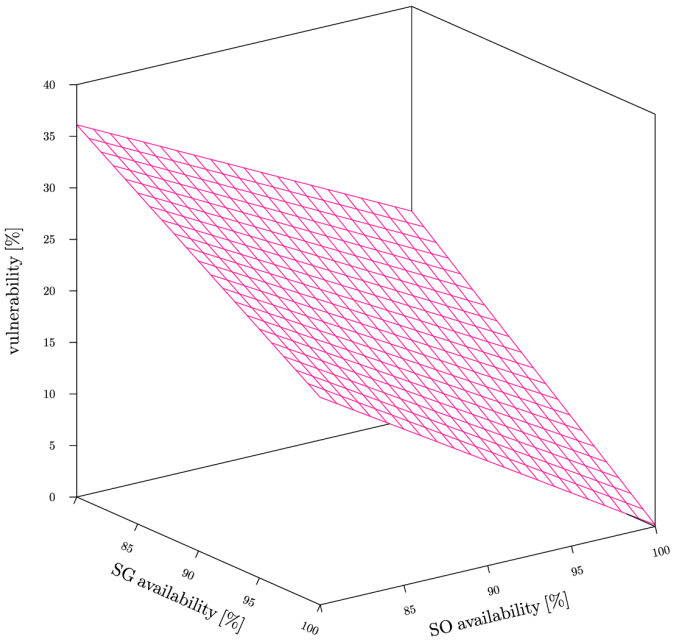


FIGURE 4.13: Study 3: SO availability VS SG availability

4.3.4.2 Scenario 2

This Section describes the results obtained by analyzing the Bayesian Network resulting from the second attack scenario (radiological attack in train and in depot). Bayesian model is depicted in Fig. 4.14.

Two different analyses have been performed:

- *depot vulnerability* with respect to the radiological attack;
- *train vulnerability* with respect to the radiological attack.

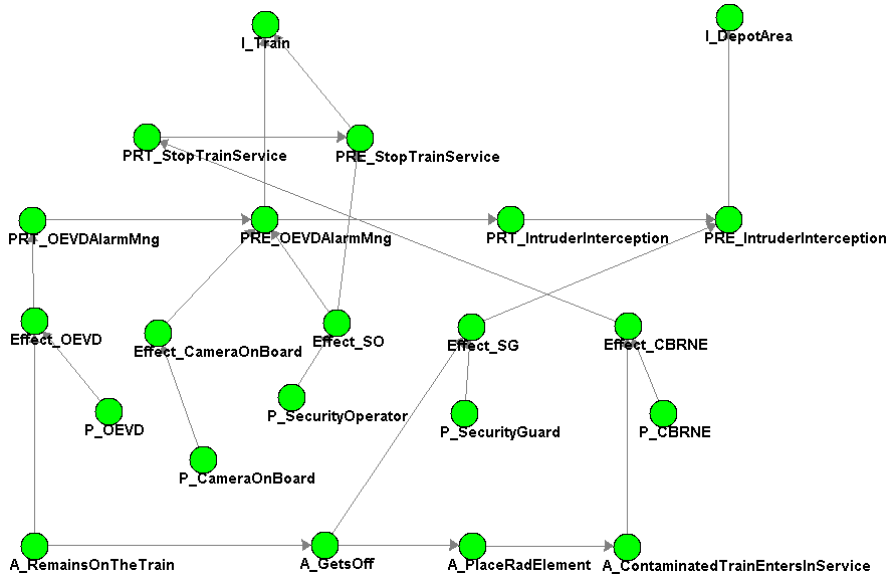


FIGURE 4.14: BN Attack Scenario 2

The depot vulnerability, evaluated using the parameters given in Table 4.1, is 17.20%, while the train vulnerability, using the same parameters, is 7.17%. These values are justifiable since the train, with respect to the considered radiological attack, is protected also by the CBRNe system while the depot is protected only by the OEVD system. Also on this network, a sensitivity analysis has been conducted. Specifically, two different studies have been performed, and they are described in the following:

1. *OEVD fnr VS CBRNe fnr*: vulnerability is evaluated by varying the fnr of the eOEVD system and the fnr of the CBRNe system;

2. *SO availability VS SG availability*: vulnerability is evaluated with respect to the availability of both SO and SG.

The results of the analyzes are plotted in the figures 4.15 and 4.16, respectively, where the green color is used for drawing the surface related to vulnerability of the depot, while the pink color is used for drawing the surface related to the vulnerability of the train. For each study, 882 evaluations (441 points for each surface, 21 values for each axis) have been conducted on the bayesian model. The computational complexity is comparable to that of the previous studies.

Study 1. Fig. 4.15 reports the values obtained for vulnerability calculated by varying the fnr of the OEVD and CBRNe systems. The range of variation in this study is 0%-20%, in order to assess the vulnerability in a very large set of possibilities. As shown by the graph the vulnerability of the depot does not depend from the CBRNe system, in fact the CBRNe protects just the train, while both depot and train depends on the fnr of OEVD. Let us note that the train vulnerability is obviously minor than the depot one. Specifically, the train vulnerability varies from a minimum of 4.32% to a maximum of 9.98%, while the depot vulnerability varies from 16.37% to 18.04% (remaining constant with respect to CBRNe fnr variation).

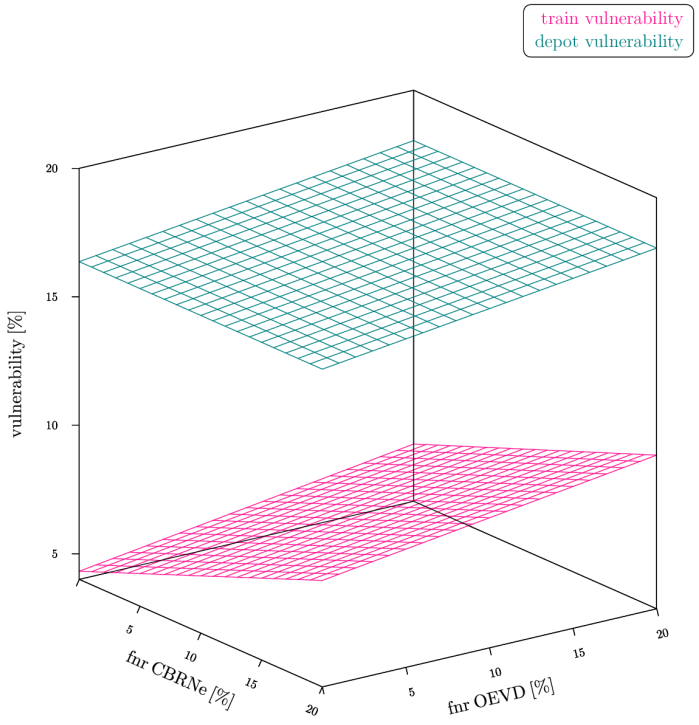


FIGURE 4.15: Study 1: OEVD fnr VS CBRNe fnr

Study 2. Fig. 4.16 reports the vulnerability trends with respect to SO's and SG's availability. These availability varies from 80% to 100% for both operators. The maximum value of depot vulnerability is 43.68% while the minimum is 12%; the train vulnerability varies from a maximum of 23.44% to a minimum of 4.3%.

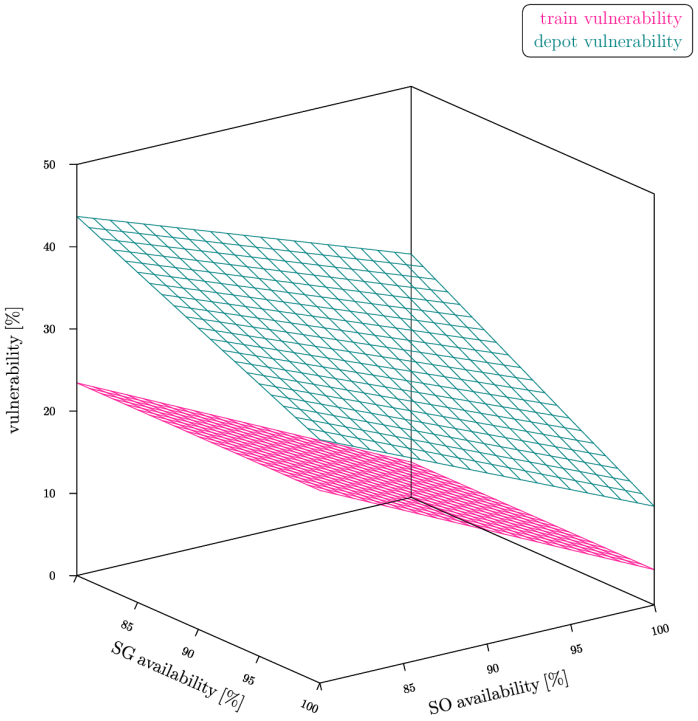


FIGURE 4.16: Study 2: SO availability VS SG availability

Conclusions

The research described in the previous chapters has addressed the issue of the physical protection of critical infrastructures, considering two different frames of reference to enhance it. The first operates at an analysis level (related to the physical infrastructure), while the second at an architectural level (related to the technological infrastructure).

At an analysis level, this thesis dealt with a model-driven process supporting the effective evaluation of a PPS. This is a basic activity for having a cost-effective physical protection, because it allows to find the weak points which are to be strengthened and also the points where the system is designed inadequately. The definition of the process is driven by the objective to generate automatically quantitative vulnerability models for CIs. The proposed process was developed within the METRIP project and it is based on a modeling approach which describes and combines three main aspects involved in the effective design of a physical protection system: *attacks*, *assets* and *protection measures*. Hence, the vulnerability evaluation can be performed taking into account the characteristics of the assets, the attack scenarios on these assets, the type and distribution of the protection devices as well as the countermeasures undertaken to block an ongoing attack. To this aim, the approach extends the Unified Modeling Language (UML) by applying profiling techniques in order to capture vulnerability and protection modeling issues, and uses proper Model-to-Model transformations to generate a bayesian model starting from UML artifacts. In the chapter 2 the CIP_VAM profile is described, as well as the transformational approach.

At an architectural level, this thesis describes an approach aimed at SoS realization, where the added value is represented by the real application scenarios and

related practical issues, addressed in the context of Secur-ED European research project. The approach described in chapter /Chapter3 enables a highly collaborative environment (in terms of technologies, suppliers, and end-users), which represents an innovative result for an open issue in the security of mass-transit domain. Thanks to adoption of a SOA-based integration framework, many advantages as well as a clear impact on the investment and operational life-cycle costs have been experimented. Specifically, it allows to [43]:

- mitigate the propagation of damages, minimizing the disaster recovery in time and space, in terms of resilience of transport systems;
- extend the life-cycle of the installed solutions by slowing down the need for the replacement and the update of technologies, since the modularity allows gradual adjustments whilst guaranteeing the service continuity;
- simplify and streamline the partners interactions despite a wide variety of technologies;
- have the seamless integration of new technologies with the existing ones, maximizing the return on investment by reducing the non-recurrent engineering costs;
- adopt standards and open tools for testing procedures without dictating any constraint about the implementation of applications, thus reducing the cost of training;
- have a flexible architecture not specific to operator, or city, or country, but applicable at any critical context after some usual setup.

In conclusion, the architectural approach has highlighted how a viable interoperability solution can contribute to enhance the security of mass transportation systems. In fact, the obtained results encourage the development of new solutions and the investment in security technologies and cooperation. This is just a preliminary SoS in this field, but the obtained results, in real world demonstration, encourages further investigation in the adoption of complex SoS architectures, which fulfill the requirements reported in this work.

At last, the case study in the chapter 4 has shown how two scenarios related to specific threats, with a selected set of protection measures, are addressed with both the approaches. The architectural one has highlighted the effectiveness of the solution in terms of reaction to the attacks, while the analytical one has allowed to assign a confidence level to the effectiveness of the proposed solution. As stated in the public summary of [103], in SECUR-ED the methodology used for performing risk assessment is purely qualitative and not quantitative. On the contrary, the analytical approach of this thesis provides probabilistic measures of the vulnerability, that can be used in risk assessment process.
Thanks to a sensitivity analysis it is possible to state what is the range of vulnerability of the solution on varying specific parameters of protection systems such as the availability and false negative rate. Furthermore, having a parameter for quantifying the vulnerability of a solution is very strategic, because it can be used for comparing multiple protection solutions. Although real tests are preferable, in the CIP field this is not always possible. For example in real metro systems, the experimentation could require the usage of specific assets (trains, stations, etc.) removing them from the operation and making them unavailable for the public service. This could be very expensive for a public operator, so the number of tests for evaluating more configurations of countermeasures could be very limited. For this reason, an ad-hoc and rigorous analysis aimed at studying the whole system under different conditions, before the tests on field, is a must. In addition, the most suitable selection of the protection systems is further encouraged if exists an open platform which allows an easy integration from a technological viewpoint. Then, combining the approaches is possible to obtain an effective enhancement of the physical protection, not only at a certain time, but during the whole life cycle of CI without constraints due to the obsolescence of the deployed technologies. The latter is one of the major feature to meet requirements in continuous evolution and in a long-term scale.

Appendix A

CIP_VAM Library

The CIP_VAM library is composed by the following three packages.

BasicDT defines the following enumerations:

- *RiskLevel* represents a qualitative classification of the risk level associated with an Asset. Possible values are negligible, acceptable, tolerable and unacceptable.
- *WeaponNature* represents the nature of a weapon. Possible values are aerosol, chemical agent, explosives, firebomb, firearms, radiological agent.
- *Tactic* is the physical nature of the weapon used to bring on the attack (or a single action inside a complex attack). Possible values are armed attack, arson, barricade, bombing, hijacking, hostage, intrusion, kidnapping, sabotage, suicide, dispersion.
- *ProtectionNature* represents the nature of the possible used protection. Possible values are: block, thermal, electrical, chemical and acoustical.
- *ActionKind* allows to discriminate between simple actions and triggers; in fact, the possible values are action and trigger.
- *Level* represents a generic qualitative level and is used in different parts of the profile such as motivation and skill levels of both attackers and human defenders. Possible values are very low, low, medium, high and very high.

- *OperatorType* allows to set the type of an operator. Possible values are: human and drone.
- *AngularUnitKind* is the measurement unit of the angle and allows to discriminate between degree and radian. In fact, possible value are deg and rad.
- *AngularSpeedUnit* represents the measurement unit of angular speed. Possible values are rad_per_sec (radian per second) and deg_per_sec (degree per second).
- *TransmissionTech* is the transmission technology of data used by a sensor. Possible values are wired, wireless and none.
- *ProcessingType* represents the kind of processing data. Possible values are digital or analog.
- *ZoomType* allows to specify the zoom type of a camera. Possible value are optical, digital and total.

GeometricDT contains both enumeration and structured data types. It defines:

- *PolygonType* is an enumeration of simple geometrical 2D shapes. Possible values are: polygon, circle, rectangle and square.
- *Point* represents a point in a 3D space. It is a dataType (a tuple) having three different fields:
  - X: x-axis coordinate of the point. It is a real value and it is optional since the point can only have y and z coordinates;
  - Y: y-axis coordinate of the point. It is a real value and it is optional since the point can only have x and z coordinates;
  - Z: z-axis coordinate of the point. It is a real value and it is optional since the point can only have x and y coordinates.
- *Shape* represents a 2D shape. It is a dataType (a tuple) having several fields:

  - type: it is a PoligonType variable and assigns the type to the shape. It is optional since the shape can be of a type not in the PolygonType set of values;
  - vertices: list of Points that constitute the border of the shape; vertices have an undefined number of Points;
  - area: value that represents the numerical value of the area of the shape;
  - perimeter: value that represents the length of the border of the shape;
  - centre: it is a Point that represents the barycentre of the shape;
  - length: length of the shape;
  - width: width of the shape;
  - radius: for circular shape, it indicates the radius of the shape.

- *Solid* represents a 3D geometrical volume. It is a dataType (a tuple) having three different fields:
  - base: shape describing the base of the solid;
  - height: value that represents the measure of the vertical dimension of the solid;
  - volume: it represents the volume of the solid.

- *Angle* is used to designate the measure of an angle. It is a dataType (a tuple) having two fields:
  - value: the size of the angle;
  - unit: unit used to represent the angle.

StructuredDT contains the following types:

- *Asset* is the data type related to the economic values and risk of an asset:
  - value: economic value of the asset;
  - vulnerability: probability of being damaged given an attack;
  - AttackProb: quantification of the probability being attacked;

  - Risk: quantification of the risk associated with the asset (according to the well-assessed formula Risk = attackProb *Vulnerability*damage);
  - riskLevel: qualitative level of the risk.

- *Weapon* represents a weapon used as a tool in an attack phase (an action). It is a dataType having two different fields:
  - failureRate: rate of failure of the weapon;
  - nature: physical nature of the weapon (kidnap, firearm, etc...) determined according to the AttackNature type previously expressed.

- *Application* represents the localization of the installation of a protection onto an item (site or object):
  - position: physical location of the application;
  - direction: orientation of the protection (let us consider as an example a camera that wants not only the point on which it has been fixed but also the one where the camera looks to);
  - installation: Item on which the protection is installed.

- *Threat* represents a threat brought by an attack to an asset:
  - name: name of the threats;
  - target: item that is the asset toward which the attack is brought;
  - effect: percentage of the value of the asset damaged by a successful threat.

- *Impairment* specializes Threats by adding some properties:
  - latency: that is the latency of the propagation of the Impairment to other affected Impairements;
  - for each propagation we have (as three arrays):
    * propEffect: affected Impairement;
    * propProb: probability of having a propagation on the affected Impairement;

    * propCond: condition under which we have the propagation of the Impairement.

- *SpeedAngular* serves to point out the speed angular of a PTZ camera. It is characterized by:
  - value: value of the angular speed;
  - speedUnit: measurement unit determined according to the AngularSpeedUnit type expressed in the BasicDT package.
- *Zoom* is a structured element for specifying the data related to the zoom of a camera:
  - value: string representing the value of the zoom (i.e 12x);
  - type: the type of zoom defined in the ZoomType type previously expressed.

Bibliography

[1] Pappalardo A. *A Framework for Threat Recognition in Physical Security Information Management*. PhD thesis, Department of Electrical Engineering and Information Technologies, University of Naples "Federico II", Italy, 2013.

[2] ISTAT. Noi italia, 2014. URL `http://noi-italia2014.istat.it/index.php?id=7&L=1&user_100ind_pi1[id_pagina]=239&cHash=ba3d0569fe90b009cc7db036abebb7ec`.

[3] Council of the European Union. Council directive 2008/114/ec on the identification and designation of european critical infrastructure (eci) and the assessment of the need to improve their protection. *Official Journal of the European Union*, Dec 2008.

[4] Urlainis A., Shohet I.M., Levy R., Ornai D., and Vilnay O. Damage in critical infrastructures due to natural and man-made extreme events - a critical review. *Procedia Engineering*, 85(0):529 – 535, 2014. ISSN 1877-7058. doi: http://dx.doi.org/10.1016/j.proeng.2014.10.580. URL `http://www.sciencedirect.com/science/article/pii/S1877705814019468`. Selected papers from Creative Construction Conference 2014.

[5] Piètre-Cambacédès L. and Chaudet C. The {SEMA} referential framework: Avoiding ambiguities in the terms security and safety. *International Journal of Critical Infrastructure Protection*, 3(2):55 – 66, 2010. ISSN 1874-5482. doi: http://dx.doi.org/10.1016/j.ijcip.2010.06.003. URL `http://www.sciencedirect.com/science/article/pii/S1874548210000247`.

[6] Gerald L Kovacich and Edward P Halibozek. *The manager's handbook for corporate security: establishing and managing a successful assets protection program*. Butterworth-Heinemann, 2003.

[7] Michael Vierhauser, Rick Rabiser, Paul Grünbacher, Christian Danner, and Stefan Wallner. Evolving systems of systems: Industrial challenges and research perspectives. In *Proceedings of the First International Workshop on Software Engineering for Systems-of-Systems*, SESoS '13, pages 1–4, New York, NY, USA, 2013. ACM. ISBN 978-1-4503-2048-1. doi: 10.1145/2489850.2489851. URL `http://doi.acm.org/10.1145/2489850.2489851`.

[8] Mary Linn Garcia. *Vulnerability Assessment of Physical Protection Systems*. Butterworth-Heinemann, Dec. 2005.

[9] Hans Günter Brauch. Concepts of security threats, challenges, vulnerabilities and risks. In Hans Günter Brauch, Ùrsula Oswald Spring, Czeslaw Mesjasz, John Grin, Patricia Kameri-Mbote, Bèchir Chourou, Pàl Dunay, and Jörn Birkmann, editors, *Coping with Global Environmental Change, Disasters and Security*, volume 5 of *Hexagon Series on Human and Environmental Security and Peace*, pages 61–106. Springer Berlin Heidelberg, 2011. ISBN 978-3-642-17775-0. doi: 10.1007/978-3-642-17776-7_2. URL `http://dx.doi.org/10.1007/978-3-642-17776-7_2`.

[10] A.A.V.V. Physical security design manual for va facilities. Technical report, Department of Veterans Affairs Washington, DC 20420, 2007.

[11] Yacov Y. Haimes. *Risk modeling, assessment, and management*. Wiley series in system engineering and management. Hoboken, N.J. Wiley-Interscience, 2004. ISBN 0-471-48048-7. URL `http://opac.inria.fr/record=b1120048`.

[12] Cardona Omar D. chapter The Need for Rethinking the Concepts of Vulnerability and Risk from a Holistic Perspective: A necessary review and Criticism for Effective Risk Management. Earthscan Publishers, London, 2003.

[13] Giannopoulos G., Filippini R., and Schimmer M. Risk assessment methodologies for critical infrastructure protection. part i: A state of the art. Publications Office of the European Union, 2012. ISBN 978-92-79-23839-0. EUR - Scientific and Technical Research Reports.

[14] Alan T. Murray. An overview of network vulnerability modeling approaches. *GeoJournal*, 78(2):209–221, 2013. ISSN 0343-2521. doi: 10.1007/s10708-011-9412-z. URL `http://dx.doi.org/10.1007/s10708-011-9412-z`.

[15] Sandip C. Patel, James H. Graham, and Patricia A.S. Ralston. Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. *International Journal of Information Management*, 28(6):483 – 491, 2008. ISSN 0268-4012. doi: http://dx.doi.org/10.1016/j.ijinfomgt.2008.01.009. URL `http://www.sciencedirect.com/science/article/pii/S0268401208000054`.

[16] X. Wang, F.B. Ma, and J.Y. Li. Water resources vulnerability assessment based on the parametric-system method: a case study of the zhangjiakou region of guanting reservoir basin, north china. *Procedia Environmental Sciences*, 13(0):1204 – 1212, 2012. ISSN 1878-0296. doi: http://dx.doi.org/10.1016/j.proenv.2012.01.114. URL `http://www.sciencedirect.com/science/article/pii/S1878029612001156`. 18th Biennial {ISEM} Conference on Ecological Modelling for Global Change and Coupled Human and Natural System.

[17] Barry Charles Ezell, Steven P Bennett, Detlof Von Winterfeldt, John Sokolowski, and Andrew J Collins. Probabilistic risk analysis and terrorism risk. *Risk Analysis*, 30(4):575–589, 2010.

[18] Willis H. et al. *Estimating terrorism risk*. RAND Corporation, 2005. ISBN 0-8330-3834-6. URL `http://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG388.pdf`.

[19] T.G Lewis, R.P. Darken, T. Mackin, and D. Dudenhoeffer. *Model-Based Risk Analysis for Critical Infrastructures*, pages 3–19. Critical Infrastructure Security - WIT Press, 2011.

[20] McGill W. *Critical Asset and Portfolio Risk Analysis for Homeland Security.* PhD thesis, Department of Civil and Environmental Engineering, University of Maryland, College Park, Maryland, 2008.

[21] White R., Boult T., and Chow E. A computational asset vulnerability model for the strategic protection of the critical infrastructure. *International Journal of Critical Infrastructure Protection*, 7(3):167 – 177, 2014. ISSN 1874-5482. doi: http://dx.doi.org/10.1016/j.ijcip.2014.06.002. URL `http://www.sciencedirect.com/science/article/pii/S1874548214000419`.

[22] K. Vellani. *Strategic Security Management: A Risk Assessment Guide for Decision Makers.* Elsevier Science, 2006. ISBN 9780080465968. URL `https://books.google.it/books?id=qkkHX9KHpysC`.

[23] Arpan Roy, Dong Seong Kim, and Kishor S. Trivedi. Attack countermeasure trees (act): Towards unifying the constructs of attack and defense trees. *Sec. and Commun. Netw.*, 5(8):929–943, August 2012. ISSN 1939-0114. doi: 10.1002/sec.299. URL `http://dx.doi.org/10.1002/sec.299`.

[24] Barbara Kordy, Sjouke Mauw, Saša Radomirović, and Patrick Schweitzer. Foundations of attack-defense trees. In *Proceedings of the 7th International Conference on Formal Aspects of Security and Trust*, FAST'10, pages 80–95, Berlin, Heidelberg, 2011. Springer-Verlag. ISBN 978-3-642-19750-5. URL `http://dl.acm.org/citation.cfm?id=1964555.1964561`.

[25] S.M. Rinaldi, J.P. Peerenboom, and T.K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE*, 21(6):11–25, Dec 2001. ISSN 1066-033X. doi: 10.1109/37.969131.

[26] Mary Linn Garcia. *Design and Evaluation of Physical Protection Systems.* Butterworth-Heinemann, Oct. 2007.

[27] B. Hennessey, R.B. Wesson, and B. Norman. Security simulation for vulnerability assessment. *Aerospace and Electronic Systems Magazine, IEEE*, 22 (9):11–16, Sept 2007. ISSN 0885-8985. doi: 10.1109/MAES.2007.4350253.

[28] Z. Vintr, M. Vintr, and J. Malach. Evaluation of physical protection system effectiveness. In *Security Technology (ICCST), 2012 IEEE International*

Carnahan Conference on, pages 15–21, Oct 2012. doi: 10.1109/CCST.2012.6393532.

[29] Valeria Vittorini, Stefano Marrone, Nicola Mazzocca, Roberto Nardone, and Annarita Drago. *Railway Infrastructure Security*, volume 1018, chapter A Model-Driven Process for Physical Protection System Design and Vulnerability Evaluation. Springer, 2015 (to appear). ISBN 978-3-319-04425-5.

[30] Peida Xu, Yong Deng, Xiaoyan Su, Xin Chen, and Sankaran Mahadevan. An evidential approach to physical protection system design. *Safety Science*, 65(0):125 – 137, 2014. ISSN 0925-7535. doi: http://dx.doi.org/10.1016/j.ssci.2014.01.003. URL `http://www.sciencedirect.com/science/article/pii/S0925753514000058`.

[31] H. A. Bennett. Easi (estimate of adversary sequence interruption) - an evaluation method for physical security systems. *Nuclear Materials Management*, 6(3):371–379, 1977.

[32] J.C. Matter. *SAVI: a pc-based vulnerability assessment program.* Jan 1988.

[33] D. Engi and D. D. Boozer. Use of isem (insider safeguards effectiveness model) in studying the impacts of guards tactics on facility safeguards system effectiveness. *Nuclear Materials Management*, 6(3):592–600, 1977.

[34] Sung-Soon Jang, Sung-Woo Kwan, Ho-Sik Yoo, Jung-Soo Kim, and Wan-Ki Yoon. Development of a vulnerability assessment code for a physical protection system: Systematic analysis of physical protection effectiveness (sape). *Nuclear Engineering and Technology*, 41(5):747–752, 2009. doi: 10.5516/NET.2009.41.5.747.

[35] Vittorini V. Flammini F., Pappalardo A. *Effective Surveillance for Homeland Security: Balancing Technology and Social Issues*, chapter Challenges and Emerging Paradigms for Augmented Surveillance. Chapman and Hall/CRC, 2013. ISBN 9781439883242.

[36] Garzia F. chapter Security System design and integration. WitPress, 2012. ISBN 978-1-84564-562-5.

[37] James I. Chong. Next generation multiâĂŘagency fusion centers -people, process & technologies. White paper, VidSys, 2012.

[38] B. F. Spencer, Manuel E. Ruiz-s, and Narito Kurata. Smart sensing technology: Opportunities and challenges. In *Journal of Structural Control and Health Monitoring, in press*, pages 349–368, 2004.

[39] Yurish S. Y. Sensors: Smart vs intelligent. *Sensors and Transducers Journal*, 114:1–6, 2010.

[40] M. Rodriguez, J. Sivic, I. Laptev, and J.-Y. Audibert. Density-aware person detection and tracking in crowds. In *Proceedings of the International Conference on Computer Vision (ICCV)*, 2011.

[41] Stavros Ntalampiras, Ilyas Potamitis, and Nikos Fakotakis. An adaptive framework for acoustic monitoring of potential hazards. *EURASIP J. Audio Speech Music Process.*, 2009:13:1–13:15, January 2009. ISSN 1687-4714. doi: 10.1155/2009/594103. URL `http://dx.doi.org/10.1155/2009/594103`.

[42] Report on consolidation of functional results. Deliverable 46.2, 2014. URL `http://www.secur-ed.eu/wp-content/uploads/2014/10/D46.2_Report_on_consolidation_of_Functional_Results.pdf`.

[43] Report on consolidation of industrial results. Deliverable 46.5, 2014. URL `http://www.secur-ed.eu/wp-content/uploads/2014/10/D46.5_Report_on_consolidation_Industrial.pdf`.

[44] Ellen Howe. Psim: An effective risk management tool. White paper, VidSys, 2014.

[45] J Roadnight. Will physical security information management (psim) systems change the global security world? Technical report, CornerStone, 2011.

[46] Physical security information management (psim)-the parallels between psim for physical security, siem for cyber security. White paper, VidSys, 2011.

[47] Counteract project. URL `http://www.transport-research.info/web/projects/project_details.cfm?id=36152`.

[48] Modsafe project. URL `http://www.modsafe.eu/`.

[49] Demasst project. URL `http://cordis.europa.eu/project/rcn/91165_en.html`.

[50] Protectrail project. URL `http://www.protectrail.eu/`.

[51] Securestation project. URL `http://www.securestation.eu/`.

[52] Valentina Casola, Alessandra De Benedictis, Annarita Drago, and Nicola Mazzocca. Sensim-sec: secure sensor networks integration to monitor rail freight transport. *International Journal of System of Systems Engineering*, 4(3):291–316, 2013.

[53] Giovanni Bocchetti, Francesco Flammini, Concetta Pragliola, and Alfio Pappalardo. Dependable integrated surveillance systems for the physical security of metro railways. In *Distributed Smart Cameras, 2009. ICDSC 2009. Third ACM/IEEE International Conference on*, pages 1–7. IEEE, 2009.

[54] Francesco Flammini, Nicola Mazzocca, Alfio Pappalardo, Concetta Pragliola, and Valeria Vittorini. *Augmenting surveillance system capabilities by exploiting event correlation and distributed attack detection.* Springer, 2011.

[55] Zhigang Zhu and Thomas S Huang. *Multimodal surveillance: sensors, algorithms, and systems.* Artech House, 2007.

[56] J.M. Wilson, B.A. Jackson, M. Eisman, P. Steinberg, and K.J. Riley. *Securing America's Passenger-Rail Systems.* RAND Corporation, 2007. ISBN 9780833044372. URL `http://books.google.it/books?id=6hf6bNizUDsC`.

[57] E. Sapori, M. Sciutto, and G. Sciutto. A quantitative approach to risk management in critical infrastructures. *Transportation Research Procedia*, 3(0):740 – 749, 2014. ISSN 2352-1465. doi: http://dx.doi.org/10.1016/j.trpro.2014.10.053. URL `http://www.sciencedirect.com/science/article/pii/S2352146514002166`. 17th Meeting of the {EURO} Working Group on Transportation, EWGT2014, 2-4 July 2014, Sevilla, Spain.

[58] Department of Homeland Security. Nipp 2013-partnering for critical infrastructure security and resilience. Technical report, U.S. Department of Homeland Security, 2013.

[59] F. Flammini. *Critical Infrastructure Security: Assessment, Prevention, Detection, Response*. Information & communication technologies. WIT Press, 2012. ISBN 9781845645625. URL `http://books.google.it/books?id=R_m8tkH338YC`.

[60] D. Macdonald, S.L. Clements, S.W. Patrick, C. Perkins, G. Muller, M.J. Lancaster, and W. Hutton. Cyber/physical security vulnerability assessment integration. In *Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES*, pages 1–6, Feb 2013. doi: 10.1109/ISGT.2013.6497883.

[61] D.C. Schmidt. Model-driven engineering. In *IEEE Computer 39 (2), pages 25–31*, February 2006.

[62] B. Selic. The less well known uml: a short user guide. In *Proceedings of the 12th international conference on Formal Methods for the Design of Computer, Communication, and Software Systems: formal methods for model-driven engineering*, SFM'12, pages 1–20, Berlin, Heidelberg, 2012. Springer-Verlag. ISBN 978-3-642-30981-6. doi: 10.1007/978-3-642-30982-3_1. URL `http://dx.doi.org/10.1007/978-3-642-30982-3_1`.

[63] M. Volter. From programming to modeling - and back again. *IEEE Softw.*, 28(6):20–25, November 2011. ISSN 0740-7459. doi: 10.1109/MS.2011.139. URL `http://dx.doi.org/10.1109/MS.2011.139`.

[64] Judea Pearl. *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1988. ISBN 0-934613-73-7.

[65] David Heckerman. A Tutorial on Learning with Bayesian Networks. In Michael I. Jordan, editor, *Learning in Graphical Models*, pages 301–354. MIT Press, Cambridge, MA, USA, 1999. ISBN 0-262-60032-3.

[66] Ben-Gal I. *Bayesian Networks*. Encyclopedia of Statistics in Quality and Reliability - John Wiley & Sons, 2007.

[67] Tom Mens and Pieter Van Gorp. A taxonomy of model transformation. *Electronic Notes in Theoretical Computer Science*, 152:125–142, 2006.

[68] K. Czarnecki and S. Helsen. Feature-based survey of model transformation approaches. *IBM Syst. J.*, 45(3):621–645, July 2006. ISSN 0018-8670. doi: 10.1147/sj.453.0621. URL `http://dx.doi.org/10.1147/sj.453.0621`.

[69] Gerti Kappel, Philip Langer, Werner Retschitzegger, Wieland Schwinger, and Manuel Wimmer. Model transformation by-example: A survey of the first wave. In Antje DÃijsterhÃűft, Meike Klettke, and Klaus-Dieter Schewe, editors, *Conceptual Modelling and Its Theoretical Foundations*, volume 7260 of *Lecture Notes in Computer Science*, pages 197–215. Springer Berlin Heidelberg, 2012. ISBN 978-3-642-28278-2.

[70] Xinhong Hei, Lining Chang, Weigang Ma, Jinli Gao, and Guo Xie. Automatic transformation from uml statechart to petri nets for safety analysis and verification. In *Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 2011 International Conference on*, pages 948–951, June 2011. doi: 10.1109/ICQR2MSE.2011.5976760.

[71] Liu Chao and Tang Tao. Epsilon-based model transformation and verification of train control system specification. In *Control Conference (CCC), 2011 30th Chinese*, pages 5562–5567, July 2011.

[72] Barry Charles Ezell. Infrastructure Vulnerability Assessment Model (I-VAM). *Risk Analysis*, 27(3):571–583, 2007. ISSN 1539-6924. doi: 10.1111/j.1539-6924.2007.00907.x.

[73] Gerald G. Brown, W. Matthew Carlyle, Javier Salmerï£¡n, and Kevin Wood. Analyzing the vulnerability of critical infrastructure to attack and planning defenses. In *Tutorials in Operations Research. INFORMS*, pages 102–123. INFORMS, 2005.

[74] Francesco Flammini, Stefano Marrone, Nicola Mazzocca, and Valeria Vittorini. Petri Net Modelling of Physical Vulnerability. In Sandro Bologna, Bernhard HŠmmerli, Dimitris Gritzalis, and Stephen Wolthusen, editors, *Critical Information Infrastructure Security*, volume 6983 of *Lecture Notes in Computer Science*, pages 128–139. Springer Berlin Heidelberg, 2013. ISBN 978-3-642-41475-6. doi: 10.1007/978-3-642-41476-3_11.

[75] P. Xie, J.H. Li, X. Ou, P. Liu, and R. Levy. Using Bayesian Networks for Cyber Security Analysis. In Roberto Setola and Stefan Geretshuber, editors, *Proceedings of the 40th IEEE/IFIP Int. Conf. Dependable Systems and Networks*, pages 211–220, 2010.

[76] Antonio Sforza, Stefano Starita, and Claudio Sterle. *Railway Infrastructure Security*, volume 1018, chapter Optimal location of security devices. Springer, 2015. ISBN 978-3-319-04425-5.

[77] A. Sforza, C. Sterle, P. D'Amore, R. Tedesco, F. De Cillis, and R. Setola. Optimization Models in a Smart Tool for the Railway Infrastructure Protection. In Eric Luiijf and Pieter Hartel, editors, *Critical Information Infrastructure Security*, volume 8328 of *Lecture Notes in Computer Science*, pages 191–196. Springer Berlin Heidelberg, 2013. ISBN 978-3-319-03964-0.

[78] OMG-MARTE. *UML Profile for MARTE: Modeling and Analysis of Real-time Embedded Systems*. OMG, June 2011. Version 1.1, formal/11-06-02.

[79] Jan Jürjens. Umlsec: Extending uml for secure systems development. In *Proceedings of the 5th International Conference on The Unified Modeling Language*, UML '02, pages 412–425, London, UK, UK, 2002. Springer-Verlag. ISBN 3-540-44254-5. URL `http://dl.acm.org/citation.cfm?id=647246.719625`.

[80] Kirsten Berkenkötter and Ulrich Hannemann. Modeling the railway control domain rigorously with a uml 2.0 profile. In *Computer Safety, Reliability, and Security*, pages 398–411. Springer, 2006.

[81] E. Bagheri and A. A. Ghorbani. UML-CI: A reference model for profiling critical infrastructure systems. *Information Systems Frontiers*, 12(2):115–139, 2010.

[82] Ricardo J. Rodríguez, José Merseguer, and Simona Bernardi. Modelling security of critical infrastructures: A survivability assessment. *The Computer Journal*, 2014. doi: 10.1093/comjnl/bxu096. URL `http://comjnl.oxfordjournals.org/content/early/2014/10/04/comjnl.bxu096.abstract`.

[83] Stefano Marrone, Roberto Nardone, Annarita Tedesco, Pasquale D'Amore, Valeria Vittorini, Roberto Setola, Francesca De Cillis, and Nicola Mazzocca. Vulnerability modeling and analysis for critical infrastructure protection applications. *International Journal of Critical Infrastructure Protection*, 6(34): 217 – 227, 2013. ISSN 1874-5482. doi: http://dx.doi.org/10.1016/j.ijcip.2013.10.001.

[84] B. Selic. A Systematic Approach to Domain-Specific Language Design Using UML. In *10th IEEE Int. Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, pages 2–9, Santorini Island, Greece, May 2007. IEEE Computer Society.

[85] Systems engineering guide for systems of systems. Technical report, Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering, Washington, DC: ODUSD(A&T)SSE, 2008. Version 1.0.

[86] Mark W. Maier. Architecting principles for systems-of-systems. *Systems Engineering*, 1(4):267–284, 1998. ISSN 1520-6858. doi: 10.1002/(SICI)1520-6858(1998)1:4<267::AID-SYS3>3.0.CO;2-D. URL `http://dx.doi.org/10.1002/(SICI)1520-6858(1998)1:4<267::AID-SYS3>3.0.CO;2-D`.

[87] White paper for public transport stakeholders, 2014. URL `http://www.secur-ed.eu/wp-content/uploads/2014/12/SECUR-ED_White_Paper_Final.pdf`.

[88] Report on consolidation of operational results. Deliverable 46.3, 2014. URL `http://www.secur-ed.eu/wp-content/uploads/2014/10/D46.3_Report_on_consolidation_of_operational_results.pdf`.

[89] Report on consolidation of the interoperability level achieved. Deliverable 46.4, 2014. URL `http://www.secur-ed.eu/wp-content/uploads/2014/10/D46.4_Report_on_consolidation_of_Interoperability.pdf`.

[90] Report on consolidation of social and ethical impact. Deliverable 46.6, 2014. URL `http://www.secur-ed.eu/wp-content/uploads/2014/07/D46.6_-_Report_consolidation_of_Societal_and_Ethical_Impact.pdf`.

[91] Kay-Uwe Schmidt, Darko Anicic, and Roland Stühmer. Event-driven reactivity: A survey and requirements analysis. In *SBPM2008: 3rd international Workshop on Semantic Business Process Management in conjunction with the 5th European Semantic Web Conference (ESWC'08)*. CEUR Workshop Proceedings (CEUR-WS.org, ISSN 1613-0073), June 2008. URL `http://sbpm2008.fzi.de/paper/paper7.pdf`.

[92] ISO. Information technology – vocabulary – part 1: Fundamental terms. ISO ISO/IEC 2382-1:1993, International Organization for Standardization, 1993. 3rd Edition.

[93] Wenguang Wang, Andreas Tolk, and Weiping Wang. The levels of conceptual interoperability model: Applying systems engineering principles to m&s. In *Proceedings of the 2009 Spring Simulation Multiconference*, SpringSim '09, pages 168:1–168:9, San Diego, CA, USA, 2009. Society for Computer Simulation International. URL `http://dl.acm.org/citation.cfm?id=1639809.1655398`.

[94] Francesco Flammini, Nicola Mazzocca, Alfio Pappalardo, Concetta Pragliola, and Valeria Vittorini. Augmenting surveillance system capabilities by exploiting event correlation and distributed attack detection. In AMin Tjoa, Gerald Quirchmayr, Ilsun You, and Lida Xu, editors, *Availability, Reliability and Security for Business, Enterprise and Health Information Systems*, volume 6908 of *Lecture Notes in Computer Science*, pages 191–204. Springer Berlin Heidelberg, 2011. ISBN 978-3-642-23299-2. doi: 10.1007/978-3-642-23300-5_15.

[95] Navjot Kaur, C Stuart McLeod, Atul Jain, Robert Harrison, Bilal Ahmad, Armando Walter Colombo, and Jerker Delsing. Design and simulation of a soa-based system of systems for automation in the residential sector. In *Industrial Technology (ICIT), 2013 IEEE International Conference on*, pages 1976–1981. IEEE, 2013.

[96] Olga Levina and Vladimir Stantchev. A model and an implementation approach for event-driven service orientation. *International Journal on Advances in Software*, 2(2 and 3):288–299, 2009.

[97] Jürgen Dunkel, Alberto Fernández, Rubén Ortiz, and Sascha Ossowski. Event-driven architecture for decision support in traffic management systems. *Expert Systems with Applications*, 38(6):6530–6539, 2011.

[98] Common alerting protocol, 2010. URL `http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html`.

[99] Jean-Louis Maréchaux. Combining service-oriented architecture and event-driven architecture using an enterprise service bus. *IBM Developer Works*, pages 1269–1275, 2006.

[100] Brahim Medjahed. Dissemination protocols for event-based service-oriented architectures. *IEEE T. Services Computing*, 1(3):155–168, 2008. URL `http://dblp.uni-trier.de/db/journals/tsc/tsc1.html#Medjahed08`.

[101] R. Moats. URN syntax. RFC 2141, 1997. URL `http://www.ietf.org/rfc/rfc2141.txt`.

[102] Web services base notification, 2006. URL `http://docs.oasis-open.org/wsn/wsn-ws_base_notification-1.3-spec-os.pdf`.

[103] Best practices for conducting risks assessments. Deliverable 31.2, 2014. URL `http://www.secur-ed.eu/wp-content/uploads/2013/04/D31.2_Best_practices_for_conducting_risks-assessments.pdf`.