10th INTERNATIONAL SCIENTIFIC CONFERENCE
ON DEFENSIVE TECHNOLOGIES
OTEH 2022
Belgrade, Serbia, 13 – 14 October 2022

SECURITY SYSTEM DESIGN USING A SOFTWARE SOLUTION

PREDRAG RANITOVIĆ
School of Business, Novi Sad, predrag.ranitovic@gmail.com

SANJA LONČAR
School of Business, Novi Sad, sanja.lonchar@gmail.com

Abstract: *The development and design of a security system is a complex process, made up of a number of specific elements. Defining and taking into account that, there are two basic elements in the design of security systems: the basic functional model of security systems and the model of management and protection of information as a key resource of security systems. There is a need to analyse the basic architecture of the security system and define its framework and to analyse the management system and information protection and to define its framework. By observing and analysing these systems in the context of the application of information technology solutions in the process of development and design of security systems, we get a key basis for the application of software solutions in the process of designing security systems. This application of software solutions is reflected in the development of conceptual software under the test name "projectdrive" the expediency of which would be characterised through a more efficient and effective manner in the approach to the design and development of security systems. This would give us a unique functional approach-concept-model of the security system, but also an information technology tool "software" (beta phase) for the purpose of designing and developing security systems.*

Keywords: *Software - Security system - ISO standards - IT system*

1. INTRODUCTION

Modern security systems are prone to global security pressures which produce unsafe activities, by creating new phenomena, models and conditions in which and under which the functioning of a security system takes place.

Therefore, security systems require reengineering and adaptation to these new tendencies, through designing a new security system based on software solutions.

Also, the generally growing dependence on information puts in focus information as a dominant resource of the security system, stating the need to ensure appropriate steps in order to form adequate information protection.

The feature of the importance of information as a resource of the security system, as well as the function of its flow speed, places them among the key elements of the security system, Figure 1 [1].

Availability, integrity and confidentiality of information are the main carriers of the function of information flow speed.

Observing current events in the world regarding information protection as well as other security aspects, it is concluded that it is impossible to predict the "dynamics" of threats to the security system.

The speed at which they arise, the forms of the attacks and their actions are on increase thus it is completely pointless to take effective measures against specific and established threats.

Modern security threats, more precisely their advanced sophistication, have imposed the need to deal with general and systemic security issues. Classical security systems such as the army, police, intelligence and security services and civil protection must adapt to the new security reality and, through adequate design of the security system, seek solutions for new "security challenges" [2].

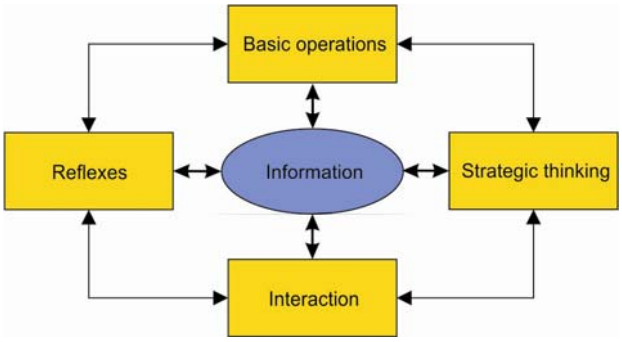

Figure 1. System function of information

Only a comprehensive, systematic approach to the design of an adequate security system on the basis of software solutions and supported by them, will contribute to establishing a satisfactory level of security.

2. MODEL OF A SECURITY SYSTEM

A security model is defined by the application of certain activities to the area of security, characterizing security as a concept of protection-security against danger, damage, loss and crime.

Taking into account the aspiration towards designing an "adequate" security system, determining the concept directly affects the design context and the approach to

designing a security system through software solutions.

By analysing the macro/micro model of the security system, we define the basic model of the security system, Figure 2 [3,4].

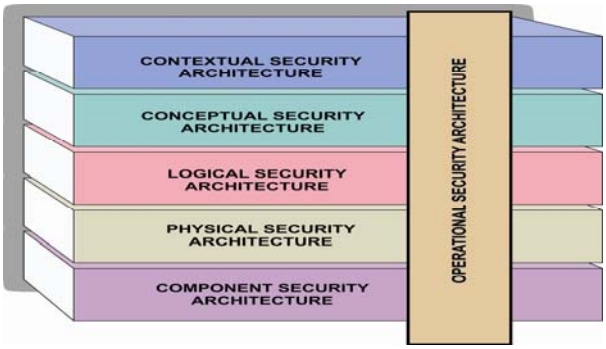

Figure 2. Basic model of the security system

The basic model of the security system includes elements defined according to the levels of their activity:

- Contextual elements represent the first level of the security system and they are conceptually defined by the formulation of the basic "framework" of the system, its flaws and approaches to solving those issues. They were designed in compliance with the following elements:
  - Field of activity,
  - Risk model
  - Process model,
  - Organisation
  - System positioning and
  - Time positioning.

- Conceptual elements represent the second level of the security system and they are conceptually defined by the formulation of the comprehensive system strategy. They were designed in compliance with the following elements:
  - Features,
  - Objective,
  - Strategy,
  - Entity model,
  - Domain model and
  - Deadline.

- Logical elements represent the third level of the security system and they are conceptually defined by the formulation of the form of the system and its effects. They were designed in compliance with the following elements:
  - Information model,
  - Policy
  - Services,
  - Entity scheme
  - Domain scheme and
  - Process cycle.

- Physical elements represent the fourth level of the security system and they are conceptually defined by the formulation of the forms of applied resources and system carriers. They were designed in compliance with the following elements:
  - Information system,
  - Procedures,
  - Mechanisms,
  - Entity interface,
  - Domain platform and
  - Time structuring.

- Component elements represent the fifth level of the security system and they are conceptually defined by the formulation of the consistency of the original form of a resource and the system carriers. They were designed in compliance with the following elements:
  - Information structure,
  - Standards,
  - Tools,
  - Identity,
  - Location and
  - Time.

- Operational elements represent the sixth level of the security system and they are conceptually defined by the formulation of the effects of the management. They were designed in compliance with the following elements:
  - Management,
  - Risk management,
  - Strategic management,
  - Management of Human Resources,
  - Operational management and
  - Time management.

- Architecture of the implementation of the system represents the seventh level of the security system. It is conceptually defined by the formulation of the security system implementation course. They were designed in compliance with the following elements:
  1. Implementation plan
  2. Implementation management
  3. Testing

- Architecture of the analysis of the system represents the eighth level of the security system. It is conceptually defined by the formulation of the security system analysis course. They were designed in compliance with the following elements:
  - Set of reports and
  - Improvement plan.

According to the characteristics of the elements they project, the "factors" of real application and the basic conceptual solution, the presented levels are formulated in the basic model of a security system. Looking at the basic model of a security system, the levels are clearly visible as the carriers of the system architecture. In order for them to be formulated more precisely through the characteristics of the elements that make them up, they are systematized into a constructive model of a security system, Table 1.

Table 1. A constructive model of a security system

Matrix	Property (What?)	Motivation (Why?)	Processes (How?)	People (Who?)	Location (Where?)	Time (When?)
Contextual elements	activity	risk model	process model	organization	system positioning	time positioning
Conceptual elements	characteristics	aim	strategy	model of an entity	domain model	deadline
Logic elements	information model	policy	services	entity scheme	domain scheme	process cycle
Physical elements	information system	procedures	mechanisms	entity interface	domain platform	time structurednes
Component elements	information structure	standards	tools	identity	position	time
Operational elements	management	risk management	strategic management	human resources management	operational management	time management

Functionally variable

3. INFORMATION SECURITY MODEL

An information security management system (ISMS) represents one of the most dominant forms of the information protection method according to the generally accepted context and an integral part of the security system [5, 6].

The basic principle that defines an information security management system (ISMS) is based on the PDCA Plan-Do-Check-Act model, Figure 3. It formulates the elements of establishment, implementation, enforcement, monitoring, analysis, maintenance and improvement of information security.

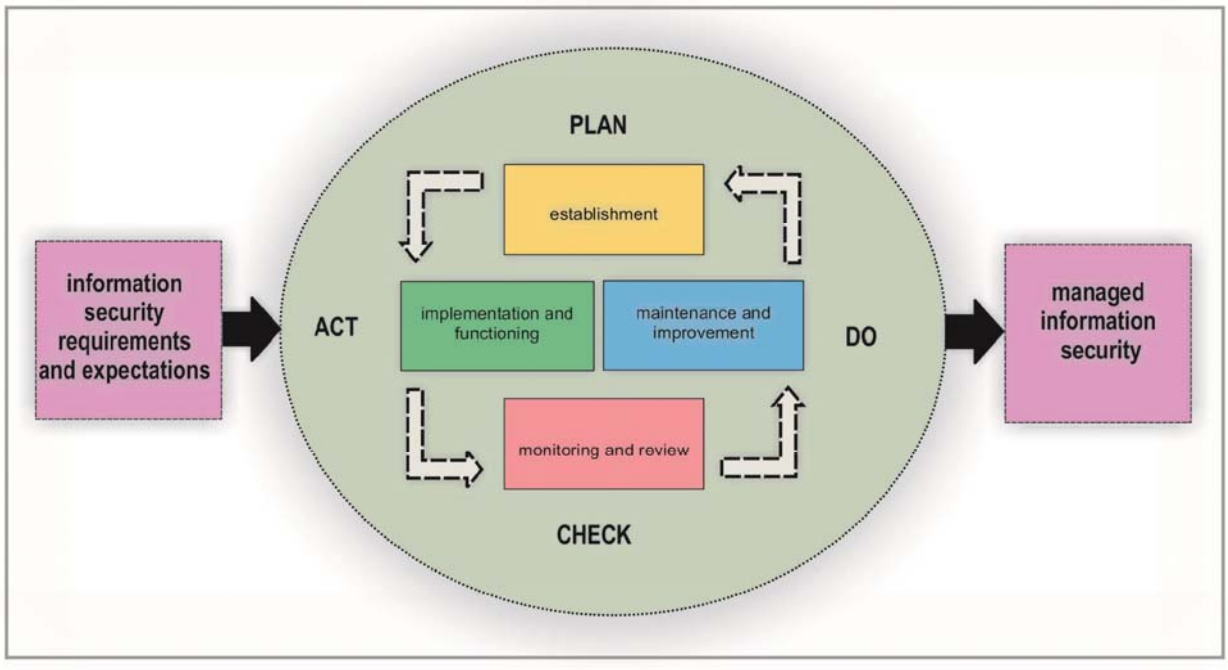

Figure 3. Information security management system (ISMS) model

PHASE (PLAN)

The Plan phase establishes the preparation of the implementation of the information security management system (ISMS). The preparation includes defining the scope and policy of the mentioned, thereby ensuring a focus on appropriate assets, human resources, system processes and risk assessment, on the basis of which risks to information are identified and analyzed. By formulating a risk assessment, the direction of the implementation of the information protection system (ISMS) is designed.

The phase (Plan) is conceptually defined by a model, Figure 4.

Figure 4. Model of (Plan) phase concept

PHASE (DO)

Phase Do implements the defined elements of the Plan phase. As the basis of the mentioned, the risk remediation project plan and its implementers are identified, thus guiding the information protection system (ISMS).

The phase (Do) is conceptually defined by a model, Figure 5.

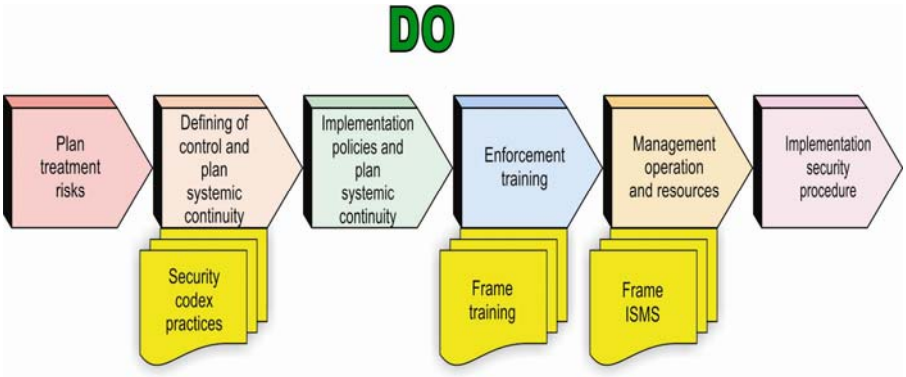

Figure 5. Model of (Do) phase concept

PHASE (CHECK)

The Check phase reviews policy, procedures and records with the aim of checking their effectiveness and efficiency in terms of risk management, while also defining the internal audit of the ISMS.

The phase (Check) is conceptually defined by a model, Figure 6.

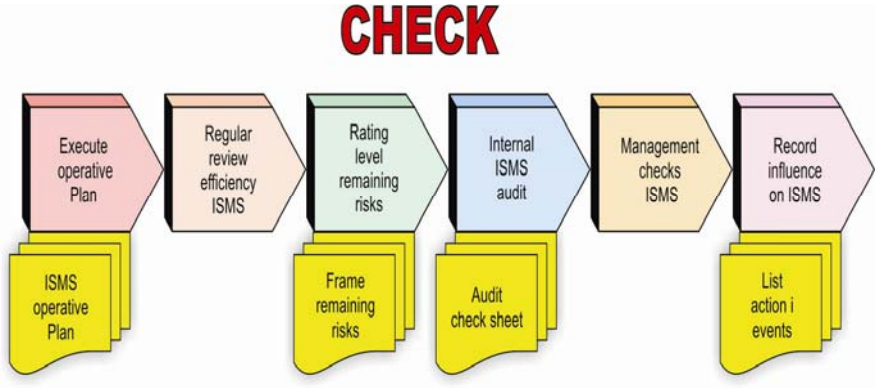

Figure 6. Model of (*Check*) phase concept

PHASE (ACT)

The Phase Act defines the improvement of an information security system (ISMS) by incorporating changes, additions, preventive measures or the overall improvement of the system and viewing security as a process of continuous review and improvement rather than a specific "destination".

The phase (Act) is conceptually defined by a model, Figure 7.

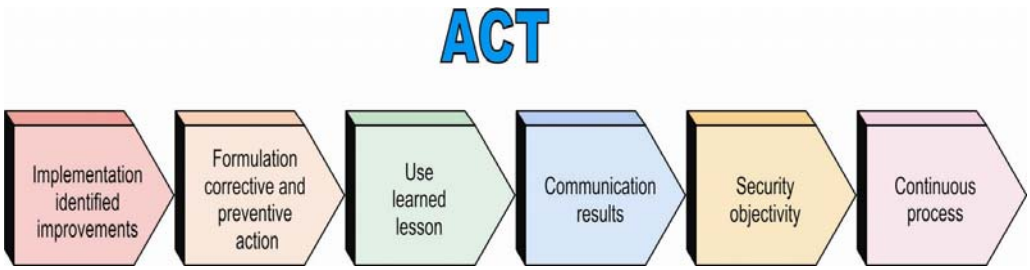

Figure 7. Model of (*Act*) phase concept

4. SOFTWARE

Model testing was performed on a pilot project - the PROJECTDRIVE software tool, Figure 8, constructed in line with a new approach-concept-model of the security system based on the intersection of the constructive model of the basic security system and the model of information protection and the basics of software design [7-11].

The PROJECTDRIVE source code is based on functionally dependent integration of security system elements and information protection methods, defined according to schemes.

PROJECTDRIVE was designed for the purpose of conducting testing of a new approach-concept-model of a security system and was constructed through a team collaboration with a software developer, making a new and completely unique software of its kind

PROJECTDRIVE

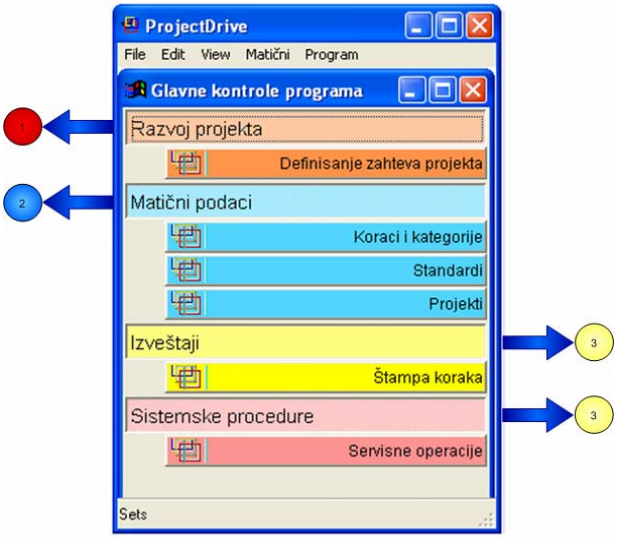

Figure 8. Software's main Interface

The concept of PROJECTDRIVE is to provide an easier approach to defining security system design requirements. The basis for this are three sub-modules marked with symbols, Table 2.

Table 2. Basic modules

1	Project development
2	Master data
3	Reports - system procedures

4.1. Project development

The development of a project defines the basic requirements of designing a security system of the civil-military management system. It is represented by a software interface for defining project requirements, Figure 9.

The concept of MODULE 1 includes 36 steps within which certain values are formulated. By characterizing the ones with the same name, a list of security system design requirements is formulated, which is a practical instruction for the formation of the security system of the civil-military management system.

The topography of the software interface (defining project requirements) is marked according to symbols, Table 3.

Table 3. Basic elements of software interface (defining the project reqiurements

1	Basic steps
2	Values
3	Tools
4	Integration values

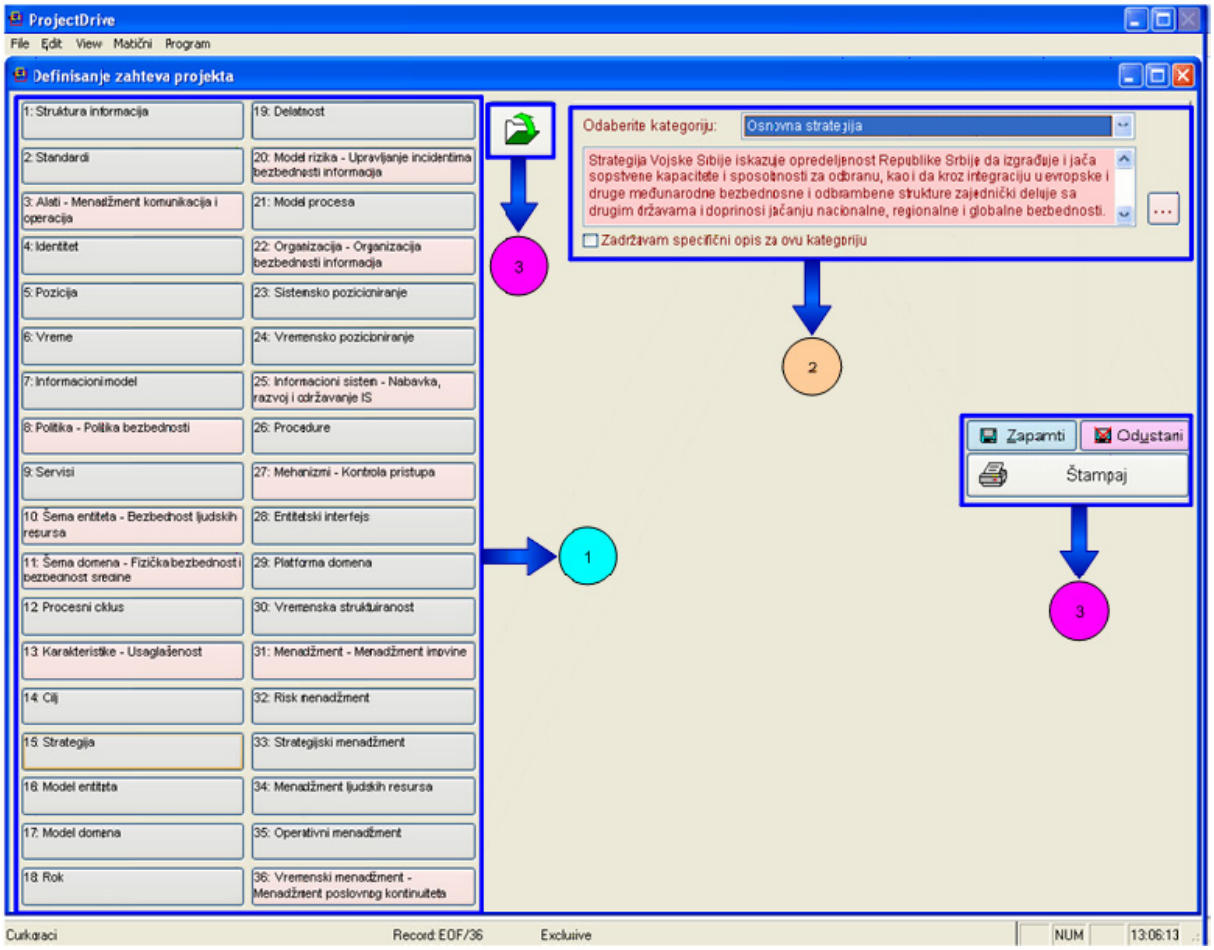

Figure 9-1. Defining project requirements Interface

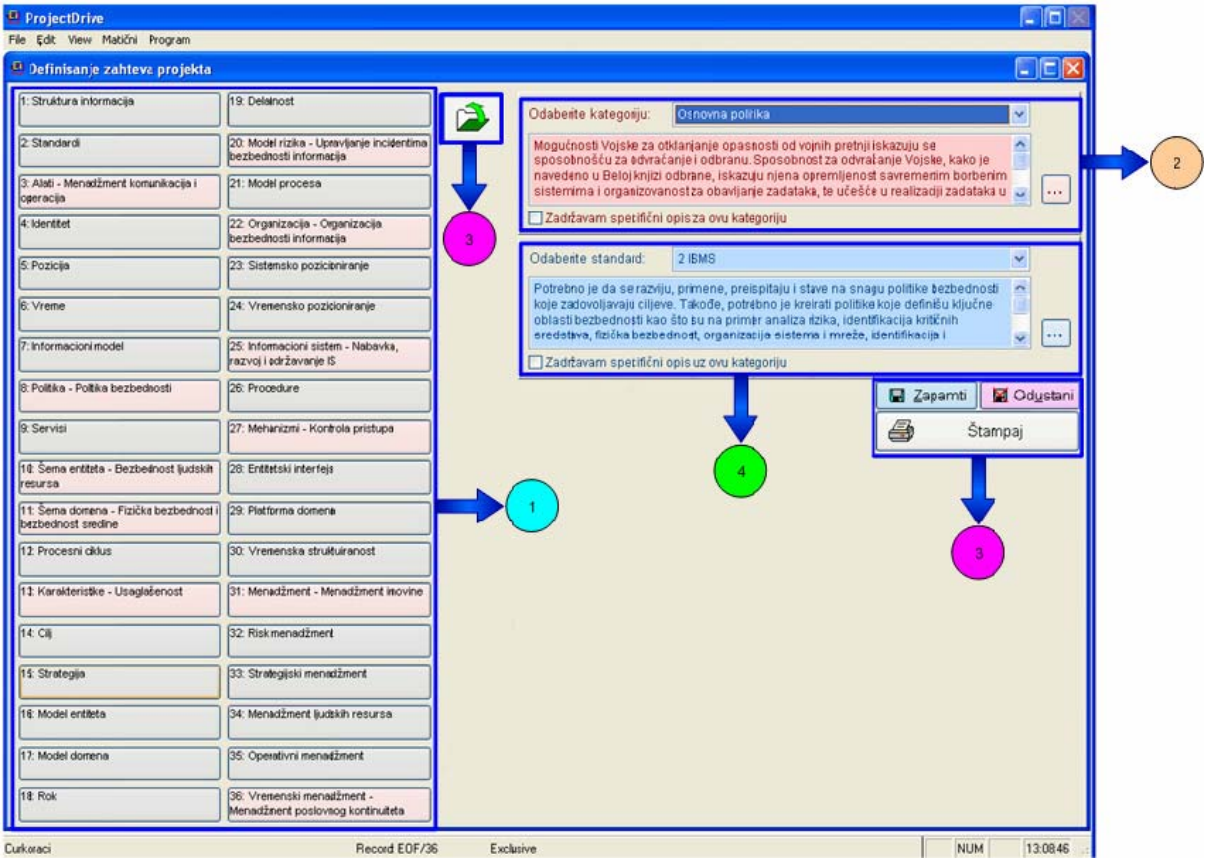

Figure 9-2. Defining project requirements Interface

4.2. Master data

The master data define the values of the security system design requirements of security system representing MODULE 2. They are logistically classified according to the software interface:

1. Steps and categories,
2. Standards and
3. Projects.

1. Steps and categories

The steps and categories define the values of the basic requirements of designing the security system. They are shown by the software interface, in steps in defining a project, Figure 10.

The concept of steps and categories of MODULE 2 includes the formulation of the values related to the 36 steps of MODULE 1. The form and the meaning of each step is determined according to the character of the steps in the process of forming the security system. The topography of the software interface (steps in defining a project) is marked according to symbols, Table 4.

Table 4. Basic elements of software interface (steps in defining a project)

1	Basic steps
2	Description of the steps
3	Step categories
4	Category values
5	Integration
6	Tools

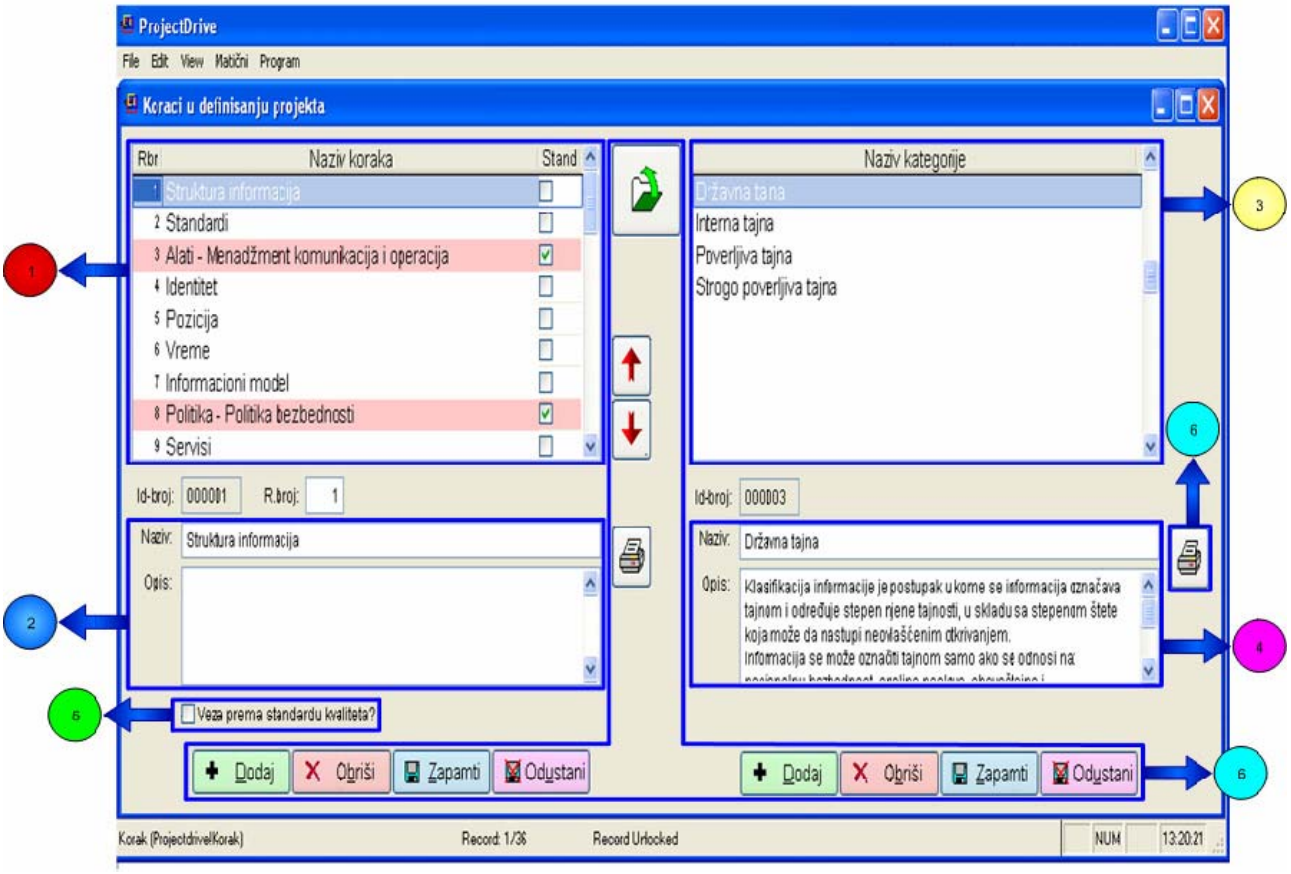

Figure 10. Interface steps in defining a project

2. Standards

Standards define the values of the integration of the basic requirements of designing a security system.. They are represented by a software interface (list of reference standards), Figure 11.

The concept of the MODULE 2 standard includes formulating the values of 11 steps of integration with 36 steps of MODULE 1. The steps of integration are formulated according to the requirements of the information protection system ISMS. The topography of the software interface (the list of reference standards) is marked according to the symbols, Table 5.

Table 5. Basic elements of software interface (a list of reference standards)

1	Основни кораци
2	Вредности
3	Алати

3. Projects

The projects define the framework of the basic requirements for designing a security system.. Projects are represented by the software interface, Figure 12.

The concept of the MODULE 2 project includes a unique marking of separate projects of the design process of a security system, indicating the possibility of limiting the scope of the project by canceling certain steps of the security system. The topography of the software interface (projects) is marked according to symbols, Table 6.

Table 6. Basic elements of software interface (projects)

1	Basic projects
2	Project description
3	Step frame
4	Step base
5	Tools

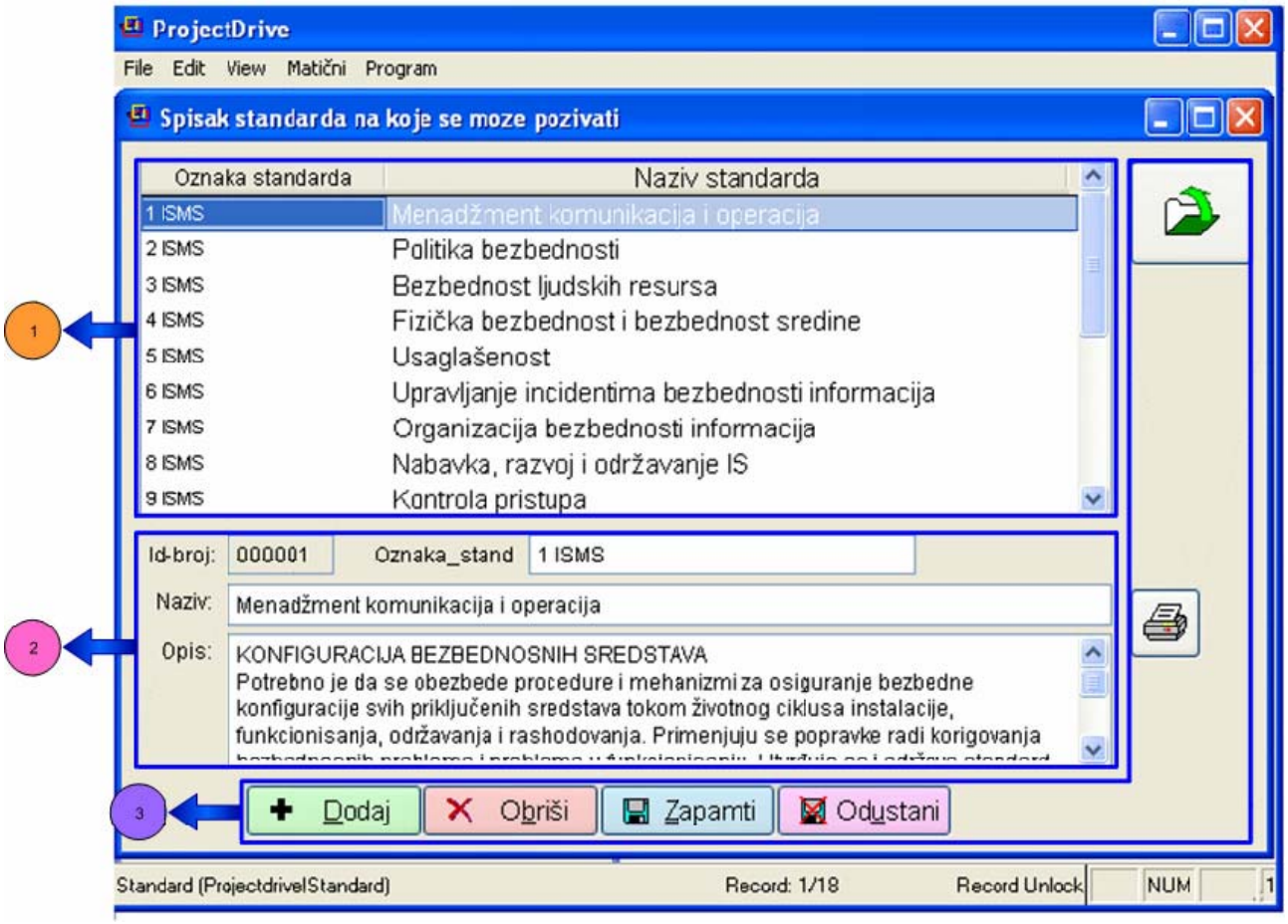

Figure 11. Interface list of reference standards

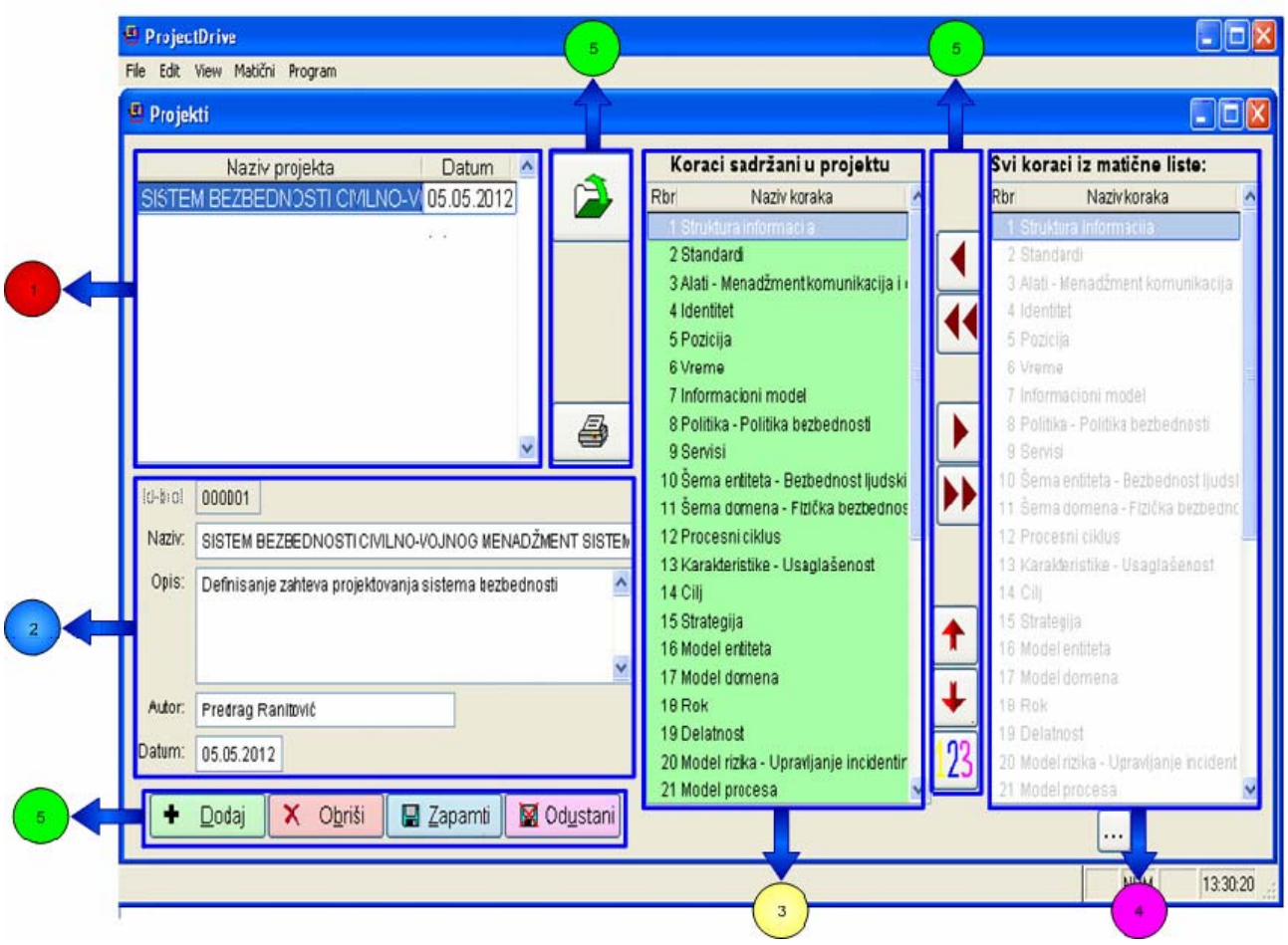

Figure 12. Interface projects

4.3. Reports-system procedures

Reports-system procedures define logistic support options for the tools for designing security systems of the civil-military management system representing MODULE 3, classified according to the hypothetical software interface:
1. Print steps and
2. Service information.

1. Print steps

Print steps should hypothetically define the archive of MODULE 1 and MODULE 2 as the conditions for designing a security system of the civil-military management system. The concept of print steps of MODULE 3 includes organizational support for the design of a security system of the civil-military management system.

2. Service information

Service information should hypothetically define the logistic basis of *HELP* of all the MODULES. The concept of service information of MODULE 3 includes the logistics support to the tools for designing a security system of the civil-military management system.

5. CONCLUSION

The main aim was to create a new approach-concept-model of the security system based on the research of the concept of functional dependence of information protection methods and the security system through a software solution.

Analyzing and observing the elements of the security architecture through the prism of the new approach-concept-model of the security system, contributed to the improvement of the existing ones and the acquisition of new practical-theoretical knowledge in the field of designing modern security systems.

The prominent key result of the paper is the formulation of unique system security schemes integrated through a security platform (software) which represents a new functional model of a modern security system.

The concept of the entire operation of functional dependence of information protection methods and security systems based on software development is defined in accordance with the conceptual flow of the basic phases of the security system.

By combining all aspects of this process, a clear picture of the scientific idea based on practical-theoretical elements is produced, Figure 13.

Figure 13. Model-concept

References

[1] Tipont, H., Krause, M.: "Information Security Management - Sixth Edition", Auerbach Publications, 2007.

[2] Andress, J.: "The Basic of Information Security", Elsevier, 2011.

[3] Andy, J., Ashenden, D.: "Risk Management for Computer Security", Elsevier, 2005.

[4] Hangos, K., Cameron, I.: "Process Modelling and Model Analysis", Academic Press, 2001.

[5] Arnason, S., Willett, K.: "How to Achieve 27001 Certification", Auerbach Publications, 2008.

[6] Calder, A., Watkins, S.: "IT Governance A Managers Guide to Data Security and ISO 27001/ ISO 27001", Kogan Page Science, 2008,

[7] Stewart, M. J.: "Certified Information Systems Security Professional", John Wiley&Sons, 2001.

[8] Alberts, C.; Dorofee, A.: "Managing Infromation Security Risk", Addison Wesley, 2002.

[9] Pour, K. M.: "Cases on Information Technology" Idea Group. 2006.

[10] Rocheleau, B.: "Case Studies on Digital Government", Idea Group, 2007.

[11] Media Garrido, J. A., Martinez Fierro, S., Ruiz Navarro, J.: "Cases on Information Technology Entrepreneurship", Igi Publishing, 2008.