SYSTEMIC APPROACH TO THE DEVELOPMENT OF SECURITY SYSTEMS FOR CRITICAL INFRASTRUCTURE PROTECTION AS A RESEARCH METHODOLOGY APPLIED AT THE CENTER OF COMPETENCE *QUASAR*

Chief Assistant Dr. Eng. Panevski V.S.
Bulgarian Academy of Sciences, Institute of Metal Science Equipment and Technologies with Hydro- and Aaerodynamics Centre "Acad. A Balevski", Sofia, Bulgaria
panevski@ims.bas.bg

Abstract: *Ensuring the security of the population is one of the fundamental policies of the European Union. Various approaches are being implemented in this area, one of which is the creation of critical infrastructure security - national and European.*
In this regard, trough the development and operation of intelligent security systems, with a focus on critical infrastructure, is expected to improve the security of the population in EU Member States. Precisely the synergy of efforts of the scientific and industrial communities in our country for performance of specific models of security systems through the establishment and operation of centres of competence is at the core of this paper.
Keywords*: CENTRE OF COMPETENCE; INTELLIGENT SECURITY SYSTEMS*

1. Introduction

Essentially, Centres of Competence (CoC) are structural cooperation units, comprising scientific and business organizations empowered to undertake strategic market-oriented research for the benefit of the industry. The initiative of the CoC is to achieve a competitive advantage in the industry through access to innovative capacity of the research community. These joint research organizations are the "*new hope"* for our country, as all participants will benefit from shared intellectual property and research, and the national industry will benefit from the knowledge gained and retained both in our country, so are those currently being generated abroad.

How can researchers benefit?

Primarily, the dynamic interaction with industry will ensure the applicability of applied scientific research. A functioning CoC provides a long-term financing mechanism for the rational use of time to achieve planned results, as well as alleviate continuity problems. It should not be overlooked that CoC's access to larger financial flows for the development of research infrastructure will not allow the use of other research schemes. For example, Europe's programme for small and medium-sized enterprises (COSME) provides enhanced access to finance in different phases of their lifecycle: creation, expansion or business transfer. It is precisely through the funding of these activities that research support can be assured.

How will benefit industry?

Through the functioning of the CoC will be provided an opportunity to participate in riskier, long-term market research that, when resolved, can bring a competitive advantage. Access to intellectual property will allow an earlier impact on the exploitation of developed products and systems. Last but not least, networking with leading and influential researchers would help to participate in research initiatives and projects at national and European level. Researchers' access to EC programs such as "Horizon 2020" and the "Marie Curie Program", which form brilliant researchers, plays a key role in the knowledge-based economy Europe is aiming for.

At the same time, EC policy documents on research and innovation state that a *systematic approach "... will ensure that challenges can be tackled while also giving rise to new competitive businesses and industries, fostering competition, stimulating private investments and preserving the level playing field in the internal market*"**[1]**.

Particular attention will be paid to ensuring a balanced and broad approach to research and innovation, which is not only limited to the development of new products and processes and services based on scientific and technological knowledge, but also incorporates existing technologies into new applications and continuous improvement and non-technological and social innovation. The right direction in this area is jointly, research and industry organizations, to build and develop a research and innovation knowledge infrastructure, as well as a mechanism for the open distribution and sharing of products developed for market realization.

For the better understanding of the following text, I will make the following clarifications, namely:

- *"center of competence"* - definition:

*„... top-level scientific complexes, in which the scientific studies are performed following the best world standards and practices"***[2]**;

- *"systematic approach"* - definition:

„*A process used to determine the viability of a project or procedure based on the experiential application of clearly defined and repeatable steps and an evaluation of the outcomes"***[3]**.

The systematic approach is the most sophisticated approach where each system or object, in this case the CoC, is seen as a set of interconnected components having an output coupled to the target and input connected with resources and communication with the outside environment (industry and market), i.e. feedback.

The aforesaid is directly related to the construction of *Center of Competence "Quantum Communication, Intelligent Security Systems and Risk Management" (Quasar)* and its contribution to the of critical infrastructure security development.

2. Quasar and intelligent security systems development

The development of Intelligent Security Systems within the scope of the CoC is closely related to *Work Package 2: "INTELLIGENT SECURITY SYSTEMS"* (WP2) which is headed by the Institute of Metal Science Equipment and Technologies with Hydro- and Aerodynamics Centre "Acad. A. Balevski" (IMSETHC-BAS). WP 2 includes certain activities and stages that ensure its correct and timely implementation (Fig. 2.1).

Within WP2, an analysis of current trends in the development of means to ensure security through the security systems of critical infrastructure (CI) will be done. Carrying out a study of the conditions and algorithm of work in the elaboration of operational procedures for the operation of various modern models of security systems will contribute to a higher level of security and protection of developments. Integration between the organization's business continuity management processes (critical infrastructure, sites of national, regional and local importance) and the development of intelligent security systems by modeling their integration into the organization's management system is essential. All this is provided through the activities and stages for implementation of WP2 **[4]**.

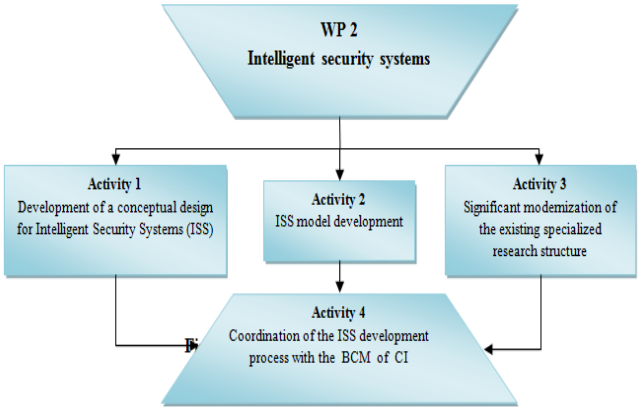

Fig. 2.1: *WP 2- general structure*

Activity 1: Development of a conceptual design for Intelligent Security Systems (ISS)

The activity involves a research of existing contemporary ISS approaches and practices. The specifics of the national critical infrastructure will also be studied, and particularly the objects of national, regional and local significance.

Stages:

– Stage 1. A study of existing contemporary ISS approaches and practices;
– Stage 2. An analysis of the national critical infrastructure, and particularly the objects of national, regional and local significance;
– Stage 3. Development of ISS conceptual design (security system models).

Activity 2: ISS model development

The complexity of this task involves: development of hardware for ISS sensor elements, tools for wireless data transmission, tools for data visualization and for system cyber security. Development of ISS operation software for: ISS sensor elements, wireless data transmission tools, data visualization tools, system cyber security tools, for decision-making in complex risk situations, as well as software for comprehensive system management and for the production of documents needed in the ISS functioning.

Stages:

– Stage 1. Development of hardware for the ISS model(s);
– Stage 2. Development of software for the ISS model(s);
– Stage 3. Development of functional documents for the ISS operation;
– Stage 4. Developing a business model for managing research and innovation in the organisation.

Activity 3: Significant modernization of the existing specialized research structure

Closely related to Activity 1 and Activity 2, Activity 3 is aiming a significant upgrade of the existing research structure, i.e. the Laboratory for Smart Sensor Systems and Technologies and the Laboratory for 3-D Modelling and Rapid Prototyping.

Stage:

– Stage 1. Substantial upgrade of the Laboratory for Smart Sensor Systems and Technologies and the Laboratory for 3-D Modelling and Rapid Prototyping.

Activity 4: Coordination of the ISS development process with the Business Continuity Management (BCM) of critical infrastructure

All activities in the process of creating an ISS model (or models) are inextricably linked to an uninterrupted operation of critical infrastructure. The ISO Technical Committee (ISO/TC 292 Security and Resilience) has laid down the main BCM principles in ISO 22301 “Societal security - Business continuity management systems – Requirements”; ISO 22300 "Societal security - Terminology"; ISO 22313 “Societal security - Business continuity management systems – Guidance” and ISO / TS 22317 “Societal security - Business continuity management systems - Guidelines for business impact analysis (BIA)”. The development of a concept for the specific interactions between these processes will provide data for their modelling and automation. This innovative approach is expected to contribute to a significant reduction of operating time and financial costs in the development, maintenance and upgrade of the organisation's security system.

Stages:

– Stage 1. Analysis of the organisation's BCM, including adopted and standardized international approaches in order to determine the stages/processes providing the input data for ISS development;

– Stage 2: Development of a conceptual model of the integrity between ISS features and BCM processes;

– Stage 3. Development of a concept of the scope of automation and coordination between BCM and ISS models.

Internal links between the WPs and the proper coordination of partners' activities play an essential role in the building up and future development of the security systems development process. This process is discussed in the next section.

3. CoC internal links facilitating the development of ISS

These WPs form the core elements of the functioning of the CoC as a system. The activities included in the work packages and the results planned to be achieved indicate internal links through which the synergy of research and applied science activities are expected.

Within Quasar will be realized four work packages (WP) as follows: WP 1 „Quantum communication“; WP 2 „Intelligent security systems“; WP 3 „Risk management“ and WP 4 „Innovative sensor technologies with multi-purpose application“ (Fig. 3.1)

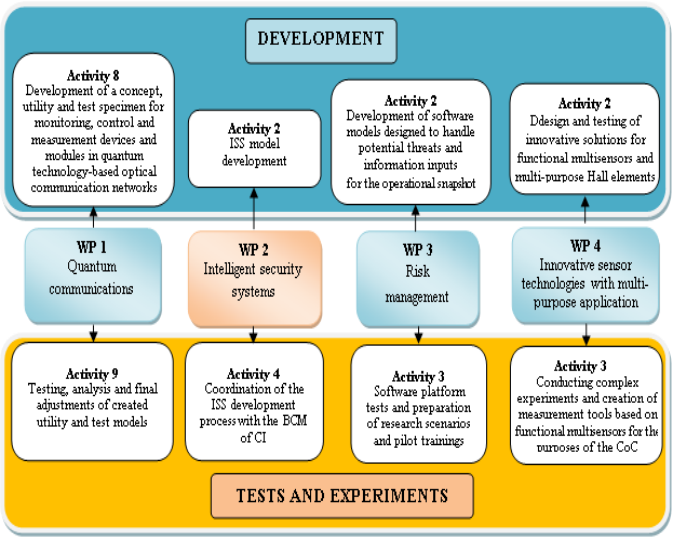

Fig. 3.1*: CoC Quasar general structure*

The activities set out in *WP 2* "Intelligent security systems" have a leading role in the development of ISS. The research methodology under this WP includes the implementation of a systematic approach in the process of analysis, evaluation, formulation and proposal, with regard to improving the process of security enhancement and protection of critical infrastructure objects by security zones building, taking into account the specifics and interactions between their elements, as well as between them, and creating models ISS, with a focus on all aspects of CI management. Also of particular interest is the link with the research into the quality of critical infrastructure protection systems carried out so far [5], which facilitates the achievement of a comprehensive approach to developing security systems.

ISS models development, in accordance with the specifics of security objects, will require the development of modern, fast-acting and fully autonomous sensor subsystems, to test the functionality of which test and simulation systems need to be developed. In this way, at a relatively low cost, through modern innovative scientific developments, the desired level of compliance will be achieved and thus – security.

Basic internal links to support of ISS development

The main areas of interaction between work packages (Fig. 3.2), related to the development of ISS, are carried out at the stages of the preparation of concepts, models and specifications of hardware and software. This ensures the technological and functional compatibility between them and avoids duplication of activities and resources.

For example, quantum communications (*WP1*) provide physically unconditional security to the network when transmitting information between sensor models built in critical infrastructure and models of managed / situational decision points that must be protected against copying or eavesdropping, and authenticity between communicating parties to be guaranteed.

Also the development in *WP3* of unified, integrated hardware and software of simulation environments to upgrade existing ones and to create new models and data for the real environment, will allow research and training in the field of security and crisis management of different nature. Creation and installation in the information environment of simulation models of objects from the national critical infrastructure, objects of strategic importance, from the technical infrastructure, etc. important for national security will facilitate the development of appropriate ISS models.

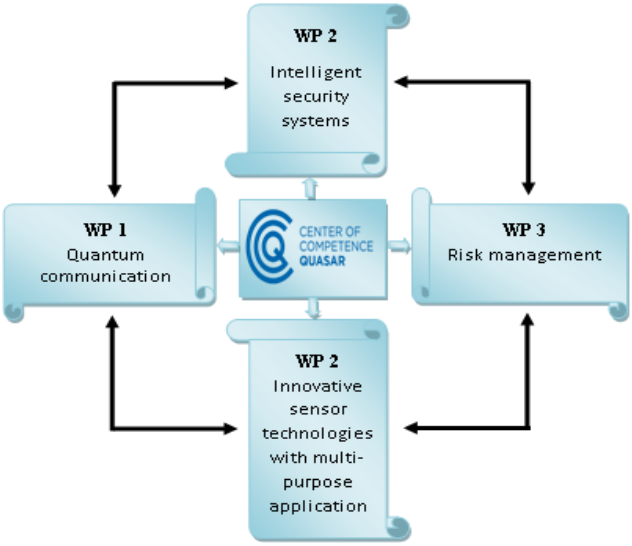

Fig. 3.2: *ISS development - basic internal links*

As a result of the implementation of *WP4*, innovative sensors will be created to record environmental and security factors for critical infrastructure sites. Innovation activities within WP4 involves the establishment of an objective database and models to predict / anticipate catastrophic earthquake processes and phenomena through a fundamentally new approach - emission of nanoparticles. This will extend the scope of ISS, contributing to the "added" reality of simulated processes.

At the same time, joint testing and experimentation of hardware and software developed in the scope of work packages will facilitate their integration to achieve the set goals and in particular for the ISS development. Removal of the found inconsistencies in the conditions of joint tests will reduce the time for correction, reduce the costs for it and achieve the planned results for timely realization on national and international markets. It is important to note that the testing of ISSs is also linked to the verification of the results obtained. Therefore, a number of approaches are known to determine the quality indicators of of critical infrastructure for protection systems **[6]**, the implementation of which guarantees compliance with the technical and operational requirements of ISS elaborated.

Last but not least, all activities in the "Development" and "Tests and Experiments" areas (Fig. 3.2) *referring to ISS models* are closely related to the good European and world practices in the sphere of Organization's Business Continuity Management (BCM). BCM "… is a sector of business practice with a long tradition of formal elements and requirements in international standards and a number of national regulatory documents with internationally recognized institutions and a network of means of disseminating best practices, many of which are an integral part of these requirements in the process of updating the standards and normative requirements against which individual companies organize and carry out their activities and achieve planned business objectives" **[7]**.

An alternative way of thinking is that BCM should adopt an "All Hazards Approach". This approach focuses on how to continue / recover services, following the materialization of risk. This in a specific way means that Resilience Evaluation (RE) should also be carried out as a result of the CI risk assessment. RE "…is the overall modeling activities, and analysis of critical infrastructure systems aimed at evaluating the ability to prevent, absorb, adapt, and recover from a disruptive event, either natural or man-made"**[8]**.

Technical and interoperability between the products or processes envisaged for substantial improvement and related research to support the development of ISS

During the development of the major areas in the structure and functioning of the CoC, the following internal links were introduced to ensure compatibility in the design and operation of the intended results. I would like to emphasize that these are only the main areas that ensure compatibility in the development of security systems models.

- *Transfer of protected information, received from ISS;*

The construction and successful commissioning in *WP1* of one or more new optical quantum channels using linearly polarized photons for quantum key-sharing will ensure that the final information transmitted between the main centers (mobile or fixed sensor security systems and points of contact) management) will be transferred to where it is and to whom it is needed, without third parties being able to access it.

- *Development of technical and operational requirements for ISS models;*

Developed in *WP3* software models and data from the real environment for conducting research and training in the fields of security, safety and crisis management of a different nature in urban / industrial / transport medium in the marine environment in the air will reduce the time and cost of financial funds in developing related ISS. The corresponding simulation models, including the methodology for assessing the risks and deciding on preventing or

counteracting will ensure compatibility between products and systems for collecting, processing, automation, verification and transmission of any credible information regarding intelligent security systems and their management.

- *Extended ISS coverage.*

The established and tested *WP 4* forecast models, algorithms and recording geodynamic modules of the modern sensor system for predicting catastrophic phenomena by emission of nanoparticles would help to expand the scope of ISS and improve their complex efficiency.

These areas are expected to contribute to the development of comprehensive research and innovation capacity, the integration of planned research with the development of contemporary and emerging ISS technologies.

4. Conclusion

The implementation of WP 2 activities will contribute to the development of an innovative, multifunctional, basic, sensory system providing security of critical infrastructure and objects of national, regional and local importance, as well as capacity building for significant modernization of existing specialized research capabilities. In this way it is expected to ensure improvement of the social security in our country, significant modernization of existing specialized research infrastructures, necessary to meet the needs of the employees in the field of research and innovation, and structuring of processes and business models for the management of the research and innovation activities in the interest of organizations/enterprises in order to increase their competitiveness.

It is through the implementation of the systematic approach and the coordination of activities between participation of different work packages that the complete research and innovation capacity will be built, the integration of the planned research with the development of new and emerging technologies and the optimization of the possibilities for implementing the research results for the development of the innovative ones. This will create mid-term competitive advantages for organizations participating in the Center of Competence "Quantum Communication, Intelligent Security Systems and Risk Management" (Quasar), engaged in research and innovation, as well as for those who apply their contemporary developments.

Literature:

[1] COM(2018) 436 final, „ANNEXES to the Proposal for a DECISION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation";

[2] „SCIENCE AND EDUCATION FOR SMART GROWTH OPERATIONAL PROGRAMME 2014-2020", Version 2.0 / Approved by EC on 11/11/2018 /, page 51;

[3] http://www.investorwords.com/19342/systematic_approach.html;

[4] " PROJECT JUSTIFICATION under the competitive project selection procedure CREATION AND DEVELOPMENT OF CENTRES OF COMPETENCE" (Creation and Development of a Center of Competence "Quantum Communication, Intelligent Security Systems and Risk Management" (Quasar);

[5] Георгиев Н. Л., Анализ на един клас специализирани сензори за защита на обекти от критични инфраструктури. 2015, ISBN:978-619-90310-4-9, 170 стр.

[6] Georgiev Nikolai, "Quality criteria for critical infrastructure protection systems", International Journal of Economics, Commerce and Management, vol VI, issue VI, ISSN 2348-0386, 2018, p. 265-271;

[7] Kiril Stoichev, Risk Analysis for Business Continuity Management of NPP, International Journal for Economics, Commerce and management, Vol. VI, Issue 11, November 2018, ISSN 2348 0386, 459-476;

[8] Associate Professor Ph.D. Dimitrov D. L., "CRITICAL INFRASTRUCTURE RESILIENCE EVALUATION – RESILIENCE APPROACH, RESILIENCE MODEL AND RESILIENCE INDICATORS", International Scientific Journal Security & Future, 1/2018, ISSN 2535-0668, p.p. 7-10.