THE CONCEPT AND THEORETICAL MODEL OF THE INTEGRATED SYSTEM FOR THE PROTECTION OF CRITICAL INFRASTRUCTURES

Colonel (ret) Professor Benone ANDRONIC, PhD

The concept of protection, the same as that of security, is a scientific and practical matter and therefore should be approached in close collaboration with the beneficiary, whith complex analysis on stages and testing in the final phases.

In fact the complexity of security and critical infrastructure protection is necessary to develop a new concept of protection which integrates the securiy and quality issues and to be able to counter the unfortunate event occurrence and ensure swift restoration of their functionality.

Keywords: *critical infrastructure; intelligence; risk matrix; assumed risk; protection strategies; integrated protection system.*

In our view, integrated systems of critical infrastructure protection could be the command and control (C4I2SR)*, which have the basic functions of information collection, transmission and processing, assisting the decision-making act and providing means for protection, security and defense.

The two axioms in the analysis of this area could be the following: failure to ensure a 100% of critical infrastructure protection (CIP) whatever this is, the lack of a unique solution, a universal system for ensuring PIC. The use of the concept of critical infrastructure protection should require implementation of the PIC in accordance with safety and evaluation, design and implementation of integrated protection mechanisms (i.e., constructive measures and equipment, organizational and procedural measures, measures related to human resources and personnel).

The critical infrastructure protection mechanisms could include: perimeter protection and physical barriers to their sustainable access control, intrusion

detection, CCTV surveillance, information system, control centers, primary and secondary power supply. In our opinion, any protection system is an integrated system for the human, technical and procedural elements, to achieve deterrence, delay, detection, evaluation and intervention against unauthorized entry attempts in the critical infrastructure area. It was found that protective measures are only inefficient and cannot ensure the integrity of the infrastructure perimeter fences. Lists were developed which were reviewed and updated regularly on the issues involved in the design and implementation of integrated critical infrastructure protection. Difficulties which are obsolete and have a major influence on the performance of the protection system are: lack of accurate data that characterize all threats (availability, "fingerprint"-specific evolutionary parameters, potentially destructive).

The risk matrix method, by applying it to the target, allows to obtain values for "assumed risk" that compares the concept of risk attitude (acceptable selective attitude is unacceptable) and causes selective tolerance (prevention and mitigation) and unacceptability (measures to ensure the maximum risk materializing cases).

Under the provisions of the law, in relation to the risk and costs incurred by the organization, critical infrastructure protection strategies have the following levels: minimal risk assumed by some (12-15)%; sufficiency, risk assumed by some (8-12)%; risk assumed by some (5-8)%; safe, risk assumed by some (3-5)%. According to the coverage of the activities of the organization (company) responsible for the PIC strategies, there are two categories: global (homogeneous or hierarchical) or partial.

But costs are very high for the global strategies, and the way of applying them depends on the functional importance of the protected system component and acceptable risk levels. The concept of integrated protection because of the social implications of industrial technology and real time processes, integrated human collectives, architectural achievements and influence of the environmental elements, their protection as an essential element of technological and social, is a fundamental condition for economic efficiency. But we can talk about economic efficiency only if the industrial process is carried out in safety and security without disasters, since they are targeted by international terrorism and the capabilities (in conjunction with issues of unfair competition). Therefore all this requires a scientific concept and implementation of protection mechanisms that are necessary for quality assurance

and counteracting unwanted, dangerous events (terrorist acts, sabotage, theft, earthquakes, floods, explosions, emissions or pollution etc).

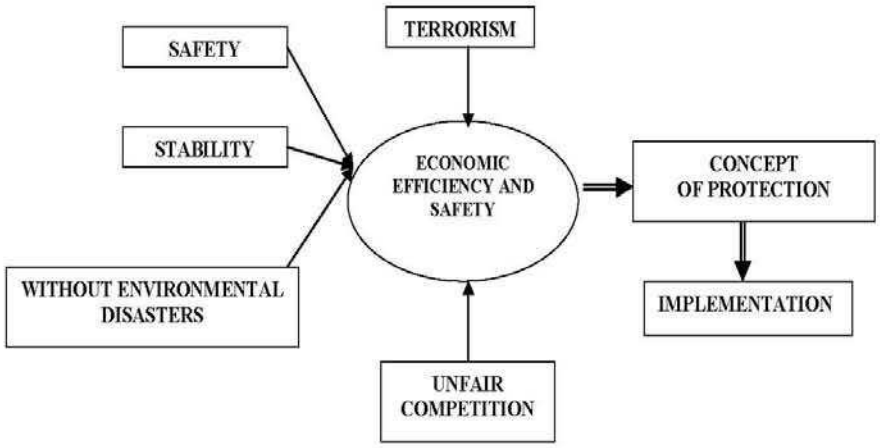

Figure 1. *The need for critical infrastructure protection concept*

Analyzing all general threats (i.e., terrorism, sabotage, concealing information, production and technological accidents, etc.), given the characteristics of industrial capacity and in terms of protection, they can be classified classified as seen in Table 1.

In accordance with the production process used, the industrial capabilities are classified into the following classes: mono-process, multi-process, and multi-cumulative consequences of insecurity.

Table 1*.Classification of the industrial capacities in terms of their protection and security*

Type of industrial capacity	**Level of risk**	**Protection class**	**Examples of industrial capacity**
Major social impact	3.2-5	E, F, G	Thermal and hydro capacity, electricity distribution, gas and oil products, technological density and large geographic area
Catastrophic consequences			Nuclear capabilities, chemical weapons and explosives and refineries

Type of industrial capacity	Level of risk	Protection class	Examples of industrial capacity
Particularly sensitive	3.2-4.5	E, F	Strategic capabilities in terms of technology and products fabrication
Subjected to high pressure	3.2-4	E	Capacities of economic efficiency and high market competition
Medium risk level	1.1-3.2	B, C, D	For small to medium size and production

This new system should meet the following requirements: analysis of threats, vulnerabilities and risks of estimated occurrence and its consequences, establishment of protection class capacity and protection strategy, depending on the risks and likely costs; defining the protection of the environment to store production capacity, defining environmental protection, construction, implementation and integration of protection mechanisms in an effective, protective structure formation, dynamic stability of the system, evaluation, testing and licensing system protection, selecting scientific maintenance measures, definition and implementation of complex insurance (damage, risk, etc.) of product protection.

The concept of protection, like that of the security, is a scientific problem, and also a practical one, and it should be implemented in close collaboration with the beneficiary, the analysis and testing complex, as well as the final stage.

The critical infrastructure protection environment should ensure: environmental protection of the critical infrastructure, protection of the production processes, quality protection, environmental protection, confidentiality, technological, physical protection (perimeters, buildings, production lines, capacity and information management, personnel, supplies), information protection (including licenses, trademarks, manufacturing recipes); a moral framework for education and behavioral protection and security of all staff (rules, privacy statement, codes of conduct) and fire prevention, protection against natural disasters, legal structure to protect the progress of works, the resources and procedures for mitigating unwanted consequences of the events and recovery of production capacity. Any critical infrastructure protection system must: prevent and deter malicious actions, detect, as early as possible, malicious actions, delay carrying out malicious action, stop action (capture and neutralize the malicious ones before finalizing the action), decrease the least possible consequences of a successful malicious acts, highlight a large number of indicators to track and prevent criminals, security and stability and

business processes, privacy and management processes, protect against fire and natural disasters, eliminate or mitigate, as much as possible, technological and work accidents, as well as the ecological consequences. To achieve the optimal functioning of critical infrastructure protection systems the following measures are required: optimal design of buildings and installations, use of state-of-the-art surveillance and alarm devices, appropriate organizational measures, implementation of an information system to support effective and safe operation. To design the critical infrastructure protection it is necessary to take into account the following principles: the security system is based on a design, the chosen strategy and careful analysis of costs and efficiency; it is adaptable and open in behavior. The protection mechanism is the practical (pragmatic) protection strategy with one of the following three forms: 1) a set of technical and organizational measures, 2) protective mechanism measures, professional equipment and personnel organization, 3) system protection based on systems theory and forecasting functions and adaptability.

Conclusions

The Romanian legislation does not provide complete rules for CIP, for preventing and minimizing terrorist attacks, human resource training to be ready to respond to attacks, an immediate response capability on site and organize the recovery from an attack. It is therefore necessary to define the concept of integrated protection concept based on the complex analysis of risks and threats to critical infrastructures.

Based on this concept to design functional integrated theoretical model of critical infrastructure protection, which ensures reduce their risks: a surveillance radar detection and warning areas, a video system, an automatic identification system; non-lethal weapons and command and control system (C4I2SR). These subsystems should not be addressed individually because otherwise this would have a robust and complete solution. In order to design and physically implement such a system, it is necessary that the cumulative conditions are met and the following steps are taken: conducting a full risk analysis and audit protection to reveal the risks and vulnerabilities, designing the protection system and defining procedures for use / intervention / project implementation and staff training intervention, results analysis and verification procedures, system maintenance and ongoing assessment of compliance procedures. The project is a multidisciplinary stage, where designers must work in all areas of attention (electronic, mechanical, computer and human protection).