Journal of Visual Languages and Computing 25 (2014) 650–657

Contents lists available at ScienceDirect

Journal of Visual Languages and Computing

journal homepage: www.elsevier.com/locate/jvlc

Short Paper

A system design for surveillance systems protecting critical infrastructures[☆]

Erland Jungert[a,*], Niklas Hallberg[a,b], Niclas Wadströmer[a]

[a] *FOI (Swedish Defence Research Agency)Box 1165, SE-581 11 Linköping, Sweden*
[b] *School of Computer Science and Communication KTH Royal Institute of Technology SE-100 44 Stockholm, Sweden*

ARTICLE INFO

Article history:
Received 1 October 2014
Accepted 1 October 2014
Available online 14 October 2014

Keywords:
Security systems
Surveillance systems
Critical infrastructure
User requirements

ABSTRACT

Critical infrastructures are attractive targets for attacks by intruders with different hostile aims. Modern information and sensor technology provides abilities to detect such attacks. The objective of this work is to outline a system design for surveillance systems aimed at protection of critical infrastructures, with the focus on early threat detection at the perimeter of critical infrastructures. The outline of the system design is based on an assessment of stakeholder needs. The needs were identified from interviews with domain experts and system operators. The system design of the surveillance system and the user requirements in terms of capabilities were then determined. The result consists of the system design for surveillance systems, comprising the systems capabilities, the systems structure, and the systems process. The outcome of the work will have an impact on the implementation of the surveillance systems with respect to the sensors utilized, the sensor data algorithms and the fusion techniques.

1. Introduction

In recent times, the risk for critical infrastructures to be subject to attacks from various groups of terrorists or criminals has become increasingly high and therefore they must be protected. To accomplish sufficient surveillance, modern information technology could be used. Such surveillance systems need to be based on modern sensors and sensor systems with advanced sensor-data analysis and data fusion. However, to accomplish systems of high quality, they must be based on the stakeholders' needs, so that needed capabilities can be provided. The means of these capabilities are to support the system operators in their work to handle upcoming events and incidents enforced by intruders and to protect the facilities from external attacks [1]. Hence, to accomplish such surveillance systems it is essential to put a sufficient amount of resources on the early stages of the development, which is to identify the stakeholder needs and to define the user requirements in terms of system capabilities. To enhance the realization of such systems they should be based on an adequate system design. Thereby, the probability to get useful systems that provide the means to support handling of incidents and crisis management will increase and help to avoid or at least minimize the consequences of attacks on critical infrastructure facilities. An approach that can be taken to determine the system design may be based on the assessment of stakeholder needs through series of interviews with a number of especially appointed domain experts and security personnel.

1.1. The P5 project

The work presented in this article has been carried out as a part of *The Privacy Preserving Perimeter Protection*

[☆] This paper has been recommended for acceptance by Shi Kho Chang.
[*] Corresponding author.
E-mail addresses: jungert@foi.se (E. Jungert), nikha@foi.se (N. Hallberg), niclas.wadstromer@foi.se (N. Wadströmer).

http://dx.doi.org/10.1016/j.jvlc.2014.10.007
1045-926X/

Project (P5), co-funded by the European Union. The objective of the project is to demonstrate an intelligent perimeter surveillance system that can operate in all weather and light conditions and with privacy preserving properties. The system will monitor the area just outside the boundary of critical infrastructure facilities and, thereby, be able to provide early warnings of terrestrial and airborne threats. The system need to have a low false alarm rate, e.g., due to animals and other innocuous events, combined with high level of threat detection sensitivity.

1.2. The objective and delimitations

The objective of the work presented in this article is to design a surveillance system aimed at protection of critical infrastructures. In particular, the surveillance systems should be able to support the security staff at the facility to detect and respond to attacks from intruders at an early stage and thus the protection and surveillance of the perimeter of the facilities will be in focus to make it possible to give early warnings. The system should alert the operators of threats carried out by different types of objects, (persons, vehicles, etc.). Eventually, these capabilities of warnings should be realized by state-of-the-art sensor solutions. However, it is out of scope of the work presented in this article to determine what sensors and what methods for sensor-data analysis and fusion to use.

2. The physical context

The physical context in which surveillance systems of critical infrastructures operate is varying from facility to facility; especially with respect to the perimeter, which also differ with respect to the type of infrastructure that should be protected. Generally, the critical infrastructure facility can be described as containing a central complex, i.e., the surveilled area of the critical infrastructure with one or several buildings and installations as illustrated in Fig. 1.

The surveilled area is surrounded by the perimeter that differs in width with respect to its extension. Thus, in general, the perimeter can be defined as illustrated in Fig. 1 where the perimeter is made up by the restricted area, the boundary of the facility, a strip of the outside area, and the airspace above the facility. In some cases, there is no restricted area and thus the boundary of the facility coincides with the boundary of the surveilled area. The outside strip of concern must also be determined from facility to facility. To observe is also that, in some cases, the facility may in part be surrounded by water. The terrain type of different facilities, perimeters differ and the surveillance system must be able to adapt to such differences in the environment.

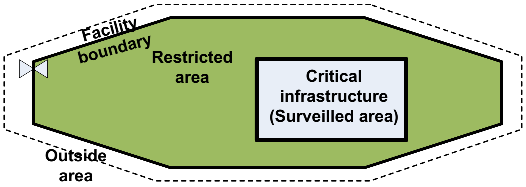

Fig. 1. An illustration of an extended perimeter surrounding a critical infrastructure facility; the perimeter is corresponding to the restricted area, the facility boundary and a strip outside the facility boundary including the airspace above the whole facility.

3. Methods

The work was carried out with two main activities: a needs assessment activity and an outline of the design of the surveillance systems.

3.1. Needs assessment

The needs assessment was performed in six steps. The initial step was to determine who the stakeholders are, which of them should be given the opportunity to influence the development of the system, and how their statements should be collected. The work was carried out during a workshop, involving the project management, in which different categories of stakeholders were identified, such as systems operators, business managers, and security managers. Thus, it was decided which categories of stakeholders should be provided the opportunity to influence the design of the system. The second step was to interview the stakeholders to get statements concerning the surveillance system. The respondents were selected as good representatives of the selected stakeholder categories. Interview questions that focus on the specific problems subject to the studies were developed based on the critical incident technique (CIT). CIT is as a technique for collecting observed incidents that have significance impact on the performing activities [2]. Each interview was carried out by two persons; one that asked the questions and another responsible for recording the answers through note taking. The third step of the needs assessment was to interpret the collected statements to determine the actual needs. When asking stakeholders about what needs they have, they will use descriptions of, e.g., problematic situations that they have experienced and technical solutions that they believe can be useful to them [3]. The voice of the customer table (VCT) was used for analyzing statements to reveal the actual needs [1,4]. The outcome from this step was a large set of unstructured and unsorted needs. An illustration of the use of the VCT can be found in Fig. 2. In the first column the captured statements are inserted, one row for each statement. The following columns describe an analysis of who asked for the need, what they want to do with it, when they want to do it, where they would like to do it, why they would do it, and how they would do it. Eventually, in the last column the concluded need can be filled in, hopefully with a correct understanding of what the statement really implied.

The fourth step was to thoroughly analyze the identified needs, to unify the formulation of the needs and, thereby, identify and discard duplicates of needs. Further, the analysis also included to determine if any needs had been left out, and if appropriate add the missing ones. To accomplish this and due to the amount of needs, it was necessary to categorize the needs. This step was performed by using affinity diagrams and hierarchy diagrams [4]. The fifth step was to validate