AiMT Advances in Military Technology
Vol. 10, No. 1, June 2015

Vital Area Identification – State-of-the-Art

T. Malachová[1*] and Z. Vintr[2]

[1] *EBIS, spol. s r.o., Brno, Czech Republic*
[2] *Faculty of Military Technology, University of Defence, Brno, Czech Republic*

The manuscript was received on 1 April 2015 and was accepted after revision for publication on 1 June 2015.

Abstract:

When it comes to designing effective physical protection of a critical infrastructure against malicious attacks, the knowledge of potential targets of the attack or areas in which these targets are placed is the basic presumption. Without knowing the attack targets it is impossible to plan sensibly the physical protection system or evaluate its effectiveness. That is the reason why a great deal of attention is paid to the identification of targets or vital areas, and a number of methods and procedures which might be used for the targets identification have been developed. The article brings the results of the extensive analysis of the current state in this area. It includes a brief historical development of the processes of attack targets identification and introduces methods and approaches used within these procedures. Admittedly the attention is paid mainly to the identification of vital areas at nuclear facilities, but the performed analysis did not address only this area of highest attention, but also the systematically examined current state of a critical infrastructure in general.

Keywords:

Target identification, vital area identification, physical protection system, fault tree, event tree, attack tree, protection tree.

1. Introduction

The events of 9/11 and subsequent terrorist attacks on civil targets changed the world in many ways. The security of critical infrastructure has been one of the key areas that came to the fore. The physical protection of critical infrastructures has received increasing levels of attention throughout the world.

The general rise in terrorist attacks in recent years and the increasingly sophisticated threat forces us to improve current security approaches in order to keep up with new and unexpected ways of attacks. The identification of potential attacker's

[*] *Corresponding author: EBIS, spol. s r. o., Křižíkova 2962/70a, CZ-612 00 Brno, Czech Republic, phone: +420 549 439 242, fax: +420 549 439 241, E-mail: malachova@ebis.cz*

targets in technologically complex facilities plays a crucial role in the overall process of the physical protection design and evaluation [1].

The process of the identification of potential attack targets at a general level has not been standardized by any means yet and in single technological branches different methods and procedures are applied within this process. This issue has been developed very thoroughly for the area of nuclear industry where the security aspects are given special attention, because the consequences of a potential attack can be really serious.

An attack can be carried out to sabotage, or gain control of, targets that are represented by the equipment, systems, structures, components, devices, operator actions or their combination (hereinafter will be abbreviated as SSC). These potential targets in which there is a need to be protected are called vital and are located within vital areas (VA) [2]. Qualified vital areas identification (VAI) becomes then one of the basic points when it comes to planning the physical protection system (PPS) of nuclear facility and evaluating the system effectiveness.

The authors of this article took part in implementing two security research projects carried out in the Czech Republic, the essential part of which was also the research and development of VAI effective methods [3], [4]. During implementing these projects, a complex analysis of well-known VAI methods and procedures utilizable during the analysis was performed. The priority in this analysis was given to the VAI at nuclear facilities, but the information in the area of the physical protection of other types of critical infrastructure was also analysed. Therefore the results of the performed analysis are applicable not only in nuclear industry, but also when planning the physical protection systems of other complex facilities and evaluating their effectiveness.

The paper brings the outline of the most important results of the analysis performed and evaluates the current state in the area of methods and procedures used for VAI. The principles of a new approach to the VAI developed within the implemented projects of security research stated above are also briefly introduced in the paper.

2. Vital Area Identification

The main goal of the vital area identification process according to the International Atomic Energy Agency (IAEA) is to identify the areas in a facility around which protection shall be provided in order to prevent or reduce the likelihood of sabotage. The process identifies a minimum set of areas of equipment, systems, structures, components, devices or operator actions that should be protected to prevent radiological consequences of sabotage [5].

Sandia National Laboratories define vital areas for the United States Nuclear Regulatory Commission (U.S. NRC) in [6] as areas that should be identified so as to protect a minimum set of systems, personnel, and equipment needed to prevent significant core damage and spent fuel sabotage. Vital area identification is often based on a safety analysis and makes it feasible to develop sabotage logic models for sabotage scenarios that may cause unacceptable radiological consequences (URC) [2]. The identification of vital areas consists of a complex process requiring the cooperation of safety and security specialists [7].

Sabotage is defined in [5] as a deliberate act against a nuclear facility or nuclear material and other radioactive material in use, storage, or transport which could directly or indirectly endanger the health and safety of personnel, the public and the environment by exposure to radiation or the release of radioactive substances. An initiating event of a malevolent origin (IEMO) is a deliberate act caused by an adversary attempting to cause a radioactive release [6]. Sabotage initiating events (IE) can be of two different types:

- Direct sabotage on nuclear material with the goal to release or disperse material by applying energy from an external source e.g. nuclear explosive device. This requires an adversary to gain direct access to material.
- Indirect sabotage on nuclear material or other inventory with the aim of releasing or dispersing material using the material's potential energy for the dispersal. Indirect sabotage requires an initiating event with results that will exceed the mitigation capability of facility systems [2].

Sabotage models must represent the total set of candidate events that may lead to a selected top-level event, such as URC, and demonstrate a relationship between the top-level event and its causes represented by initiating events of malevolent origin on equipment, systems, structures, components, devices, operator actions (SSC) and nuclear material [2].

Sabotage logic models identify the events or combinations of events that could lead to a top-level event. A logic model can be a statement, an algebraic expression or most usually a graphical representation, such as a fault tree. Logic models are developed to the component level using a top-down approach. The logic models should be created in sufficient detail to allow events to be linked to facility locations [2]. Vital area identification is intended to be applied to technologically complex facilities, such as nuclear power plants that have multiple redundant or diverse safety systems to control or mitigate potential consequences. VAI may be employed in other complex facilities with high potential consequences, such as other critical infrastructure facilities [8].

3. Current Situation in Vital Area Identification

Since the 1970s, tree structures have been used to determine VA in the nuclear security field in the U.S. (the Los Alamos and Sandia laboratories). The approach based on fault trees was designed for and validated on nuclear facilities [9]. The U.S. NRC issued NUREG-1178 [12] where it was claimed that vital areas shall be protected against radiological sabotage based on VAI. Until then, areas comprising of all safety-related equipment were required to be considered as vital [6, 12]. The NRC Regulation 10 CFR 73.55 [13] includes requirements to conduct VAI. It sets minimum SSCs to be located within the vital areas.

The relevant documents dealing with VAI originate also in the IAEA. The Nuclear security recommendation on Physical protection of nuclear material and nuclear facility was issued in the 5th revision in 2011 [5] and the Comprehensive Technical Guide Identification of Vital Areas at Nuclear Facilities presenting a structured approach to identify the vital areas was issued in 2012 [2]. The comprehensive description of the overall process of the design and evaluation of a PPS including VAI is described by Garcia in [14] and [15] originating in Sandia. Sandia issued a comprehensive publication that describes a systematic method for the identification of vital areas at complex nuclear facilities in 2005. The document was made publically available in 2008 [8]. In the same year Sandia elaborated VAI requirements for the U.S. operators [6] describing a systematic process for the identification of the minimum set of areas that must be designated as vital. In 2000 the Korea Atomic Energy Institute started to develop a VAI methodology and the VAI Package Expert (VIPEX) to help identify vital areas using the

Probabilistic Safety Analysis (PSA) [16], [17]. This methodology and SW tool is not publicly available.

At present, there is no legislation in the Czech Republic that requires the identification of vital areas in nuclear facilities. Equipment, systems, structures, components and devices were categorized into 3 categories according to their importance. The categorization is conducted according to the Decree of the State Office for Nuclear Safety (SUJB) No. 144/1997 Coll.

There is a major difference in the categorization approach and VAI. The categorization approach determines a category for a specific SSC based on the partially prescriptive approach (as prescribed in the Decree) and partially on the logic tree analysis. The VAI approach involves a thorough analysis of all SSCs.

In 2015 the new Atomic Law and the corresponding decree is expected to come into force. One of the main reasons is to harmonize the Czech legislation with international recommendations, standards and good practises. VAI is currently one of the changes that are expected to be required by this legislation. VAI determines the vital areas much more precisely based on a detailed analysis and it is currently the most sophisticated and accepted approach world-wide.

Due to the expected legislation the TARGI (TARGet Identification) project [3] has been supported by the Ministry of the Interior to develop appropriate tools and methodology to be able to fulfil the legislation requirements. Its main goal is to elaborate methodology and a software tool for the identification of vital components and areas of a nuclear facility in respect to physical protection. The software tool is to increase the effectiveness of the identification process of vital SSCs and areas according to the designed methodology. The newly-developed methodology is to determine vital areas by utilizing information from the probabilistic safety assessment (PSA). PSA is broadly applied for the safety evaluation of nuclear power plants and other facilities.

4. Methods for Vital Area Identification

Relevant methods currently used in vital area identification and their background will be described hereinafter. These methods exploit tree structures and include fault tree analysis (FTA), event tree analysis (ETA), attack tree analysis (ATA) and novel attack tree-based VAI method and tool called TARGI.

4.1. Fault Tree Analysis

The fault tree analysis was developed in the 1960s at Bell Telephone Laboratories to evaluate the safety of the Minuteman Intercontinental Ballistic Missile Launch Control System [18]. The fault tree analysis is one of the most commonly used methods for the safety analysis of complex industrial systems, especially for the PSA of nuclear facilities [16].

A fault tree is a logic flow diagram depicting conditions or other factors that cause or contribute to the occurrence of a defined undesirable outcome. This outcome is called a top-level event. A top-level event is the event of interest under which a fault tree is developed. The top-level is often referred to as the final event, or as the top outcome. A fault tree has a top-down structure, showing events or combination of events that can lead to the top-level event. A fault tree analysis can be qualitative or quantitative [6].

An event is an occurrence of a condition or an action, the lowest level of inputs in a fault tree. A primary event is an event that is at the bottom of a fault tree. Sabotage fault trees consider an IEMO as a primary event. A logical relationship between events and the top-level event is defined by a gate. The gate is a symbol which is used to establish a symbolic link between the top-level event and the corresponding events [6]. A fault tree uses graphical symbols to represent the logic:

- OR gate - the output event occurs if any of the input events occur. If any of the input events can be prevented, the event described above the AND gate is prevented.
- AND gate - the output event occurs only if all of the input events occur. All the inputs into an OR gate must be prevented in order to prevent the event described above the OR gate [6].

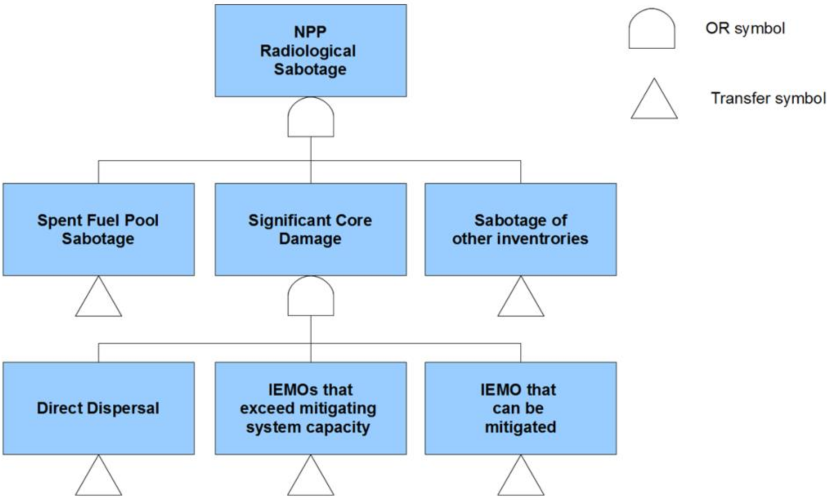
NPP Radiological Sabotage
OR symbol
Transfer symbol
Spent Fuel Pool Sabotage
Significant Core Damage
Sabotage of other inventrories
Direct Dispersal
IEMOs that exceed mitigating system capacity
IEMO that can be mitigated

Fig. 1 Example of the top three levels of a Nuclear Power Plant (NPP) sabotage fault tree [6]

During the process of a tree evaluation, a minimal cut set shows a minimum, or the smallest set of events needed to occur to cause the top-level event. A sabotage fault tree aggregates such sabotage scenarios (a scenario is defined as a path in a tree consisting of SSCs or their combinations leading to the tree's top-level) that could lead to a top-level event, e.g. URC. Most facilities occur in different states, such as full operation vs. downtime. For each state it is necessary to create a separate tree. Fig. 1 shows an example of the top three levels of a sabotage fault tree for a nuclear facility [6].

4.2. Event Tree Analysis

The event tree analysis was developed in 1974 in the U.S. to analyse NPP safety. An event tree is a graphical model that illustrates the possible outcomes that result from a sabotage. The difference among the FTA and ETA is such that the ETA is used for analysing the consequences of an IEMO. A fault tree analysis is used when analysing top-level event causes. The ETA shows possible event sequences from an IEMO up to the potential consequence outcome. The mitigating factors are depicted so that their influence may be evaluated separately [6].

The ETA is not used to identify the initiating event; this is the role of the FTA. The ETA is an inductive method unlike FTA, which is a deductive method. Both methods have therefore different roles in the VAI process [6][22]. An event tree begins with an event or IEMO and continues with binary (YES and NO functions) branches for the associated systems up to the potential consequences. Fig. 1 shows an example of an IEMO and the further development of the event, showing the actions of mitigating systems.

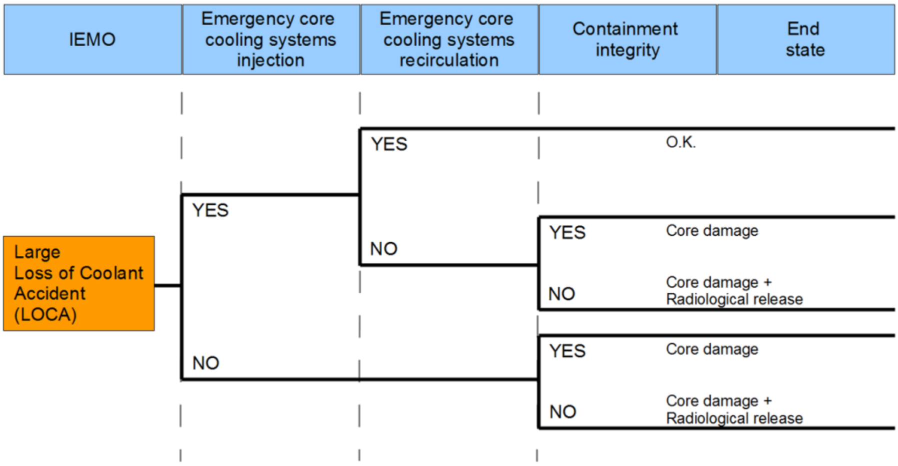
IEMO
Emergency core cooling systems injection
Emergency core cooling systems recirculation
Containment integrity
End state
Large Loss of Coolant Accident (LOCA)
YES
NO
YES
NO
O.K.
YES
Core damage
NO
Core damage + Radiological release
YES
Core damage
NO
Core damage + Radiological release

Fig. 2 Example of an event tree [6]

4.3. Attack Tree Analysis

Attack tree (AT) models represent a rigorous, engineering-like approach to a threat analysis. ATs enable the systematic categorization of the different ways a facility and a material may be attacked by a threat [23]. AT models are extremely well-suited to assess situations where events have never happened or happen infrequently [23], which is exactly the case in which malevolent acts of human origin are directed against a nuclear facility and nuclear material.

ATs have been used in various fields since the 1980s [23]. Weiss in 1991 [24] and Amoroso in 1994 [25] published attack tree concepts, although they were called threat trees. ATs were popularized by Schneier [26] in 1999 and formalized by Mauw and Oostdijk [27] and further extended in a paper [28] by Jurgenson et al. that presents computing outcomes of multi-parameter ATs. A large number of papers have been published since then with different uses and variations of trees.

Tree structures – fault trees, threat logic trees, attack trees, defend trees, attack-defend trees are nowadays often used in cyber security models, e.g. in [29], although rarely in the physical protection effectiveness evaluation models [31]. An extensive survey of attack-tree uses both in cyber security and physical security has been done by Kordy et al. in [31]. Attack trees were used by Opdahl in [33] for security threat identification, where different methods were compared. Attack trees were found to be more suitable for threat identification.

The concept of Ordered Weight Averaging (OWA) operator trees was introduced by Yager in [34]. OWA trees are an extension to ATs. The AND and OR operators are extended in this concept. The OWA nodes enable to model a situation in which there is some probabilistic uncertainty.

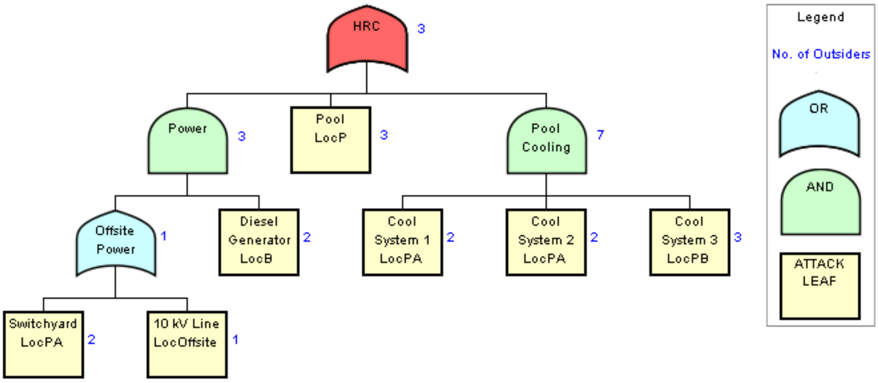

Fig. 3 Attack tree example [36]

Attack trees are used for the analysis of various security events caused by acts of a malevolent origin. An attack tree has the structure of a flow diagram, which depicts the logical relations between the attack target (represented by a top-level event, e.g. URC) and initiating events, which need to be accomplished to achieve the top-level event. Initiating events or SSCs are represented by tree leaves and may be assigned different variables. A possible attack is represented by any path leading from the leaf nodes to the top-level event. There are 2 operators used in the attack tree nodes similarly as in FTA: the AND and OR operator.

- AND – all events listed under these gates have to be achieved in order to fulfil the AND node goal,
- OR – a minimum of one event must be achieved in order to fulfil the OR gate goal [26].

Each initiating event may be characterized by several variables. These variables may be of two types:

- Boolean type, e.g. the attacker is able or unable to conduct some action etc.,
- nominal value type, e.g. the number of attackers, time to accomplish goal etc. [26].

Fig. 3 depicts a simplified example of an attack tree, decorated with only one attribute – no. of outsiders, each leaf representing a SSC has an assigned location [36].

4.4. TARGI – a New Approach to Vital Area Identification

Due to the increasing need for critical infrastructure protection, the authors present a novel approach and the tool TARGI to enhance the target identification process and to support complex critical infrastructure facilities in identifying their vulnerable targets. TARGI not only considers current approaches and exploits vast experience from the nuclear sector, but also provides the opportunity to enhance and simplify the whole current process of target identification using ATA. This approach has been described in [36] and [37]. The reasons why the current approaches have been innovated are numerous. The main key points are described below.

Tree structures currently used in VAI focus exclusively on the facility’s SSCs which a potential adversary is willing to defeat. AT makes it feasible to model the SSCs and the threat characteristics, as well as their mutual interaction. This is considered a great improvement. When using fault tree structures, experts need to assess, if the current threat is capable of carrying out and successfully accomplishing a selected scenario. Scenarios can be very complex in themselves and the number of scenarios may be immense for large and technologically complex facilities like nuclear facilities. A scenario is defined as a path in a tree consisting of SSCs or their combinations leading to the tree's top-level event e.g. URC. The complexity and extent of scenarios may be very demanding for expert assessment. The main contribution of the ATA is the substantial particularization of the VAI process. Experts are required to assess the specific capabilities of a threat in relation to a specific SSC, not to an overall scenario as is with fault trees.

The VAI process is also simplified with ATs. Each leaf node that represents SSC is decorated with attribute values – these values represent conditions in which the specific SSC can be defeated. Attribute values are assigned once for the whole tree (unless there are changes in the facility). Attributes may include capabilities, such as the number of adversaries, equipment or weapons they need and knowledge of the facility. Once these attribute values are assessed and an AT is decorated, a so-called threat agent is applied to the AT. A threat agent is a threat represent that possesses specific threat capabilities. A threat agent may be quickly and effectively changed and can be consequently applied to the AT. This fact enables a prompt response to threat changes, as it is obvious that threats are very dynamic variables. The importance of well-designed and scaled attributes is crucial for the above-mentioned described VAI using ATs. The use of ATs enhances the whole VAI process, reduces possible expert errors and enables a fast and effective response to threat changes.

Fig. 4 depicts a flow chart that describes the VAI process using the ATA according to [36]. The facility data serve as an initial input to the process, with the AT based on a Facility Functional Model (1). AT leafs (representing SSCs) are decorated with threat attribute values (2). The input data entered in this step include a threat attribute set, a supplementary attribute set and attribute functions.

The third step assigns SSC locations to all leaf nodes (3). The assignment of SSC locations enables the identification and display of vital SSCs in areas later in the process. This step is of a crucial importance from the security point of view.

Most of the VAI analyses are based on the data from the previously conducted safety analysis, e.g. the probabilistic safety analysis (PSA). The safety analysis often considers SSCs of the same functionality that are located in one room as a separate SSC that provide backup to each other in case of malfunction. From the safety point of view, there is a certain probability that they will not malfunction at once. However, from the security point of view, if SSCs are not separated or compartmentalized, they may be destroyed by a malevolent act at once in all probability. Therefore, the required back-up functionality may not be present as stated by the safety analysis. This is one of the main reasons, why a safety analysis must be carefully considered while used in the security area dealing with malevolent threats.

Once AT values have been calculated (4), the selected threat agent representing the threat's capabilities and motivation is applied to the AT (5). Tree pruning reduces the number of scenarios based on the threat agent's capabilities and eliminates non-achievable goals.

If the threat has sufficient capabilities to achieve the top-node event in one or more scenarios (6), the process continues. The Protection Tree (PT) (7) may be created as a Boolean complement of the original AT. The PT is decorated with PT attribute sets and PT values are calculated (8). Vital area scenarios (also called vital area candidate sets) are sorted and evaluated based on the selected criteria (e.g. the impact on facility operation, emergency response, the cost of VA protection, etc.). The vital area or areas are selected based on the chosen criteria.

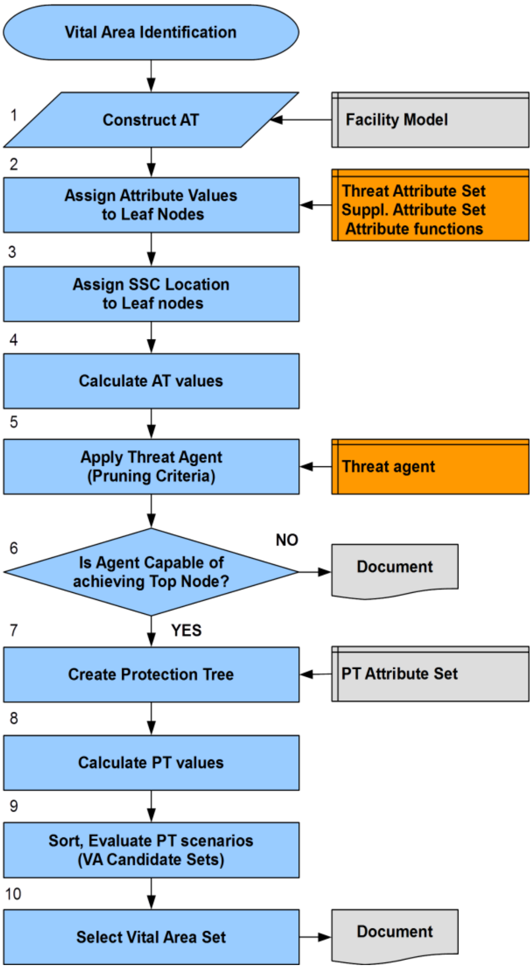

Fig. 4 TARGI approach to VAI [36]

4.5. Protection Tree Analysis

A Boolean complement of an AT is called a protection tree or a defence tree. Different resources introduce names like Attack-Response Tree or Attack-Countermeasure Tree. The PT model identifies those systems, structures and components or their combination that have to be protected in order to prevent an attacker achieving a top-level event.

Creating a PT using the Boolean complement of AT was described for example in [31]. PTs allow other parameters to be considered, these PT attribute help with further analysis, according to which the protection sets may be further sorted based on economic or other mitigating factors. The PTA determines where to allocate resources for protection.

Fig. 5 depicts a simplified example of a protection tree, decorated with the protection tree attribute – "Cost of Protection". According to this protection tree, the operator may decide which vital area candidate set (scenario) to select.

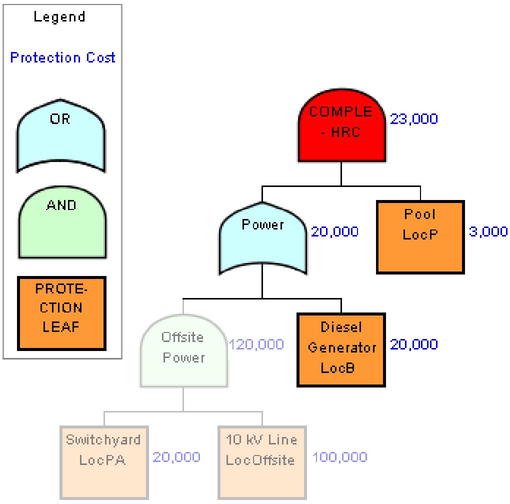

Fig. 5 Protection tree example [36]

5. Attack Tree Threat Attributes

In the previous chapters, it was mentioned that threat characteristics are the essential input for the whole vital area identification process. It is important to mention that threat attributes are not known to be used in AT-based VAI. The need of this new approach has risen from the newly-developed novel approach of AT-based VAI. A threat attribute, sometimes also called a threat metric or indicator, is a threat description which is designed and scaled to be used in an AT and can acquire a specified range of values. Sandia in [45] defines a threat attribute as a discrete characteristic, or distinguishing property, of a threat. Threat attributes describe a threat's willingness and capability to pursue its goals.

Available works use different types of threat and other attributes as an input into the AT models. The literature describes different types of attributes. However, these are mainly related to cyber security or, less frequently, physical protection system effectiveness evaluation. No current available work, to the best of author's knowledge, describes attributes for AT-based VAI. Moreover, the description of how to transform the DBT into a form that could be used in VAI models is not available either. Schneier's models use attributes, such as the "Cost of an Attack", "Special tools required", "Probability", "Severity", "Impact" and "Consequence" [26]. In 2004, Byres [46] used attributes including "Technical difficulty", "Severity of impact" and "Likelihood of detection" related to the assessment of vulnerabilities in network security.

Attributes related to automotive on-board networks in [47] include: “Severity”, “Success probability” (comprising of time for attack preparation, knowledge of the system, window opportunity to access the target of attack, equipment needed for the attack) are used as well as a probability attribute - the “Controllability of an attack” in terms of impact.

A cyber-security related paper by Sandia [48] describes the combined attributes of a threat's willingness and ability to pursue its goal. The paper also points out the necessity of removing dependencies among threat attributes. Two types of attributes are described, including commitment attributes that specify the threat's willingness (the determination of the threat to pursuit its goal, the level of threat's secrecy, the time to plan and prepare the attack) and a resource-type attribute describing the threat's capabilities (human resources needed to conduct an attack, knowledge and level of access needed).

Kordy et al. in [38] brings an extensive overview of attributes for attack trees, as well as suggesting attributes for attack-defence trees (ADTrees), which were formalized in [39]. Attack tree approaches usually consider attributes in relation to a threat. AD Trees use defence attributes such as the “Costs of defence”, “Response time”, “Detectability”, “Difficulty”, “Impact”, “Penalty”, “Profit”, “Social costs” and “Special skills”. Meta-attributes provide additional information about attributes; for example “Confidence”, which indicates the certainty or confidence of an expert while assigning values for attributes in specific tree leaves. Kordy et al. describes among her case studies a physical security case [39]. Broad description of observations during the ADTrees attribute decoration is described, as well as addressing the preparation of attribute values.

A very comprehensive description of attacker attributes related to security may be found in Ingoldsby [23]. Various attributes are introduced, among them the cumulative attribute “Ease of attack”. Ease of attack is the product of “Cost”, “Technical ability” and “Willingness to be noticed”. Ingoldsby uses utility functions to describe the threat's capability and willingness to perform an attack. Every attack has a different attractiveness for an adversary, which is characterized by attacker benefit utility functions. Ingoldsby introduces the attribute “Desirability of an attack” that is defined as “Attack benefits” over “Attack costs”. Finally, attribute “Attack propensity” is the product of the “Ease of an attack” and the “Attack benefit”. The propensity in this example relates to the expression of the relative frequency of an attack or the relative probability [23].

The concept of OWA trees described by Yager in [34] describes OWA attack tree attributes including the “Probability of success” and “Cost of an attack”. In [43] Edge uses attributes such as the “Probability of success”, the “Cost to attack”, the “Impact on the system”, the “Risk”, and the “Cost of implementation”. Their attributes (or metrics as the paper calls them) can acquire different values, such as probability (range 0÷1), a numerical value (0-infinity) and a numerical scale (0÷10).

The Novel Threat-Risk Index report [49] describes a quantitative approach employing scientific and engineering concepts for a threat-risk index development. This model consists of five analyses: the targeting model that estimates the probability of a terrorist attack; the human reliability model; the physical system model that includes failures; the probabilistic risk analysis model including FT and ET program; and the consequence/loss model. This report is mainly focused on dam security. The main attributes include the “Number of terrorists”, their “Resources”, “Schedule”, “Likelihood of success”, “Loss of life”, “Primary economic loss” and “National stress and inconvenience”. This model evaluates not only the vital areas, but also joint risks and consequences.

The paper [50] revisits the notion of attack trees attribution. It describes how explicit attribute values of child nodes are aggregated to form the attribute of the parent node and propose an attribution approach. This approach uses the attribution within the context of analysing the weakest and strongest links of a security system.

The paper on threat characterization in VAI process [36] co-written by the authors of this papers describes the importance and use of the threat attributes in VAI. The main contribution of an attack tree-based VAI is the possibility to decorate the AT with attributes. FT and ET models suffer from the impossibility of inputting threat attributes directly into leaf nodes, as it was described earlier. The important finding of this paper is that threat attributes must be quantitative to enable AT-based VAI.

6. Conclusion

The physical security of nuclear facilities and materials has assumed importance over the last two decades. The mounting concern of terrorist attacks urges society to development of sustainable security technologies and methods to prevent or mitigate probable malevolent attacks. The threat is changing rapidly these days, which demands new approaches and methods to be able to ensure security.

One of the basic problems when securing critical infrastructure elements is the right identification of potential attack targets because if we do not know the attack target, we can neither plan a rational physical protection system, nor evaluate its effectiveness. Therefore a great deal of attention is to be given to the research and development of the methods and procedures which enable us to identify potential attack targets effectively. Within the performed analysis, a number of international regulations and recommendations (mainly for the area of nuclear industry) dealing with the VAI aspects have been identified along with a relatively big amount of technical literature devoted to the methods and procedures used for VAI.

However, there was no method which would enable us to identify vital areas objectively, considering not only the nature of a protected facility, but also the capabilities of a potential attacker. The TARGI method makes it feasible to model the mutual interaction between SSCs and a potential attacker.

The TARGI method is based on the application of an attack tree and uses the quantitative description of attacker capabilities including a wide range of characteristics. The method enables fast reaction to threat changes, which makes it a very up-to-date and state-of-the-art method in today's fast-paced world. It is the new approach itself which indicates a long-term direction of development in the area of VAI.

Acknowledgement

The research was supported by the Ministry of the Interior of the Czech Republic in the projects “Evaluation of Physical Protection System Effectiveness Based on its Modelling” (project no. VG20112015039) and “Elaboration of methodology and computer tools for evaluation of components importance of nuclear facility in relationship to physical protection and design basic threat” (project no. VG20112015040).

References

[1] LOVECEK, T., RISTVEJ, J. and SIMAK, L. Critical Infrastructure Protection Systems Effectiveness Evaluation. *Journal of Homeland Security and Emergency Management*, 2010, vol. 7, issue 1, article no. 34.

[2] IAEA. *Nuclear Security Series No. 16 - Identification of Vital Areas at Nuclear Facilities.* Vienna: International Atomic Energy Agency, 2012. 37 p.

[3] *Elaboration of methodology and computer tools for evaluation of importance of components of nuclear facility in relationship to physical protection and design basic threat (TARGI)* [on line]. Brno: EBIS. [cited 2015-03-22]. Available from: <http://www.targi.cz>.

[4] *Evaluation of Physical Protection System Effectiveness based on its modeling (HUSFO)* [on line]. Brno: EBIS. [cited 2015-03-22]. Available from: <http://www.husfo.cz>.

[5] IAEA. *Nuclear Security Series No. 13 - Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*. Vienna: International Atomic Energy Agency, 2011. 57 p.

[6] VARNADO, GB. and WHITEHEAD, DW. *Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants - Sandia report SAND2008-5644*. Albuquerque: Sandia National Laboratories, 2008. 41 p.

[7] WINS. *An Integrated Approach to Nuclear Safety and Nuclear Security*. Vienna: World Institute for Nuclear Security, 2011.

[8] HOCKERT, J. BECK, DF. *Systematic Method for Identifying Vital Areas at Complex Nuclear Facilities – Sandia report SAND2004-2866.* Albuquerque: Sandia National Laboratories, 2008. 100 p.

[9] BOTT, TF. and THOMAS, WS. Reactor Vital Equipment Determination Techniques. In: *Proceedings of the 11th Water Reactor Safety Research Information Meeting*. Washington: U.S. NCR, 1983, p. 51-58.

[10] CAMERON, D. F. Vital Areas at Nuclear Plants. In *Proceedings of the 7th International System Safety Conference*. Unionville: International System Safety Society, 1985.

[11] RICHARDSON, JM. *Rank Ordering of Vital Areas Within Nuclear Power Plants - Sandia report SAND82-0332.* Albuquerque: Sandia National Laboratories, 1982. 38 p.

[12] U. S. NRC. *Vital Equipment/Area Guidelines Study: Vital Area Committee Report (NRC report NUREG-1178).* Washington: U. S. Nuclear Regulatory Commission, 1988.

[13] *U. S. NRC Regulations: Title 10, Code of Federal Regulations - § 73.55 Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage*. Washington: Nuclear Regulatory Commission, 2013.

[14] GARCIA, ML. *The design and evaluation of physical protection systems*. Boston: Elsevier/Butterworth-Heinemann, 2008. 351 p.

[15] GARCIA, ML *Vulnerability assessment of physical protection systems*. Boston: Elsevier Butterworth-Heinemann, 2006. 382 p.

[16] JAEJOO, H., JUNG, WS. and PARK CK. The Application of PSA Techniques To The Vital Area Identification Of Nuclear Power Plants. *Nuclear Engineering and Technology*, 2005, vol. 37, no. 3, pp. 259-264.

[17] LEE, YH., JUNG, WS. and LEE, JH. Importance of location dependencies such as cable and pipe runs when identifying the vital areas. *Nuclear Engineering and Design*, 2012, no. 242, pp. 458-467.

[18] VINTR, Z., MALACH, J. and VINTR, M. Does Appropriate Software Support for Target Identification exist? In *45th annual IEEE International Carnahan Conference on Security Technology*. New York: IEEE, 2011, p. 133-137.

[19] IEC 61025:2006, *Fault tree analysis*.

[20] VESELY, W. E. et al. *Fault tree handbook (NRC report NUREG-0492*). Washington: U.S. Nuclear Regulatory commission, 1981. 208 p.

[21] IEC 62502:2006, *Analysis techniques from dependability - Event tree analysis.*

[22] VINTR, Z., VINTR, M. and MALACH, J. Evaluation of physical protection system effectiveness. In: *Proceedings - 46th Annual IEEE International Carnahan Conference on Security Technology*. Piscataway: IEEE, 2012, pp. 15-21.

[23] INGOLDSBY, T. *Attack Tree-based Threat Risk Analysis*. Calgary: Amenaza Technologies, 2010. p 36. [cited 2015-03-22] Available from: <http://www.amenaza.com/downloads/docs/AttackTree ThreatRiskAnalysis.pdf>

[24] WEISS, JD. A System Security Engineering Process. In *Proceedings 14th National Computer Security Conference*. Washington: National Institute of Standards and Technology, 1991, p. 572-581.

[25] AMOROSO, E. *Fundamentals of computer security technology*. Upper Saddle River: Prentice-Hall, 1994, 432 p.

[26] SCHNEIER, B. Attack Trees. *Dr. Dobbs Journal of Software Tools,* 1999, vol. 24, no. 12, p. 21-29.

[27] MAUW, S. and OOSTDIJK, M. Foundations of Attack Trees. In *Information Security and Cryptology - ICISC 2005*. New York: Springer, 2006, p. 186-198.

[28] JÜRGENSON, A. and WILLEMSON, J. Computing Exact Outcomes of Multi-parameter Attack Trees In: *On the Move to Meaningful Internet Systems: OTM*. Heidelberg: Springer-Verlag, 2008, p. 1036-1051.

[29] BULDAS, A, LAUD, P., PRIISALU, J., SAAREPERA, M. and WILLEMSON, J. Rational Choice of Security Measures Via Multi-parameter Attack Trees. In: *CRITIS'06 - Proceedings of the First international conference on Critical Information Infrastructures Security*. Heidelberg: Springer-Verlag, 2006, p. 235-248.

[30] FOVINO, IN., MASERA, M. and DE CIAN A. Integrating cyber attacks within fault trees. *Reliability Engineering and System Safety*, 2009, vol. 94, issue 9, p. 1394-1402.

[31] VINTR, Z., VALIŠ, D. and MALACH, J. Attack tree-based evaluation of physical protection systems vulnerability. In: *Proceedings - 46th Annual IEEE International Carnahan Conference on Security Technology*. Piscataway: IEEE, 2012, p. 59-65.

[32] KORDY, B., PIÈTRE-CAMBACÉDÈS, L. and SCHWEITZER, P. DAG-Based Attack and Defense Modeling: Don’t Miss the Forest for the Attack Trees. *Computer Science Review*, 2014, vol. 13-14, p. 1-38.

[33] OPDAHL, AL. and SINDRE, G. Experimental comparison of attack trees and misuse cases for security threat identification. *Information and Software Technology*, 2009, vol. 51, issue 5, p. 916-932.

[34] YAGER, RR. OWA trees and their role in security modeling using attack trees. *Information Sciences*, 2006, vol. 176, issue 20, p. 2933–2959.

[35] OPEL, A. *Design and Implementation of a Support Tool for Attack Trees*. [Internship thesis]. Magdeburg: Otto-von-Guericke Universitat, 2005.

[36] MALACHOVÁ, T., VINTR, Z. and MALACH, J. Threat Characterization in Vital Area Identification. In: *Proceedings - 47th Annual IEEE International Carnahan Conference on Security Technology*. Piscataway: IEEE, 2013, p. 79-84.

[37] MALACHOVA, T., MALACH, J, VINTR, Z. TARGI – A Novel Tool and Method for Target Identification. In *Proceedings of 48th Annual IEEE International Carnahan Conference on Security Technology*. Piscataway: IEEE, 2014, p. 1-5.

[38] BAGNATO, A., KORDY B., MELAND, PH. and SCHWEITZER, P. Attribute Decoration of Attack-Defense Trees. *International Journal of Secure Software Engineering*, 2012, vol. 3, issue 2, p. 1-35.

[39] KORDY, B., MAUW, S., RADOMIROVIĆ, S. and SCHWEITZER, P. Foundations of attack-defense trees. In: *FAST'10 - Proceedings of the 7th International conference on Formal aspects of security and trust*. Heidelberg: Springer-Verlag, 2011, p. 80-95.

[40] KORDY, B., KORDY, P. MAUW, S. and SCHWEITZER, P. ADTool: Security Analysis with Attack-Defense Trees. In: *The Proceedings of the 10th International Conference on Quantitative Evaluation of Systems (QEST'13).* Heidelberg: Springer-Verlag, 2013, p. 173-176.

[41] KORDY, B., MAUW, S. and SCHWEITZER, P. Quantitative Questions on Attack-Defense Trees. In: *Information Security and Cryptology – ICISC 2012*. Heidelberg: Springer-Verlag, 2013, p. 49-64.

[42] ROY, A., KIM, DS. and TRIVEDI, KS. ACT: Towards unifying the constructs of attack and defense trees. *Security and communication networks*, 2012, vol. 5, issue 8, p. 929-943.

[43] EDGE, KS., DALTON, GC. RAINES, RA. and MILLS, RF. Using Attack and Protection Trees to Analyse Threats and Defenses to Homeland Security. In: *Military Communications Conference*, Piscataway: IEEE, 2006, pp. 1-7.

[44] EDGE, KS. *A Framework for Analysing and Mitigating the Vulnerabilities of Complex Systems via Attack and Protection Trees*. [Dissertation thesis] Wright-Patterson Air Force Base: Air Force Institute of Technology, 2007. 195 p.

[45] DUGGAN, DO. and MICHALSKI, JT. *Threat Analysis Framework - Sandia report SAND2007-5792*. Albuquerque: Sandia National Laboratories, 2007. 31 p.

[46] BYRES, EJ., FRANZ, M. and MILLER, D. The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems. In: *International Infrastructure Survivability Workshop*. Piscataway: IEEE, 2004. 9 p.

[47] HENNIGER, O., APVRILLE, A., FUCHS, A., ROUDIER, Y. RUDDLE, A. and WEYL, B. Security requirements for automotive on-board networks. In *9th International Conference on Intelligent Transport Systems Telecommunications (ITST 2009).* Piscataway: IEEE, 2009, p. 641 – 646.

[48] MATESKI, M., TREVINO, C., VEITCH, C., MICHALSKI, VJ. HARRIS, M., MARUOKA, S. and FRYE, J. *Cyber Threat Metrics – Sandia report SAND2012-2427.* Albuquerque: Sandia National Laboratories, 2012. 38 p.

[49] PLUM, MM. et al. *Novel Threat-Risk Index Using Probabilistic Risk Assessment and Human Reliability Analysis*. Idaho Falls: Idaho National Engineering and Environmental Laboratory, 2004. 39 p.

[50] WHITLEY, JN., PHAN, RCW., WANG, J. and PARISH, DJ. Attribution of attack trees. *Computers and Electrical Engineering*, 2011, vol. 37, issue 4, p. 624–628.