SAFETY & SECURITY MANAGEMENT CONCERNING SPORT EVENTS

Julien Piwowar*[*]
PACIFA decision
Troyes, France
E-mail: julien.piwowar@pacifa-decision.com

Patrick Laclémence
University of Technology of Troyes
Troyes, France
E-mail: patrick.laclemence@utt.fr

ABSTRACT

A lot of industries or power plants are using multicriteria models to improve the management of their safety and security systems. But most of the accidents that occur are due to technical failures or human errors and find rarely their origins in intentional malevolent acts, more unpredictable. After having established a wide scope of necessity to define a complete framework including multicriteria applications to face up various threats of agressions, we noticed that current targets are infrastructures receiving sport events, and particularly football stadiums.
So, we have developped an entire process associated to a software wich permits to assess and represent vulnerabilities around those complex systems. The final result provides to the safety manager a dynamic and decisional tool. It is then possible to efficiently build and optimize the security system according to real needs at a given moment by confronting potential attacks and various responses choosen among a list of appropriated options of prevention and protection.

Keywords: Decision Making, Security, Safety, Optimization, Human Resources Management

1. Introduction

Sadly, violence and football are often linked up in media and press releases. Even if it is a real fact that violent events are arising each week around football stadiums or surroundings, that violence comes from various origins, such as politics or historical rivalities between supporters (Pilz, 2009). And we are not looking about those sociological points, because that rage is just a reflect of our society and we can not manage it with any analytical tool or mathematical framework.
So, we are just trying to provide to managers and stakeholders of such infrastructures a dynamical tool to make the decision to set up the best security plan.

2. Concept

We have developped a thesis (Piwowar, 2010) in the University of Technology of Troyes in France to define a step by step approach to assess vulnerabilities around critical infrastructures. For doing that, we have worked on a real case, which is the "*Stade de l'Aube*", Stadium of Troyes where is playing the club of ESTAC in first league at the moment of we were evaluating threats.
We have processed as the following:

- 1 - Systemic analysis;
- 2 - Interactions between aggressors' profiles and systems: ranking system;
- 3 - Vulnerabilities assessment and determination of key places;

[*] Corresponding author

- 4 - Building of attacks scenarios;
- 5 - Updating the security systems.

We have chosen a stadium because that kind of infrastructure gathers several interesting parameters in order to observe the pertinence of such a methodology (Branscomb, 2004):

- Numerous of people (with various social origins);
- A reduced space in a limited time (average of 50.000 persons in a 3miles square area during 3 hours)
- Dependence to geopolitical context;
- High mediatic visibility.

The experimental application has permitted to us to test our mathematical development of assessment of vulnerabilities and criticities that we are going to explain below.

2.1 Criticity assessment

First of all, we want to precise what difference we make between vulnerability and criticity because it is fundamental to understand why we really focus on criticity more than vulnerability.

A point of the global system could be very vulnerable with zero defensive protections, but totaly not critic because of it non-importance for the whole system integrity. For example a door unlocked or a broken fence on the far surroundings of the main area is really vulnerable but not really critic because of the numerous of other check points until to link the main area.

That is why we are going to assess and be aware about critical spots on the site. To calculate them, we are using a multicriteria model based on the model of B.C. Ezell (Ezell, 2004). We have added to it several specific inputs or forms, such as distinguish the "intrinseque criticity" (C(x)) and the "target criticity" (C'(x)) of an access.

To estimate intrinseque criticity, we use the following function:

$$C_{(x)} = w{*}v_{(xi)} \qquad (1)$$

with

$$v_{(xi)} = p_1.d_1 + p_2.d_2 + p_3.d_3 + p_4.r \qquad (2)$$

and

$$\Sigma\, p_j = 1 \qquad (3)$$

The criteria are the following:

- w: weight of importance of the component within the system;
- d_1: dissuasion – apparent difficulties which could annoy an attacker;
- d_2: detection – probability to detect the attacker before he could do his malevolent act;
- d_3: delay – time to release an action to disturb the aggressor;
- r: response – time to stop or mitigate the effects of the attack (including time of logistic and organizational delay).

The parameters pi permits to give alternatives of the importance we want to apply on each of the criterion {d1, d2, d3, r}. According to the judgements or the willingness of the head of security of the infrastructures we work for, we could determine using the eigenvector which rate will match the most with managers expectation to assess criticity and so to protect the system (Saaty, 1990).

That point is fundamental because it is going to insure that none of the systems we work for are using the same mathematical ratios to assess vulnerable spots on their infrastructure and that protect them (and us) to malicious people which could be tempted to make a parrallel study or copy to foresee where are the critical areas (Piwowar, 2009).

Then, a simple analytic scale is necessary in order to assess easily criteria. We propose one for example between 1 and 6 with differents sensibilities (Figure 1 below) which are going to guide (as a tutorial) the experts in their assessment of each component of the system.

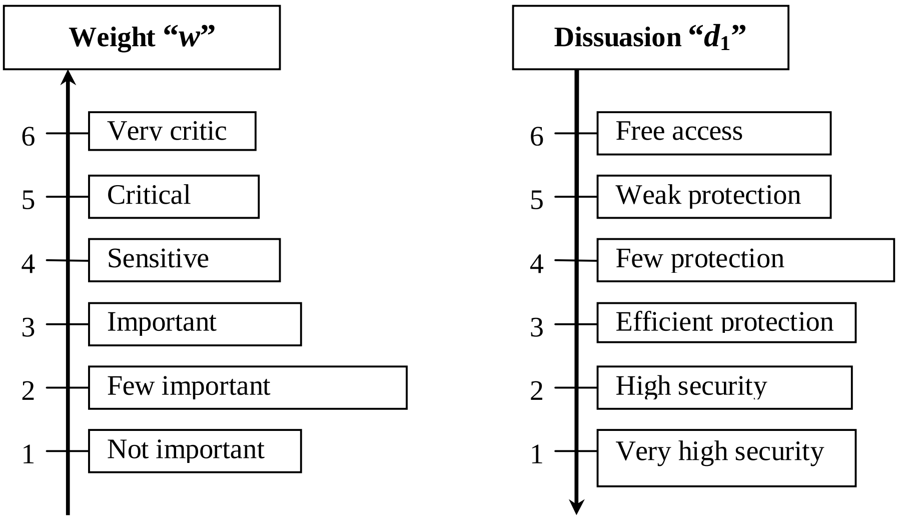

Figure 1: An example of a scale of assessment

All the judgments of the experts are then updated with calculation of uncertainty (based on deviations and fuzzy logics about their own experience within the studied system), and the results are inputting on the database.

Then, a new criticity ($C'_{(xi)}$) assessment can be obtained according to the geographical links within the system following the expression:

$$C'_{(x)} = w*\Pi(v_{(xij)} .y_{ij}) \tag{4}$$

with y_{ij} representing the "distance" between an access i and j.

So it permits to watch the plausibilities of attacks depending of the different ways to reach it. Added to that, it is possible to define aggressors profiles, geopolitical context at the moment of the study to precise the reality of an event organisation. And so, it will be possible to determine the real needs in order to set up the best security plan with video monitorings or staffs availabilities (stewards and police).

3. Set up the security plan

All the parameters we have described before are loading in a special software interface that we have created in the company PACIFA decision and it permits to simulate in a dynamical 3D software the impact of a dispositive of security facing up potential threats or simply to manage crowds interactions.

So, as we can see on the Figure 2 below, it is possible to look at the critical scale of each access and a colour code is going to represent the spot which are "over-secured" (in blue in the model) and on the other side, the ones which are "under-secured" (in red in the model).

Then, it is really easy to make simulations of optimization because the user just need to drop or add staff element to observe the response in term of criticity of the access (obviously each kind of staff element are not giving the same "security answer" according to his experience or his formation: a policeman is going to reduce the vulnerability more than a first-year experience steward at the same place).

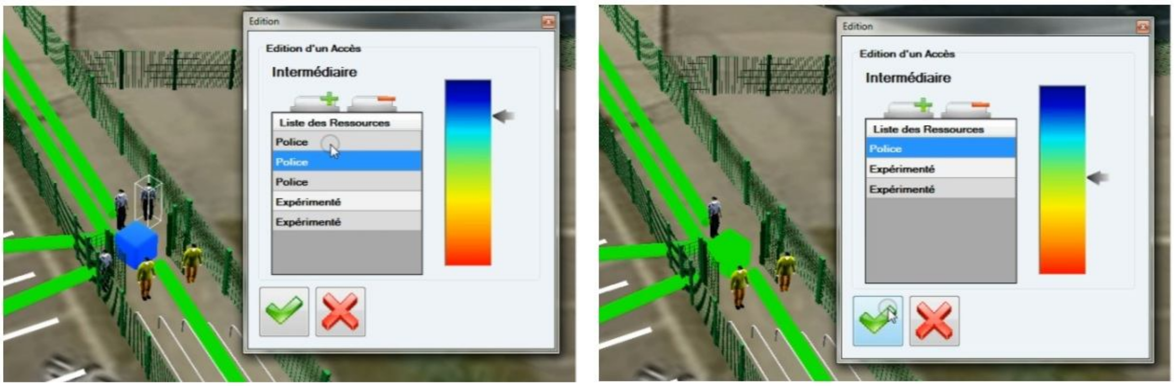

Figure 2 : Optimization of staff elements on an access to match with the real needs of the security plan

The obvious aim of using such a tool is to adapt the security organization to prevent and anticipate an eventual malevolent act which could disturb the good running of an event. However, it is really necessary to take care of security changes in order to avoid potential conflicts between safety and security. Actually, safety and security can be antagonistic (Deleuze, 2008) and we think it is interesting to illustrate it.

To really make the difference between safety and security, we can succintly define these terms as:

- Safety: capability of a system to avoid accidents.
- Security: capability of a system to avoid a malevolent act.

As an example of antagonism in a stadium, we can speak about a real past event which took place in 1989 in the stadium of Hillsborough located in Sheffield – England (MacLeary, 2004):

To enforce security face up to hooliganism, barriers have been placed between stands and ground to avoid that the crowd invading it. And with a mistake of a steward who decided to open a non-controlled entrance to mitigate the numerous crowd (arrived late) outside the stadium, this led to a non-controlled flow of people running through the same stand, already occupied by supporters who died crashed against the barriers or trampled. With a consequence of 96 dead people, it still is one of the worst sport tragedy.

It really shows how it is important to foresee unusual scenarios and to train its staffs to react with appropriated decisions. In that way, our software could a really useful decision making tool for stadiums managers.

4. Conclusion

To insure sustainability to an entertainment area, questions of safety and security are fundamental. So, managers and stakeholders need to anticipate risks and foresee event by event the best safety and security plan to set up. More particularly, they have to elaborate which kind of system is going to match at the maximum with D-day availabilities (stewards, policemen, barriers, etc.) and specific inputs (spectators attendance, frequentation rates by blocks and rows, geopolitical context, video monitoring, etc.)

To answer to that problematic, PACIFA decision step by step process permits to make efficiently the decision and to optimize the security management taking into account human behaviors.
Combining audits, expertises and innovative algorithms, our software gather all the necessary informations to allow to assess vulnerable spots and to adjust safety and security plan of actions according to various simulations on a 3D interactive and dynamical application.
It also permits to manage crowds interactions and capability of entrance for every access. Finally, an expansive database is built and allows to have numerous feedbacks and an experience legacy.

Using the multicriteria approach is appearing vital to assess with efficiency human behaviors and the power of various alternatives of evaluation given by analytic hierarchy process allow to provide a safe evaluation of the future security plan to set up.

REFERENCES

Pilz, G.A. (2009). La sociologie de la violence sportive en Allemagne : un état des lieux et un itinéraire, entretien réalisé par Christophe Jaccoud et Dominique Malatesta. IRSV *International Review on Sport and Violence, n°3 – Football, violence et sécurité*, 37-47.

Piwowar, J. (2010). Analyse des risques de malveillances sur infrastructures critiques : anticipation et aide à la décision dans le cadre sécurité globale. *Thèse de l'UTT, spécialité OSS*, 294 pages.

Branscomb, L. (2004). Protecting civil society from terrorism: the search for a sustainable strategy. *Technology in Society 26*, 271-285.

Ezell, B.C. (2004). *Infrastructure Vulnerability Assessment Model (I-VAM)*

Saaty, T.L. (1990). *The Analytic Hierarchy Process*, RWS Publication.

Piwowar, J. et al. (2009). An efficient process to reduce infrastructure vulnerabilities facing malevolence, *Reliab. Eng. & Syst. Safety, 94 (11),* 1869-1877.

Deleuze, G. et al. (2008). Are safety and security in industrial systems antagonistic or complementary issues? *Esrel08*. Proceedings on CD, Valencia, Spain.

MacLeary, J. (2004). Hillsborough disaster: 15 years on. *Guardian*.