UDC 621.396

Piotr Sienkiewicz ***(PhD, Professor, Director of the Security Systems Engineering Institute)***
Piotr Gawliczek ***(Associate Professor, Rector's Representative for the Innovation)***

National Defence University, Warsaw, Poland

THEORY AND SECURITY SYSTEMS ENGINEERING

The article presents the basic notions and definitions of systems security. The model of threats for systems security and a general model of a safe system (i.e. secured against outside and inside threats) were discussed. The problem of systems security management, considering particularly the management of risk, was defined. The paper has been presented the current problems of research and education in the science of safety and security, treated as an area of systems research (systems analysis, systems engineering).

The attention is paid to the phenomenon of both the growth of security threats (for the individual, local, global), as well as the growth in popularity of study at the field of national security and related (e.g. internal security, health security). On the background of these phenomena it has been presented author's original project of interdisciplinary studies in security systems engineering as a field of study carried out by both institutions, social university and technical university. A general model of threats, systems' safety and safety management has been presented. The model of safety management is considered in terms of a duplex control over the allocation of means and security measures.

Keywords*: security systems; models of threats; security models.*

"There is no such thing as an isolated person or situation. There is only a relation between a person and their environment. A relation, which essence is expressed by the word 'threat".

A. Magnusson

Introduction

Dynamic changes of security environment that have been in process since last decades resulted in forming a national security concept. Subjects of national security are directly related to the security paradigm changes. Traditional concept of security has been broadened to cover not only object's endurance but welfare and development as well. Likewise, national security concept is an extension of state security concept – it refers to protection and defence of state but either comprises protection of nation (the society and individuals as well), it's values, needs, development goals, goods, heritage and natural environment, from military and non-military threats. A system analysis of security of any objects is sensible when danger exists, that is to say when there are threats that can cause either an interruption of functioning (existence, progress) of those objects, or a loss of certain properties thereof. Security is a ambiguous notion, regarding to: [1] lack of danger; [2] a system of institutional and non-institutional guarantees of threats' elimination or minimization; [3] one of the existing existential values, related to sense of stability, an enduring favorable state of affairs, a sense of lack of threats, confidence. In terms of political science and national (international) security related studies, both the coverage criterion (e.g. regional security, global security) and the subject criterion (military, economic, ecological, technical, cultural security) are applied. On the other hand, on the basis of system analysis, two dominant approaches exist, namely:

Security understood as an object's property, qualifying its resistance to the emergence of dangerous situations (threats), the major accent being put on the object's security failure, that is its susceptibility to real or potential threats;

Security of a system understood as its capability to protect its intrinsic values against outside threats.

We need to notice two aspects of security: the objective one, when conditions exist to create real threats, and the subjective one, which expresses the feeling of security or insecurity. In systemic studies, the relation is highlighted between the security of systems and other system characteristics, such as e.g. stability, balance, reliability, resilience, readiness, etc., especially their effectiveness (in terms of efficiency and/or economy).

Research results

Model of threats.

A threat to the system's security is any occurrence (process, event) that is undesirable in terms of uninterrupted functioning of the system (table 1). Such occurrences or their accumulation in the given time and place, by affecting it destructively, create a threatening situation for the system's existence (development). It should also be noted that there is a possibility of creating situations dangerous to the system, causing internal threats resulting from e.g. system's failure (fig. 1).

Table 1

Classification of threats

No.	Classification criterion	Threats
1	Physical properties	Material threats (on the road, in the air, etc.) Energy threats (heat, radioactivity, etc.) Information threats Non-material threats (mental, social, political)
2	Duration time	Short-term, occasional threats, Long-term, increasing, evolving threats, Cyclical, recurrent threats;
3	Range	Local threats, Extensive threats (regional, global);
4	Stability of territorial coverage	Spreading threats, Non-spreading threats.

Source: own elaboration of the authors

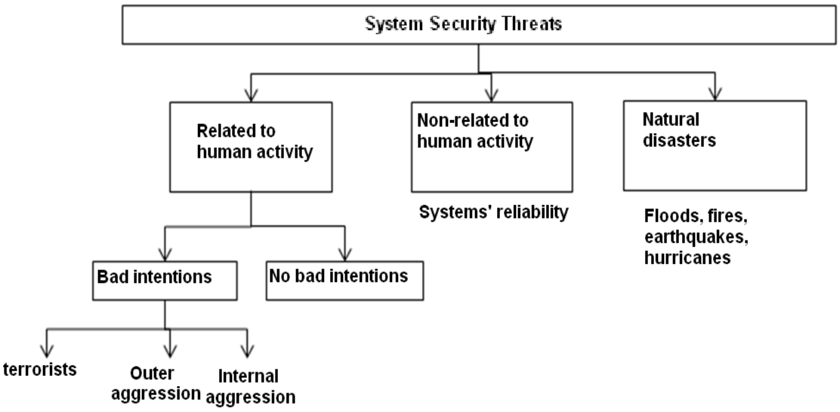

Figure 1. General typology of threats for the security of systems

Source: own elaboration of the authors

System's **situation** is taken into consideration [9,12] $\Sigma=\langle S,E,R\rangle$

Where: S – the system, which is the **object** of threats: $S<M.Rw>$, M – a set of elements, Rw – a set of relations between elements; E – the environment, consisting of elements, which are the **sources** of threats; $Rz\subset SxE$ – a set of relations.

A system analysis of threat situations can be "scaled" according to two **criteria**:

a) Probability criterion (*security*) of emerging of a state of threat (or other measure of the possibility of threat occurrence, e.g. fuzzy measurement);

b) Importance criterion (*severity*) of the state of threat (e.g. the risk and the value of the system in question or the value of resources it disposes).

If the system S has a function of security threats z(t) assigned to it and the function of reliability is Rel(t), then the function of the systems effectiveness is (fig. 2):

$$E(t)=f(u(t),K(t)\equiv\phi(z(t), Rel(t)),$$

where U(t) – utility function,

K(t) – cost (expenditure) function.

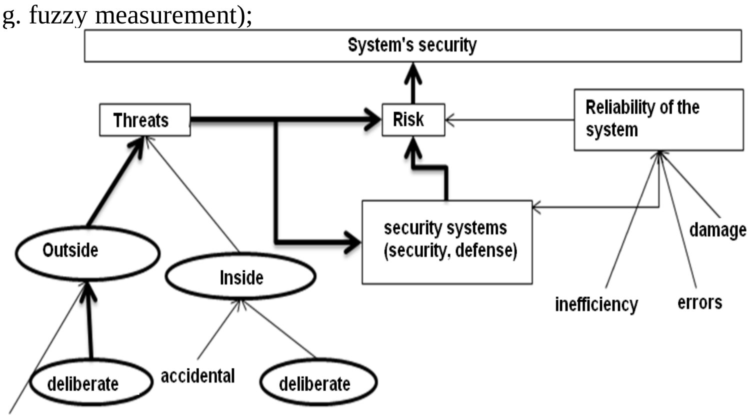

Figure 2. A concept of system analysis of security

Source: authors' own work

System's security model.

If the threats have been recognized, then the system's security depends on equipping it with a specified resistance potential (security). In particular, it can be a particular, usually layered security system, protecting against threats.

Let us consider, as before, a given system situation Σ and assume that the data is as follows:

Outside threats A(t) coming from the system's (S) environment (E), to which a function of threat potential corresponds;

System's (S) resistance to outside threats B(t), which corresponds to the function of the defense (security) potential.

Above situation characteristics are random functions with known probability distribution:

$$F(a,t)=\Pr\{A(t)<a,\ a\geq 0\},$$

$$G(b,t)=\Pr\{B(t)<b,\ b\geq 0\},\ t\in T$$

A generalized indicator of the system's security can be expressed by the probability that the threats will not exceed a given critical (permissible) point $a_o\geq 0$ and the system's resistance will be greater than a specified limit $b_{o,}$ which is $\beta(t)\equiv\beta(a_o,b_o)=\Pr\{A(t)\leq a_{o,}\ B(t)>b_o\}$ which, in terms of statistical independence of the values in question, gives us an indicator of the system's security: $\beta(t) = F(a_o, t)\ [1 - G(b_o, t)]$.

Accepting the desirable level of system's security as $\beta o>0$, we may say that the system is safe within time T, provided that in every moment $t\in T$ the condition $\beta(t)\geq\beta o$ is met. In the case of technical objects, analyses of the object's security utilize certain simplified procedures, which boil down to determining the probability of "destruction" $P=p(P_S\leq P_e)$, $P_e\equiv A(t)$, $P_S\equiv B(t)$.Which means that there is a possibility of generalized resistance (bearing capacity) P_s is no larger than a generalized threat (encumbrance) P_e.

Apart from crisis situations, where national or business security is at stake, special attention is paid to crisis situations caused by extensive threats (e.g. chemical and energy disasters, weather anomalies, viral epidemics, etc.) and local threats (e.g. road accidents, building disasters, explosions, etc.).

Procedures and standards are set for various types of crisis situations, setting out e.g. threat classes and threat objects' classes, severity of the threats' results, etc.

Security management

In the system analysis of security it has been assumed that the following have im-pact on the system's effectiveness (fig.3):

System's reliability, its capability to operate smoothly (with no failure, damage, errors, etc) in the given time;

System's security, its capability to protect itself efficiently against the effects of outside threats.

System security management is an integral part of system management and is associated with rationalizing the choice of measures (methods, technologies) providing secure (consistent with its purpose) functioning of the system in a dangerous environment (tab. 2).

If there are no outside threats, then system security management can be reduced to managing over the system's reliability: we must chose such a reliability strategy, which criterion value (function of system's reliability) is at maximum, assuming that the cost of the reliability increase (or keeping reliability on the desirable level) does not exceed the permissible limit.

If, however, threat to the system's security exists, then security management can be reduced to choosing such security strategy (means for protection against threats) from a set of permissible strategies, which anticipated value of the effects of threats (losses) is minimal, assuming that the cost of applying this strategy (implementing security measures) does not exceed the permissible limit.

It should be pointed out, that both the problem of reliability management and the problem of system security management, can be reduced to the following: [1] minimizing the risk function, provided the value of effects (utility) obtained due to the functioning of the system are greater than the desirable limit or [2] maximizing the function of the system's effectiveness, provided the function of risk is no greater than the permissible (safe) limit.

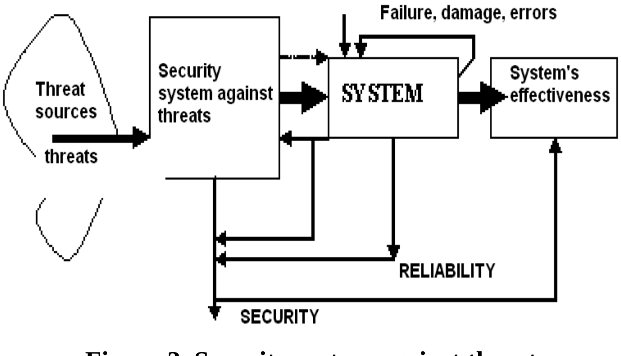

Figure 3. Security system against threats

Source: authors' own work

Table 2

Security management

THREATS	RELIABILITY	
	Low	**High**
Non-existent	reliability management: minimizing the costs for a desired level of reliability (risk, effectiveness)	reliability management: sustaining the state of reliability for the permissible level of expenditure for protection against failures
Existent	security management: minimizing the costs for a desired level of reliability and security (risk)	security management: minimizing the costs for the desired level of risk and sustaining the level of reliability

Source: authors' own work

Let us assume that a system is given as the object of threat (fig.4), , characterized by a generalized function of security

$$\beta = f(P_e, P_S, \nu)$$

where ν - system's value, $0 \le P_e \le P_{Omax,}$ $0 < P_S \le P_{Smax}$, $\nu > 0$

And the function of cost of security against threats

$$K = \varphi(P_S, \nu) > 0.$$

It is assumed, that the costs are directly proportional to both the system's value and the security potential.

The problem of optimization of security management can be formulated as determining such a value P_S, which maximizes the level of security, that is $\beta \to \max$, provided that*:* $K \le K_{\mathbf{0}}$, where K_0 represents the permissible value of expenditure for system security against possible threats P_e.

Let us assume there are N relatively independent systems, every one of them characterized by the following values (fig.5):

$$\{P_e^i, P_S^i, \nu^i, \beta_i, K_i, \quad i=1,2,\dots,N\}$$

A primary management system, which administers central security measures (resources) W. Depending on the local threat situations, the primary decision-making center may assign a specified W value to i system in order to enhance its security.

In such a case, security management can be formulated as a problem of duplex optimization, namely:

a) Primary problem

$$\beta = F(\beta_1, \dots, \beta_N) \to \max$$

where

$$\beta_i = \beta_i(P_S^i, W_i), \qquad W_i \ge 0 \quad , \sum_{i=1}^{N} W_i = W$$

Provided that

$$K = \sum_{i=1}^{N} K_i(P_S^i, W_i) \le K_O \;;$$

b) Local problem:

$$\beta_i = f_i(P_S^i, W_i) \to \max$$

$$K_i(P_S^i, W_i) \le K_O^i, \quad i = 1, 2, \dots, N$$

It is assumed that the primary management system – thanks to the processes of monitoring and diagnosis of threats situations – possesses information on the threats, which means that $\{P_O^i,\ i=1,2,\dots,N\}$ for the moment t (or the period T). This information is the basis for optimization of W_i resources allocation to individual systems. It can also be assumed, that the primary system (center) allocates the measures directly to the i local system, for internal security purposes, or indirectly, for enhancing the outside security system (fig.5).

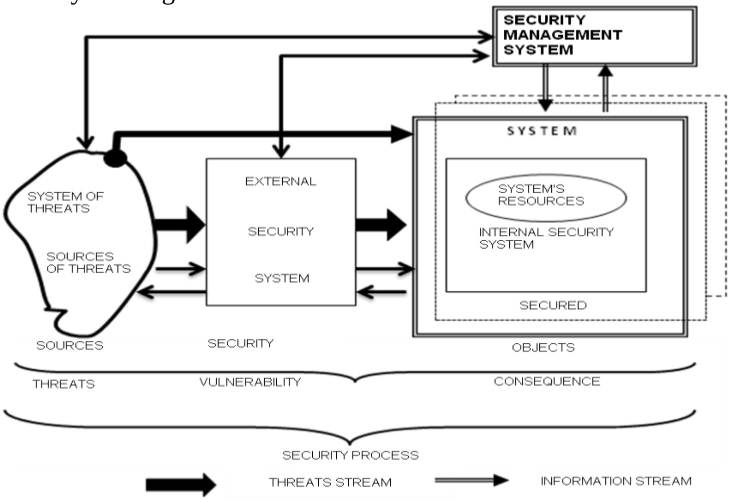

Figure 4. A model of security management

Source: Sienkiewicz P., Teoria bezpieczeństwa systemów, AON Warszawa 2004

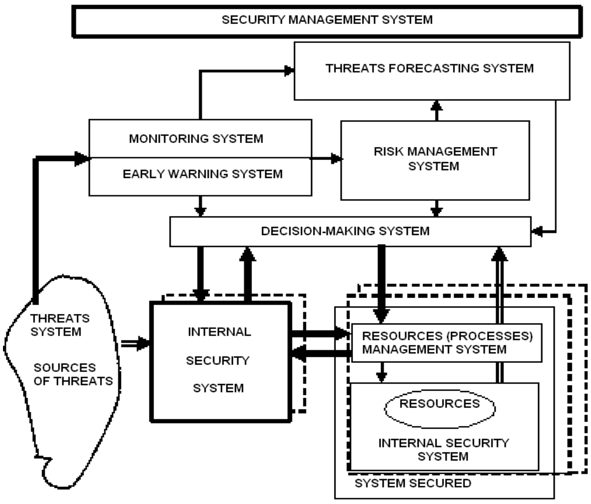

Figure 5. A model of security management

Source: Sienkiewicz P., Teoria bezpieczeństwa systemów, AON Warszawa 2004

Conclusions

Security of technical systems may be considered in two basic aspects, namely [1] as the security of technology in terms of its negative consequences (threats) to the environment (social environment, natural environment); [2] as the security of the technical system, resulting from its functional states (reliability-unreliability, readiness, resilience, etc.).

In the first case, we are dealing with a necessity to analyze the technological risk, which is best shown by the example of Chernobyl syndrome, whereas in the latter case, the risk can be expressed by communication security (e.g. in air transport), affected by unreliable technology. Although the disaster at Chernobyl nuclear power plant was caused by technical system breakdown, resulting from human error, the social (health and biological) and ecological effects were the consequence of the specific properties of nuclear technology.

Scientific study over technical systems' security have a long history. Its beginnings should probably be sought in the old ages, when giant structures (e.g. cathedrals, aqueducts) were created that needed to meet safety conditions of building constructions. A method proposed by Ch. Coulomb (1736-1806) was known as allowable stress method and is a deterministic method. In the 1930's it was assumed that a catastrophe, failure or breakdown must be treated as a random event and the reliability (security) must be analyzed with probabilistic methods.

In the late 60's and 70's, at the Military University of Technology, a foundation was made for the original school of study over exploitation in military technology (e.g. the works of S. Ziemba, S. Piasecki, J. Konieczny), including the issues of wear and tear (durability, resistance), reliability and control over the processes of exploitation (handling and attendance) of technical equipment. In the late 80's and 90's, the main research centers have developed in: Systems Research Institute of the Polish Academy of Sciences (systems' reliability: Piasecki, Hryniewicz), Warsaw University of Technology (reliability and security in transport: Ważyńska-Fiok, Szopa), Gdańsk University of Technology (Brandowski) and Air Force Institute of Technology (Lewitowicz, Jaźwiński). Scientific achievements in this field were summarized during national conferences in Kiekrz under the common title *Systems Security* (1986, 1988, 1990, 1992, 1994, 1996), as well as KONBIN International Conferences on Security and Reliability (1999, 2001, 2003). National Defence University conducts extensive research on military and non-military security issues (on theory and security systems engineering).

During these conferences, which presented over a 1000 lectures, a creation of uniform foundations of security studies was repeatedly postulated (S. Ziemba, L. Brandowski, K. Ważyńska-Fiok, J. Jaźwiński, A. Szymanek, J. Lewitowicz, P. Sienkiewicz). There have also been attempts on creating uniform concepts of security and insecurity, threats and risk of both technical and social systems (P. Sienkiewicz, A. Szymanek).

Presently, two main research trends can be distinguished: [1] creating theoretical basics of (technical and social) systems security, [2] designing security systems, including security management and hence risk management methods as well (especially in crisis situations). We can, therefore, speak of security science, which includes the theory and engineering of systems security.

Basic methodological conclusions of widely understood systems research over security of social and technical objects, may include the following:

Security is a system category, as it concerns complex objects (technical, biological, socio-technical, social), considered as a structuralized whole, active and operating in an active environment;

Security of a system is a state and a process, in which the system can develop (realize its development goals)

System security is a relative concept, always related to the general outside situation, moreover, it can either mean a lack of threats (objective state) or lack of sense of danger (subjective state);

Every conflict situation, in which the particular system participates, includes potential or real threats to the system's security;

The system's security depends both on the risk volume (intensiveness and outside influence effectiveness) and on the effectiveness of security system;

One of the basic tasks of system analysis is to identify dangerous (critical) situations, including the recognition and evaluation of the sources of threats, their intensiveness, forms and the risk of their potential effects;

One of the basic tasks of system security engineering is developing methods of designing efficient security systems, providing a desirable level of security to the systems;

The issue of systems security is a strictly interdisciplinary problem that will become more and more significant in view of the creation of a new world order (globalization, information society); the most important issues are likely to include international and national security, transport and communications systems security, energy systems security, information and ecological security, etc.;

Research methods over systems security should mainly be based on modern methods and system concepts, such as synergetics, nonlinear thermodynamics, catastrophe theory, fuzzy sets theory, probabilistic and possibilistic methods, developing systems theory, conflict theory, crisis management, etc.;

An urgent need to develop a general systems security theory is observed, as it would be one of modern systems theories and an important branch of systems study, as well as of development program of system security engineering (security management system engineering).

References

1. Findeisen W. (1985), Analiza systemowa, podstawy i metodologia. WNT, Warszawa. **2. Jaźwiński J.,** Ważyńska–Fiok K. (1993), Bezpieczeństwo systemów. PWN, Warszawa. **3. Konieczny J.** (2001), Zarządzanie w sytuacjach kryzysowych, wypadkach i katastrofach. Poznań. **4. Murzewski J.**, (1989), Niezawodność konstrukcji inżynierskich. Arkady. **5. Sienkiewicz P.** (1990) Conditions of Conflict and Security in Systems. ISA, Washington. **6. Sienkiewicz P.** (1995), Analiza systemowa. Bellona, Warszawa. **7. Sienkiewicz P**. (2005), Teoria bezpieczeństwa systemów. AON. **8. Sienkiewicz P**. (2007), Optymalizacja w zarządzaniu bezpieczeństwem systemów. AGH Kraków. **9. Sienkiewicz P.,** Świeboda H. (2009), Modele bezpieczeństwa we współczesnych badaniach systemowych. ZN AON Nr 3(76) Warszawa. **10. Szymanek A.** (2006), Bezpieczeństwo i ryzyko w technice. Politechnika Radomska, Radom. **11. Tarczyński W.,** Mojsiewicz M. (2001), Zarządzanie ryzykiem. PWE, Warszawa.

ТЕОРІЯ ТА ПРОЕКТУВАННЯ СИСТЕМ БЕЗПЕКИ

Пьотр Сінкевич ***(д-р філософії, професор, директор інституту проектування систем безпеки)***
Пьотр Гавлічек ***(доцент, представник ректора з інновацій)***

Національний університет оборони, Варшава, Польща

У статті представлені основні поняття та визначення безпеки систем. Були обговорені модель загроз для безпеки систем і загальна модель безпечної системи (тобто захищеної від зовнішніх та внутрішніх загроз). Була визначена проблема управління безпекою систем, враховуючи особливості управління ризиком. У статті наведено поточні проблеми наукових досліджень у сфері захисту та безпеки, які розглядаються як область системних досліджень (системний аналіз, проектування систем).

Увага приділяється явищу зростання загроз безпеці (індивідуальні, локальні, глобальні), а також зростання популярності навчання у галузі національної безпеки та пов'язаних із нею галузях (наприклад, внутрішньої безпеки, безпеки здоров'я). На фоні цих явищ був представлений авторський оригінальний проект міждисциплінарних досліджень щодо проектування систем безпеки як галузь досліджень, які проводяться у гуманітарному та технічному університеті. Була представлена загальна модель загроз, безпеки та управління безпекою систем. Модель управління безпекою розглядається в аспекті дуплексного контролю за розподілом засобів і заходів безпеки.

Keywords*: системи безпеки; модель загроз; моделі безпеки.*

ТЕОРИЯ И ПРОЕКТИРОВАНИЕ СИСТЕМ БЕЗОПАСНОСТИ

Петр Синкевич ***(д-р философии, профессор, директор института проектирования систем безопасности)***
Петр Гавличек ***(доцент, представитель ректора по инновациям)***

Национальный университет обороны, Варшава, Польша

В статье представлены основные понятия и определения безопасности систем. Были обсуждены модель угроз для безопасности систем и общая модель безопасной системы (т.е. защищенной от внешних и внутренних угроз). Была определена проблема управления безопасностью систем, учитывая особенности управления риском. В статье приведены текущие проблемы научных исследований в области защиты и безопасности, которые рассматриваются как область системных исследований (системный анализ, проектирование систем).

Внимание уделяется явлению роста угроз безопасности (индивидуальные, локальные, глобальные), а также рост популярности обучения в области национальной безопасности и связанных с ней отраслях (например, внутренней безопасности, безопасности здоровья). На фоне этих явлений был представлен авторский оригинальный проект междисциплинарных исследований по проектированию систем безопасности как область исследований, которые проводятся в гуманитарном и техническом университете. Была представлена общая модель угроз, безопасности и управления безопасностью систем. Модель управления безопасностью рассматривается в аспекте дуплексного контроля за распределением средств и мер безопасности.

Keywords: *системы безопасности; модель угроз; модели безопасности.*

Отримано: 17.03.2015 року