EFFICIENT MARITIME PORT CRITICAL INFRASTRUCTURE PROTECTION: A PROJECT MANAGEMENT AND CRITICAL THINKING PERSPECTIVE[1]

Mihai Anton PALFI

Abstract

This paper analyses a project for the design of an Integrated Security System for the critical infrastructure protection of a maritime port. Accordingly, critical thinking principles are applied to the management of this type of project, and its risk analysis is also detailed.

Keywords: Integrated Security System, critical infrastructure, project management, risk management, critical thinking

[1] This article is based on Mihai Palfi's MA dissertation *Efficient Maritime Port Critical Infrastructure Protection: a Project Manangement and Critical Thinking Perspective* presented within the framework of the Interdisciplinary Master Programme "English Language Education and Research Communication for Business and Economics", ASE Bucharest, 2008, having Dr. Liviu Mureşan and Dr. Cristina Neesham as academic supervisors.

The critical infrastructure concept

Infrastructure is essential for economic prosperity, national security and the quality of life in any country. Infrastructures can be grouped in three big categories, depending on their location, role and importance for the stability and functioning of the society, as well as for the safety and security of systems:
(a) ordinary infrastructures, (b) special infrastructures, and (c) critical infrastructures.

Critical infrastructures are defined as those infrastructures with an important role in ensuring the security for the functioning of systems and the unfolding of economic, social, political, informational and military processes.

Infrastructures are considered critical due to: their singularity within the frame of infrastructures of a system or process; their vital importance as a material or virtual (net-like) support in the functioning of systems and the unfolding of processes - economic, social, political, informational, military, etc.; the important, non replaceable role they play in the stability, reliability, safety, functionality and, especially, the security of systems; the increased vulnerability to direct threats, as well as to threats targeting the systems these infrastructures are part of; and, a special sensitivity in case of variation of the conditions and, especially in case of sudden changes of the situation.

The importance of critical infrastructures results also from the fact that they can be defined as being those industrial capabilities, services and facilities, which, in case of interruption of their normal functioning, can affect human life, and can harm or destroy human life.

The predominant criteria for analysis, as mentioned in the specialized literature, are: the physical criterion, regarding the positioning within other infrastructures, size, spread, endurance, reliability, etc.; the functional criterion, regarding the infrastructure's role (what it does); the security criterion (its role in the overall safety and security of the system); the flexibility criterion (reflecting the dynamic and flexibility in defining infrastructures as critical; some of the ordinary infrastructures become under certain circumstances critical ones and vice-versa); the unpredictability criterion (some ordinary infrastructures can suddenly become critical infrastructures).

Critical infrastructures are, according to a European definition, *"physical and technological installations of information, networks, services and assets, which, in case of stopping or destruction, can cause serious damage to the citizens' health, security and economic well-being or to the activities of the Member States' governments"*.

According to the documents of the European Commission, critical infrastructures include: installations and networks in the energy sector (especially the installations for producing electricity, oil and gas, installations for storage and refineries, transport and distribution systems); communication and information (telecommunications, radio transmission systems, programmes, the information materials and networks, including the internet, etc.); finance (the banking sector, the stock market and the investments); the health care sector (hospitals, medical equipment for patients and blood banks, pharmaceutic laboratories and products, emergency services, searching and saving services); the food sector (security, means of production, distribution and agro-alimentary industry); water supply (reserves, storage, treatment and distribution systems); transport (airports, ports, railways, mass transit networks, traffic control systems); production, storage and transport of dangerous substances (chemical, biological, radiological and nuclear materials); and administration (basic services, installations, information networks, assets, important places, national monuments).

Of course, it is not possible to protect all critical infrastructures completely and at all times. In this context, the management of security is defined by the European Commission as a *"deliberate process which envisages the evaluation of risk and the implementation of the actions aimed at bringing the risk at a determined and acceptable level, at an acceptable cost"*.

Maritime critical infrastructures protection

An Integrated Security System for a maritime port area has to accomplish the following objectives: (1) advanced detection of any attempts to intrude into the port security areas; (2) transmitting alarm and sabotage signals to the software, giving it the possibility to remotely control the activation and deactivation of security areas and to acknowledge alarm signals; (3) surveillance for threats; and (4) security data dissemination at the port's local and central authority levels, as well as at the other institutions involved in discarding security events.

The Integrated Security System for a maritime port area is an instrument for the guvernamental and economic (state and private) structures directly involved in safety port's activities, in ensuring security of ships and other port facilities.

The main threat categories for port facilitiy security refer, in broader terms, to issues such as theft and sabotage, terrorism, neighboring conflict, illegal traffic or migration, various forms of violence, environmental threats, and larger-scale accidents. A detailed list of these categories is provided in Appendix 1.

Another category of risks consists of the asymmetric non-classical ones, which may be deliberate armed or non-armed actions, with the purpose of affecting the

national security. Those may affect, directly or indirectly, social-economic national standards. A more detailed list of items in this category of risks there is available in Appendix 2.

To implement an integrated security system for a critical maritime infrastructure, it is necesary to specify that any port area is physically characterized by: perimeter boundary; access points; infrastructure (transports, communication system, utilities, maritime flow command and control, etc); the port's roadstead (water area in the coast environs, having a natural or artificial defense system, where ships can stay during hard winds, waves or sea currents); moorages (technical and strategic) to ensure the ship-port interface; protection dikes for moorages and levees against waves; a maximum tonnage for moorages, maximum depth for levees (which determine a certain annual operating capacity, and, therefore, certain types of ships to operate); ports operators who perform several activities (piloting, towing, binding and unbinding ships to jetties, ship supplying ships, operating ships); and, capacities for heaping merchandise.

Regarding the latter, in order to ensure the security and the safety of all these ports, one of the main functions of the security system is to control the access flow inside the port area, which implies the necessity to prevent unauthorized accesses through access points. To prevent this, there are some specific measures to care about in an access control security system, which will allow only authorized traffic of persons, transport vehicles and desired merchandise. Alternative technical methods should be used to intercept weapons, NBC substances, drugs, etc. Also, to prevent unauthorized access by breakthrough the perimeter fencing, it is necessary to develop a perimeter security system.

Because of the complexity of activities and large areas to survey in a port, it is highly necessary to implement an Integrated Security System, having as a center of analysis and decision a Principal Centre of Strategic Command and Control (Control Room). This will centralize all data regarding security and safeness of the completely protected area, in order to take best decisions for action.

Project management structures principles for a integrated security system - critical infrastructure protection for a maritime port

Generally, a project can be defined as a temporary effort to create a system (product) or a unique, well- defined service.

A synopsis of a project's unfolding plan is shown in Table 1 below.

Table 1 Project unfolding plan

Initiation	Planning	Execution	Closeout
Ideas/User requirements	System specifications / statement of Work	Contract award	Test and evaluation
Statement of Requirements	Evaluation plan	Detailed planning	System acceptance
Market research/product availability	Final business plan	Tracking and monitoring	Operational evaluation
Project charter/Budgetary estimates	Project approval Request for proposal	Product or service development	Project closeout
Preliminary business plan	Evaluation/selection		
Preliminary approval	Contract(s)		

In the **initiation** stage there are mainly activities about defining requirements, establishing the project's position on the market, estimating the budget and establishing a preliminary business plan to sustain a preliminary approval for the proposal.

During the **planning** stage, the project management's activity is mainly based on data from the project's unfolding plan. This represents the formal approved document, used in project execution. At the same time, there are established system specifications. Based on them there will be named a project team and the project business plan will be finalized.

The **execution** stage of the project starts after winning the contract. It begins with detailed planning for implementing the project. There are many possibilities to organize and present a project plan, but most of them focus on: a description of the way to approach the project from management or strategic point of view; establishing the project's content, including objectives and estimated concrete results; Work Breakdown Structure (WBS) - to the last control level; cost estimation, planning the start and the end date of the project, responsibilities assignation to each of the delivers of WBS; reference levels to technical content, to time planning and cost planning (budget on large periods of time); milestones (markers) for project and a date for each of them; necessary personnel, together with their cost and effort estimation; a risk management plan, including major identified risks, suppositions and constraints, planned measures and emergency plans (wherever needed); and, other management plans (of content, time schedule, of costs, quality plan, personnel involved, communication plan, risks, acquisitions

plan, etc.). Each of these above may be included in the project plan, together with their details.

At this stage, there are activities in accordance to service and product development, and specific processes within the project are organized.

The **closeout** stage of the project includes mainly: (1) testing and evaluation of the developed system; (2) acceptance of the project; (3) operational assessments; and, finalization of the project (system). This latter activity corresponds with system's delivery to its beneficiary.

Critical analisys of risk management regarding an integrated security system project for critical infrastructure protection for a maritime port

1. Purpose and objectives

The main objectives are: to provide a basic understanding of project risk management and how it differs from other forms of risk management; to provide an understanding of how project risk management is directly related to effective project and organizational management; to define the activities of risk management; to present the project risk management; and, to establish a connection between risk levels and measures.

2. Risk Analysis

Risk is a major factor to be considered during this business analysis. Management must control and be aware of the risks if this business is to stand a chance of being successful.

From the activity types this business involves, we consider two types of risk that could affect our business: business risk, and project risk.

Business risk covers the threats associated with a project. It includes such areas as: strategic direction, commercial issues, market change, the consequences to the corporate body in case of failure or limited success, legislative changes, political factors including public opinion, and environmental issues.

Project risk is the collection of threats to the management of the project and hence to the achievement of the project results within cost and time.

3. Risk management activities

The key risk management activities are: 1. Planning; 2. Identification; 3. Definition; 4. Analysis; 5. Mitigation / Monitorization / Watching / Acceptance; 6. Measurement; 7. Closing / Archiving; and 8. Emergency Plan.

3.1 Planning

Risk management activities related to planning include: establishing the definitions and terminology; establishing the processes to be followed; establishing the risk management team and the responsibilities of each member; establishing the level of effort (human, material and financial) according to project size.

The Mitigation Plan and Emergency Plan are also established at this stage.

3.2 Risk identification

Risk identification must be performed at each and every stage of the project.
In the initiation and planning phases, the risk items have higher levels and the purpose of this activity is to identify the amount of contingency involved, and whether to still proceed with the project.
In the execution phase, the risk items are more specific and can be expressed as an impact statement.

3.3 Risk definition

This activity includes the folowing directions: establishing the risk type with reference to cost, schedule and performance; establishing the risk probability of occurrence; establishing the risk impact level; establishing the risk impact period (timeframe in which the risk item is likely to trigger a problem); and, establishing who has the control of the outcomes (for feedback).

3.4 Risk analysis

This activity is necesary to: develop the Mitigation Strategy; Mitigate – Monitor – Watch – Accept (assign or defer); identify mitigation steps; identify significant milestones; determine trigger points for executing mitigation plans; assign person responsible; and, establish priorities.

3.5 Risk mitigation/monitorization/acceptance

This activity is accomplished through: re-visiting the risk item periodically; re-assessing probability and priority; re-assessing impact period (in case other events may have changed the impact period); performing mitigation steps, or taking metrics; objectively monitoring what is happening; logging significant events that contribute to the risk item (for or against); and, re-assessing mitigation strategy and contingency plan periodically.

3.6 Risk emergency plan

This activity is a very special situation in the project framework, therefore it is necessary to take measures to: identify the trigger points; know what to do when the risk item triggers the identified problem; identify usage of contingency funds; design work-around plans.

3.7 Risk measurement

At this stage for each risk will be asigned an appropriately importance level and an occurrence probability.

Risk Closeout/Archive

The closeout activity of the risks takes place when: risk goes away; the impact period has passed; other events overtake the risk item; or, the risk item is merged with another or split into more than one item.

3.9 Reports

This activity includes the folowing directions: 1. status reporting of project risks; 2. currency of data (the number of overdue mitigation steps is counted in this activity); and, 3. distribution of data.

Critical analysis of risk management

During the critical analysis of risk management, the following problems must be addressed: making the correct correspondence between the description of the project proposal and the beneficiary's demands; presenting the project analysis description according to the principles that must be applied; establishing the best analysis plan for the risk management of the project; establishing measurable results for each stage of the project risk analysis plan; establishing a correct correlation between the demands of the analysis and financial amounts; establishing the best project partners; correctly establishing the project management process.

In order to obtain the best solution, the following critical thinking techniques or activities should be applied: Analysis; Interpretation; Inference; Explanation; Evaluation; and, Self-regulation (Facione, 2007).

Critical thinking (CT) skills required

The elaboration of the risk analysis documentation starts by analyzing the program's demands, in which the proposed project is included. All the prescriptions imposed by the contract's officials with respect to the obligatory format of the documents have to be verified.

A table of reasons and objections for and against the project proposal (the technical part) is presented in Table 2 below.

Table 2: Reasons and objections related to the project proposal (the technical part)

No.	Reasons	Objections
1.	Efficient planning of risk management activity: • Creating a Work Breakdown Structure, planning stages, periods of time, etc. • Establishing levels of authority and the structure of reports • Making a corresponding map of risk reduction • Planning for unexpected situations	Incorrect definition of risk impact on the project Results: ▪ Exceeding the material and financial spending ▪ Encroaching upon the project's unfolding schedule ▪ Inadequately defining risks probabilities Results: ▪ Misfit planning of effort levels
2.	Correct identification of risks: • Risks identification in the initialization and planning stages of the project • Identification of risks impact at the execution stages	Not identifying all risks about subcontractors Results: ▪ Encroaching upon the project's unfolding schedule ▪ Exceeding the material and financial spending
3.	Defining the content of the risks: • Establishing types of risks by costs, schedule and performances • Correct appreciation of occurrence probabilities • Appreciation of risk impacts • Appreciation of risk impact's period of time	Incorrect appreciation of the impact Results: ▪ Uncontrollable rising of costs if foreseen risk becomes a real problem ▪ Exceeding the material and financial spending, if the period of impact is larger than previously thought
4.	Correct risk analysis: • Development of a strategy to diminish/reduce risks • Establishing the responsible personnel • Establishing priorities correctly	Wrong appreciation of points to apply the risks reduction plan Results: ▪ Raising costs ▪ Uncontrollable increase of probabilities that risks may

No.	Reasons	Objections
		become real problems if the risk reduction plan is not applied on time
5.	Activity management to minimize/monitor acceptance of risks: • Periodic review and re-analysis of expected risks • Objective monitoring of the progress of the project • Periodic re-evaluation of risk reduction plans and measures for emergency situations	Not implementing the risk reduction plan or not taking periodic measurements Results: ▪ Exceeding the material and financial spending ▪ Uncontrollable increase of probabilities that risks may become real problems ▪ Losing control of the project
6.	Reaction to emergency situations: • Identifying points where contingency plans will be applied • Establishing what to do in case the identified risks become real problems • Identifying how to use the emergency funds	Inadequate management of contingency funds Results: ▪ Exceeding the material and financial spending
7.	The progress of the closeout/archiving activity: • Assurance of the project's necessary feedback • Database for future projects	Inadequate management of the closeout/archiving activity Results: ▪ Unjustified blockage of material and financial resources
8.	Progress of the reporting activity: • Reporting stages of risks which may interfere in the project's progress • Time cast of information • Reallocation of funds unspent in risk management	Inadequate information traffic Results: ▪ Losing control of the project management ▪ Unjustified blockage of material and financial resources

Based on this analysis, a map of arguments has been elaborated (Appendix 3). Following this map, a proper way to apply the required critical thinking skills is the following:

1. Analysis

1.1 Reasons - Efficient planning of risk management activity

Efficient planning of risk management activity includes the folowing directions: creating a Work Breakdown Structure, planning stages, periods of time, etc.; establishing levels of authority and the structure of reports; making a corresponding risk reduction map; and, planning for unexpected situations.

1.2 Objections - Incorrect definition of risk impact on the project

The results of incorrectly defining risk impact on the project can exceed the material and financial spending or the project progress schedule.

2. Interpretation

2.1 Reasons - Reaction to emergency situations

This chapter presents the risk management reactions for: identifying points where contingency plans will be applied; establishing what to do in case the identified risks become real problems; and, identifying how to use the emergency funds.

2.2. Objections- Inadequate management of contingency funds

Inadequate management of contingency funds using an incorrect risk management leads to exceeding the human, material and financial spending.

3. Inference

3.1 Reasons - Defining the content of the risks

Defining the content of the risks by costs, schedule and performances, and the occurrence probabilities in order to establish the risk management plan and reduce the impact.

3.2 Objections - Incorrect appreciation of impact

Incorrect identification and appreciation of risks impact leads to uncontrollable rising of costs (if foreseen risk becomes a real problem) or to exceeding the material and financial spending (if the period of impact is larger than initially thought).

4 Explanation

4.1 Reasons - Correct identification of risks

Risks identification, in the initiation and planning stages of the project, determines the risk control and lower material and financial spending.

4.2 Objections - Not identifying all risks about subcontractors

Incorrect identification and appreciation of the risk elements regarding the subcontractors will generate impact on the project.

5. Evaluation

5.1 Reasons - Activities management to minimize/monitor/acceptance of risks

The project must follow the minimize/monitor/acceptance of risks activities. These activities include: the periodical review and re-analysis of expected risks; the objective monitoring of the project's progress; and, the periodical re-evaluation of risk reduction plans and measures for emergency situations.

5.2 Objections - Not putting in practice the risk reduction plan or not taking periodical measurements

An incorrect evaluation of risk measurements and the inadequate utilization of the risk reduction plan lead to an uncontrollable risk or even losing control of the project.

6. Self-regulation

6.1 Reasons- The progress of the closeout/archiving activity

The closeout/archiving activity leads to assurance of the project's necessary feedback. This activity guarantees the achievement of the risk management plan and reduces the material and financial spending used for risk reduction.

6.2 Objections - Inadequate management of the closeout/archiving activity

Inadequate management of this activity leads to: unjustified blocking of material and financial resources; not finishing the project on time; and, not fulfilling the project requirements.

Conclusions

The conclusions of this study can be summarized as follows:

1. Present and future relationships can be established by analysis between concepts and their presentation, and a correct and detailed argument of these concepts can be made. This procedure can also reveal possible flaws that might show up while working on the project risk management plan.

2. Certain aspects with impact on the content of the project proposal can be highlighted and motivated by interpretation.

3. Important aspects of the risk project can be identified through inference, latter detailed in the project description. The project can be blocked if the aspects mentioned above are not correctly identified.

4. Explanation presents as correctly and as coherently as possible the project risk description. A presentation with inaccurate requests can lead to an uncontrolled increase in the project costs and execution period.

5. The important aspects of a project can be highlighted through evaluation, which is also the foundation of the risk monitor activity.

6. Self – regulation must be applied in order to appreciate the connections across the different stages of the project risk management plan. The entire activity of risk management design is self-regulating.

7. Critical thinking skills must not be applied mechanically when the project risk management activity takes place. In each situation one must apply the skill that fits best.

8. In the project risk management activity, the following must be highlighted: reasons and objections must be correctly established; the map of reasons must be correctly drawn; and, the interactive application of critical thinking skills must be emphasized.

9. During the project risk management documentation, the following must be highlighted: no chapters are less important than others, so all chapters must be approached with equal attention; critical thinking skills must be applied as an integrated package; and, a correct approach order must be established for the project proposal description.

10. All the conclusions and experience gained in the development of a project must be used and developed on similar activities.

11. All the activities of the risk manager converge towards the following: project managers need to make best use of their time; effective delivery of the product or service is Business Managers' main requirement; customers need a quality product or service at an optimum cost and schedule; and, to be effective, project staff need to focus on the task and understand that somebody is looking forward and managing potential roadblocks.

12. Project Management exists if and only Project Risk Management exists.

References and bibliography

Civil Protection Law No 481/08 November 2004.

Cottrell, S. 2005. *Critical Thinking Skills: Developing Effective Analysis and Argument*. London: Palgrave.

European Commission. 2004. *Communication from the Commission to the Council and the European Parliament: Prevention, preparedness and response in terrorist attacks*, Brussels 20.10.2004, COM(2004) 698 final.

European Commission. 2004. *Communication from the Commission to the Council and the European Parliament: Prevention, preparedness and response in terrorist attacks*, Brussels 20.10.2004, COM(2004) 700 final.

European Commission. 2004. *Communication from the Commission to the Council and the European Parliament: Prevention, preparedness and response in terrorist attacks*, Brussels 20.10.2004, COM(2004) 701 final.

European Commission. 2004. *Communication from the Commission to the Council and the European Parliament: Prevention, preparedness and response in terrorist attacks*, Brussels 20.10.2004, COM(2004) 702 final.

Facione, P. 2007. *Critical Thinking: What It Is and Why It Counts. 2007 Update*, http://www.insightassessment.com/pdf_files/what&why2006.pdf, last accessed 30 March 2009.

Maylor, H. 2003. *Project Management* (3nd edn.). Harlow: Pearson Education.

Mureşan, L., A. Cazacu, S. Gal, S. Arion, M. Grădinaru. 2007. *Critical Infrastructures Protection: A Romanian Perspective*. International Conference organized by EURISC Foundation and partner organisations, Bucharest, Romania, 23 November 2007.

Romanian Government. 2006. *The National Security Strategy*, Supreme Council for National Defence, Decision No. 62/17 April 2006.

Watts, R. B. Fall 2005. *Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment*. Homeland Security Affairs I, no. 2.

The author

Mihai Anton Palfi was in the past a colonel engineer, head of the Testing & Evaluation service in the Armament Department of the Romanian Ministry of Defense. Currently, he is head of the Testing & Evaluation Department of the Security and Military Systems Division - SC UTI Systems S.A. and vice president of the Bucharest AFCEA chapter (Armed Forces Communications & Electronics Association).

Appendix 1

Main threat categories for port facility security:

- Stealing from ships and from port area
- Terrorism: bomb attacks, taking hostages
- The existence of conflict zones right next to the seaside, which are responsible for the large numbers of illegal immigrants
- Traffic with substances forbidden by law
- Sabotage: deliberate wreckage or destruction of port facilities, data communication network, parts of ships, equipments or cargo, vandalism
- Illegal human traffic
- Piracy/armed robbery: violence, looting or suppression/threat
- Attacks on water, land, or air
- Environmental threats: casting or deliberate or/and accidental throwing into the water of some polluting substances
- Contraband
- The existence of free zones
- Some accidents: collision, explosion, fire, flood, technical problems
- The proliferation of weapons of mass destruction, of related technologies and nuclear substances, of unconventional killing methods and weaponry
- The proliferation and development of terrorist networks, trans-national organized crime, illegal traffic with humans, drugs, weapons and ammo, strategic and radio-active materials, etc.
- Clandestine migration and the advent of major fluxes of refugees
- Actions that incite to extremism, intolerance, separatism or xenophobia, which may affect the Romanian state and the promotion of democratic values
- Some discrepancies between the existing levels of security and the stability of Romania's neighbouring states
- Restrictive rights for Romania for some regional resources and opportunities, with major importance for the protection of national interests.

Appendix 2

Types of asymmetric risks:

- ✓ political trans-national and international terrorism, including its biological or informational forms
- ✓ actions that may harm the safety of national and international transport systems
- ✓ individual or group actions of illegal access to informational data systems
- ✓ deliberate actions that can affect (in different forms and varied circumstances) Romania's image abroad, in order to destroy its credibility and seriousness in accomplishing its engagements
- ✓ economic-financial aggression
- ✓ deliberate acts of ecological hazard.

MEDIUM
LEVEL

Appendix 3