Towards a Criticality Analysis Methodology: Redefining Risk Analysis for Critical Infrastructure Protection

Marianthi Theoharidou[1], Panayiotis Kotzanikolaou[2], Dimitris Gritzalis[1]

[1] Information Security and Critical Infrastructure Protection Research Group,
Dept. of Informatics, Athens University of Economics and Business,
76 Patission Ave., Athens, GR-10434, Greece
{mtheohar, estoug, dgrit}@aueb.gr

[2] Dept. of Informatics, University of Piraeus,
Karaoli & Dimitriou 80, 185 34 Piraeus, Greece
pkotzani@unipi.gr

Abstract. Critical Infrastructure Protection requires the prioritization of critical assets and the evaluation of the criticality of infrastructures. However, criticality analysis is not yet standardized. In this paper we examine the relation between security risk and criticality. We analyze the similarities and differences in terms of scope, aims, impacts, threats and vulnerabilities and we suggest how existing risk analysis can be applied when examining Critical Infrastructures. Based on the identified relation between risk and criticality, we propose a generic risk-based Criticality Analysis methodology. We place key emphasis on the definition of examined impact types, which are social-centric and/or sector-centric, in contrast to traditional risk analysis methodologies that mainly examine organization-centric impacts. We propose a detailed list of impact criteria in order to assess the criticality level of an infrastructure.

Keywords. Risk Analysis, Criticality, Impact, Critical Infrastructures, Critical Infrastructure Protection.

Towards a Criticality Analysis Methodology: Redefining Risk Analysis for Critical Infrastructure Protection

1. Introduction

Critical Infrastructure Protection (CIP) is a relatively recent term that is related to traditional information and communication technology (ICT) security. We usually refer to a ***Critical Infrastructure*** (CI) as a "service, facility or a group of services or facilities, the loss of which will have severe adverse effects on the physical, social, economic or environmental well being or safety of the community" [8]. Critical Infrastructures are perceived to include material and information assets, networks, services, and installations [3]. All CIs widely use ICT and depend strongly on them [2].

The need for assessing the criticality of CIs, prioritizing between them and protecting them with adequate security controls has been highlighted both by the EU Commission [5] and the US government [DHS-09], as well as other governments [8],[23]. Clearly, there is a close correlation between the protection of CIs and the mitigation of the security risks that threaten CIs. However, the ***criticality*** of infrastructures is a term that has not been formally defined. Neither standardization bodies nor academic research have designed criticality analysis methodologies, compared to ICT security risk analysis methodologies, which are widely used and standardized. CIP currently has no specific standards, though the security and safety standards are been used as auxiliary standards [2]. The CIP-002-1 Standard (Critical Cyber Asset Identification) of the North American Electric Reliability Corporation (NERC) requires a risk-based assessment methodology to be used in order to identify Critical Assets. However, it does not suggest a specific method or sets more detailed requirements [21]. Thus, there is a need to define how existing risk analysis methodologies can be properly utilized in order to concentrate on the assessment, categorization, prioritization and protection of CIs.

Contribution. In this paper we examine the relation between security risk and criticality. By analysing similarities and differences in terms of their scope, aims, impacts, threats and vulnerabilities, we clarify how existing risk analysis results can be useful while examining CIP. Based on the identified relation between risk and criticality, we define *Criticality Analysis* as a *special-purpose* and *societal-centric* Risk Analysis process, performed on large-scale systems and infrastructures that provide services to a large number of users/citizens, with an extended scope in terms of *inter-dependent systems* and *examined impacts.* A more formal definition of Criticality Analysis is provided on Section 3. Then we will propose a generic risk-based *Criticality Analysis methodology,* which is structured on well-defined phases. We place key emphasis on the definition of the examined impact types, which are social-centric and/or sector-centric, in contrast to traditional risk analysis methodologies that mainly examine isolated organization-centric impacts. Then, we propose a detailed list of impact criteria in order to assess the criticality level of a CI.

Structure of the paper. The rest of this paper is organized as follows. In Section 2 we overview related work on CIP and then, in Section 3, we examine the relation of security risk and criticality and we formally define the process of Criticality Analysis. Based on our findings, we present a generic criticality analysis methodology in Section 4. Finally, Section 5 concludes this paper.

2. Criticality: current approaches

The most common approach used in order to characterize a CI as critical, is to assess the impact level in the presence of security-related threats. Most methods focus on the consequences of an event, meaning the “outcome of a situation or event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain” [8]. Impact factors, also named as *critical asset factors*, are criteria used to prioritize critical assets and infrastructures. They may affect persons, stakeholders, communities, the economy and the environment [8].

A general categorisation used when evaluating impact regards three primary characteristics in relation to catastrophic events [5], [7], [8], [16]: (a) *Scope or spatial distribution* - the extent of the geographic area which could be affected by the loss or unavailability of a CI, (b) *Severity or intensity or magnitude* - the consequences of the disruption or destruction of a particular CI, and (c) *Effects of time or temporal distribution* - the point that the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other).

The intensity characteristic is usually analyzed in further, detailed criteria, both qualitative and quantitative. For example, the European Commission [5], [7] defines a minimum set of criteria that the member states should take into account on their CI assessments: (a) *public effect* (number of population affected, loss of life, medical illness, serious injury, evacuation), (b) *economic effect* (GDP effect, significance of economic loss and/or degradation of products or services), (c) *environmental effect* (effect on the public and surrounding location), (d) *interdependency* (between other critical infrastructure elements), (e) *political effects* (confidence in the ability of government), and (f) *psychological effects*. These criteria need to be evaluated in relation to both scope (e.g. local, regional, national and international effect) and time (during and after the incident).

The latest US National Infrastructure Protection Plan [27] also presents criteria to evaluate consequences: (a) *public health and safety*: effect on human life and physical well-being (e.g. fatalities, injuries/illness), (b) *economic*: direct and indirect economic losses (e.g. cost to rebuild asset, cost to respond to and recover from attack, downstream costs resulting from disruption of product or service, long-term costs due to environmental damage), (c) *psychological*: effect on public morale and confidence in national economic and political institutions, and (d*) governance/mission*: effect on government's or industry's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions.

[12] uses the following criteria: (a) *complexity*, i.e. physical complexity, organizational complexity and speed of change of a CI, (b) *dependence*, i.e. dependence on other infrastructures, dependence for other infrastructures, intra-infrastructure dependence, and ICT control, (c) *vulnerability*, i.e. by external impact (like natural hazards, construction work, etc.), technical/human failure, cyber attacks, or been a terrorist target, and (d) *market environment*, i.e. liberalisation degree, control inadequacy, and speed of change. [12] also calculates the degree of criticality for these sectors by estimating the scope, magnitude and effects of time of an event.

A Canadian approach [23] differentiates in the sense that the criteria used are accompanied by impact scales. The criteria are: (a) *concentration of people and assets*, (b) *economic*, (c) *critical infrastructure sector (*on an international, national, provincial or regional level), *(d) interdependency* (physical, geographic, or logical), (e) *service delivery* (acceptable downtime, availability of substitutes, the time and costs required for the service restore) and (f) *public confidence* (in the ability of a state to preserve public health and safety, economic security, or to assure the provision of essential services).

In a different Netherlands approach [14], criticality is identified by the term *vitality*.

Indirect vitality is defined as the amount other vital products and services contribute to the dependability of the vital service or product, and *direct vitality* as the contribution that a product or service delivers to the continuity of the society. The direct vitality is related to indirect vitality of a CI and the resulting graph defines its criticality (the term vitality is used). The higher the direct and the indirect vitality are, the more vital the product or service is to society. In order to measure dependability, two concepts are used: the input from other vital products and services (*backward dependency*) is related to the level of delivered services (*forward dependency*). Finally, the *failure vs. recovery* criterion is used, e.g. the time required for recovering a minimum service quality level, the time that the impact really hits society, the time required for full recovery.

In the national risk assessment method for the CIs of the Netherlands [16], impact is assessed based on the following: (a) *territorial security* (infringement of the Netherlands' territory and the international position), (b) *physical safety* (fatalities, seriously injured and chronically ill or physical suffering), (c) *economic security*, (d) *ecological security*, (d) s*ocial and political stability* and (e) *social psychological impact*. All these criteria are evaluated in terms of range and duration.

The variations in the terminology of criticality are highlighted in Table 1 and a summary of the above criteria is presented in Table 2.

Table 1: Criticality approaches – Terminology

Term	Approach
Criticality	[5], [7], [12], [23]
Vitality	[14]
Risk (Impact or Consequences)	[16], [27]

Table 2: Criticality approaches – Impact Factors

Impact criteria	Approach
Public health and safety	[5], [7], [16], [27]
Economic	[5], [7], [16], [23], [27]
Environment	[5], [7], [16]
Political/governance/mission	[5], [7], [16], [27]
Psychological /Social/ Public Confidence	[5], [7], [16], [23], [27]
Interdependency	[5], [7], [12], [14], [23]
Complexity	[12]
Vulnerability	[12]
Market environment	[12]
Concentration of people and assets	[23]
Scope/Range	[5], [7], [16], [23]
Service Delivery/Recovery time	[5], [7], [14], [16], [23]
National/Territorial security	[16], [27]

In [24] four principal classes of possible interdependencies are presented: (a) *physical*: the state a CI is dependent on the material output(s) of another one. (b) *cyber*: the CI's state depends on information transmitted through the information infrastructure, (c) *geographic*: a local environmental event can create state changes in all of them, and (d) *logical*: the state of each CI depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection. Another categorization is the following [22]: (a) *physical*, e.g. a falling tree during a thunderstorm results in a loss of power, (b) *informational*, e.g. the loss of a supervisory control and data acquisition (SCADA) system that monitors and controls elements on the electrical power grid, (c) *geospatial*, e.g. a flood or a fire may affect all the assets located in one building or area, (d) *policy/procedura*l, e.g. halting all transportation in a metro system, even though only one station is affected, (e) *societal*, which refers to public opinion, public confidence, fear, and cultural issues, e.g. the change in the public confidence regarding safety of air travel, after the 9-11 attacks, led to financial problems in the airline sector.

3. Security Risk and Criticality

Many of the criteria used in order to measure the criticality of a system or infrastructure are basically impact factors which are also used in various risk analysis methodologies. Obviously, there is a correlation between the *criticality level* of an ICT system/infrastructure, with the security impacts and the associated *security risk levels*. Below, we shall investigate this relation in order to re-define the criticality level of a system in relation with its risk level.

Criticality as a (partial) subset of risk. Several impact factors identified in the CIP literature (e.g. health and safety, national security, financial loss, service loss or loss of public confidence) are also commonly used impact criteria in risk analysis methodologies. However, widely used risk analysis methodologies (e.g. CRAMM [9], OCTAVE [18] etc.) also evaluate additional impact factors, which are not considered as criticality criteria. Examples include the competitive disadvantage (due to commercial and economic interests), legal or regulatory sanctions (due to law enforcement or incompliance with legal or regulatory obligations), or system operation malfunction (due to lack of management and business operations).

During a typical risk analysis, risk is assessed based on impact factors, combined with threat and vulnerability. Thus, as a side-effect, the criticality of the system is also evaluated, at least partially. Indeed, the evaluated risks which are associated with the criticality-related impact factors consist of the criticality-related risks. Note that during risk analysis, some of the evaluated risks are based on impact types which are not associated with the criticality level of a system. In this sense, criticality can be identified as a partial subset of the risk.

Risk as a (partial) subset of criticality. There are several criticality factors which are not taken into account as impact types in traditional risk analysis methodologies. Examples may include scope (number of affected people or geographical range), economic impact (in terms of GDP effect), environmental effect, intra-sectoral or inter-sectoral effects.

As a result, a risk analysis conducted in a single system/organization (or even in multiple organizations of the same sector) will not evaluate risks which are associated to impacts *external* to the examined organization, e.g. social and/or sector-oriented consequences. For example, a criticality analysis may also need to consider the social impacts from an incident that affects the international banking sector. Such impacts are not evaluated within the scope of a risk analysis conducted for an individual banking institution. In fact, if a risk analysis for a single banking institution examined the impact of an event causing unavailability for the whole national banking sector, it would eventually had resulted in a lower risk level, as opposed to an event of service unavailability only at that specific examined organization. This is due to the fact that the bank in question would not lose its competitive disadvantage or face legal/regulatory consequences. In that sense there are also criticality factors that are not considered as typical risks and, thus, risk can be viewed as a partial subset of criticality.

Risk vs. Criticality: Similarities and differences. As explained above, impact is the basic connecting element between risk and criticality. However, other issues should also be considered in order to redefine their correlation and define how a risk analysis can be used while evaluating CIs.

a. *Interdependency of infrastructures*. Risk analysis methods mainly focus on information systems, which they treat as isolated entities. Thus, they fail to represent the complexity of CI interconnections and usually do not consider cross-sector impacts, possible dependencies with other systems or infrastructures or the likelihood of a high cascading effect within the sector or across other sectors. Integration of some of the leading CIP models within risk analysis methodologies is critical if specific CIP needs are to be met. This includes CIP models, e.g.: CIP layers, implications resulting from dependencies between layers, and the multi-dimensional vector of an incident's impact [1]. Various approaches of identification, modelling, visualisation and simulation of interdependencies have been proposed [4], [11], [20], [24], [25].

b. *Impact scope*. A risk analysis mainly evaluates *internal* impacts (within the scope of the examined organization). On the other hand, a criticality analysis also considers impacts *external* to the examined CI, i.e. social/societal impacts, sector impacts or impacts to people/citizens who are not directly related to the examined organization/system (e.g. users, customers, candidate customers, third parties with contracts, etc.). As a consequence, risk analysis only evaluates the risk factors that are related to the internal impacts, while a criticality analysis mainly focuses on the security risks related to the external impacts (societal/sector based impacts).

c. *Impact scales.* Since external and cascading impacts also need to be taken into account, the evaluated impacts tend to be higher than internal/organization-oriented impacts. New impact scales in criticality factors need to be defined and evaluated, which will differentiate not only in the type of impact, but also in the level of impact.

d. *Objectives*. Although the protection objectives in CIP may seem similar to the ones of Information Assurance, i.e. Confidentiality, Integrity and Availability, achieving them appears to be much more complex. Extra efforts concern the global dimension of the CIP, its complexity due to inter- and intra-dependencies, new kinds of threats, dependability and survivability [2]. More specifically the attacks can be the result of structural threats (e.g. natural disasters, accidents, staff shortages due to strikes or epidemics, technical or personal failures, human errors, technical outages, dependencies and supply shortages) or intentional attacks, which may range from disgruntled employees to even terrorists or hostile states, a threat not common in risk analysis [3].

Based on the above, criticality analysis can be defined as follows:

Definition 1. *Criticality*: Following [14], the criticality level of an infrastructure can be defined based on the following criteria;

(a) the level of contribution of the infrastructure to the society in maintaining a defined minimum quality level of (1) national and international law & order, (2) public safety, (3) economy, (4) public health, (5) ecological environment, or

(b) the impact level to the citizens or to the government administration at a national scale from the loss or disruption of the infrastructure.

Definition 2. *Criticality Analysis*: Criticality Analysis is the process of assessing the criticality level of an infrastructure. Following a risk-based approach, Criticality Analysis can be considered as a *special-purpose* and *societal-centric* Risk Analysis process which aims to protect infrastructures critical for the society. Thus, criticality analysis mainly considers impacts for the society instead of impacts for a specific organization operating a system. The scope of a criticality analysis is extended in order to cover *inter-dependent systems* and thus possible threats against and vulnerabilities of interdependent systems. Finally, criticality analysis is performed on large-scale infrastructures that provide services to a large number of users/citizens and thus it usually requires higher scales of impacts.

Table 3 summarizes the similarities and differences between risk analysis and criticality analysis methodologies.

Table 3. Similarities and differences between risk analysis and criticality analysis

	Aims	Scope	Impact Types	Examined Threats	Examined Vulnerabilities	Scale of Impacts
Criticality Analysis	Societal-centric	Internal assets and inter-dependent systems	Possible impacts for the society / citizens	Threats against the system itself and the interdependent systems	Vulnerabilities of the system and its interdependent systems	Higher impacts scales
Risk Analysis	Organizational-centric.	Internal assets	Possible impacts for the organization / users	Threats against the system itself	Vulnerabilities of the system	Variable impact scales

Obviously, while analysing the criticality level of an infrastructure, previous results of a risk analysis on the examined infrastructure and/or its interdependent infrastructures would provide an initial input for the criticality analyst. Since there are also commonly examined impacts, threats and vulnerabilities in both processes former risk analysis results would provide some preliminary metrics, by examining those security risks that derive from commonly used impacts and threats.

4. A Generic Criticality Analysis Methodology based on Risk Analysis

Based on the correlation between security risk and infrastructure criticality as examined in Section 3, we propose a generic criticality analysis methodology, which consists of the following phases:

Step 1: Identification of Critical Assets. As in typical risk analysis methodologies, the assets of the examined CI are documented (i.e. facilities, services, hardware, software, information, human resources etc.). The selection and evaluation of the infrastructure assets can be performed with the assistance of the system owners.

Step 2: Define infrastructure inter-connections and dependencies. During this phase, the majority of the infrastructures which are interconnected with the examined infrastructure should be defined. These can be categorized into two subcategories: a) the *depended infrastructures*, *i.e.* those infrastructures that depend on the examined infrastructure for their normal operation and b) the *requisite infrastructures*, which include all those which are required by the examined infrastructure for its normal operation. Although this process has similarities with the definition of third-parties during a risk analysis it has a different goal. During a risk analysis interconnections with third parties are only considered if such interconnections imply security risks for the examined system/organization (for example inter-dependencies with service providers, software/hardware suppliers, customers etc). During a criticality analysis the interconnections with infrastructures which may imply any social risk should be considered, even if these may not imply security risks for the examined CI. Examples of depended infrastructures may include public services (e.g. e-government services, health services), transport services (traffic control), law enforcement services (police), emergency response services etc. Examples of requisite infrastructures may be other infrastructures which provide basic services to the examined infrastructure and may not be considered in a typical risk analysis. The definition of the interconnections and dependencies will ensure that the criticality impacts will not consider only organization/system-oriented impacts. It will also assist in the definition and evaluation of global threats and common vulnerabilities with the interconnected systems. For example, a physical disaster that causes power loss may be considered a higher threat if interconnected power infrastructures are affected.

Step 3: Evaluate criticality impact. After the infrastructure interconnections and dependencies have been identified, the criticality impact factors are examined. As explained in Section 3, such impact factors have an extended scope and focus on the societal rather than the internal impacts, e.g. impacts to public safety, public services, economic sectors etc. An extended list of criticality impact factors is implemented in Section 4.1. It allows the assessment of impact in a three fold manner: scope, severity and relation to time. The analysis may take into account several scenarios where a critical asset or service is unavailable (e.g. loss of service for 15 minutes, 1 hour, 3 hours, etc.), or where the confidentiality or the integrity of information are affected.

Step 4: Define threats. Since the criticality of the infrastructure also depends on the interconnected infrastructures, a list of possible threats must be conducted, in order to examine the infrastructure against them. Examples of threats that could be evaluated are the following: Masquerading of User Identity, Unauthorized Use or Misuse of resources, Introduction of Damaging or Disruptive Software, Communications Interception or Manipulation, Communications Failure, Technical Failures, Air Conditioning Failure, Software Failure, Operations Errors, Maintenance Errors, User Errors, Fire, Water Damage, Natural Disaster, Staff Shortage, Power Failure, Theft, Willful Damage, Terrorism, Espionage [9].

Step 5: Evaluate threat and vulnerability levels. Possible threats are evaluated for each examined asset of the infrastructure. The threat levels should take into consideration the possibilities of realizing a threat not only within the examined infrastructure but also within the scope of the interconnections and dependencies. The likelihood that a threat may occur to a CI can be based on the history of previous incidents, examining literature and interviewing people about, or from, similar circumstances. The threats that may affect a CI are a more expanded set than the one used in traditional risk analysis. In parallel, the vulnerabilities that allow an incident to occur need to be identified and evaluated. This is not a trivial task, as vulnerabilities can be inherited by other dependent or connected CI.

Step 6: Evaluate the associated criticality risks factors. As in typical risk analysis risk is quantified by combining all the possible combinations of threats, vulnerabilities and criticality impacts for each asset (risk = threat × vulnerability × impact).

4.1. Criticality impact assessment

We selected a set of criteria, which we compiled based on the review of current CIP approaches (see Section 2) and we enriched them by utilizing criteria from other more generic risk methodologies, for example CRAMM [9]. The selected impact scale is a four-level Likert item, ranging as {Very High, High, Medium, Low}. A Likert scale is a psychometric scale commonly used in survey research. When responding to a Likert questionnaire item, respondents specify their level of agreement to a statement [13]. The resulting set of impacts are categorized in terms of scope (see Table 4), severity (see Table 5) and time aspects of impact (see Tables 6 and 7). The numerical scales are usually based on national policies, thus they have significant variations among different methods. To the best of our knowledge there is no standard or report indicating statistical data or widely accepted ranges for these scales. In the following tables we will present indicative examples of how the scaling can be determined, so as to demonstrate the characteristics of each impact factor and how these scales may differ from traditional risk analysis.

Scope can be represented in three suggested ways:

People affected. It measures the number of people that get affected by an incident. It does not evaluate the type of the impact. An example is presented in table 4, based on [23].

Concentration of people. The higher the concentration of people, the greater the potential for catastrophic effects. The notion of population density is been used by the Dutch approach in terms of number of persons/ km^2 [16]; we present an adjusted scale for this criterion.

Range. It evaluates the geographical scope of an event. It can be quantified in terms of distance (for example {max. 100 km^2, 100 – 1000 km^2, 1000 – 10.000 km^2, > 10.000 km^2} [16]) or in a qualitative way {International, National, Regional, Local} [23].

Table 4: Scope-related Impact Factors

Impact Factor	Very High	High	Medium	Low
People affected	Greater than 10,000 people	Between 1,000 and 10,000 people	Between 100 and 1,000 people	Less than 100 people
Concentration of people	> 750 pers/ km2	500 – 750 pers/ km2	250 – 500 pers/ km2	<250 pers/km2
Range	International	National	Provincial / Regional	Local

All these three criteria evaluate scope in a different manner; the first one attempts to quantify the affected individuals, while the following two do not evaluate scope in absolute terms: concentration estimates how much populated an area or vicinity is, and range uses a more abstract representation in terms of geographical effect.

Severity is quantified by the following criteria:

Economic impact. This criterion measures potential direct economic impact from an incident. It includes the losses to the infrastructure itself from service degradation or loss of assets and information, recovery costs, as well as the estimated loss from cascading effects, so it can be analysed in this three types of costs. Although table 5 suggests a scaling, this can be adjusted according to national policy and currency. For example, the Canadian approach [23] indicates the following scaling for direct damage and restoration {over $1 billion, from $100 million to $1 billion, $10 to $100 million, under $10 million}, where as the Dutch approach suggests the following {<50 million €, <500 million €, <5 billion €, <50 billion, >50 billion €} [16]. We observe that these scales are significantly higher than the ones in risk methods, which reach a maximum level of 1 million in losses [9]. Another way is to estimate it in terms of the effect on the national Gross Domestic Product. These ranges vary according to the scope of the assessment and the overall value of the critical assets and they should be adjustable, as in traditional risk methods [9].

Interdependency. It assesses the likelihood of a high cascading effect resulting from an incident within the sector and across sectors. Types of interdependencies can be (a) physical, (b) cyber, (c) geographic, and (d) logical [24].

Public Confidence. This criterion assesses possible impacts on the public's confidence in the ability of the government to preserve public health and safety, economic security, or to assure the provision of essential services and goods [27]. The scaling used is based on [23].

In the following, we describe 5 additional criteria that are used in risk analysis [9], as well as other CIP-based approaches. These are the impacts that receive a relative high assessment by [9], i.e. assessment of 7-10 in a ten-item scale, and are not applicable in normal commercial organisations. One can observe that the applicable impacts and their scaling from traditional methodologies are those that refer to impacts on a societal level.

International relations. This criterion evaluates the potential effect of an incident in the diplomatic relationships of a state with other countries [9], [16]. The implications may vary from demonstrations aimed against the country, threats against embassies/representations, negative publicity in the media and/or on websites to diplomatic ones, i.e. expulsion of diplomats and/or termination of diplomatic relations, refusal or cancellation of important visits by foreign representatives, boycott of goods, refusal or cancellation of trade agreements and other commercial treaties

[16].

Public order. It attempts to estimate the possible implications a loss of a CI may have on the public order of a country. This impacts may be caused both by disclosure of confidential information and of unavailability of critical services to the public (i.e. water supply). The scaling used [9] have been adjusted to fit a four-item scale by.

Policy and Operations of Public Service. It refers to the ability of the government to maintain its policies and normal operation. It varies from public confidence, as it not evaluates the general belief of the public (psychological effect) but the actual ability of the government to maintain its operations. The scaling used [9] have been adjusted to fit a four-item scale.

Safety. It relates to the welfare of individuals when an incident affects the health of the populations; it includes injuries, chronically illnesses and fatalities. It can also refer to pain, grief and suffering of victims [16]. This criterion examines the result of an incident in the health of individuals and not the number of the affected people or the percentage of the population. These parameters are assessed with the scope criteria.

Defence. It describes possible implications in the ability of a government to protect its population from hostile attacks [9], either due to unavailability of CIs or by modification or disclosure of critical information. This is a criterion that we could not attribute a "low" scale, so it ranges from medium to very high.

Table 5: Severity-related Impact Factors

Impact Factor	Very High	High	Medium	Low
Economic Impact	$100 million and higher	$10 to $100 million	$1 to $10 million	under $1 million
Interdependency	Debilitating impact on infrastructures or other sectors	Significant impact on infrastructures or other sectors	Moderate impact on infrastructures or other sectors	Minor impact on infrastructures or other sectors
Public	High risk & ability to	Perception of high national	Perception of moderate risk &	Perception of low risk & high

Confidence	control in doubt internationally	risk & ability to control in doubt	moderate ability to control risk	ability to control risk
International relations	Seriously damage relations with other governments	Raise international tension	Materially damage diplomatic relations	Adversely affect diplomatic relations
Public Order	Threaten directly the internal stability of the country	Widespread industrial action	Demonstrations, or significant lobbying, or industrial action	Localised or community level protest
Policy and Operations of Public Service	Shut down or otherwise substantially disrupt significant national operations	Seriously impede the development or operation of major government policies	Impede the effective development or operation of government policies	Undermine the proper management of a public sector organization and its operation
Safety	Widespread loss of lives	Severe injuries or chronically illnesses on individuals that may lead to casualties	Severe Injuries on individuals or chronically illnesses	Minor Injuries on individuals
Defence	Grave damage to the operational effectiveness or security of allied forces	Grave damage to the operational effectiveness or security of a nation	Minor damage to the operational effectiveness or security of a nation	N/A

Regarding the time aspect of an incident, a criterion which indicates the intensity of the impact is *Recovery Time*. It measures the time required in order to recover from an incident and it is affected by the availability of substitutes and the cost incurred before the asset or service is restored.

However, time relates to criticality in multiple ways. The duration of the impact effect may vary significantly in a CI. The *Impact Duration* is not per se identical with recovery time, because although some services may recover and become fully functional at some point, the long term effects of an incident may still affect the infrastructure and its environment. Examples include effects in the confidence of the citizens to the government or economic impacts following an incident, although the infrastructure may recover its functionality.

Possible ways to represent time factors are {2 to 6 days, 1 to 4 weeks, 1 - 6 months, 1/2 year or longer} [16] or {years, months – year, days – weeks, hours – days}[23]. Traditional risk analysis methods usually assess smaller time frames, like {<15 mins, 1 hour, 3 hours, 12 hours, 1 day, 2 days, 1 week, 2 weeks, 1 month, > 2 months} [9]. We chose an assessment which ranges from hours to years.

Table 6: Time-related Impact Factors

Impact Factor	Very High	High	Medium	Low
Recovery Time	Years	Months	Days	Hours
Duration	Years	Months	Days	Hours

These two time-related criteria are considered as impact factors (see Table 6), while the following two indicate that the analyst needs to identify “time-critical moments” for an infrastructure and calculate various levels of criticality for these (see Table 7).

Impact peak. It is the point of time that an incident causes the most serious effect. It can vary, i.e. immediate, 24-48 hours, one week, etc.

Critical Time Frames. The moment that an incident occurs may also affect criticality. One incident may be less critical at a given moment and more at another. A characteristic example is the availability of a communication service during a crisis and during normal operation. The two figures vary significantly. That means that criticality may vary over time and one needs to identify the events that indicate higher levels of criticality.

Table 7: Critical Points of Time

<table>
<tr><th>Factor</th><th colspan="4">Points of Time</th></tr>
<tr><td><b>Incident impact peak</b></td><td>Immediate</td><td>Within hours</td><td>Within Days</td><td>Within Months</td></tr>
<tr><td><b>Critical Time Frames</b></td><td colspan="4">Identify events that indicate variations in criticality.</td></tr>
</table>

When one tries to calculate overall criticality he needs to evaluate the applicable scope, severity and time-related criteria for a given incident or threat. It is also essential to define when the incident impact peak is expected to occur and also to identify critical time frames of operation for a CI when the particular incident may have more catastrophic results. For these critical points of time, different impact levels are expected in terms of severity, scope and time. We recommend applying a "worst-case" approach as opposed to calculating the average impact. This means that one needs to evaluate the impacts that apply to a particular incident (e.g. safety impact) in respect of these time points or frames, and select the worse impacts to calculate the overall impact.

4.2 Example

Here we present a simple example of an assessment that will assist on the understanding of the methodology. Let's consider that we assess the criticality of an infrastructure of the transport sector, and more specifically the facilities of a metro infrastructure. The particular network offers transportation services to 975.000 travellers daily and is interconnected with other infrastructures, like buses and trams. We would like to evaluate the critical asset "Main train station" in regards of the threat "Fire". One needs to assess what impact a fire incident may have to the train station on a worse case scenario basis. We identify two critical points of time {normal traffic, rush hour} and we perform different assessments for each one. These are the applicable criteria we evaluated:

Criteria Type	**Impact Factor**	**Normal traffic**	**Rush hour** (from 6:30 until 9:30 a.m. and from 3 to 5 p.m. weekdays)
Scope	*People affected*	**Low** (Less than 100 people)	**Medium** (Between 100 and 1,000 people)
Severity	*Economic Impact*	**Low** (under $1 million)	**Medium** ($1 to $10 million)
	Interdependency	**Medium**	**Medium**

		(Moderate impact on infrastructures or other sectors)	(Moderate impact on infrastructures or other sectors)
	Public Confidence	**High** (Perception of high national risk & ability to control in doubt)	**High** (Perception of high national risk & ability to control in doubt)
	Safety	**High** (Severe injuries or chronically illnesses on individuals that may lead to casualties)	**High** (Widespread loss of lives)
Time-related	*Recovery Time*	**High** (Months)	**High** (Months)
	Duration	**Low** (Hours)	**Low** (Hours)

One can observe that the rush hour time frame differs in regards of the people affected (i.e. more employees and people present at the train station) and the economic impact (e.g. more vehicles were crossing the station). Also due to the number of the people in the station, rescue and evacuation presents difficulties that may lead to a higher safety impact.

Interdependent infrastructures will be affected due to the presence of connecting stops within or close to the train station. Also, due to the fact that passengers will require other means of transportation during the recovery period, congestion is expected in the other stations or means of transportation and rescheduling of routes and time-tables is required. Thus, the impact on the interconnected infrastructures is considered moderate.

Due to the presence of fire control measures and the proximity of the fire department station, the duration of the fire was estimated to hours. However, the recovery time required in order to restore the station to its previous condition is estimated to 1.5 months. The incident impact peak was estimated within one hour for both time frames. One of the highest impacts is also the effect on public confidence on a national level, both regarding the infrastructure's safety and the ability of the government to handle the crisis. We observe that the overall criticality level is assessed as *high* (based on a worse impact assessment) for both time scales.

In order to assess the associated criticality risks factors, one needs to estimate the possibility of a fire occurring in the main train station, based on statistics of previous incidents or similar facilities, which can be provided by the fire department. Also the vulnerabilities that may assist in the occurrence of a fire incident need to be identified. Examples include the presence of flammable materials, the bad maintenance of circuits and cabling, high heat temperatures etc. Although the impact was assessed as high, the overall risk may be assessed as low, if the possibility of the threat is low and there are not significant vulnerabilities to facilitate its occurrence.

5. Conclusions – Future Work

Although CIP receives increased attention both from research and governmental bodies, existing approaches for the evaluation and categorization of CI are mainly based on criticality impact factors and do not fully exploit existing results from well-defined risk analysis methodologies. The lack of an overall criticality analysis methodology may lead to critical infrastructure categorization and prioritization results that are inherently biased on isolated, organization-oriented impacts and security risk factors. In this paper we proposed a risk-based criticality analysis methodology, which also considers societal and sector-based impact factors, as well as infrastructure interdependencies. We have also implemented a more detailed list of criticality criteria. Our results show that although risk analysis results of CIs can provide helpful insight on their criticality, a targeted criticality analysis can provide a more deep inspection of possible large-scale risks. Our future work will focus on the definition of criticality-oriented threats and vulnerabilities, in order to fully implement the proposed methodology. Another step is to quantify the qualitative criteria discussed in this paper, which will allow a numerical assessment of risk in CIs.

References

[1] Adar E., Wuchner A., Risk Management for Critical Infrastructure Protection Challenges, Best Practices and Tools, in *Proc. of the 1st IEEE International Workshop on Critical Infrastructure Protection* (IWCIP ‘05), pp. 90-100, 2005.

[2] Bialas, A., Information Security Systems vs. Critical Information Infrastructure Protection Systems – Similarities and Differences, in *Proc. of the International Conference on Dependability of Computer Systems*, pp. 60-67, Poland, May 2006.

[3] Brunner E. M., Suter M., *International CIIP Handbook 2008/2009*, An Inventory of 25 National and 7 International Critical Infrastructure Protection Policies, Wenger A., Mauer V. and Dunn Cavelty M. (Eds.), Center for Security Studies, ETH Zurich, 2008.

[4] Casalicchio E., Galli E., Metrics for Quantifying Interdependencies in Goetz, E.; Shenoi, S. (Eds.) *Critical Infrastructure Protection*, IFIP Series, Vol. 253, pp. 215-228, 2008.

[5] Commission of the European Communities, *Green Paper on a European Programme for Critical Infrastructure Protection*, Brussels, November 2005, COM(2005)576 final.

[6] Commission of the European Communities, *Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection*, COM(2006)787 final, Brussels, 2006.

[7] Commission of the European Communities, *A European Programme for Critical Infrastructure Protection*, Brussels, December 2006, COM(2006)786 final.

[8] Emergency Management Australia, *Critical Infrastructure Emergency Risk Management and Assurance Handbook*, January 2003.

[9] Insight Consulting, *CRAMM User Guide*, Issue 5.1 July 2005.

[10] ISO/IEC, *Risk management-Vocabulary-Guidelines for use in standards*, ISO/ IEC Guide 73: 2002, ISO, 2002.

[11] Kopylec J., D’Amico A., Goodall J., Visualizing Cascading Failures in Critical Cyber Infrastructures, in Goetz, E.; Shenoi, S. (Eds.) *Critical Infrastructure Protection II*, IFIP Series, Vol. 280, pp. 351-365, 2009.

[12] Kröger W., Critical Infrastructures at Risk: A Need for a New Conceptual Approach and Extended Analytical Tools, *Reliability Engineering & System Safety*, Vol. 93, Is. 12, pp. 1781-1787, December 2008.

[13] Likert, R., A Technique for the Measurement of Attitudes, *Archives of Psychology*, Vol. 140, pp. 1–55, 1932.

[14] Luiijf E., Burger H., Klaver M., Critical Infrastructure Protection in The Netherlands: A Quick-scan, in *EICAR Conference Best Paper Proceedings*, 2003.

[15] Luiijf E., *Threat Taxonomy for Critical Infrastructures and Critical Infrastructure: Risk Aspects at EU-level*, Vital Infrastructures Threats and Assurance (VITA) Project (PASR-2004-004400), Deliverable D1.2, July 2006.

[16] Ministry of the Interior and Kingdom Relations, *National Risk Assessment Method Guide 2008*, National Security Programme, The Netherlands, June 2008.

[17] Moteff J., *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*, CRS Report for Congress RL32561, February 2005.

[18] *OCTAVE Method Implementation Guide Version 2.0*, Carnegie Mellon University, June 2001.

[19] National Institute for Standards and Technology, *Risk Management Guide for Information Technology Systems*, NIST Special Publication 800-30, USA, July 2002.

[20] Nieuwenhuijs A., Luiijf E., Klaver M. Modeling Dependencies in Critical Infrastructures, in Goetz, E.; Shenoi, S. (Eds.) *Critical Infrastructure Protection*, IFIP Series, Vol. 253, pp. 205-214, 2008.

[21] North American Electric Reliability Corporation (NERC), *Standard CIP–002–1, Cyber Security-Critical Cyber Asset Identification*, May 2, 2006. http://www.nerc.com/files/CIP-002-1.pdf (accessed 12.03.09)

[22] Pederson P., Dudenhoeffer D., Hartley S., Permann M., *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*, Idaho National Laboratory, August 2006.

[23] Public Safety Canada, *Selection Criteria to Identify and Rank Critical Infrastru-cture Assets*, January 2004. http://www.ocipep.gc.ca/critical/nciap/nci_criteria_e.asp (accessed 10.08.08)

[24] Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K., Identifying, understanding, and analyzing critical infrastructure interdependencies, *IEEE Control Systems Magazine*, Vol. 21, Is. 6, pp. 11-25, 2001.

[25] Setola R., Bologna S., Casalicchio E., Masucci V., An Integrated Approach for Simulating Interdependencies in Goetz, E.; Shenoi, S. (Eds.) *Critical Infrastructure Protection*, IFIP Series, Vol. 253, pp. 229-241, 2008.

[26] US Critical Infrastructure Assurance Office, *Vulnerability Assessment Framework* (ver. 1.1), KPMG, USA, 1998.

[27] US Dept. of Homeland Security, National Infrastructure Protection Plan 2009, Partnering to enhance protection and resiliency, USA, 2009.