Multimed Tools Appl (2016) 75:10667–10690
DOI 10.1007/s11042-014-2047-6

Risk assessment for a video surveillance system based on Fuzzy Cognitive Maps

Piotr Szwed · Pawel Skrzynski · Wojciech Chmiel

Received: 29 December 2013 / Revised: 16 April 2014 / Accepted: 20 April 2014 /
Published online: 25 May 2014

Abstract For various IT systems security is considered a key quality factor. In particular, it might be crucial for video surveillance systems, as their goal is to provide continuous protection of critical infrastructure and other facilities. Risk assessment is an important activity in security management; it aims at identifying assets, threats and vulnerabilities, analysis of implemented countermeasures and their effectiveness in mitigating risks. This paper discusses an application of a new risk assessment method, in which risk calculation is based on Fuzzy Cognitive Maps (FCMs) to a complex automated video surveillance system. FCMs are used to capture dependencies between assets and FCM based reasoning is applied to aggregate risks assigned to lower-level assets (e.g. cameras, hardware, software modules, communications, people) to such high level assets as services, maintained data and processes. Lessons learned indicate, that the proposed method is an efficient and low-cost approach, giving instantaneous feedback and enabling reasoning on effectiveness of security system.

Keywords Security · Risk assessment · Video surveillance · Fuzzy cognitive maps

P. Szwed (✉) · P. Skrzynski
AGH University of Science and Technology, Department of Applied Computer Science,
al. Mickiewicza 30, 30-059 Kraków, Poland
e-mail: pszwed@agh.edu.pl

P. Skrzynski
e-mail: skrzynia@agh.edu.pl

W. Chmiel
AGH University of Science and Technology, Department of Automatics and Biomedical Engineering,
al. Mickiewicza 30, 30-059 Kraków, Poland
e-mail: wch@agh.edu.pl

1 Introduction

For various IT systems security is considered a key quality factor. In particular, it might be crucial for video surveillance systems, as their goal is to provide continuous protection of critical infrastructure and other important facilities.

Risk assessment is a key process in the management of IT systems security. It can be considered an extensive study of assets, threats and vulnerabilities, likelihoods of their occurrences, potential losses and theoretical effectiveness of security measures [24]. Several risk assessment processes are defined by over 15 standards or methods [18], including most popular: ISO/IEC 27005 [31], NIST 800-30 [46] and CRAMM [17]. The standards, apart of defining risk scoring methods, specify organizational foundations for performing risk assessment in the broader context of IT security risk management.

Even a quick research [25, 33] can indicate that automated video surveillance systems are potentially exposed to risks of various types. Firstly, they use a number of technologies: computer vision, networking and big data for video storage. Secondly, they rely on several hardware elements: cameras, network infrastructure or servers. Finally, they may integrate components complying various standards.

There have been several attempts to provide design guidelines for video surveillance systems taking into consideration security issues [55]. Moreover, such systems may deploy several mature multimedia protection technologies, as watermarking, encryption or fingerprinting [21]. Despite those facts, it seems that there is a significant lack of research on overall assessment of IT security risk for this domain.

This paper discusses an application a new *lightweight* risk assessment method [60] to an automated video surveillance system. The method consists in identifying assets and expressing dependencies between them in form of a Fuzzy Cognitive Map (FCM). Then, FCM based reasoning is applied to aggregate risks assigned to lower-level assets (e.g. hardware, software modules, communications, people) to such high level assets as services, maintained data and processes.

The complete method description is given in the paper, as well as an assessment of a relatively complex system comprising several detection modules, components implementing human interfaces, databases and a workflow serving as an integration platform. The subsequent assessment steps are discussed on a real example and their results are discussed.

The paper is organized as follows: in Section 2 we provide an overview of risk assessment methods. Section 3 introduces Fuzzy Cognitive Maps, followed by Section 4, in which risk assessment methodology is described. Further, in Section 5 the analyzed system is presented, then in Section 6 application of the proposed risk assessment method is discussed. Finally, Section 7 gives concluding remarks.

2 Related works

This section is divided into three subsections. The first gives an overview of risk assessment methodologies. The second discusses modern automated video surveillance systems. Finally, the last subsection provides the problem definition.

2.1 Overview of risk assessment methodologies

According to [24, 51] *security* is the protection afforded to an information system in order to preserve integrity of data and system functions, their availability, authenticity and confidentiality.

Risk assessment has its roots in the nuclear power industry, where probabilistic models were built to analyze potentially catastrophic faults in nuclear power facilities [51]. In 1979 the National Bureau of Standards proposed the Annual Loss Expectancy (ALE) metric [30] as applicable for non safety-critical systems. It defined risk as a sum of products of *frequencies* of harmful events and induced *losses* expressed in dollars. This approach to risk characterization influenced many methodologies and standards, e.g. CRAMM [17] or recently NIST 800-30 [46]. In some frameworks the statistical term *frequency* is replaced by *likelihood* or *probability*, *loss* by *impact*. Furthermore, as it is difficult to estimate absolute values of probabilities and losses, ordinal scales (e.g.: low, medium, high) defining coarse levels are used.

In spite of the popularity of the ALE metric, its application to the risk assessment is considered problematic due to a cognitive bias in estimating likelihoods of threats [28], lack of statistical data, difficulties in calculating losses and extremely high costs of the whole process.

In numerous standards and methods listed in the ENISA Inventory [18], including most popular: ISO/IEC 27005 [31], NIST 800-30 [46] and CRAMM [17], the risk assessment is not only perceived as a method of estimating risks; it is rather considered a complex process in the management of IT system security. Typically, it is built up of several activities, such as identification of assets, threats and vulnerabilities, the likelihoods of their occurrences, potential losses and the theoretical effectiveness of security measures. Hence, the standards, apart of defining risk scoring methods, specify organizational foundations for performing risk assessment in the broader context of IT security risk management.

Practical implementations of risk assessment and management include various approaches. *Integrated Business Risk-Management Frameworks* e.g. SABSA [50] abstract from technical details and embed IT security within a holistic business risk management context. *Valuation-Driven Methodologies* ignore difficult to assess likelihoods and simply recommend safeguards using as a sole criterion estimated values of assets. *Scenario Analysis Approaches* focus on eliciting and evaluating scenarios compromising security. Finally, *Best Practices* rely on standardized lists of safeguards eligible for given types of assets.

Parallel to business practice, the ongoing (mainly academic) efforts aiming at building risk models going beyond ALE and applying them to real or hypothetical systems might be observed. In several cases they were followed by proposals of methodologies or guidelines, often accompanied by dedicated interactive software packages. Furthermore, these guidelines were frequently combined with modeling techniques that are widely applied in reliability and safety engineering, such as Fault Trees, Event Trees, Markov Chains, and FMEA (Failure Mode Effects Analysis) [7, 52, 66]. These techniques provide a representation of system operations and undesirable events and a validation of the system safety level [9, 12, 16, 42, 53].

Han, Yang and Chang described an expansible vulnerability model in order to qualitatively assess the security of an active network aiming at solving a problem that it is more suited for an active network, than a traditional one [27]. Eom, Park and Han introduced a risk assessment method based on asset valuation and quantification [19]. Baudrit and

Dubios proposed a risk assessment method taking into account two types of uncertainty: randomness and imprecision [6]. Sun, Srivastava, and Mork introduced a risk assessment model based on Dempster-Shafer evidence reasoning [54]. Chen put forward a quantitative hierarchical threat assessment model and a corresponding quantitative calculation method exploiting the statistics of system attacks that occurred in the past [13]. Wang et. al. analyze network security by using a probable attack graph generated on the basis of security case reasoning, carrying out qualitative risk assessment for the network system mainly from an attacker perspective [68].

Attack trees, proposed by Schneier [47], specify which combinations of adversarial actions should be employed to compromise an asset (the goal of an attack). Hence, a tree with AND-OR nodes represents several attack scenarios. As each tree node can be assigned with various attributes: a probability, a cost of an adversarial action or a loss, various metrics can be calculated indicating the probability of success of a given attack and helping to find potential vulnerabilities. An application of attack trees to assess security risks in heterogeneous telecommunication networks was reported by Szpyrka, Jasiul et al. [56].

Lazzerini and Mkrtchyan [39] proposed a method using Extended Fuzzy Cognitive Maps (E-FCMs) to analyze the relationships between risk factors and risks. E-FCMs are suggested by Hagiwara [26] to represent causal relationships in a more natural way. The main differences between E-FCMs and conventional Fuzzy Cognitive Maps (discussed in Section 3) are the following: E-FCMs have nonlinear membership functions, conditional weights, and time delay weights.

2.2 Review of video-surveillance systems

Automated video surveillance is a complex technology combining recent developments in computer vision, hardware (cameras, video storage), networking and data bases. It is applied to protect various types of objects: state borders, industrial infrastructure, public areas, buildings, hospitals, offices, malls and parking lots. Automated systems gradually displace installations using solely human observers, as they are considered costly and ineffective.

Typical video analysis components include such functions as background maintenance, object detection, classification, object tracking and activity (event) recognition [25]. Moreover, the detection software usually necessities in auxiliary configuration information about an observed scene, e.g. definition of polygon shaped zones, crosslines, regions of interests, etc.

Appearance of a recognized object within such region, its movement or partial overlapping produces an alarm (event), which is further processed by other system components. In particular it can be delivered to a system operator to bring his or her attention to a detected suspicious situation.

Industrial video surveillance systems differ in alarm handling and detection capabilities and, at the some time, publish very little information on algorithms used. We review some of them to give an idea of their complexity and potential challenges for securing the systems themselves.

The Bosch IVA (Intelligent Video Analysis) security system is a leader in this field [8]. It is a comprehensive solution designed for conducting intelligent video surveillance. IVA includes alarm transmission subsystem and centralized management. Bosch VMS (Video Management System) provides complete surveillance, management of video signals and alarms handling. Alarms coming from IVA system are combined with general motion detection alarms. VMS system allows combining specific alarming conditions and ordering them

according to their importance, resulting in possibly complex rules to manage emergency scenarios.

IndigoVision company [29] provides tools supporting integration and management of alarming systems. Its solutions include a centralized management of distributed monitoring systems through automated handling of alarms detected anywhere in the supervised areas. The system allows to define responsibilities for performing alarm responses, assigning them to registered users, integration of alarm zones and reports creating .

VMS (Video Management System) system is developed by Mirasys Carbon company [41]. It is highly scalable and provides efficient analysis tools for handling thousands of video recorders and cameras. The system supports the centralized management of user profiles, constant monitoring of system status and generation of alarms associated with hardware failures. An important feature is the ability to define the procedures for handling registration and reporting of alarms.

Axis Company offers and promotes decentralized systems, which perform essential calculations on cameras [5]. A key feature of this approach is free of charge, open standard to support network cameras (Axis network cameras VAPIX). This allows not only to create own applications for intelligent video analysis, but simplifies also the development of a surveillance system, as the standard includes ready-to-use solutions.

System from Securiton company [48] is equipped with functions of location and geo-referenced positioning of objects and 3D technology. IPS-Outdoor is a high quality video surveillance system for monitoring of people and objects in outdoor areas. IPS-Indoor allows to track simultaneously up to 50 objects inside buildings and in outdoor areas and to visualize objects' trajectories, also on large maps (geo-referencing).

The Verint company [65] has developed Nextiva PSIM^{TM} Actionable Intelligence system that integrates a large number of detectors and automatically identify dangerous situations. Solutions provided by PSIM platform are scalable and are based on an open architecture. The software includes PSIM scenario generator that allows to define scenarios launched in case of such events, as: explosion, flood, aggressive crowd behavior or gas leak. Execution of procedures is controlled through control lists.

Detection of complex temporal scenarios was the goal of a system developed at INRIA [67]. This system used VSIP platform for recognizing such people behaviors, as fighting or vandalism in a subway scene observed by a single or multiple cameras. This work has been performed in the framework of the European project ADVISOR [1], which aims at building a generic environment facilitating integration of algorithms for video processing and analysis. ADVISOR allows to flexibly combine and exchange various techniques at the different stages of the video understanding process.

2.3 Problem definition

The paper has two goals. The first is to verify, whether a new method of risk assessment, which was originally proposed for an e-health system [61], can be applied to a much more complex system belonging to another domain. The developed, but still not deployed, video surveillance system SIMPOZ (described in Section 5) seemed a perfect case, as the method enables detecting vulnerable points and performing "what if" analysis related to implemented countermeasures.

The second goal is more general. In spite of the fact, that the protection of video surveillance systems seems to be an important issue, there is a significant lack of research devoted to overall risk assessment of such systems. Hence, our intention was to propose a method

of risk evaluation that would fit the needs of this domain. This is also the main contribution of the paper.

Surprisingly, as mentioned above, just a few papers related to IT security of video surveillance systems can be found. Several reasons to such situation can be given. Firstly, most works are focused on surveillance tasks and not on threats that can be attributed to systems themselves. Secondly, in most cases only certain aspects together with related technologies are addressed, eg. privacy protection [11, 23, 49], camera tampering [15, 20], eavesdrop protection [64] or forging video material [40]. Finally, for implemented systems or off-shelf solutions it would be unreasonable to unveil their weak points and expose them to attacks. In case of the SIMPOZ system we were in a privileged position, as we analyzed a prototype system that has not been yet deployed in a working environment and indicated risks could have been mitigated during the final transition.

A work by Karimaa [33] gives a systematic review to security problems for video surveillance systems. The author divides their architecture into several layers: business, logic, resource and access and discuss risks and solutions related to each layer. Main identified challenges are related to heterogeneity, large volumes of data being transferred, protection against eavesdroppers in communication over public networks, multiple security domains, design of storage systems and user-friendliness of interfaces.

Xie and Ma [69] analyze a social public security video surveillance project in China and discuss the risk management model based on a dynamic life cycle risk management theory. With comprehensive analysis and identification of risk factors related to such projects, the paper provides a basic risk identification table. Finally, the authors give the solutions to a project risk for a discussed case study. However, the paper covers a wide area of topics, while focusing more on project management than the risk assessment.

One of the aspects frequently covered in articles on security in video surveillance systems is privacy. The general conclusion of various reports is that giving up privacy does not necessarily result in a greater security, and the greater security does not necessarily require a loss of privacy [23, 49]. Various technologies that protect privacy in video surveillance exist, but their implementations in current security systems have been limited compared to those of surveillance technology. Referring to these reports, Cavallero discusses [11], how recent advances in video surveillance threaten privacy and how state of art signal processing technologies can protect privacy without risking security – some of those techniques have been applied in the system presented in this paper. From the above review we may conclude that well designed and selectively used video-surveillance systems are powerful tools for physical object protection and monitoring. However, badly designed systems merely generate a false sense of security, while also intruding into our privacy and negatively impacting other fundamental rights.

3 Fuzzy Cognitive Maps

Cognitive maps were first proposed by Axelrod [4] as a tool for modeling political decisions, then extended by Kosko [34, 35] by introducing fuzzy values. A large number of applications of fuzzy cognitive maps (FCM) were reported, e.g. in project risk modeling [39], crisis management and decision making, analysis of development of economic systems and the introduction of new technologies [32], academic units development [57], ecosystem analysis [44], signal processing and decision support in medicine. A survey on Fuzzy Cognitive Maps and their applications can be found in [2] and [45].

FCMs are directed graphs whose vertices represent concepts, whereas edges are used to express causal relations between them. A set of concepts $C = \{c_1, \ldots, c_n\}$ appearing in a model encompasses events, conditions or other relevant factors. A system state is an n-dimensional vector of concept activation levels ($n = |C|$) that can be real values belonging to $[0, 1]$ or $[-1, 1]$.

Causal relations between concepts are represented in FCM by edges and assigned weights. A positive weight of an edge linking two concepts c_i and c_j models a situation, where an increase of the level of c_i results in a growing c_j; a negative weight is used to describe the opposite rapport. In the simplest form of FCM, the values from the set $\{-1, 0, 1\}$ are used as weights. They are graphically represented as a minus $(-)$ sign attached to an edge, an absence of edge or a plus $(+)$ sign. While building FCM models, more fine-grained causal relations can be introduced. They are usually specified as linguistic values, e.g.: *strong_negative*, *negative*, *medium_negative*, *neutral*, *medium_positive*, *positive*, *strong_positive* and in a computational model they are mapped on values uniformly distributed over $[-1, 1]$.

A representation of FCM that used during reasoning is an $n \times n$ influence matrix $E = [e_{ij}]$, whose elements e_{ij} have values equal to weights assigned to edges linking c_i and c_j or are equal 0 values, if there is no link between them.

Figure 1 gives an example of an FCM graph, whose vertices were assigned with concepts c_1, c_2, c_3 and c_4, whereas the edges were assigned with linguistic weights defining mutual influences. Corresponding E matrix is defined by (1). The selection of values corresponding to linguistic values is arbitrary; in the example the values: -1, -0.66, -0.33, 0, 0.33, 0.66 and 1 were used.

$$E = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -0.33 \\ 0.66 & 0.33 & 0 & 0 \\ 0 & 0.66 & -1 & 0 \end{bmatrix} \tag{1}$$

Reasoning with FCM consists in building a sequence of states:

$$\alpha = A(0), A(1), \ldots, A(k), \ldots$$

starting from an initial vector of activation levels of concepts. Consecutive elements are calculated according to the formula (2). In the $k + 1$ iteration the vector $A(k)$ is multiplied

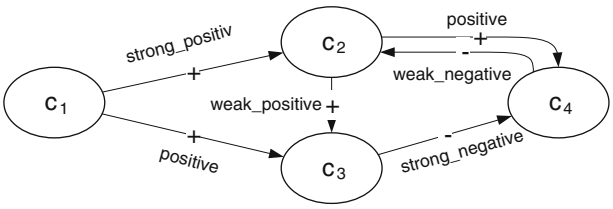

Fig. 1 An example of FCM graph. Vertices are assigned with concepts, directed arcs with linguistic weights of specifying influence

by the influence matrix E, then the resulting activation levels of concepts are mapped onto the assumed range by means of an *activation* (or *splashing*) function.

$$A_i(k+1) = S_i\left(\sum_{j=1}^{n} e_{ij}\, A_j(k)\right) \tag{2}$$

The selection of the activation function depends on assumptions regarding the calculation model, in particular the selected range and the decision to use continuous or discrete values. Multiplication of an n-dimensional square matrix E, both containing elements whose absolute values are bounded by 1, results in a vector having elements in $[-n, n]$. Values from this interval should be mapped by an activation function into the range $[-1, 1]$ (or $[0, 1]$) preserving monotonicity and satisfying $S(0) = 0$ (or $S(0) = 0.5$ in the second case.)

In the further analysis three activation functions were used:

$$S_{cut}(x) = \begin{cases} -1, & \text{if } x < -1 \\ +x, & \text{if } x \geq -1 \text{ and } x \leq 1 \\ 1, & \text{if } x > 1 \end{cases} \tag{3}$$

$$S_{exp}(x) = \begin{cases} 1 - \exp(-mx), & \text{if } x \geq 0 \\ -1 + \exp(-mx), & \text{if } x < 0 \end{cases} \tag{4}$$

$$S_{tanh}(x) = \frac{\exp(mx) + \exp(-mx)}{\exp(mx) - \exp(-mx)} \tag{5}$$

Function $S_{cut}(x)$ given by (3) maps arguments into the interval $[-1, 1]$ replacing values laying outside the interval by the lower or upper bound. Function $S_{exp}(x)$ has similar shape to do $S_{cut}(x)$, but more smoothed and flattened, what is controlled by the coefficient m typically having a value ranging from 1 to 5. Function $S_{tanh}(x)$ is a modification of the hyperbolic tangent consisting in introducing m coefficient (5) that allows to adjust the curve slope.

Basically, a sequence of consecutive states $\alpha = A(0), A(1), \ldots, A(k), \ldots$ is infinite. However, it was shown that after k iterations, where k is a number close to the rank of matrix E, a steady state is reached or a cycle occurs. Hence, the stop criterion for the reasoning algorithm in the k step is the following:

$$\exists j < k\colon d(A(k), A(j)) < \epsilon, \tag{6}$$

where d is a distance and ϵ a small value, e.g. 10^{-2}.

A sequence of states α can be interpreted in two ways. Firstly, it can be treated as a representation of a dynamic behavior of the modeled system. In this case there exist implicit temporal relations between consecutive system states and the whole sequence describes an evolution of the system in the form of a *scenario*. Under the second interpretation the sequence represents a non-monotonic fuzzy inference process, in which selected elements of a steady state are interpreted as reasoning results. An occurrence of a cycle can be treated as a form of undecidability.

In this paper FCMs are considered to be a tool for risks modeling and the focus is put on the second approach.

4 Methodology of risk assessment

The methodology for risk assessment comprises basic steps common to various standards and guidelines, see [24, 31, 38, 46]. The salient difference is the use of an FCM model capturing influences between assets and allowing their dependencies to be tracked during a risk aggregation.

The assumed conceptual model (Fig. 2) assigns an abstract *utility value* to an *asset* and organizes assets into the *added value tree*, a hierarchical structure, in which components of a lower level deliver value to parent elements. The top of the tree is occupied by key processes; they are identified according to business drivers. The utilities of processes depend on used data and invoked services. Various data sources including software may contribute to the utility of data. Services depend on software, hardware and communication, but also on involved staff, physical infrastructure (buildings, rooms, electricity) and external services (e.g. Public Key Infrastructure).

Utility values assigned to assets can be interpreted as aggregations of various quality attributes: security, reliability, usability, etc. Changes of utility values assigned to lower-level assets influence higher-level components that use them.

The risk model presented in Fig. 3 assumes that the utility of an asset can be compromised by a threat, which decreases its value. A negative influence of a threat on an asset can be compensated by an appropriate countermeasure. Countermeasures themselves do not add value to the utility, they only reduce the risk.

For evaluation purposes we define

- *utility* assigned to assets as a value from range $[-1, 1]$
- *risk* related to an asset as the negative difference between assumed utility and the value calculated at the end of the reasoning process.

The reasoning process takes into account influences of threats and countermeasures directly linked to assets, but also changes in utility resulting from relations captured in the added value tree.

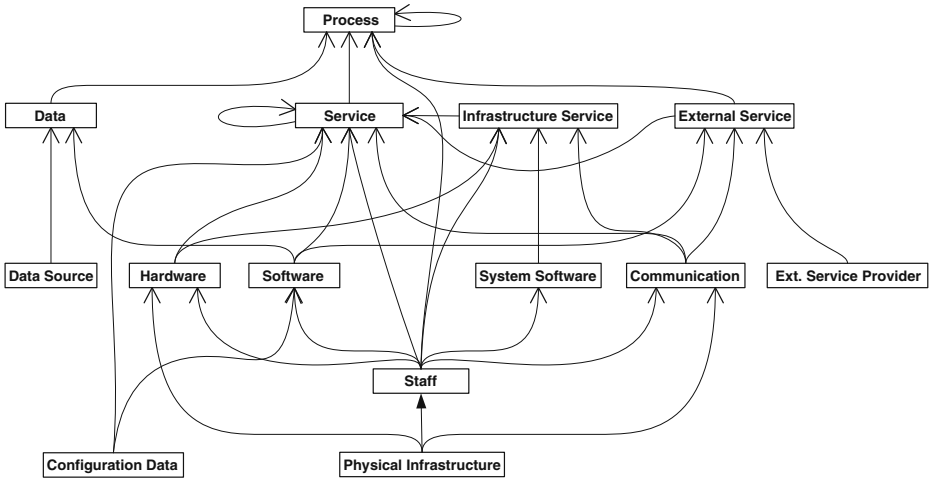

Fig. 2 Classes of assets appearing in an added value tree and their influences

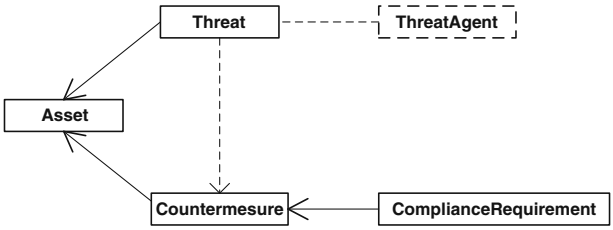

Fig. 3 Relations between assets, threats and countermeasures

The proposed risk assessment process comprises six steps briefly discussed below.

1. *Identification of assets*. The input for this step are existent documents specifying a system vision, its operational concept and an architecture, but also interviews with designers and development teams. The outcome is a list of assets identifying key processes, services, data, software modules, hardware, communication, providers of external data and services, involved people and physical premises.
2. *Building added value trees*. This step aims at making an assessment of how lower-level assets contribute to higher-level ones (see Fig. 2). Technically, the obtained added value tree is represented by an FCM influence matrix.
3. *Identification of threats*. For this purpose a general taxonomy of threats, e.g. an available ontology can be used and customized to the case analyzed. We use an asset-based model of threats, i.e. we identify threats that are related to a particular asset.
4. *Risk assessment for individual assets*. As a basic tool we use a questionnaire, in which various involved stakeholders reply to questions concerning the applied countermeasures. A list of standard countermeasures reflecting the best practices in the field of IT security is used and adapted to a particular set of assets. The outcome of this phase is an assignment of risk values (real numbers normalized to the interval [0, 1]) to assets.
5. *Risk aggregation*. This step consists of an FCM reasoning aiming at establishing how risks assigned to low-level assets accumulate to yield risk profiles of high-level assets.
6. *Interpretation of results*. In particular, this step may include *what if* analyses. If an application of additional countermeasures at various levels of individual assets is assumed, then step 5 is repeated.

5 Presentation of the SIMPOZ system

SIMPOZ project aims at building a highly configurable video surveillance system utilizing recent results of research on intelligent video analysis [10, 22, 43, 59], real-time video processing [36, 37] and image understanding [62, 63]. SIMPOZ is an acronym of the Polish project name that can be translated as: *System of Intelligent Monitoring of Objects and Areas of Special Importance*.

The project is divided into two phases: during the first of them, dedicated to development, the system components were built and a prototype instance serving as a proof-of-concept was integrated. The goal of the next phase is to provide an industrial deployment by reconfiguring and integrating the implemented earlier components. The deployment is to be performed by a company specialized in video surveillance installations. Currently, the development phase is completed and the deployment has just started. Hence, it is a perfect moment to perform evaluation of the system IT risks.

Video detection components within SIMPOZ system provide several monitoring functions [14]: violation of protected zones, detection of movement in a forbidden direction, object abandonment, theft, loitering, crowd gathering, vandalism (graffiti and devastation) and fight. Trajectory collision detection is a special feature dedicated to protection of such facilities as airports. In the delivered prototype and the first planned deployment we focused on three functions: zone violation and movement detection, object abandonment and trajectory collision.

As the developed system provides a number of components to be configured and tailored to specific needs, it necessitates in an integration platform. This role in SIMPOZ is assigned to a workflow subsystem. The workflow executes processes triggered by various events, for example an alarm occurrence or a user request. The processes coded in XPDL language define sequences of operations resulting in information flows, e.g. from video detector to operator station and alarm database, then to members of an intervention group or a security officer. A set of workflow participants or plugged in components can be flexibly chosen. Moreover, new processes can be easily defined to support end-user needs. Examples of processes elaborated for a prototype implementation can be found in [58].

Figure 4 shows the architecture of the SIMPOZ system. Video detectors perform surveillance tasks. Each of them has a certain degree of freedom in communicating with the rest of system using specialized interfaces designed in line with SOA (Service Oriented Architecture) approach. Information about an event detection triggers appropriate response procedures (written in XPDL language) executed by a workflow engine.

Video camera streams are registered by the Video Server. Registered material is protected by watermarking against forging. It can be used for preparing evidence data at request of law enforcement agencies.

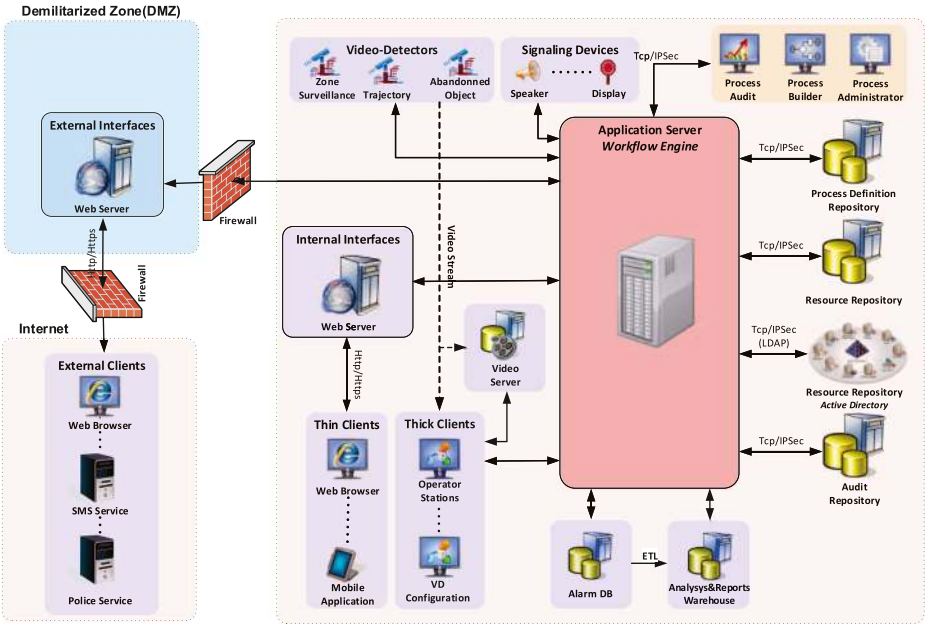

Fig. 4 Architecture of the SIMPOZ system

Operator station gives access to monitoring information, which comes from various types of detectors and running processes. In the case, when a suspicious situation is detected or an alarm is generated, the information about the event is passed to the operator. The operator can also communicate with intervention groups and other parties. In order to better assess the situation, current and archive video streams can be checked.

Interfaces of signaling devices allow processes managed by the workflow system to communicate with them and other elements of building automation systems (i.e. sirens, displays, emergency exit, illumination, floodgate, HVAC, etc.).

Mobile devices support communication between operators and members of intervention groups. Within designed processes, they are used for sending confirmation of the call reception and for reporting current status of an intervention.

External communication interfaces allow for sending automatic notification to emergency services (police, army, fire department) relevant to the detected danger. They can be also used to notify selected users about alarm situation with such means as SMS or e-mail.

The Alarm DB database records information on detected alarms and other events, e.g. operator decisions and messages sent. Their history is stored in Analysis&Reports Warehouse, which can be queried by Reports software tools.

The system includes also Process Definition Repository, Resource Repository, Active Directory providing basic authorization functions and Audit Repository storing a logged history of all processes executed by the workflow engine

As it can be observed, the workflow component participates in almost every information flow. Due to performance reasons, the video streams (from camera to operator station and videoserver) and ETL (feeding Analysis&Reports Warehouse) flow directly between components.

6 Risk analysis for the SIMPOZ system

In this section we perform risk analysis for SIMPOZ system according to the methodology defined in Section 4. It should be noted, that the system being assessed has not been deployed yet. The advantage of such analysis is that high risk areas, e.g. related to missing software functions can be earlier detected and corrected before the final transition. On the other hand, the disadvantage is that in many cases it is necessary to make an educated guess, for example to assume that that certain security standards and practices would be preserved during deployment realized by a professional company specialized in CCTV installations.

While selecting the scope of the risk analysis, we decided to include three areas: *IT security*, understood as protection against adversarial actions and accidental leak of sensitive data, *business continuity* that can be mapped on such quality attributes as reliability and availability of services and protection against *operational incidents*, such as errors in data or process execution. For a video surveillance system, they can stem from erroneous classification, software failures, camera configuration and unmotivated or untrained staff.

6.1 Identification of assets

The first step of the risk assessment was performed within two brainstorming sessions, in which the members of the project development team participated. During the sessions,

existent project documents and architectural views were analyzed and discussed. As the result more then 70 assets divided into 10 groups were identified:

1. Key processes: *Restricted zone violation&response*, *Abandoned object detection&response*, *Trajectory collision detection&response*, *Reporting* and *Evidence collection*. We have considered only those processes, which were implemented (designed and coded in XPDL language) in the prototype system.
2. Services: *Serv. Zone surveillance*, *Serv. Abandonned object*, *Serv. Trajectory*, *VD configuration*, *Video storage&watermarking*, *Alarm data storage*, *Streaming* and *LDAP (security)*.
3. External services: *SMS notification*, *E-mail notification*, *Police WS*, *Medical WS* and *Fire brigades WS*.
4. Infrastructure services: *Process execution*, *Service execution*, *Process repositories*, *Active Directory* and *Auditing*.
5. Data: *Stored video*, *Alarm data*, *Configuration data camera*, *Configuration data VD* and *Reports*.
6. Software modules: *Operator station*, *VD zone surveillance*, *VD abandonned object*, *VD trajectory*, *VD configuration*, *Alarm DB*, *Streaming (video repository)*, *Reporting & Analysis*, *Mobile application*.
7. Hardware: *Indoor camera*, *Outdoor camera*, *VD processor*, *Operator workstation*, *Workflow server*, *Alarm DB server*, *Video server*, *Warehouse server*, *Smartphone*, and *Network infrastructure*.
8. Communication: *Camera-VD*, *Camera-Operator Workstation*, *Intranet*, *Extranet (https)* and *Other*.
9. People: *Operator*, *Administrator*, *Camera maintenance*, *Process developer*, *Intervention group member Security officer* and *Management*.
10. Infrastructure provided by a third party (communications, electricity).

6.2 Building added value tree

The assets identified in the previous step constitute a network of dependent elements, i.e. the processes depend on services that are provided by software and hardware modules and refer to data which is stored and exchanged within the system as shown in Fig. 2. Influences between assets were identified based on architectural views, but particular weights were established during interviews with software architects and developers. They were then described in the form of an FCM influence matrix, using the following linguistic values: *high*, *significant*, *medium*, *low* and *none*.

To give an example, the utility of the *Restricted zone violation* process is *highly* influenced by the service *Serv. Zone surveillance*, significantly by *VD configuration*, at medium level by *LDAP (security)*. External services have low influences and from the data group: *Alarm data* has significant influence on the process. Analogous statements were made for all assets.

The resulting influence matrix E is usually very sparse. As during the assessment about 70 assets were considered, E has about 5000 elements, however, only 295 non-zero influences were indicated including default 1s at the matrix diagonal. Figure 5 shows probably the most dense part of the established matrix.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
	Process						Service							External service						Infrastructure servic		
	Restricted zone violation	Abandonned object detection	Trajectory colision detection	Reporting	Evacuation	Evidence collection	Serv. Zone surveillance	Serv. Abandonned object	Serv. Trajectory	VD configuration	Video storage&watermarking	Alarm data storage	Streaming	LDAP (security)	SMS notification	E-mail notification	Police WS	Medical WS	Fire brigades WS	Process execution	Service execution	Process repositories
Restricted zone violation	1	0	0	0	0	0	1	0	0	0.75	0	0	0	0.5	0.25	0.25	0.25	0	0	0.25	0	0.25
Abandonned object detection	0	1	0	0	0	0	0	1	0	0.75	0	0	0	0.5	0.25	0.25	0.25	0.25	0.25	0.25	0	0.25
Trajectory colision detection	0	0	1	0	0	0	0	0	1	0.75	0	0	0	0.5	0.25	0.25	0.25	0	0	0.25	0	0.25
Reporting	0	0	0	1	0	0	0	0	0	0	0	0.75	0	0.5	0	0	0	0	0	0.25	0	0.25
Evacuation	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0.25	0.25	0.25	0.25	0	0.25
Evidence collection	0	0	0	0	0	1	0	0	0	0	1	0.5	1	0.5	0	0	0.25	0	0	0.25	0	0.25
Serv. Zone surveillance	0	0	0	0	0	0	1	0	0	0.5	0	0.5	0	0.5	0	0	0	0	0	0	0	0
Serv. Abandonned object	0	0	0	0	0	0	0	1	0	0.5	0	0.5	0	0.5	0	0	0	0	0	0	0	0
Serv. Trajectory	0	0	0	0	0	0	0	0	1	0.5	0	0.5	0	0.5	0	0	0	0	0	0	0	0
VD configuration	0	0	0	0	0	0	0	0	0	1	0	0	0	0.5	0	0	0	0	0	0	0.25	0
Video storage&watermarking	0	0	0	0	0	0	0	0	0	0	1	0	0	0.5	0	0	0	0	0	0	0.25	0
Alarm data storage	0	0	0	0	0	0	0	0	0	0	0	1	0	0.5	0	0	0	0	0	0	0.25	0

Fig. 5 Partial influence matrix. Linguistic terms *high*, *significant*, *medium*, *low* and *none* are mapped to values: 1.0, 0.75, 0.50, 0.25 and 0 respectively

6.3 Threats

The identification of threats was based on available sources, e.g. [24, 38, 46], as well as on previous experience. The elicited list of threats to be considered in a vulnerability analysis comprised 62 elements grouped in twelve families corresponding to classes of assets.

The families are: *Process* (e.g bad design), *Software* (e.g. quality failures, lack of maintenance, malware), *Hardware* (quality failures, resource exhaustion), *Communications* (protocol weakness, service disruption), *Data* (confidentiality or integrity breach), *External services* (loss of PKI, SMS gate, PaaS, SaaS), *Physical infrastructure* (premises, electricity, air condition), *People*, *Natural conditions*, *Economical conditions* and *Legal*.

We maintain a set of threats as a reusable ontology formalized in OWL language. Figure 6 shows the taxonomy of threats applicable to the SIMPOZ system. (The presented tree view comes from the Protégé ontology editor.)

6.4 Risk assessment for individual assets

This step in the risk assessment process combines two activities identified in various methodologies, namely: the analyses of vulnerabilities and of effectiveness of countermeasures. Technically, the assessment is performed using questionnaires, in which answers reflecting best practices are attributed with weights describing their influence on a risk profile.

In the case of the SIMPOZ system, we used a questionnaire comprising about 190 questions divided into 12 groups of threats and countermeasures.

A logical structure of a sample questionnaire related to the video detector (VD) is presented in Table 1. For each question (a security feature), at most three answers (ratings) were defined. The answers were attributed with weights $q_{ij} \in [0, 1]$ that can be interpreted as their impact on the asset's risk profile. The weights are assigned after a voting process (questionnaires for the given asset type are prepared in advance and they represent "best practices"). Moreover, the influences of features can be differentiated with weight w_i shown in the last column of the table. These weights are not visible to the interrogated members of the development team, software architects and other involved stakeholders. The values that are underlined in Table 1 represent the answers for the SIMPOZ system.

Fig. 6 Taxonomy of threats identified for the SIMPOZ system

It should be observed, that a questionnaire defines in fact a structure of a Fuzzy Cognitive Map, in which weights express influences. Moreover, they were selected in a voting process, which is a typical practice of an FCM construction.

The risk RA_s for an asset s is calculated with the formula (7) based on the values of answers a_{ij} to k_s questions Q_i, $i = 1, \ldots, k_s$. Values 1 and 0 are used for positive and negative answers. Hence, $a_{ij} = 1$ if the j-th answer to i-th question is given and 0 in other cases.

$$RA_s = \frac{1}{W} \sum_{i=1}^{k_s} w_i \sum_{j=1}^{3} a_{ij} q_{ij}, \text{ where } W = \sum_{i=1}^{k_s} w_i \tag{7}$$

The normalization factor W in formula (7) plays an analogous role as an activation function in (2).

To illustrate the calculations, the answers to the questionnaire obtained during the interview with the project development team were marked in Table 1 by using underlined, bold font. The application of formula (7) yields the value 0.355, which indicates that threats are not fully neutralized by countermeasures (which would hold, if the calculated value were equal to 0). The values resulting from the questionnaires relating to particular assets were then used in the next step aiming at the calculation of aggregated risks.

6.5 Calculation of aggregated risk with FCM

The calculations were preceded by a normalization of the matrix of influences. While preparing the matrix we used five linguistic variables to describe influence: *high*, *significant*, *medium*, *low* and *none*. Then, they were mapped to weights {1.0, 0.75, 0.5, 0.25, 0} and for

Table 1 Risk assessment questionnaire related to the video detector (VD)

Question Q_i	$Answer_1$	q_{i1}	$Answer_2$	q_{i2}	$Answer_3$	q_{i3}	w_i
Is VD hardware protected against sabotage?	**yes**	0	no	1.0	partially	0.5	0.9
Is VD hardware protected against atmospheric conditions?	**yes**	0.2	no	0.8	partially	0.5	0.6
Is camera tampering detection implemented?	**yes**	0	no	1.0			0.7
Is a heartbeat protocol implemented?	yes	0.2	**no**	0.8		partially	0.7
Is a watchdog forcing the system restart in case of deadlock implemented?	yes, logged	0	**yes, not logged**	0.4	no	1.0	0.6
Is it possible to update the software remotely?	from intranet	0.2	from internet	0.8	**no**	0.0	0.5
Is implemented a formal procedure for software updating (e.g. required personal assistance of guard at place)?	yes	0.1	**no**	0.9			0.4
Are all events (alarms, problems, maintenance operations) logged in a local persistent storage (to be crosschecked during testing procedures)?	yes	0.1	**no**	0.8	partially	0.5	0.4
Are defined distinct roles to maintain VD software and perform audit log access?	yes, fine grained roles	0.2	**no**	0.8	yes, coarse grained roles	0.4	0.3
Does VD implement a testing mode (alarms are not sent or marked with a testing flag)?	yes	0	**no**	1.0	lack of information	0.5	0.5
Are notification on entering/leaving testing mode sent?	yes	0	**no**	1.0	lack of information	0.5	0.4
How VD configuration is stored?	centrally	0.5	locally	0.9	**both**	0.1	0.4
Does the communication camera - VD use SSL?	**yes**	0	no	1	no verification of SSL certificate	0.5	0.5
Does the communication VD - workflow use SSL?	**yes**	0	no	1	no verification of SSL certificate	0.5	1.0

Answers obtained during an interview with a project development team are marked with underlined bold font

each row $i = 1, \ldots, n$ the normalized values of influences were determined according to formula (8).

$$\overline{e}_{ij} = \begin{cases} 0, & \text{if } e_{ij} = 0 \\ \exp(m \cdot e_{ij})/Z_i, & \text{if } e_{ij} \geq 0 \end{cases}, \tag{8}$$

where $Z_i = \sum_{\substack{j=1 \\ e_{ij} \neq 0}}^{n} \exp(m \cdot e_{ij})$ and m is a positive constant (in the calculations the value $m = 1.0$ was used) and e_{ij} describes an influence of i low-level assets on j a high-level asset.

Such normalization gives a probability distribution. Motivation for assuming the assumed distribution stems from the Game Theory. Suppose, that a high-level asset a_h depends on low-level assets $a_{l_1}, \ldots, a_{l_k}$, with influences $e_{hl_1}, \ldots, e_{hl_1}$. If a *threat agent* treated as an adversarial player is to select a low-level asset to launch an attack on, it should choose an element a_{l_m} giving the highest influence e_{hl_m} on the risk profile of a_h. However, the player can make errors in an estimation of influences. Resulting probability of adversarial actions depends on distribution of errors, which, in general, is difficult to track. However, assuming a double exponential distribution of errors, we arrive at a *logit* model [3] given by the formula (8).

For the final calculation of aggregated risks two sequences of vectors were constructed:

$$\alpha^{nr} = A^{nr}(0), \ldots, A^{nr}(i), \ldots$$

and

$$\alpha^{r} = A^{r}(0), \ldots, A^{r}(i), \ldots$$

by successively applying an FCM state equation (2).

The *no-risk sequence* α^{nr} starts with a vector $A^{nr}(0)$, in which all elements expressing the utility of assets are set to 1. For the *risk sequence* α^{r} the initial vector $A^{r}(0)$ is the difference of vectors of asset utilities $A^{nr}(0)$ and related risks RA established in the previous phase, using formula (7): $A^{r}(0) = A^{nr}(0) - RA$.

Finally, by subtracting the corresponding elements of α^{nr} and α^{r} we obtain a sequence of aggregated risk values

$$\rho = R(0), \ldots, R(i), \ldots,$$

where $R(i) = A^{nr}(i) - A^{r}(i)$. This sequence converges to values that express aggregated risks for all assets at different levels of the added value tree.

Values of aggregated risks for high-level assets: processes, services and data are presented in Tables 2, 3 and 4 respectively. For comparison, risk levels obtained by using three activation functions: S_{cut}, S_{exp} and S_{tanh} defined by formulas (3), (4) and (5) are reported.

Table 2 Aggregated risks for processes

	Risk - S_{cut}		Risk - S_{exp}		Risk - S_{tanh}	
Process	calc.	max	calc.	max	calc.	max
Restricted zone violation	0.1859	0.5640	0.0156	0.0868	0.0277	0.1657
Abandoned object detection	0.1788	0.5536	0.0148	0.0831	0.0263	0.1590
Trajectory collision detection	0.1943	0.5699	0.0170	0.0892	0.0304	0.1700
Reporting	0.1564	0.4609	0.0121	0.0593	0.0210	0.1123
Evidence collection	0.1417	0.4475	0.0118	0.0534	0.0205	0.1022

Table 3 Aggregated risks for services

	Risk - S_{cut}		Risk - S_{exp}		Risk - S_{tanh}	
Process	calc.	max	calc.	max	calc.	max
Serv. Zone surveillance	0.2041	0.6424	0.0166	0.1071	0.0292	0.2058
Serv. Abandonned object	0.2041	0.6424	0.0166	0.1071	0.0292	0.2058
Serv. Trajectory	0.2546	0.6785	0.0254	0.1246	0.0469	0.2345
VD configuration	0.2380	0.6626	0.0225	0.1241	0.0411	0.2321
Video storage & watermarking	0.1184	0.4161	0.0082	0.0436	0.0136	0.0850
Alarm data storage	0.1165	0.3967	0.0081	0.0405	0.0134	0.0785
Streaming	0.1210	0.4479	0.0084	0.048	0.0140	0.0942
LDAP (security)	0.1150	0.419	0.0080	0.0442	0.0131	0.0866

Each value given in *calc.* column is accompanied by its range (maximum level) in *max* column. The later is determined by switching off safeguards. In some cases, however, e.g. related to physical protection, we have made assumptions that a safeguard will be present.

The comparison indicates that qualitative results for all activation functions are quite similar. Basically, higher risk levels are attributed to all services and processes involving detection, i.e. *Restricted zone violation*, *Abandoned object detection* and *Trajectory collision detection*. It is quite natural, as they are influenced by more risk factors. From those, *Trajectory collision detection* returned the highest risk. This reflects the fact that the camera observing an outdoor scene is exposed to weather conditions, e.g. fog, snow, heavy rain, which cannot be compensated.

6.6 Results of assessment

Our findings indicate acceptable level of aggregated risks related to assets placed at the top of the utility tree (processes, data and services). The highest determined risks never exceeded 40 % of the reference value, what places them at low or medium level.

Regardless of a method used, the benefit of making a risk assessment is that the whole process involves asking questions related to architectural decisions. In consequence, several suggestions for improvements can be made, what in turn, may decrease risks.

Table 4 Aggregated risks for data

	Risk - S_{cut}		Risk - S_{exp}		Risk - S_{tanh}	
Process	calc.	max	calc.	max	calc.	max
Stored video - utility	0.1045	0.4386	0.0072	0.0464	0.0119	0.0910
Stored video - confidentiality	0.1045	0.4386	0.0072	0.0464	0.0119	0.0910
Alarm data	0.1247	0.5042	0.0087	0.0568	0.0145	0.1137
Configuration data camera	0.1247	0.5042	0.0087	0.0568	0.0145	0.1137
Configuration data VD	0.1247	0.5042	0.0087	0.0568	0.0145	0.1137
Reports	0.1364	0.4263	0.0096	0.0445	0.0160	0.0870

During the analysis several problems were found. Limited by the paper space, we focus on issues pertaining to the Videodetector, which was discussed in Section 6.4.

1. Lack of heartbeat function may cause that a VD failure may be not noticed for a long time. We suggested to add this functionality, moreover to designate a server that would keep track of states of all video detectors.
2. Although a watchdog implementing self-restart was implemented, such event is not logged. Hence, there is no information on the frequency of failures. After the VD system is restarted, the detection algorithms build their background models. In consequence, during at least 90 seconds the scene is unattended. If the restart frequency is high, e.g. 20 times a day, the total time, during which automatic video analysis can be not effective can reach 30 minutes. It was proposed to save the background model on a regular basis. In case of restarting, last saved background model can be used.
3. Videodetector does not implement a testing mode. Hence, false alarms can be generated or it may happen that an operator is not informed after the test were completed.

Suggested implementation of the heartbeat function, restart logging and testing mode for the Videodetector may decrease the risk calculated according to the questionnaire in Table 1 from 0.355 to 0.139. This what would significantly improve the risk assigned to detection functions within the system.

7 Conclusions

In this paper we study an application of a a new method for risk assessment of IT systems based on Fuzzy Cognitive Maps. It was originally developed to establish risks for a telemedicine system [60, 61], however, our intention was to make it general enough, to be applied to a variety of IT systems. The method include steps present in various standards and methodologies: identification of assets, threats, analysis of vulnerabilities and effectiveness of countermeasures, however, it relies on FCM reasoning to calculate risks. A cornerstone of the proposed method is *added value tree* expressing dependencies between assets. A salient feature of the method is, that it uses an abstract term *utility* (and a loss of utility caused by a threat) in place of financial loss. This makes the method applicable for IT system, for which financial loss is difficult to estimate.

The methodology presented in the paper is general, however the focus on a particular system or a class of systems is implemented in the step 4: *Risk assessment for individual assets*. The assessment is based on a list of questions related to implemented countermeasures (reflecting best practices in the field) which are specific to the system type. The list of questions, together with their influences on a risk profile are prepared by domain experts in a kind of a voting process. Moreover, such list can be reused during assessment of another systems (from a given domain/class).

In this paper the authors make two major contributions. Firstly, the problem of IT security assessment for a video surveillance system is tackled. As it was indicated in Section 2.3, till now this topic has been addressed by merely a few papers. Secondly, an application of the risk assessment method to a new class of IT system is described.

Following the method guidelines, the tasks performed during risk assessment were as follows: preparing lists of assets based on architectural views and interviews, building influence matrix reflecting an added value tree, identifying threats, calculating non-aggregated risks related to assets with use of questionnaires based on best practices and finally performing reasoning with FCM techniques. It should be mentioned, that the analyzed video

surveillance system was far more complex that the example discussed in [61], as it combined various technologies: video detection, workflow and database management. Moreover, the number of assets, which were considered during evaluation, doubled.

An important result of the performed risk assessment was the proposal of several small extensions and functions that might be introduced to ameliorate the developed system. In spite the fact, that the suggested changes were not so much extensive, they significantly improved the system reliability and robustness.

Another advantage of the method is that the prepared risk assessment questionnaires (c.f. Table 1) related to various types of assets can be reused for various system deployments. In case of changes or new system instances only last steps of the risk analysis (filling in questionnaires and performing risk aggregation) are required.

The proposed method can be considered as a *lightweight* approach to risk assessment, suitable for small and medium size systems [60]. In the case of the SIMPOZ system, the data was collected during five interviews and brainstorming sessions, in the meantime questionnaires used in previous analyzes by the assessment team were adapted to reflect specific assets and threats.

Lessons learned indicate, that the proposed method is an efficient and low-cost approach, giving instantaneous feedback and enabling reasoning on effectiveness of a security system. It can be considered as an alternative to heavy assessment processes defined by standards.

References

1. ADVISOR project (2013). http://www-sop.inria.fr/orion/ADVISOR
2. Aguilar J (2005) A survey about fuzzy cognitive maps papers (Invited Paper). Int J 3(2):27–33
3. Anderson S, De Palma A, Thisse J (1992) Discrete choice theory of product differentiation. MIT Press, Boston
4. Axelrod RM (1976) Structure of decision: the cognitive maps of political elites. Princeton University Press
5. (2013). Axis comm. AB. URL http://www.axis.com
6. Baudrit C, Dubois D, Guyonnet D (2006) Joint propagation and exploitation of probabilistic and possibilistic information in risk assessment. IEEE Trans Fuzzy Syst 14(5):593–608
7. Birolini A (2000) Reliability engineering: theory and practice, 3rd ed. Springer Verlag, Berlin
8. Birolini A (2013) Bosch intelligent video analysis (IVA). http://www.boschsecurity.us
9. Bowles JB, Wan C (2001) Software failure modes and effects analysis for a small embedded control system
10. Brémond F, Thonnat M, Zúñiga M (2006) Video-understanding framework for automatic behavior recognition. Behavior Research Methods 38(3):416–426. doi:10.3758/BF03192795. http://dx.doi.org/10.3758/BF03192795
11. Cavallaro A (2007) Privacy in video surveillance 3
12. Cervesato I., Meadows C (2003) Fault-tree representation of NPATRL security requirements
13. Chen XZ (2006) Hierarchical threat assessment and quantitative calculation method of network security threatening state. J Softw 17(4):885–897
14. Chmiel W, Kwiecień J, Mikrut Z (2012) Realization of scenarios for video surveillance. Image Process Commun 4:231–240
15. Cox IJ, Kilian J, Leighton FT, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process 6(12):1673–1687
16. Craft R, Vandewart R, Wyss G, Funkhouser D (1998) An open framework for risk management, p 1
17. CRAMM CRAMM. http://www.cramm.com/. Accessed Jan 2013
18. ENISA Inventory of risk management / risk assessment methods. http://rm-inv.enisa.europa.eu/methods/rm_ra_methods.html. Accessed Jan 2014
19. Eom JH, Park SH, Han YJ, Chung TM (2007) Risk assessment method based on business process-oriented asset evaluation for information system security. In: Proceedings of the 7th international

conference on Computational Science, Part III: ICCS 2007, ICCS '07. Springer-Verlag, Berlin, pp 1024–1031
20. Fridrich J (1998) Image watermarking for tamper detection. In: 1998 International conference on image processing, 1998, ICIP 98. Proceedings, vol 2. pp 404–408. doi:10.1109/ICIP.1998.723401
21. Furht B, Kirovski D (2005) Multimedia Security Handbook. CRC Press
22. Geerinck T, Enescu V, Ravyse I, Sahli H (2009) Rule-based video interpretation framework: Application to automated surveillance. In: 5th international conference on image and graphics, 2009, ICIG '09, pp 341–348. doi:10.1109/ICIG.2009.140
23. Granick J (2006) Security versus privacy: the rematch. Wired news
24. Guttman B, Roback EA (1995) An introduction to computer security: the NIST handbook. Secur 800(12):1–290
25. Haering N, Venetianer P. L, Lipton A (2008) The evolution of video surveillance: an overview. Mach Vis Appl 19(5-6):279–290. doi:10.1007/s00138-008-0152-0. http://dx.doi.org/10.1007/s00138-008-0152-0
26. Hagiwara M (1992) Extended fuzzy cognitive maps. In: Proceedings of the IEEE international conference on fuzzy systems, IEEE computer society, pp 795–801
27. Han YJ, Yang JS, Chang BH, Na JC, Chung TM (2004) The vulnerability assessment for active networks; model, policy, procedures, and performance evaluations. In: ICCSA (1), pp 191–198
28. Hubbard D, Evans D (2010) Problems with scoring methods and ordinal scales in risk assessment. J Res Dev 54(3):1–10
29. IndygoVision (2013) http://www.indygovision.com
30. Institute for Computer Sciences and Technology (1979) Guideline for automatic data processing risk analysis. National Bureau of Standards, Institute for Computer Sciences and Technology
31. ISO/IEC (2011) Information technology – security techniques – information security risk management, ISO/IEC 27005:2011. Tech. rep., International Organization for Standardization
32. Jetter A, Schweinfort W (2011) Building scenarios with Fuzzy Cognitive Maps: an exploratory study of solar energy. Futures 43(1):52–66. doi:10.1016/j.futures.2010.05.002
33. Karimaa A (2009) Security aspect of the complexity of modern surveillance systems - an experience report. In: 2009 14th IEEE international conference on engineering of complex computer systems, pp 120–125. doi:10.1109/ICECCS.2009.47
34. Kosko B (1986) Fuzzy Cognitive maps. Int J of Mach Stud 24:65–75
35. Kosko B (1992) Neural networks and fuzzy systems: a dynamical systems approach to machine intelligence. Prentice Hall
36. Kryjak T, Komorkiewicz M, Gorgon M (2011) Real-time moving object detection for video surveillance system in FPGA. In: Nurmi J, Ahonen T (eds) DASIP, pp. 209–216. IEEE
37. Kryjak T, Komorkiewicz M, Gorgon M (2012) FPGA implementation of camera tamper detection in real-time. In: DASIP, IEEE, pp 1–8
38. Landoll DJ (2005) The security risk assessment handbook: a complete guide for performing security risk assessments. Auerbach Publications
39. Lazzerini B, Mkrtchyan L (2011) Analyzing risk impact factors using extended fuzzy cognitive maps. IEEE Syst J 5(2)
40. Lin ET (2001) An overview of security issues in streaming video. In: Proceedings of the international conference on information technology: coding and computing, ITCC '01, IEEE computer society, Washington, pp 345–. http://dl.acm.org/citation.cfm?id=876870.878133
41. Lin ET (2013) Mirasys Carbon VMS. http://www.mirasys.com
42. Modarres M, Kaminskiy MVK (1999) Reliability engineering and risk analysis. CRC Press
43. Oliver N, Rosario B, Pentland A (2000) A bayesian computer vision system for modeling human interactions. IEEE Trans Pattern Anal Mach Intell 22(8):831–843. doi:10.1109/34.868684
44. Ozesmi U, Ozesmi S (2004) Ecological models based on people's knowledge: a multi-step fuzzy cognitive mapping approach. Ecol Model 176(1-2):43–64. doi:10.1016/j.ecolmodel.2003.10.027
45. Papageorgiou E (2012) Learning algorithms for fuzzy cognitive maps: A review study. IEEE Trans Syst Man Cybern Part C Appl Rev 42(2):150–163. doi:10.1109/TSMCC.2011.2138694
46. Ross RS (2011) Guide for conducting risk assessments. NIST Special Publication NIST SP 800-30rev1 (September), 85
47. Schneier B (1999) Attack trees. Dr Dobb's J 24(12):21–29
48. Securiton AG (2013) http://www.securiton.com
49. Senior A (2009) Protecting privacy in video surveillance, Springer
50. Senior A Sherwood Applied Business Security Architecture: SABSA. http://www.sabsa-institute.org/the-sabsa-method. Accessed Jan 2013
51. Soo Hoo KJ (2000) How much is enough: A risk management approach to computer security. Ph.D. Thesis, Stanford University, Stanford. AAI9986202

52. Stamatis DH (2003) Failure mode and effect analysis: FMEA from theory to execution. Milwaykee. ASQ Quality press, Wisconsin
53. Stathiakis N, Chronaki C, Skipenes E, Henriksen E, Charalambus E, Sykianakis A, Vrouchos G, Antonakis N, Tsiknakis M, Orphanoudakis S (2003) Risk assessment of a cardiology ehealth service in hygeianet
54. Sun L, Srivastava RP, Mock TJ (2006) An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. J Manage Inf Syst 22(4):109–142
55. Supervisor EDP (2010) The edps video-surveillance guidelines. https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/Guidelines
56. Szpyrka M, Jasiul B, Wrona K, Dziedzic F (2013) Telecommunications networks risk assessment with Bayesian networks. In: Computer information systems and industrial management proceedings of the 12th IFIP TC8 international conference CISIM 2013, LNCS, vol 8104, pp 277–288. Springer
57. Szwed P (2013) Application of fuzzy cognitive maps to analysis of development scenarios for academic units. Automatyka/Automatics 17(2):229–239. doi:http://dx.doi.org/10.7494/automat.2013.17.2.229
58. Szwed P, Chmiel W, Jedrusik S, Kadluczka P (2013) Business processes in a distributed surveillance system integrated through workflow. Automatyka/Automatics 17(1):127–139
59. Szwed P, Komorkiewicz M. (2013) Object tracking and video event recognition with fuzzy semantic Petri nets. In: Ganzha M, Maciaszek LA, Paprzycki M (eds) FedCSIS, pp. 167–174
60. Szwed P, Skrzynski P (2014) A new lightweight method for security risk assessment based on fuzzy cognitive maps. J Appl Math Comput Sci 24(1):213–225
61. Szwed P, Skrzynski P, Grodniewicz P (2013) Risk assessment for SWOP telemonitoring system based on Fuzzy Cognitive Maps. In: Dziech A, Czyżewski A (eds) Multimedia communications, services and security, communications in computer and information science vol. 368, pp. 233–247. Springer, Berlin. doi:10.1007/978-3-642-38559-9
62. Tadeusiewicz R (2011) Introduction to intelligent systems. In: The industrial electronics handbook - intelligent systems, pp. 1–12. CRC Press, Boca Raton
63. Tadeusiewicz R, Ogiela M, Szczepaniak P (2009) Notes on a linguistic description as the basis for automatic image understanding 19(1):143–150. doi:10.2478/v10006-009-0013-7. http://dx.doi.org/10.2478/v10006-009-0013-7
64. Tangwongsan S, Kassuvan S (2001) A security model of voice eavesdropping protection over digital networks
65. Tangwongsan S, Kassuvan S (2013) Verint Systems Inc. http://www.verint.com
66. Vesely WE, Goldberg FF, Roberts NH, Haasl DF (1981) Fault tree handbook, technical report nureg-0492
67. Vu Vt, Bremond F, Thonnat M (2003) Automatic video interpretation: A novel algorithm for temporal scenario recognition. In: Proceedings 8th international joint conference artificial intelligence, pp. 9–15
68. Wang Y, ea (2003) Research on and application of the analyzing method of network security based on security case reasoning. Minitype Comput Syst 24(12):2082–2085
69. Xue-mei X, Xiao-yu M (2009) Risk management of social public security video surveillance project based on life cycle theory. In: International conference on management and service science, 2009, MASS '09, pp. 1–4

Piotr Szwed received the M.Sc. degree in electronics and control engineering in 1988 and Ph.D. in computer science in 1999 both from the AGH University of Science and Technology in Krakw, Poland. Since 1999 he has been working there as an assistant professor. Currently he is with the Department of Applied Computer Science at the Faculty of Electrical Engineering, Automatics, Computer Science and Biomedical Engineering. His research topics include various aspects of software engineering including modeling, assessment of software architectures and formal verification. He is particulary interesed in fuzzy reasoning, application of ontologies and Petri nets.

Pawel Skrzynski Graduated AGH University of Science and Technology: received M.Sc. in Computer Science 2002 AND M. Sc. in Business and Management 2004. Received Ph. D. in Computer Science in 2011 at the same University. Interested in Enterprise Architecture, software development, distributed systems, software and IT security, Java technologies, mobile technologies. Works at Department of Applied Computer Science and has been involved in development and management of several big IT projects including: internet/mobile banking systems for the biggest polish banks, VISP project (EU FP6). Married, two children.

Wojciech Chmiel received his Ph.D. in Automatics from the AGH University of Science and Technology in Krakow and has been affiliated with this University since 1992. He is associated with the Department of Automatics and Biomedical Engineering in the Faculty of Electrical Engineering, Automatics, Computer Science and Biomedical Engineering. He is the author of several research papers and main research interests are focused on the area of operation research, approximation algorithms, automated reasoning methods, modeling discrete optimization problems, workflow management systems, fuzzy optimization and decision making. He has taken part in several international research projects in optimization and artificial intelligence area.