European Risk Assessment Methodology for Critical Infrastructures

M.H.A. Klaver, H.A.M. Luiijf, A.H. Nieuwenhuijs, F. Cavenne, A. Ulisse, and G. Bridegeman

***Abstract*— Most risk assessment methodologies aim at the risk at the level of an individual organization or company. The European Union commissioned a study to define the elements for a uniform and scalable risk assessment methodology which takes into account critical infrastructure dependencies across organizations and sectors. The method can be applied at the sector level, cross-sector level and the multinational (EU) level. The advantage is the re-use of risk assessments at lower levels of aggregation scaling up to the European level. The approach to risk assessment and external dependencies can also be used by companies with multiple sites.**

***Keywords*— risk, risk assessment, dependency, critical infrastructure**

I. Introduction

The security and economy as well as the well-being of citizens in nations depend on certain infrastructure and the services they provide. The destruction or disruption of some of these infrastructures and their services could have a serious impact on the economy, ecology, public health, public confidence and morale, politics and the functioning of governments. Such infrastructures are called critical infrastructures (CI) [5]. In order to counteract the potential risk to the European CI and those of its Member States (MS), the European Council started the European Programme for Critical Infrastructure Protection (EPCIP). Dealing effectively with threats and vulnerabilities to CI up to the European level requires methods for risk assessment and risk management for CI. Risk management processes already exist or are under development for different critical and non-critical sectors in the MS. Moreover, most CI operators use risk analysis techniques to assess their risk factors at the business unit/company/ organization level given their normal business operating environment. However, these risk management processes deal with different sets of threats and different approaches and can not be compared or re-used easily.

This research was partly funded by the EU Commission as part of the EPCIP Programme under contract number JLS/2006/EPCIP/033.

M.H.A. Klaver , H.A.M. Luiijf, and A.H. Nieuwenhuijs are with TNO Defence, Security and Safety, The Hague, The Netherlands. Phone: +31 70 3740112, fax: +31 70 3740642, e-mail: {marieke.klaver , eric.luiijf, albert.nieuwenhuijs}@tno.nl.

F. Cavenne and A. Ulisse are with Thales Security Security Solutions & Services Division, Chessington, UK e-mail:{Fabien.Cavenne, Adrian.Ulisse}@thalesgroup.com.

G. Bridgman is with ERTICO, Brussels, Belgium. e-mail g.bridgeman@mail.ertico.com

The EPCIP programme requires a wider co-ordination of these risk management processes with common basic elements and a transversal approach within critical sectors, across critical sectors and/or cross-border while taking into account the dependencies of CI. In order to accomplish this, there is a need for a common understanding and information sharing about threats, vulnerabilities and risk by all CI stakeholders, e.g., operators, emergency management centers, policy makers, and independent regulators. The project EUropean Risk Assessment Methodology (EURAM) [1] which ran from November 2006 to November 2007 was sponsored by the EPCIP programme. The objectives of EURAM were to:

- identify basic elements for a EU methodology for general risk assessment [2],
- identify elements for a common methodology for analysis of (inter)dependencies [3],
- support information sharing by defining procedures for creating qualified and trusted expert networks [4].

This paper discusses the combined results of the first two objectives.

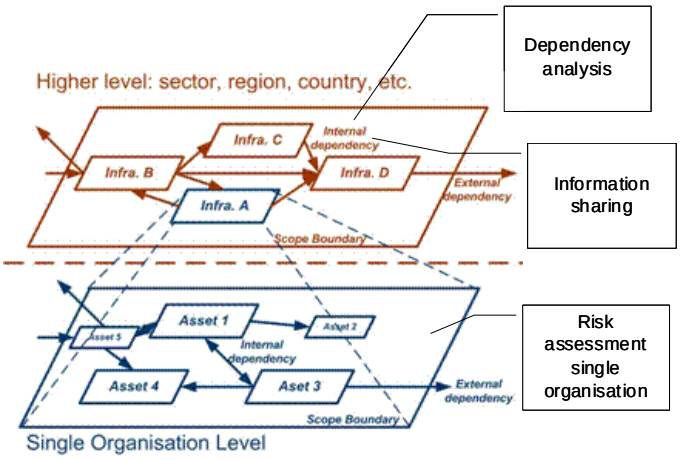

Fig. 1. The elements of the EURAM approach

II. Holistic Risk Assessment

For CIP it is important to use a 'holistic approach of security'. Holistic security risk management aims at managing the security risk in a joined approach. The

dimensions of security which are referred to are, e.g., physical security, ICT security, organizational security, human aspects of security. Approaching these dimensions in a holistic way ensures that the decisions on protection measures are based on a balanced evaluation of these dimensions. In order to be able to perform risk assessment across CI at different levels of analysis (e.g. within a company, a holding, a sector, cross-sector, cross-national), much effort is put on elements that ensure the *consistency* and *interoperability* of the methods and the results.

The process of holistic security assessment proposed by EURAM consists of seven steps as depicted in Figure 2. These seven steps are straightforward and not uncommon to most risk assessment methods. For details on each of these steps we refer you to [2].

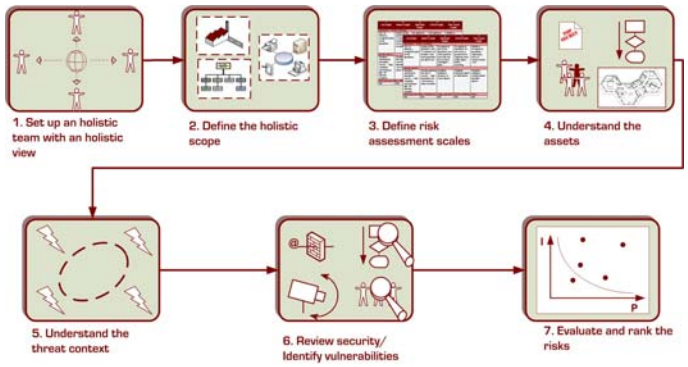

Fig. 2. Generic steps for risk assessment.

A. *Aggregation of risk assessment results*

Whereas other risk assessment methodologies end at the risk for one organization or entity, the EURAM approach has to ensure a coherent and consistent approach and re-usability of lower level results at the next level of aggregation. As such, the results of earlier risk analyses carried out by each organization or infrastructure have to support the identification of risk factors at a higher level of aggregation (CI sector, cross-sector, region, countries, etc.), even – with some more effort – if one has used another risk assessment methodology.

The first prerequisite for these activities is to have a scope defined for the risk analysis (CI sector, a region involving several CI sectors, etc.) under the authority of a relevant party, the "interest group". This group is constituted by business and security experts from the various infrastructures included in the scope of the risk assessment(s). The value of taking a common approach to the identification of CI dependencies and security risk by the interest group is that each member of the "interest group" can be put in charge of contributing with the information concerning his/her area of expertise in a way that ensures correct interpretation and usability. Special emphasis needs to be put by this "interest group" on identifying dependencies across the various infrastructures. Therefore, a dependency analysis can be carried out using the dependency methodology described in Section III. The result of that analysis will provide a clear identification of specific and relevant risk scenarios associated to CI dependencies.

The objective of this aggregation step is not to collate all single risk factors identified by each CI operator. This would infringe on the sensitive nature of this information. The risk factor information collated in this step comprises:

- high level information from the CI operators about their level of resilience over time to risk types without giving details about the associated vulnerabilities in the infrastructure,
- information of each CI about their level of resilience over time for external dependencies.

This aggregation of risk factors results in:

- identification of the main risk factors for the chosen scope and a first understanding of impacts incurred by the CI,
- information sharing between the various parties which will allow some of the CI operators to identify external risk factors they have not initially considered;
- insight in good practices used within the "interest group". This will enable all members of the group to benefit from these good practices, enhancing the resilience of the scope as a whole.

B. *Common elements for consistency*

In order to create a coherent and consistent approach for the security activities at various aggregation levels of analysis, a common understanding and common definition of the following items is needed:

- Consistent scales for impact, probability and risk evaluation. Within an organization, one may use e.g. a five point scale. When spanning multiple organizations, CI, and aggregation levels an extended scale may be required. Based on the EU definition of severity in [6], an example scoring method and set of scales for severity were developed recognizing the public effect (number of members of the population affected), the economic effect (significance of economic loss and/or degradation of products or services), the environmental effect, the political effects, the psychological effects, and the public health consequences of serious CI disruptions or destruction (see Appendix A).
- A comprehensive list of threat classes for threat context identification: to provide a common understanding of threats a list of classes of threats can be used. The EURAM methodology draws upon the threat classifications for CI derived by the EU VITA project [7].

III. COMMON ELEMENTS FOR DEPENDENCY ANALYSIS

One of the main elements in analyzing the risk across CI, is the risk of cascading effects due to dependencies between CI. The EURAM project performed an inventory study of various methods to analyze (inter)dependencies and described some of the common elements for dependency analysis.

A. Underlying Principles

In order to prevent duplication of efforts and unnecessary translation of results, it is very important that dependency analysis re-uses knowledge and earlier results obtained by the separate organizations at a lower abstraction level. This way, the effort is distributed over a large number of people and organizations. The effort is kept close to the source of the expertise and the responsibility for the dependency analysis is kept in place. This distributed approach, however, requires that the assessments are performed in a consistent manner. Moreover, a dependency analysis method that is to be used by many different CI organizations, sectors and nations, should minimize the sharing of sensitive information and should establish clear procedures for trusted information sharing.

B. Steps for Performing a Dependency Analysis

The process of dependency analysis can be performed in various ways and at various levels of abstraction: organization, sector wide, cross-sector, national and international [6]. The result of a dependency analysis is information about the threat, the vulnerability, and the severity of dependencies. This information can subsequently be used in a risk management process for prioritization of mitigating measures. The following common steps can be distinguished:

- Establish scope: the scope of the dependency analysis needs to be established first matching the objective(s).
- Information gathering, a quintessential process to the quality of results. The results should describe the dependencies of other CI and the measures taken to counter risk stemming from these dependencies. This includes internal dependencies between all objects in the scope, external dependencies between objects in the scope and objects outside the scope, and mitigating measures taken to manage the risk stemming from the identified dependencies.
- Information processing: processes the gathered dependency information to make it suitable for risk management. This step combines the information on all separate dependencies to assess the risk of cascading effects. The most suitable method of processing the gathered information depends on the level of aggregation. At high aggregation levels, a scenario-based analysis by an expert panel is best suited. At lower aggregation levels, where the objects are more technical and behave more predictable, a model-based analysis is more appropriate. The result of this stage is a complete assessment of all dependencies within the scope which are fit for use as input to the holistic risk assessment described in Section II.

C. Issues taken into Account

- The dependency analysis approach combines a *bottom-up* approach with a *top-down approach*. The dependency analysis method is meant to be performed bottom-up; starting at the lower organizational levels and ending at the cross-organizational and cross-sector levels, possibly even cross-border and EU levels. In this way, the most detailed analyses can be performed at the lowest levels, enabling the higher levels to concentrate on relevant high level dependency issues only, requiring less detailed information. Dependency issues dealt with at a lower level do not require the exchange of sensitive information to higher levels. Dependency issues that cannot be dealt with at a lower level should be communicated to the next higher level.

  To complete the dependency analysis at the lower aggregation levels, information about the remaining risk to the external objects (at the higher abstraction levels) is required. This requires an effective (cross-CI) top-down information channel from the higher organizational levels to the lower level(s).

- *Subsidiarity principle*: By using a bottom-up approach and because at higher levels of abstraction only that information is exchanged which is relevant to that specific (or higher) level, risk mitigation responsibilities are automatically assigned to the lowest level that is able to handle them.
- Minimized dealing with *confidential and sensitive information*: using the methodology described above, sensitive threat and vulnerability information is automatically kept to the lowest levels where they are required.
- *Uniformity*: In order to prevent duplication of efforts and unnecessary time-consuming translation of results, it is important that the dependency analysis is performed in a uniform manner at every level of abstraction.

IV. CONCLUSION AND WAY FORWARD

The EURAM approach combines common elements for risk assessment, and dependency analysis while dealing with sensitive information sharing. The fact that CI stakeholders expressed that these elements are ‘nothing new’ but combine well-known elements from various risk assessment methods is viewed as a strong advantage. Although the obtained results are promising and show a way forward, more work is required on:

- How to aggregate the results from risk assessments of separate organizations, especially on how to cope with the high sensitivity of the aggregated risk data.

- Common scales to make results from risk assessment across CI sectors, MS and EU comparable. Those common scales need to be defined in close interaction with both CI policy makers, CI sector representations, Member States and the EU.
- Using an all hazard approach or not. Not all CI sector stakeholders agree on the need to use an all hazard approach as they cover the non-terror risk themselves. Some CI sector stakeholders deem a strict separation between 'security' and 'safety' necessary.
- Information sharing requires the establishment of clear information sharing rules.

It is recommended to apply the EURAM approach across a single CI sector in order to refine the approach and find a set of scales which can be applied across multiple CI sectors.

The authors are planning to review the EURAM approach in the context of the power sector.

REFERENCES

[1] EURAM project, Management Summary, TNO November 2007.

[2] EURAM Project, *Deliverable D3.1: Risk Assessment*, Thales Security, November 2007.

[3] EURAM Project, *Deliverable D3.2: Dependency Analysis*, TNO, November 2007.

[4] EURAM Project, *Deliverable D3.3: Information Sharing*, ERTICO, November 2007.

[5] European Commission, *EC COM(2006) 787 final, Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection*, Brussels 12.12.2006.

[6] Luiijf, Eric A.M., Klaver, M., "International Interdependency of C(I)IP in Europe (Internationale Verflechtung von C(I)IP in Europa)", In: B.M. Hämmerli, S. Wolthusen (Eds), *Proceedings of CIP Europe 2005 - Critical Infrastructure Protection*, GI CIS Forum, Bonn, Germany, 19 September 2005.

[7] Luiijf, H.A.M., and Klaver, M.H.A. (eds.), *Threat Taxonomy for Critical Infrastructures and Critical Infrastructure Risk Aspects at EU-level*, VITA project deliverable D1.2, July 2006.

[8] ACIP consortium, *Analysis and Assessment for Critical Infrastructure Protection (ACIP) final report*, EU/DG Information Society and Media, Brussels, Belgium, 2003.

APPENDIX A

The development of the example severity scales shown in Table 1 is based on the following considerations and reflections when looking at the EC definition in [4] for severity:

- The public effects (number of people) are not independent of some of the effects while other scales are not affected at all by the number of people. For that reason, this aspect is not added as a separate severity scale, but can be found as aspect within some of the other scales, e.g., in Table 3.
- The economic effects shall use the same metric, preferably either in euro or dollars (or another one-to-one conversion). The economic effects shall include all direct losses and losses made over time using the Net Present Value (NPV) method.
- The environmental/ecological effects can be expressed in terms of the size of the impacted area (in km^2) times a severity subclass based on recovery time. A conversion table is used to convert these two factors into a score that equates a measure for the environmental severity of the specific risk.
- Considering risk assessment of political effects, it is obvious that only those political aspects can be considered that can be assessed beforehand. Risk assessment, *unless it considers the re-evaluation during or just after an incident*, can not and shall not take into account heightened political sensitivities between two parties, election period, sequences of events which may have led to a political change. The only political effects that can be assessed are the risk of policy changes that affect the process or structure of the business or the sector after an incident or near miss.
- The psychological effects can be expressed in terms of the duration of the impact, the number of people affected, and recovery time. A conversion table is used to convert these three factors by multiplication into a score that equates a measure for the environmental severity of the specific risk.
- The health consequences are expressed in terms of person life years lost, meaning the sum of:
  - half the life expectancies of the people who lost their lives,
  - the total period that people are hospitalized and in recovery, percentage inability to live a normal life times the period affected, and the period of decreased life expectancy.

It is obvious that the establishment of such scales which have enough table entries to span from the individual organization up to the EU-wide level require a lot of additional study and debate. The example set above presents a first step for demonstration of the EURAM methodology.

Table 1: example severity scales

1 No impact	2 Low impact	3 Medium impact	4 Significant impact	5 Severe impact	6 Major impact
← ORGANIZATION LEVEL →					
			← SECTOR LEVEL →		
Economic effect – economical loss (including long-term effects)					
Minor	Up to 100,000 €	100,000 to 1 million €	1 to 10 million €	10 to 100 million €	Over 100 million €
Environmental/ecological effect (recovery time * extent) - see Table 2					
Negligible damage	1 to 3 points	4 to 6 points	8 points	9 or 10 points	12 or 15 points
Political effects					
No discernable effects	No direct business impact, but limitations to business flexibility as result of (potential) failure	Adaptations required to business process as result of (potential) failure	Adaptations required to business process and structure as result of (potential) failure	Major national policy changes affecting the process or structure of the entire national CI sector as result of (potential) failure	Major EU policy changes affecting the process or structure of the entire European CI sector as result of (potential) failure
Psychological effects / immaterial damages (duration * people affected * impact) – see table 3 below					
Negligible effects	<6 points	>= 6 points	>= 12 points	>= 30 points	>=80 points
Health consequences (life years lost)					
<1000 person years	>1.000 person years	> 10.000 person years	> 100.000 person years	> 1 million person years	> 10 million person years

Table 2: Determining the environmental/ecological severity

	1 point	2 points	3 points	4 points	5 points
Extent	Area up to 25 km^2	Area between 25 and 250 km^2	Area between 250 and 2500 km^2	Area between 2500 and 25000 km^2	Area more than 25000 km^2
Recovery time	Recovery within 1 year	Recovery within 1 - 5 years	Recovery longer than 5 years		

Table 3: Determining the psychological severity

	1 point	2 points	3 points	4 points	5 points
Duration	Less than a week	Less than a month, more than a week	More than a month, less then a year	One to ten years	More than ten years
People affected	> 10.000	> 100.000	> 1 million	> 10 million	> 100 million
Impact	Annoying		Disruptive		Disfunctioning

Impact severity:

- Annoying: Irritating for the individual, but not disruptive for his/her daily routine.
- Disruptive: The individual will have to adapt his/her daily routine.
- Disfunctioning: the individual is no longer able to continue his/her daily routine.