International Journal of Economics, Commerce and Management
United Kingdom Vol. VI, Issue 4, April 2018
http://ijecm.co.uk/ ISSN 2348 0386

QUALITY INDICATORS FOR PROTECTION SYSTEMS

Georgiev Nikolai
Institute of Metal Science, equipment, and technologies with Center for Hydro- and
Aerodynamics - BAS, Sofia 1574, Shipchenski prohod № 67, Bulgaria
niki0611@abv.bg

Abstract

Using a variety of modular protection systems makes current problem of selecting appropriate indicators of their quality. Against this background, the current article proposes an approach to define them taking into account the system's properties of the modules, i.e. their participation in the tasks of the protection system as a whole. This contributes to increasing the efficiency and effectiveness of protection systems and improving their management.

Keywords: indicators, quality, system, protection

INTRODUCTION

On the basis of the common definitions for the concept of "quality" (http:/asq.org/glossary/q.html 2017, http://www.kaminata.net/topic-t46853.html 2017), the quality indicators of the modules, used in critical infrastructure protection systems, can be defined as a quantitative feature on the degree of their participation and their contribution to the objectives of the security system.

The primary purpose of the systems for object protection is to prevent attacks against them or to reduce the effects of such attacks on the protected objects (Stoichev K, 2012). This could be achieved by preventing attacks and destroying or damaging the attackers, and by hindering their access to areas from which they can attack.

In general, the description of those characteristics includes the probabilities for and magnitude of the impacts both of the attacking devices on the protected objects and on the modular systems for their protection, as well as those caused by the systems and means for protection against the attackers.

Let us assume that there are "I" possible types of means for attack against "J" protected objects. Let's also assume that there are "M" types of modular security systems, each of which is designed to cover one or more objects.

Let's introduce the following labels:

- Pij - the probability for "i"-type of attacking, to inflict a real impact on the "j"-type of protected object (i=1÷I, j=1÷J);
- Qi/j - the probability for the security system to actually impact the "i" type of attack by covering the "j" object;
- Rim/j - the probability for this type of attack to actually effect the "m"-type of protection module, when attempting to impact the "j" protected object;
- αij - loss caused by "i" type of attack in real impact on a "j" protected object, without the covering of "m" type protection module;
- γim/j - loss caused by "i" type of attack in real impact on the "m" type protection module, when attempting to impact on "j" covered object
- βi - loss caused to the "i" type of attacking mean by the protection system;

There are different indicators of the quality of protection systems, with the main ones being (Tsonev S., Vitlievemov V., Coege P.,2012, Dochev D., Petkov Y, 2008 , Stoichev K., Integrated model for security and protection of critical infrastructure, 2014, Stoichev K. Security Levels of Critical Infrastructure, 2014):

Average total losses of the covered objects and protection modules S1, where:

$$S1 = \sum\sum\sum PijRim/j\alpha ij\gamma im/j \qquad (1)$$

where summing is for i=1÷I, j=1÷J and m=1÷M.

Average losses of the protected objects S2, where:

$$S2 = \sum\sum Pij\alpha ij \qquad (2)$$

where summing is for i=1÷I, j=1÷J.

Average losses of the attackers S3, where***:***

$$S3 = \sum\sum Qi/j\ \beta i \qquad (3)$$

where summing is for i=1÷I и j=1÷J.

It is also possible to use other indicators obtained through different combinations of the basic quality indicators and representing their modifications. With more complex protection systems, it may also be possible to apply a fragmentation of the environment (by functional, territorial, situational, priority or other), grouping certain sets of security objects, modular systems and attacking means, and defining different key performance indicators for quality for each individual group.

QUALITY INDICATORS OF THE MAIN SUBSYSTEMS OF THE SECURITY SYSTEM

It can be seen that the main quality indicators of the security systems contain two main components. The first is related to the likelihood that the security system will actually impact the "i" type of attack means by covering the "j" object - Qi/j.

It is well known that defense systems generally have three basic subsystems - intelligence, communication and control and impact. In this aspect, the probability Qi/j can be considered as depending on the likelihood that the intelligence subsystem will, in a timely manner, detect the "i" means of attack (Qi/j1), the likelihood of this information being transmitted in the required quality and, on its basis, to be made a decision for impact against the "i" type of attack(Qi/j2) and the likelihood that the impact of the protection system to be effective, i.e. the impact on the "i" type of attack (Qi/j2) to realize loss βi (Qi/j3). It can therefore be assumed that:

$Qi/j = Qi/j1Qi/j2Qi/j3$ (4)

On the other hand, the probability that "i" type of attack can actually affect the "j" protected object (Pij) depends on maintaining the attacking means ability to act until the realization of the attack. Assuming the impact is "at the earliest opportunity", this condition is most often transformed into the condition of preserving the capabilities of the "i" type of attack mean to reach the so-called room for attack against the "j" protected object.

If βi is relative and reflects the rate of decrease of the abilities of the "i" type of attack (ie, βi = 1 upon its complete destruction), it can be assumed with some approximation that during the operation, the value of Pij is relatively constant (Pij0) and it can change significantly with a coefficient Kij, dependent mainly on the actions of the system for protection, where:

$Kij = 1 - Qi/j \beta i = 1 - Qi/j1Qi/j2Qi/j3 \beta i$ (5)

i.e.

$Pij = Pij0 Kij$ (6)

or:

$Pij = Pij0 (1 - Qi/j1Qi/j2Qi/j3 \beta i)$ (7)

Similarly, assuming that during the operation the value of Rim/j is relatively constant (Rim/j0) and it can change significantly with a coefficient Kij, depending mainly on the actions of the protection system, we get:

$Rim/j = Rim/j0 (1 - Qi/j1Qi/j2Qi/j3 \beta i)$ (8)

From the expressions and *formulas* received *(1-3)*, assuming that due to the nature of the process Qi/j (ie Qi/j1, Qi/j2 and Qi/j3) are probabilities of events, occurring once in the realization of the given hypothesis (ie in attack of "i" type of attacking mean on the "j" protected object, the probability of impact on it Qi/j must be counted only once, regardless of the fact that it affects both Pij and Rim/j) we get:

$S1 = \sum\sum\sum Pij0Rim/j0\alpha ij\gamma im/j(1 - Qi/j1Qi/j2Qi/j3\ \beta i)$ (9)

$S2 = \sum\sum Pij0\alpha ij(1 - Qi/j1Qi/j2Qi/j3\ \beta i)$ (10)

$S3 = \sum\sum Qi/j1Qi/j2Qi/j3\beta i$ (11)

QUALITY INDICATORS OF THE SECURITY SYSTEM MODULES

Formulas (9-11) provide the ability to formulate aggregate performance indicators for the individual subsystems of the security system. It can be seen that the general description of the protection system performance indicators is given in *Formula 9* - in it are involved all system factors - losses of attack and protection means (including protection modules), probabilities of impact, and features of the subsystems for intelligence, communication and control and impact. Therefore, when defining the security module indicators, we will use the first base indicator for the quality of the protection system, that for average total losses (ie Formula 9).

A summary indicator for the quality of the intelligence subsystem according to Formula 9, can be taken to be the probability Qi/j1, which expresses the degree of involvement of the intelligence subsystem in the formation of the summary indicator S1. It can be seen that, through Formula 9, the indicator Qi/j1 takes into account the system's interconnection of the intelligence subsystem with the environment, the type of threat and the characteristics of protected objects, ie. takes into account the involvement of this subsystem in a particular environment: the type of "i" attack mean, where it is scouted (in its impact action against the "j" protected object), the probabilities for performing the tasks of the other subsystems for communication and control and impact, the losses which the attacker can cause to the protected objects and to the protection modules, ie on Pij0, Rim/j0, Qi/j1, Qi/j2, Qi/j3, βiαij and γim/j.

Let's introduce *Formula 9* as:

$S1 = \sum\sum (1 - Qi/j1\ Qi/j2Qi/j3\ \beta i)Pij0\alpha ij\sum Rim/j0\ \gamma im/j$ (12)

Where summing is in the sequence of i=1÷I, j=1÷J and m=1÷M.

Let's introduce the markings:

- $Zi/j1 = Qi/j3\ \beta i$ - private vulnerability coefficient of the attack means;
- $Zi/j2 = Pij0\alpha ij$ - private vulnerability coefficient of the protected objects;
- $Zi/j3 = \sum Rim/j0\ \gamma im/j$ - private vulnerability coefficient of the security system.

These coefficients are private, because they describe the respective vulnerabilities only for the "i" attack mean on the hypothesis that it targets impact against the "j" protected object.

Replacing the specified private coefficients in Formula 9 we get:

$S1 = \sum\sum (1- Qi/j1\ Qi/j2\ Zi/j1)\ Zi/j2\ Zi/j3 =$

$= \sum\sum (1 - Qi/j1\ Уi/j1)\ Zi/j2\ Zi/j3$ (13)

where summing is in the sequence of $i=1\div I$, $j=1\div J$, and $Уi/j1 = Qi/j2\ Zi/j1$ - is private coefficient, accounting the influence of the communication and control subsystem.

Obviously, in a relatively homogeneous environment - relatively uniform means for attack and protection objects, in a situation-independent ability of the communication and control subsystem, ie when presenting the result Zi/j2 and Zi/j3 as a relatively constant coefficient "X", Formula 13 becomes;

$S1 = X\sum\sum (1 - Уi/j1\ Qi/j1\ )$ (14)

With equal capabilities of the intelligence subsystem (ie regardless of the type of attack mean and which protected object it attacks), ie, when $Qi/j1 = Q1$ and $Уi/j1 = У1$ it is:

$S1 = IJX(1 - У1Q1) = N1(1 - У1Q1)$ (15)

Where I and J can be interpreted as multi-purpose coefficients of the protection subsystem (showing I - the number of attacking means that the subsystem can scan and J - the number of protected objects it can provide with intelligence information), and N1 - the coefficient.

It can be seen that N1 and Y1 - have meaning as weight coefficients of the intelligence subsystem, reflecting its impact on the overall efficiency of the security system.

The probability Qi/j1 (or in isotropic for collecting intelligence environment - Q1) depends on the nature and organization of the intelligence subsystem. Generally, for each "i" attacking mean, the individual "m" intelligence module, for each point of the space (with some approximation for the routing to prevent its attack on the "j" protected object) is characterized by a certain probability of detection , which can be denoted by Qmi/j1 (in isotropic for collecting intelligence environment - Qm1). When merging the information from the separate intelligence modules by a 1/M type algorithm, ie. when a target finding solution is accepted at its detection by at least one of the intelligence modules, it is:

$Qi/j1\ = 1- \Pi(1- Qmi/j1)$ (16)

$Q1 = 1- \Pi(1- Qm1)$ (17)

where the result is from $m=1\div M$.

In relatively uniform characteristics of the individual intelligence modules in the attack area of the attacking means, ie. $Qm1 = Q11 = const$, Formula 17 becomes:

$Q1 = 1 - (1 - Q11)^{M}$ (18)

When integrating the information from individual intelligence modules through other algorithms - e.g. of the K/M type (ie when a detection solution is only accepted when at least "K" of the intelligence modules have detected the target), the probability Qi/j1 is calculated using the combinatorial methods.

Taking into account the above, and based on the accepted aggregate quality indicator of the intelligence subsystem Qi/j1, a quality indicator of the "r" module of the intelligence subsystem can be introduced - the probability Qri/j1. By integrating the information from the separate intelligence modules by a 1/M type of algorithm, according to Formula 16, the probability Qri/j1 can be defined as:

$$Qi/j1 = 1- (1- Qri/j1)\Pi(1- Qmi/j1) =$$

$$= 1- \Pi(1- Qmi/j1) + Qri/j1\, \Pi(1- Qmi/j1) \qquad (19)$$

where the result is from $m=1 \div M$; $m \neq r$

Obviously the expression $Qi/j1(-r) = 1- \Pi(1- Qmi/j1)$ is a quality indicator of that part of the intelligence system that includes all modules except the "r" module.

Then the quality indicator of the "r" module of the intelligence system can be determined by the expression:

$$Qi/j1 = Qi/j1(-r) + Qri/j1(1 - Qi/j1(-r)) = Qi/j1(-r) + \Delta Qi/j1(-r) \qquad (20)$$

where $\Delta Qi/j1(-r)$ is the increase of the likelihood for detection by the intelligence system of the "i" attacking mean after the inclusion of the "r" module.

Since a quality indicator can also be used for a uniquely related parameter, due to the linear nature of the dependence expressed by Formula 20, for the quality indicator of the "r" module of the intelligence system, can be used the easily calculated parameter $\Delta Qi/j1(-r)$, ie.

$$\Delta Qi/j1(-r) = Qri/j1(1 - Qi/j1(-r)) = Qri/j1\, \Pi(1- Qmi/j1) \qquad (21)$$

where the result is from $m=1 \div M$; $m \neq r$

When Qm1 = Q11 = const the effectiveness of all the intelligence system modules is the same and can be determined by the expression:

$$Q1 = 1 - (1 - Q11)^{M} = 1 - (1- Q11)(1 - Q11)^{M-1} \qquad (22)$$

$$Q1 = 1- (1 - Q11)^{M-1} + Q11(1 - Q11)^{M-1} = Q1(-1) + \Delta Q1(-1) \qquad (23)$$

in this case, the quality indicator of an intelligence system module can be defined as:

$$\Delta Q1(-1) = Q11(1 - Q11)^{M-1} \qquad (24)$$

Applying this approach for a summary indicator for the quality on the subsystem for comunication and control can be used the expressions for the probabilities Qi/j2 (or Q2/Q3) and Qi/j3 (or in isotropic for the impact modules against the attacking means environment - Q3). The determination of these quality indicators can be done through formulas similar to Formulas 16,17,18,21 and 24, replacing index 1 respectively with indexes 2 or 3.

CONCLUSION

Formulas have been proposed to determine the quality indicators of the different modules from the object protection system. They are applicable to a specific type of situation and to a specific, relatively uniform (i.e. limited) spatial area of the surrounding areas of the protected sites. Apparently, the indicators for the quality of the protection modules change their values in different areas of space and in different types of threats, i.e. in various scenarios for the development of the situation. For a more complete description of the quality indicators of the protection modules, it is advisable to use the methods of situational analysis or mathematical modeling.

REFERENCES

Dochev D., Petkov Y., Theory of Decision Making. Varna, Science and Economics, 2008

http://www.kaminata.net/topic-t46853.html 2017

http:/asq.org/glossary/q.html 2017

Stoichev K., Conditions for Increasing the Viability of Critical Infrastructure Objects. Journal of Applied Security Research, 2012, ISSN:1936-1610; print / 1936-1629, DOI:10.1080/19361610.2

Stoichev K., Integrated model for security and protection of critical infrastructure. Open Access Library Journal, 1, 2014, ISSN:2333-9721, DOI:http://dx.doi.org/10.4236/oalib.1101124

Stoichev K., Security Levels of Critical Infrastructure. Journal of Applied Security Research, 2014, DOI:10.1080/19361610.2014.913233, 10

Tsonev S., Vitlievemov V., Coege P., Methods for Optimization, Ministry of Education and Science, Rousse, 2004,ISBN 954-712-229-0