Information Security System Survivability Assessment Method

Valeriy Dudykevych, Iurii Garasym

Abstract **—The paper is devoted to creating an approach of designing embedded information security systems with survivability property.**

***Index Terms*—information security system, survivability assessment, survivability property.**

I. Introduction

THE growing number of instances of breaches in information security in the last few years has created a compelling case for efforts towards secure electronic systems. Embedded systems, which will be ubiquitously used to capture, store, manipulate, and access data of a sensitive nature, pose several unique and interesting security challenges. Security has been the subject of intensive research in the areas of cryptography, computing, and networking. However, security is often mis-construed by embedded system designers as the addition of features, such as specific cryptographic algorithms and security protocols, to the system. In reality, it is an entirely new metric that designers should consider throughout the design process, along with other metrics such as cost, performance, and power [1].

Considering uncertainty situations, destabilizing factors (DF) influences, probable system structural elements (SE) failures requires survivability assessment as an information security systems (ISS) functioning efficiency characteristic [2]. Transition to ideology of survivable ISS designing and development allows: to achieve the general-purpose function in pre-contingency operating conditions, to provide ISS adaptive management, to build ISS on a "what if" schemes instead traditional "defence from" schemes that are inefficient in distributed ISS [3].

The survivability assessment models and methods developing is actual to improve functioning quality under the uncertainty DF influences for embedded systems security [4].

II. Information Security Systems with Survivability Property

Nowadays information security systems that are highly distributed improve the efficiency and effectiveness of organizations by permitting whole new levels of organizational integration. However, such integration is accompanied by elevated risks of intrusion and compromise. These risks can be mitigated by incorporating survivability capabilities into an organization's systems. As an emerging discipline, survivability builds on related fields of study (e.g., security, fault tolerance, safety, reliability, reuse, performance, verification, and testing) and introduces new concepts and principles. Survivability focuses on preserving essential services in security systems environments, even when systems in such environments are penetrated and compromised [5].

III. The Survivable Information Security Systems Definition

Information security system survivability – a security system property, which is the ability to store and carry their own set amount of target features (privacy of information, it's integrity, availability implementation) in the appropriate environment, taking into account various external and internal destabilizing factors (including threat models and the offender), which can lead to failures of its functional elements (nodes and/or communication channels) through appropriate changes in the structure and system behavior (which is based on the estimation of parameters of survival), while maintaining a minimum level as functioning according to the levels of degradation with the subsequent resumption of the preliminary effective operation for a preset time [6].

Thus, technical, software, information, methodological, linguistic and organizational support for security system should contain the following facilities, which would react to certain situations that lead to poor performance and preserve the system of information security.

Given the complexity survival security system to solve specific one-time events is impossible. Necessary is a continuous directed defined actions that would be carried out throughout the life cycle of ISS. Difficulty of ISS survivability properties due to embedded systems

Valeriy Dudykevych is with Information Security Department, Lviv National Polytechnic University, 12 St. Bandera St., 79013 Lviv, Ukraine (e-mail: vdudykev@polynet.lviv.ua).

Iurii Garasym is with Information Security Department, Lviv National Polytechnic University, 12 St. Bandera St., 79013 Lviv, Ukraine (corresponding author to provide phone: +38 (096) 893-15-22, +38 (032) 235-77-49, +38 (032) 235-74-77, e-mail: garasym_yr@polynet.lviv.ua).

complexity – the complexity of modern information systems designed to automate these processes.

Survival is complicated by the fact that in today's modern ISS may generate new features by itself that were not incorporated in the terms of reference or in the draft system, not to mention the inadequate reaction to the occurrence of various unpredictable situations [5].

IV. Survivable Information Security Systems Characteristics

A key characteristic of survivable security systems is their capability to deliver essential services in the face of attack, failure, or accident [7, 8]. Central to the delivery of essential services is the capability of a system to maintain essential properties (i.e., specified levels of integrity, confidentiality, performance, and other quality attributes) in the presence of attack, failure, or accident. Thus, it is important to define minimum levels of quality attributes that must be associated with essential services. For example, a launch of a missile by a ISS is no longer effective if the system performance is slowed to the point that the target is out of range before the system can launch [9].

These quality attributes are so important that definitions of survivability are often expressed in terms of maintaining a balance among multiple qualities attributes such as performance, security, reliability, availability, fault-tolerance, modifiability, and affordability. Quality attributes represent broad categories of related requirements, so a quality attribute may contain other quality attributes. For example, the security attribute traditionally includes the three attributes: confidentiality, integrity, and availability.

The capability to deliver essential services (and maintain the associated essential properties) must be sustained even if a significant portion of the system is incapacitated. Furthermore, this capability should not be dependent upon the survival of a specific information resource, computation, or communication link. In a military setting, essential services might be those required to maintain an overwhelming technical superiority, and essential properties may include integrity, confidentiality, and a level of performance sufficient to deliver results in less than one decision cycle of the enemy. In the public sector, a survivable financial system is one that maintains the integrity, confidentiality, and availability of essential information and financial services, even if particular nodes or communication links are incapacitated through intrusion or accident, and that recovers compromised information and services in a timely manner. The financial system's survivability might be judged by using a composite measure of the disruption of stock trades or bank transactions (i.e., a measure of the disruption of essential services).

Key to the concept of survivability, then, is identifying the essential services (and the essential properties that support them) within an operational system. Essential services are defined as the functions of the system that must be maintained when the environment is hostile or failures or accidents are detected that threaten the system.

There are typically many services that can be temporarily suspended when a system is dealing with an attack or other extraordinary environmental condition. Such a suspension can help isolate areas affected by an intrusion and free system resources to deal with its effects. The overall function of a system should adapt to preserve essential services [9].

It was linked the capability of a survivable system to fulfill its mission in a timely manner to its ability to deliver essential services in the presence of attack, accident, or failure. Ultimately, mission fulfillment must survive not any portion or component of the system. If an essential service is lost, it can be replaced by another service that supports mission fulfillment in a different but equivalent way. However, the identification and protection of essential services is an important part of a practical approach to building and analyzing survivable systems.

V. Information Security Systems Features

Today, security in one form or another is a requirement for an increasing number of embedded systems, ranging from low-end systems such as PDAs, wireless handsets, networked sensors, and smart cards, to high-end systems such as routers, gateways, firewalls, storage servers, and web servers. Technological advances that have spurred the development of these electronic systems have also ushered in seemingly parallel trends in the sophistication of security attacks. It has been observed that the cost of insecurity in electronic systems can be very high [1].

Describing ISS define the following characteristics: openness, concurrency, scalability, fault tolerance, transparency, community resources, complexity and unpredictability reaction to DF influences [5].

For such systems, there are several factors that are moving security considerations from a function-centric perspective into a system architecture design issue. For example [1]:

--an ever increasing range of attack techniques for breaking security such as software, physical and side-channel attacks require that the embedded system be secure even when it can be logically or physically accessed by malicious entities. Resistance to such attacks can be ensured only if built into the system architecture and implementation;

--the processing capabilities of many embedded systems are easily overwhelmed by the computational demands of security processing, leading to undesirable tradeoffs between security and cost, or security and performance;

--battery-driven systems and small form-factor devices such as PDAs, cell phones and networked sensors often operate under stringent resource constraints (limited battery, storage and computation capacities). These constraints only worsen when the device is subject to the demands of security;

--embedded system architectures need to be flexible enough to support the rapid evolution of security mechanisms and standards;

new security objectives, such as denial of service and digital content protection, require a higher degree of co-operation between security experts and embedded system architects.

Information security systems in embedded systems consist of interrelated and interacting SE large number which can perform multiple functions, thereby increasing their sensitivity to the DF influences. These aspects unlike the branches of ships, aircraft and information systems design leads to a different survivability assessment approach [5].

VI. The Method Exploitation

The method is an engineering process that delivers an assessment of the survivability of current systems, proposed systems and modifications of existing ISS. This is a four-step process. *Step 1*, mission objectives and usage requirements for the security system are examined and the architecture is determined. *Step 2*, based on the mission objectives and failure consequences, the essential services (those services which must be survivable) and essential assets (those assets that must be maintained during an attack) are identified. Then usage scenarios are determined for the above based on how the business functions. The above are then combined and associated with the architecture of the ISS to define essential SE (ones that must be able to deliver the essential services and protect the essential assets during an attack). *Step 3*, intrusion scenarios are selected to determine the compromisable SE (the ones that can be penetrated). The final step is to determine the vulnerable SE of the architecture (the essential SE that are compromisable). *Step 4*, the SE are analyzed for the three key survivability properties of resistance, recognition and recovery. The deliverable is a Survivability Map, which is a chart associating all attack scenarios with the corresponding vulnerabilities to associate the current and recommended architecture strategies for resistance, recognition and recovery [9].

The above process is carried out by two teams, the company team (CT) and the outside security team (ST). The two teams interact through a series of meetings. The CT delivers the mission statement, business processes and system architecture to the ST. The ST then uses the information to determine the essential SE and reports it back to the CT. The ST then does the attack analysis and reports back the compromisable SE to the CT. Then the Survivability Map is determined by the ST and given to the CT.

The above process is not necessarily linear. Information can be revised at any joint meeting and the revisions used to update the results of any step. This is called a “spiral process” to point out that overall process can turn back on itself. Any step can be repeated and even at the end, the first step could be done again if new information is presented.

VII. Security system degradation levels

Analyzing ISS automated control system survivability it is established a connection between ISS automated control system degradation levels, ISS equipment and ISS degradation levels.

Information security systems in accordance with its parameters, management system state, equipment and its management system may be subjected to different functioning quality degradation levels (fig. 1).

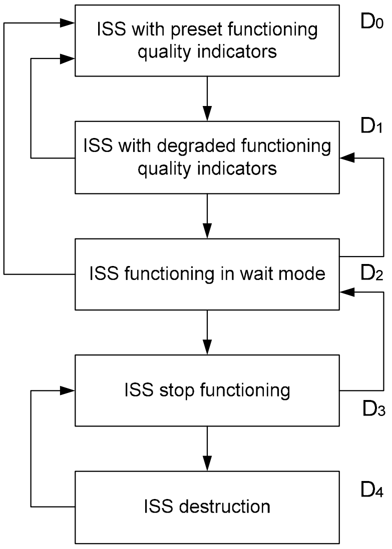
ISS with preset functioning quality indicators
D0
ISS with degraded functioning quality indicators
D1
ISS functioning in wait mode
D2
ISS stop functioning
D3
ISS destruction
D4

Fig. 1. Information security system functioning degradation levels

Information security system works with desired functioning quality indices both in stationary and instationary (extreme conditions) modes meets the requirements that apply to it, and is a zero level (Surv≥0.7) of degradation (D_0).

On the first level of (D_1) information security system degradation (0.4≤Surv<0.7) works with downgraded functioning quality indices and lower than the nominal output parameters. Transition on the first level of degradation can be caused by failures in the security system management, security system equipment, such equipment management system, and power requirements. Economic losses at this checkpoint are small. The period of stay at this level of degradation for ISS may be transient, sufficient to recover equipment that has denied. Then ISS returns to zero level of degradation.

Under certain conditions, ISS can switch to the second level (Surv<0.4) of degradation “idling” (D_2), that is casual security system disconnect from the electricity circuit. At the second level of degradation ISS can go from the zero or first level of degradation. An economic loss in the transition of ISS work is increasing. On the second level of degradation ISS may return to the first or zero level of degradation.

The ISS third level of degradation is the “stop” (D_3). The security system forced stop causing large economic losses. At this level of degradation ISS can go from any previously described levels of degradation.

At zero or first level of degradation for ISS may return through the implementation of the algorithm run.

Last, the fourth level of degradation (D_4), is a catastrophic state of ISS irreversible “destruction” (Surv=0). At this level economic losses reach considerable size, physical loss may be caused (ISS SE physical destruction, terrorist acts, etc.).

The security system transition from the work mode with desired functioning quality factors at the level of degradation is determined by changes in the security system parameters, ISS management degradation, ISS equipment and management system of this equipment, energy system state.

While security automated control system is investigating, determine the appropriate connectivity between security management system degradation levels and security system equipment with information security system, as a management object.

VIII. ISS Survivability Assessment Method

Structural elements states description [2]. Each SE is injected two logical variables: x_i – i-th element efficiency indicator (x_i=1, if it is efficient and x_i=0 otherwise), y_i – efficient element status (y_i=1, if the element is working, y_i=0 otherwise). The z_{ij} indicators are introduced to avoid the DF influence on functional elements:

$$z_i = V_{(j)} z_{ij},$$

where z_{ij}=1, if j-th type DF affects the i-th functional element, z_{ij}=0 otherwise. Now it is possible to express the structural elements state indicators:

$$u_{i0} = 1[e_0] = x_i y_i \bar{z}_i; \; u_{i1} = 1[e_1] = x_i \bar{y}_i \bar{z}_i;$$

$$u_{i2} = 1[e_2] = \bar{x}_i \vee x_i z_i.$$

Setting logical dependencies. Logical equations for efficient element’s unknown states are based on physical processes dynamic models preliminary analyses taking into account the actions of emergency protection, management and reconfiguration:

$$y_i = f_{y_i}(x_k, y_j, z_k, k = 1,...,N, j \in M_i), \quad (1)$$

i=1,…,N, where *N* – number of elements in the system, M_i – elements set which are adjacent to the *i*-th element. A set of expressions as (1) creates a logical equations closed system representing in vector form as

$$Y = f_Y(X, Y, Z). \quad (2)$$

The advantage of this record is that for efficient element description are used only his immediate environment and not necessary to examine the entire system. Then more of these and rather simple dependencies efficient element explicit dependence of other elements and DF efficiency characteristics can be found using different mathematical methods. System efficiency is determined using its elements efficiencies and dependencies as (2). The main for many systems is a source elements relatively small group state. System efficiency is determined considering the state of all other elements, because of the indirect links that appear in (2). For the system which consist on one function efficiency logic functions write as

$$F = f(X, Y, Z). \quad (3)$$

As a multifunctional system dependence as (3) is written for each function separately. If it is necessary to simultaneously perform all functions, then

$$F = \&_{(i)} f_i(X, Y, Z). \quad (4)$$

where f_i – logical function $\&_{(i)}$ – i-th system feature indicator. The proposed method for system states describing does not require all elements states combinatorial enumeration. The f_i functions are logical equations formal systems.

Solving systems of logical equations. The equation system (2) is linear and can be brought to be the form:

$$y_i = a_i \vee a_{i1} y_1 \vee a_{i2} y_2 \vee ... \vee a_{iN} y_N, a_{ij} = 0, \quad (5)$$

where a_i and a_{ij} – factors that clearly expressed by x_i and z_i. There are different ways of logical equation systems solving including the determinants method, lookup method, matrix method etc. Solving (5) type $Y=g_Y(X,Z)$ it is necessary to substitute in (3) or (4) and obtain an explicit expression

$$F = f(X, g_Y(X, Z), Z) = g(X, Z). \quad (6)$$

Note that the logical equation solution needs to be done many times: once for the basic structure of S_0, when all z_{ij}=0, and yet many times as there are different kinds of DF. In the end, turning over all kind of disturbances in single and multiple DF it is possible to get a full set of functioning institutions in the system. The (6) function admits, therefore, *d*-survivability and *m*-survivability analysis through sorting elements state vector.

Structural elements and external influence probabilistic description. Every ISS structural element that is presented in probabilistic model with probability p_i=P(x_i=1) that element is efficient any moment. When DF is appear z_{ij}=1 then i-th element resistance to the j-th DF (DF for ECN ISS consider only from threats model) can be counted using a_{ij} probability that element maintain efficiency when there are DF influence. Besides set the probability of getting the element in the DF *j*-th factor sphere of influence.

Capacity function transformation to a form transition to replacement. It can be switched to distinguish the full or partial replacement form. The full replacement forms are perfect disjunctive normal form (PDNF), form in basis “logical conjunction-negation” and orthogonal forms disjunction. After bringing to one of these forms it is possible to replace logical variables and logical operations on probability and arithmetic. It is possible to take the transition form to partial replacement if such transformations are difficult because of their complexity.

Mixed form notation. Replacing variables in irretrievable converted efficiency function is partial substitution which resulted in some variables and logical operations replace on probabilistic and arithmetic operations, other variables and operations are moving in the arithmetic expressions exponent. Received form is called mixed form because it contains both logical and probability variables, and two groups of operations: arithmetic and logical.

Survivability indicator definition. Using logical variables substitution procedure in mixed forms that are compiled for the S_0 basic structure and other efficient structures S_i it is possible to find $P(t/S_0)$ and $P(t/S_i)$ probability, then conditional survivability function $G_i(t)$. Next step – find survivability function, unconditional survivability function, average number of DF.

Enabling the integration between ISS SE after DF influence. In case of successful malicious attacks implementation occurs functioning quality degradation which causes denial of services, system losses, time delays, security service reduce – ISS resources lack situation. In this case it is necessary to estimate ISS survivability using streaming model. The results of it functioning enable efficient information flows redistribution between ISS SE. The challenge is to find the original graph collapse on *p* components probability; the edges (or vertices) existence probability; two graph peaks membership to one component probability; existence graph upper and lower probability limits, ribs of which exist with probability p [2]. Establishing contact with a given percentage of graph vertices after a single DF influence probability:

$$\beta = 1 - \exp\{-d\sum_{k=0}^{k_s-1}\frac{5^k}{k!}e^{-5}b\} \tag{7}$$

vertices number remaining:

$$\sum_{k=1}^{k_s-1} g_k^1(\eta) \tag{8}$$

where b – connection establishing probability for attacks density 100 per minute; certain graph peak defeat probability $\Delta/D=0.05$; $k_s=1$.

IX. Conclusion

The logic-probabilistic method in comparison with the exhaustive hypothesis search method and equivalent circuits method has the following advantages: simplicity, is subject to automation, used to analyze the survivability of not only systems with the same SE (as opposed to the exhaustive hypotheses method), accuracy and speed (unlike the equivalent schemes method), using streaming survivability assessment model enables (quantitative) to communicate between ISS SE after DF influences and determine the ISS SE number which will remain after DB influences.

References

[1] Kocher P. Security as a new dimension in embedded system design / P. Kocher, R. Lee, G. McGraw, A. Raghunathan, S. Ravi // Proceedings of the 41st annual Design Automation Conference. – 2004. – P. 753-760.

[2] Garasym I. Information security system survivability assessment method based on logical-probabilistic models / I. Garasym // Proceedings of the XIth International Conference CADSM 2011. – Polyana, Svalyava (Zakarpattya), Ukraine, 2011. – P. 160-161.

[3] Dudykevych V.B. System to protect information that tend to survivability. Concepts / V.B. Dudykevych, J.R. Garasym / / Scientific and technical journal "Modern information security," Special issue. 2010. № 4. P. 6-13 (in Ukrainian)

[4] Garasym J. Develop a model assessment of viability for information security systems // Computer Science and Engineering: Proceedings of the IV International Conference of Young Scientists CSE-2010. Lviv: Publishing House of Lviv Polytechnic National University, 2010. P. 320-321 (in Ukrainian)

[5] Dudykevych V. Survivable security Systems Analysis / V. Dudykevych, I. Garasym // Computer science and information technologies: Materials of the VIth International scientific and technical conference CSIT 2010. – Lviv : Publishing House Vezha&Co, 2010. – P. 108-110.

[6] Garasym J.R. Notion of survivability systems for information protected corporate networks / J.R. Garasym, V. Dudykevych // Proceedings of the Third International Scientific Conference "Information and Economic Security (INFECO-2010)". Kharkov, 2010. Issue 3 (84). P. 107-109.

[7] Ellison R. J. A Case Study in Survivable Network System Analysis / R. J. Ellison, R. C. Linger, T. Longstaff, N. R. Mead // CMU/SEI-98-TR-014, ESC-TR-98-014. – 1998. – P. 1-37.

[8] Ellison R. J. Survivable Network Systems: An Emerging Discipline / R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, N. R. Mead // CMU/SEI-97-TR-013, ESC-TR-97-013. – 1999. – P. 1-51.

[9] Dudykevych V.B. Behavior of protection under the influence of destabilizing factors / V.B. Dudykevych, J.R. Garasym // System analysis. Informatics. Management (SIAU 2011): Proc. of the II All-Ukrainian Scientific Conference. Kiev: CPU, 2011. P. 76-78.

Prof. Valeriy Dudykevych is Honored Inventor of Ukraine, a Head of West Regional Research-Scientific Information Security Center, a Head of the Information Security Department of Computer Technologies, Automation and Metrology Institute of Lviv Polytechnic National University.

Date of his birth is 23.11.1941, Lugansk (Ukraine).

Education and Degrees Received:

1963 – Speciality: “Electrical Appliances”, Qualification: electrical engineer, Lviv Polytechnic Institute, Lviv (Ukraine);

1969 - 1971 – Ph.D. student, Lviv Polytechnic Institute, Lviv (Ukraine);

1971 – PhD in “Automatics and Telemechanic elements and devices”, Lviv Polytechnic Institute, Lviv (Ukraine);

1973 – Associate Professor, Automation and Telemechanics Department, Lviv Polytechnic Institute, Lviv (Ukraine);

1991 – Doctor in “Devices and Methods of Measuring Electrical Quantities”, Lviv Polytechnic State University (Kyiv, Ukraine);

1993 – Professor of Automation and Telemechanics Department, Lviv Polytechnic State University, Lviv (Ukraine);

1993 – Academician of International Academy of Computer Science and Systems;

1994 – Honored Inventor of Ukraine.

Professional Activity:

1963 - 1969 – Assistant, Automation and Telemechanics Department, Lviv Polytechnic Institute, Lviv (Ukraine);

1972 - 1976 – Assistant Dean of Automation Faculty, Lviv Polytechnic Institute, Lviv (Ukraine);

1992 - 2001 – Dean of Automation Faculty, Lviv Polytechnic National University, Lviv (Ukraine);

1993 – Head of Automation and Telemechanics Department, Professor, Lviv Polytechnic State University, Lviv (Ukraine);

2004 – Head of West Regional Research-Scientific Information Security Center, Lviv (Ukraine);

2006 - present – Head of Information Security Department, Professor, Lviv Polytechnic National University, Lviv (Ukraine).

Research interests are transducers frequency signals, the number-switching converters codes for measurement devices and control, medical instrumentation, test measurement systems, methods and techniques information protection.

More than 500 publications, including 2 textbooks, 187 patents, 1 glossary of information security, methodological manuals, scientific-research papers and conference proceedings.

Iurii Garasym is an Assistant of Information Security Department of Computer Technologies, Automation and Metrology Institute of Lviv Polytechnic National University.

Date of his birth is 11.08.1987, Lviv (Ukraine).

Education and Degrees Received:

2004 - 2009 – Master Degree in Information Security with limited access and automated processing, Lviv Polytechnic National University, Lviv (Ukraine);

2010 - present – Ph.D. student, Information Security Department, Lviv Polytechnic National University, Lviv (Ukraine).

Professional Activity:

2010 - present – Assistant, Information Security Department, Computer Technologies, Automation and Metrology Institute, Lviv Polytechnic National University, Lviv (Ukraine).

Research interests are secure enterprise communication networks, information security systems survivability, socio-technical security, information security systems audit.

More than 45 publications, including methodological manuals, scientific-research papers and conference proceedings.