Planes de Protección de Infraestructuras Críticas

Critical Infrastructure Protection Plans

Gabriel J. Correa ; José M. Yusta [1]

***Resumen*— En los últimos años se ha intensificado la preocupación de todos los países y gobiernos por la seguridad del abastecimiento energético, y particularmente sobre la protección de las infraestructuras críticas para el suministro de energía. Una visión más amplia relacionada con la seguridad energética, en un contexto geopolítico internacional, se relaciona directamente con las estrategias de defensa nacional, la estabilidad económica, todo lo cual está sujeto al funcionamiento de la infraestructura crítica. Por tal motivo, la definición clásica de la seguridad energética, inicialmente limitada al suministro de energía suficientemente asequible, ahora es un concepto tan amplio que las estrategias deben estar sintonizadas en la protección frente a distintas amenazas. A los marcos de referencia internacionales de la Directiva 2008/114/CE de la UE y el Plan Nacional de Protección de Infraestructuras de EE.UU de 2009, se suma en España la aprobación de la Ley 8/2011 y del Real Decreto 704/2011 sobre identificación y protección de infraestructuras críticas.**

En este trabajo se muestran, en el marco de estas referencias, distintas estrategias internacionales de organización de la protección de infraestructuras. La revisión se centra en las diferentes definiciones de la seguridad energética, infraestructura crítica y recursos clave, presentando las experiencias en países considerados como de referencia internacional sobre el tema. Para lograr el objetivo de proteger la infraestructura energética crítica en cualquier nación, se requiere involucrar a cada componente de la infraestructura energética para implementar un programa de gestión de riesgos que se inicia con un análisis de vulnerabilidades y evaluación de riesgos, así como la aplicación de medidas de mitigación de amenazas. Por tal motivo, en el trabajo se introduce un marco conceptual para los programas de gestión de riesgos, los cuales incluyen la identificación de los mismos y la posterior reducción de su frecuencia de e impacto. Lo anterior constituye la piedra angular de toda la actuación en la protección de infraestructura crítica y constituye una aplicación práctica en los resultados de esta publicación.

***Palabras Clave* — Seguridad, riesgos, energía, infraestructuras.**

***Abstract*— In recent years, concerns on energy supply security have raised up for many countries and governments, and particularly on energy critical infrastructure protection. A broader vision regarding energy supply security within an international geopolitical context is directly related to national defense strategies and economic stability, which are also dependent to appropriate operation of critical infrastructure. Therefore, the classical definition of energy supply security, initially limited to warranty enough power affordability, has now become a broader concept that includes protection strategies against various threats. The international frameworks of the EU Directive 2008/114/EC and the U.S. National Infrastructure Protection Plan since 2009, is now accompanied by the recent approval in Spain of Act 8/2011 and Royal Decree 704/2011 on the identification and protection of critical infrastructures.**

In this article, on behalf of such references, different international strategies for infrastructure protection management are shown. The reference's review focuses on different definitions for energy supply security, critical infrastructure and key resources, showing several experiences in countries that are now considered as international reference on such area. In order to achieve the goal of protecting critical energy infrastructure in any nation, it is required to involve each infrastructure component into the implementation of risk management enterprise program. This begins with vulnerability analysis, risk assessment and threat mitigation actions.

Thus, the paper introduces a framework for risk management programs, which include their identification. This is the cornerstone of all action in the protection of critical infrastructure, which is a practical application of the results of this publication.

***Index Terms* — Security, risks, energy, infrastructures**

I. INTRODUCTION

State governments nowadays consider security of supply as one the principal objectives within their energy policies, including institutional efforts that are focused on protection in order to warranty homeland security, economic activities, public health, etc.

This fact evidences the close relationship between global security of energy infrastructures with other critical infrastructure sectors of the economy. It is not possible to achieve energy sustainability goals, economic goals, or social development if vulnerabilities threaten infrastructure networks in transportation systems, communications, energy, etc.

This concern has been addressed by both European Commission and US Homeland Security Department regarding the security of countries' infrastructures, as a response against new international threats. In 2005, the green book "European programme for critical infrastructure protection" was released by the European Commission [1]. Later, the European Council adopted Directive 2008/114/CE [2], which gave rise to the "European Programme for Critical Infrastructure Protection (EPCIP)." In 2009, the United States (US) National Infrastructure Protection Plan (NIPP) [3] was launched, following the release of several frameworks established by the US Department of Homeland Security [4, 5]. In the particular

[1] The authors are with the Department of Electrical Engineering, Universidad de Zaragoza, 50018, Zaragoza, Spain (e-mail: 621424@unizar.es; jmyusta@unizar.es).

case of a country like Spain, legislation has been accomplished through Law 8/2011 and Royal Decree 704/2001 [6, 7], which delegates in "Centro Nacional para la Protección de las Infraestructuras Críticas" (CNPIC) the coordination and supervision of those plans emitted by all agents involved into national critical infrastructure protection.

In order to achieve the goal of energy infrastructure protection, policies suggest implementation of risk management programs involving vulnerability analysis, threat assessments and risk control measures.

Precisely strategic interest associated with countries' energy security becomes the motivation to develop this article. First part of the article discusses different definitions to the concepts of energy security, critical infrastructure and key resources. It also presents some international experiences, derived from EPCIP and NIPP, which constitute the international reference regarding infrastructure protection. The second part of the article contains a proposal of a qualitative methodology for identification of security threats in electrical infrastructure.

II. CRITICAL INFRASTRUCTURE PROTECTION PLANS

The concept of Critical Infrastructure includes all assets that are so vital to any country that their destruction or degradation would have a debilitating effect on the essential functions of government, homeland security, national economy or public health [8]. Interrupting one critical infrastructure sector, because of terrorist attacks, natural disasters or manmade damage, is likely to have cascading effects on other sectors [9]. Many sources of available information show that countries in North America, Latin America, the European Union and Australia / New Zealand are those with major advances in planning for critical infrastructure protection. Some of their definitions are explained as follows:

According to the US Patriot Act of 2001: Critical infrastructures consist of those systems and assets, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such systems and assets have a high impact on the national economic security, public health, national security, or any combination of these issues [10].

According to EU Directive 2008/114/EC: Critical infrastructures are defined as any element, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, physical integrity, security, social and economic welfare of the population and the disruption or destruction would seriously affect a Member State since it may failure to maintain those functions [2].

As previously explained in the Introduction, concerning critical infrastructure protection has given rise to well defined programs (EPCIP, NIPP) that clearly emphasize the critical areas in which efforts must be focused to develop plans for threat prevention and protection. This also applies to energy critical infrastructures, i.e., those related to electric infrastructure value chain.

These programs provide useful tools to both governments and private operators in order to leverage the collective experience to more clearly define alerting procedures in planning continuity activities in order to improve the reliability of critical infrastructures. Such programs are concentrated in the sectors of energy, transportation, information technology and communications.

A. NIPP: US National Infrastructure Protection Plan

The US NIPP (National Infrastructure Protection Plan) provides a comprehensive and unified framework for the protection of Critical Infrastructure and Key Resources (CI / RC), through federal, state, local entities and the private sector [4], including specific partners in security. NIPP identified three specific areas of interest: the interdependencies between sectors, cyber security, and the international nature of threats to critical infrastructure [11].

The risk management framework of NIPP defines six distinct stages: establishing safety goals, identifying assets, systems, networks, and functions; risk assessment, prioritization of actions, implementation of protection programs, and measuring effectiveness. Additionally, it provides a framework for feedback and continuous improvement, in a flexible and adaptable to situations of risk of each sector. The outline of this plan is presented in Fig. **1**. An explanation of each stage can be summarized in the following paragraphs [12]:

From an industry perspective and in the context of risk management the first step is **establishing safety goals**. Crucial issues such as loss of life, economic impact, and impact of national security, should be considered in the formulation of safety goals.

The second stage, **identifying resources, systems, networks and functions**, requires the development of a complete inventory, containing basic information about the resources, systems and networks in the country, and including material goods, human features and system information. This is the first step to ensure resilience.

The stage of **risk assessment** requires the use of methodologies either quantitative or semi-quantitative, so they deliver results through complete reasonably measurable, systematic and rigorous processes.

For stage of **prioritization of actions**, the NIPP proposes working with partners on security and set priorities based on risk assessments. This item requires a comparison of the relative levels of risk and resources sectors, along with options for achieving security goals. Thus, the protective measures are applied where possible to reduce the security risk, resulting in a more cost-effective decision.

In the stage of **implementation of proactive programs**, protection measures are aimed at reducing the risk.

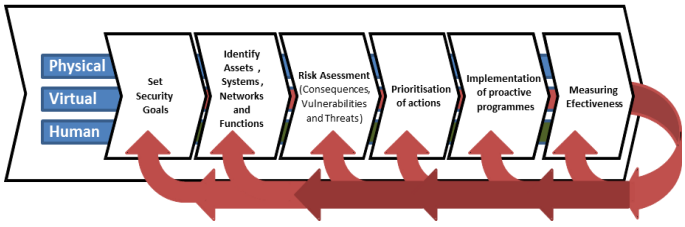

Fig. 1: Framework for the Protection of Critical Infrastructure and Key Resources [3].

The stage of **measuring effectiveness** is established from a system of indicators to provide information on achieving specific security goals, as defined in NIPP [3]. Such result indicators are descriptive and process-based.

B. EPCIP: European Programme for Critical Infrastructure Protection

The overall EPCIP objective is to enhance the protection of critical infrastructure in the European Union. This task will be achieved through the implementation of European legislation as directives and recommendations released by the European Commission [13]. The legislative EPCIP framework consists of the following elements [12, 14]:

- A procedure for the identification and designation of European Critical Infrastructures (ECI) and a common approach to assess the need to improve their safety, the latter being established by a Directive.
- Measures to facilitate the EPCIP improvements, which include an action plan, a warning system on critical infrastructures (CIWIN), by the creation of boards on Critical Infrastructure Protection (CIP) at the level of European Union, procedures for sharing information about the CIP, identification and analysis of interdependence.
- Help to Member States (MS) to improve the security of critical national infrastructure (CNI) and intervention plans [15].
- Complementary financial procedures and, in particular, the specific programme "prevention, preparedness and consequence management of terrorism and other security risks" for the period 2007-2013, that makes available new financing measures for critical infrastructure protection.

The European energy sector gives higher attention to the protection of its large scale energy infrastructure and facilities. It has also been established a network of critical energy infrastructure operators from electricity, gas, and oil sectors to exchange their experience at European level on security related issues [12, 15].

Both world leading programs, NIPP and Directive 114/08, define critical areas in which efforts must focus on prevention and protection of infrastructure. Table 1summarizes the list of critical infrastructure as defined by each of those approaches.

TABLE 1
LIST OF CRITICAL INFRASTRUCTURE SECTORS, IN NIPP (USA) AND EU DIRECTIVE 114

MACROSECTORS US NIPP	MACROSECTORS EU DIRECTIVE 114/08	
Agriculture & food	Energy	Electricity
Bank & finances		Oil
Communications		Natural Gas
Military installations and defense	Transport	Roads &highways
Energy		Railroads
Technologies of Information		Aviation
National Monuments and Icons		Inland waterways
Transportation Systems		Shipping and ports
Drinking water treatment plants		

A broader vision is specified by the NIPP, as it covers more sectors in which it identifies critical infrastructure. Although the approach given by the *European Commission green paper* [14] had initially aimed to cover as much infrastructure as possible, the Directive 114/08/EC [2] finally agreed mainly in the sectors of energy and transport, also including the value chain and supply [12].

C. Other International Experiences

Almost all countries have clear political objectives of critical infrastructure protection, with a commitment and visible support from a national leadership standpoint, reflected in the structure and organisation of the role and responsibility of each government. Most countries have established committees, task forces and working groups, whose mandate includes scenario definition, risk assessment, and establishment of early warning systems.

Each country has an organization according to their culture. However, most countries have a vertical organization, which is directed from the highest levels of their government [12]. Some important cases are referred as follows:

- ***Australia***: The *National Strategy for Critical Infrastructure Protection* provides general principles for the protection of critical infrastructure, describes the main tasks and assigns responsibilities for their implementation. This strategy defines the national critical infrastructure as "those physical facilities, supply chains, information technologies and telecommunications networks which, if destroyed, degraded or unavailable for an extended period of time, could cause a significant impact on social and economic welfare of the nation or affect Australia's ability to conduct national defence and homeland security". [16]

  The strategy is designed according to the methodology contained in Australian Standard AS/NZS 4360:1999, which is a generic guide for implementing the risk management process. It engages the context, identification, analysis, assessment, treatment, communication and on-going monitoring of risks in companies and corporations [17]. Additionally, the strategy applies not only to all levels of government, but also to the owners and operators of the infrastructure, which is largely managed on a commercial basis.

  The main mechanism used in Australia for the exchange of relevant information related to critical infrastructure

protection between the government and the private sector is the "*Trusted Information Sharing Network for Critical Infrastructure Protection*", which was established in 2004 and comprises a group of analysts in nine specific areas that cover the areas of banking and finance, communications, energy, emergency services, food chains, health, transport and places of high concentration of people.

The Government of Australia plays an important role in protecting critical infrastructure through its respective agency: *National Infrastructure Information*. Critical infrastructure operators and owners have the responsibility to properly secure their assets and apply risk management techniques into their processes.

- ***Canada***: The *Strategy for the Protection of National Critical Infrastructure* is currently, in early 2011, under implementation. It promotes an integrated risk management of critical infrastructure, including physical and cyber components, applied to both public and private sectors. Since exchange of information is essential for protecting and securing critical infrastructure, it also implements emergency management acts, aiming to facilitate the exchange of information on emergencies, including warnings of threats, business continuity plans and vulnerable assets.

  The Canadian security policy is contained in the communication "*Securing an Open Society: Canada's National Security Policy*". The purpose of this policy is to ensure that the government is prepared to face and respond to various security threats including terrorism, infectious diseases, natural disasters, cyber attacks on critical infrastructure and domestic extremism [18]. Likewise the North American Electric Reliability Corporation (NERC) is a joint program of protection of critical infrastructure for the grid of North America (US and Canada) which develops mandatory regulations, risk assessments, dissemination of critical alerts information across the industry and awareness of key issues.

- ***Latin American countries***: Governments of Latin American countries have entrusted critical infrastructure protection to both owners and operators of the systems and networks that comprise it. This task is always performed through a strong relationship with civil and military authorities, in order to guarantee the protection of both assets and networks composing the infrastructure. Most critical infrastructure protection plans in Latin American countries are based on risk management frameworks as those conceived in standards either as the Australian [17] or the ISO 31000 [19].

  However, since 2008 it has emerged a significant concern, particularly in the area of network security systems and information technology, for whose protection follow the examples and recommendations of international organisations and experts (UN, OAS, NATO, ITU) to combat cyber attacks and cybercrime.

  Policies for protection of information infrastructure are focused on two areas: Internet and telecommunications, in accordance with the CERT/CSIRT methodology. Both sectors cannot be separated as they are closely linked, and the interests of Internet and telecommunications providers to operate secure networks are interrelated. CERT (Computer Emergency Response Team) is a name given to expert groups that handle computer security incidents. The generic term CERT/CSIRT refers to an essential part of national coordination centers that involve government boards and corporations in cybersecurity.

  Among the major initiatives of Latin American countries account the formation of governmental groups that rely on the ministries of defence, in countries like Brazil[20] and Colombia [21], that pioneered the implementation of strategies against attacks. Other countries like Argentina, Chile, Mexico, Uruguay and Venezuela, are still in process of analysis and creation of government CERTs.

- ***France***: The inter-ministerial coordinating tasks in matters of defence and national security are managed by the General Secretary of Defence and National Security (*Secrétariat general de la défense nationale* [22]). The SGDSN leads defence councils and high-level ministerial meetings held under the chairmanship of the French President, the Prime Minister or his senior aides.

  SGDSN also assumes certain permanent functions or ad-hoc assignments, entrusted to the Prime Minister on the basis of character or inter-institutional evolution. SGDSN in recent years has seen a significant expansion of its scope to national security challenges inside and outside France. The SGDSN has led the White Paper on Defence and National Security, an initiative born out of the European Directive 2008/114/EC. In addition, some groups have been launched as the "*Centre opérationnel de la sécurité des systèmes d'information*" (COSSI) and it has also given rise to *PIRANET Plan* for the prevention and protection against cyber attacks.

- ***Netherlands***: The Dutch government has established the National Critical Infrastructure Advisory (*Nationaal Adviescentrum Vitale Infrastructuur* [23]) which is the agency that has the knowledge and experience in the security of critical infrastructure. NAVI aims to share its experience with companies and other government agencies IN critical areas. NAVI offers support for risk assessment and safety advice, best practices and international contacts.

  In the Netherlands the exchange of information takes place in different forums including the regular meetings of the *National Crisis Centre* and others that exchange information between government and the private sector. One important issue is the agreement between the government and major suppliers of critical infrastructure

for the latter to report certain faults or interruptions which may occur while handling those systems.

- ***Spain***: This country has launched the "*Plan Nacional de Protección de Infraestructuras*", and created the "*Centro Nacional de Protección de Infraestructuras Críticas*" [24]. The main mission of this agency is the coordination of activities of those involved in the protection of critical infrastructure, both in the public and the private sector, in order to develop general and sector-specific plans for protection. The CNPIC is the national director and coordinator board of all activities related to the protection of critical infrastructure as it has been designated by the ministry of home affairs, of which it depends. This governmental agency has been ratified through the Law 8/2011[25], which establishes the Spanish state policies on critical infrastructure protection plans.

  The breadth of the concept of critical infrastructure, and the multiplicity of sectors concerned, requires addressing their protection from a multidisciplinary perspective, with the involvement of numerous public and private agencies under a single direction, coordination and supervision of all activities related to national critical infrastructure protection.

  On the initiative and coordination of CNPIC has also promoted the creation of CCN-CERT, a government body responsible of reporting incidents of information security. This initiative has been promoted by the *National Cryptologic Center* and by the *National Intelligence Centre* (CNI). It was created in early 2008, and it is active in major international forums sharing goals, ideas and information on overall security [26].

  The CNPIC has clearly focused its efforts on protecting critical infrastructure from an integrated perspective including both physical infrastructures and cyber security.

- ***United Kingdom***: The British government has established the *Centre for the Protection of National Infrastructure* [27]. There are nine critical infrastructure sectors that have been identified on this initiative: communications, emergency services, energy, finance, food, government, healthcare, transportation and water. Each sector includes resources and services that are critical at all levels of society. CPNI is interdepartmental, with funding from industry, academia and a number of departments and agencies. These include the "*Cabinet's Secret Service Committee*", the "*National Technical Authority in the UK for Information Assurance*" (CESG) and other government departments responsible for national infrastructure protection.

III. RISK IDENTIFICATION IN VALUE CHAIN FOR ELECTRIC INFRASTRUCTURES

Risks related to electrical systems are not located only at the stage of electric generation. Risks and threats generally affect all stages of the value chain: generation, transmission, distribution and trading of electricity.

From the point of view of infrastructure, the transmission network has some critical nodes in which the system needs to be secure enough to allow controlled interruption in case of an unforeseen event. In other cases, critical nodes have to be so robust that they ensure autonomous operation during hours, days, weeks or even longer, if required. Consequently, strengthening power infrastructure system involves activities that extend beyond and deeper than traditional procedures. In general, high vulnerability of the electrical system may be detected in those nodes where failure could spread and cause cascading outages within a region or into one or more countries.

Risk identification stages focus on discovering the major kinds of risks [17, 28]. This is a qualitative exercise that results in a complete list of risks as well as their components applicable to both the value chain and the life-cycle of the infrastructure network [29], with especial emphasis on the following aspects:

- Assets, buildings, equipment and company headquarters owner / operators of electrical infrastructure.
- Electricity generation plants.
- Transmission and distribution power grids.
- Interdependencies with other critical infrastructure sectors.
- Critical nodes of the grid.
- Regulations and policies that impact the operation of the system.
- Impact on the affected population.

One technique that allows most comprehensive holistic analysis of the vulnerability of a system infrastructure may be conducted through **risk maps** [12, 30]. Under a risk management framework the *identification* stage determines the possible events that affect those resources required for the achievement of the infrastructure operational objectives. A proper investigation of each of the risks must conduct to the identification of its components.

In order to construct a risk map it is essential to collect and manage large amounts of information, which is often difficult due to the absence, inaccessibility and lack of reliability of much of the data needed. **Fig. 2** shows the construction of risk map that requires analytical-descriptive instruments in order to collect data from primary and secondary sources in companies that own or operate electric infrastructures (transmission and distribution). The technique used for the collection of information may be based on expert advice by using the *Delphi* method through open questions, interviews and revision of proprietary information.

The *risk map* allows the simplification of the amount of categories clustering the components of risk by grouping them e.g. in either technical or non-technical. This methodology allows a better representation of the interrelationships among risks, thus becoming an important alternative in the identification step within electric infrastructures.

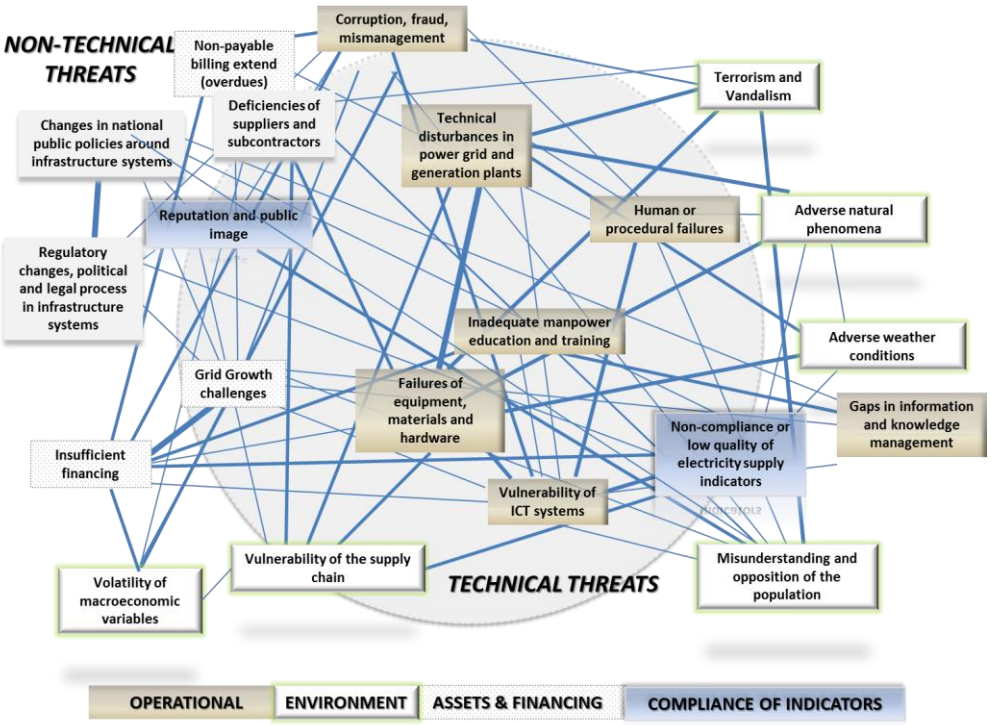

Fig. 2: Proposed interconnected risk map for electric critical infrastructures

Basically, the following categories of risks can be distinguished along with its respective operating electrical company [31]:

- **Compliance of indicators**: a category that gathers those threats related to the issuance of policies, laws, regulations and their impact on economic and social development of the region or nation in which operates the infrastructure system.
- **Assets & financing**: to this category belong those risks derived from market volatility and the real economy, which impact the normal operation and/or expansion of electric infrastructures. Also included in this category are those risks associated with debt collections, as well as the impossibility of obtaining the necessary funds for the payment of incurred obligations to the growth of electric infrastructures.
- **Environment**: a category grouping those risks related to regulatory issues, political, social, natural phenomena, among others, affecting normal operations and performing of electric infrastructures.
- **Operational**: the group of risks that affect the activities, systems, people and value chain within electric infrastructures. They reveal failures in the execution of activities, lack or absence of procedures, insufficiency of human capital, lack of technological and administrative management, etc., which impact the operation and growth of the network infrastructure.

Furthermore, the convenience to indicate the origin of technical or non-technical risks, will help to define their treatment responsibilities, as proposed in [32].

- **Technical threats**: includes financial and operational risks. Other technical threats are those caused directly by people, systems, procedures, whose decisions or actions affect the infrastructure.
- **Non-technical threats:** includes environment risks, strategic risks and resource allocation risks. Other non-technical threats are those resulting from external factors to the infrastructure, such as natural disasters, socio-political situations, actions of third parties, authority decisions, regulation policies, and others.

Both the risk map and the risk components become part of the know-how in companies that own or operate critical infrastructure systems. Some risks may affect the value chain as well as the assets and different subsystems. According to the abstraction level (from strategic point of view to operational jobs) the risk map may vary in order to adapt to particular cases within the organisations.

Developing a risk map for electrical infrastructure should collect all the requirements established at this article's section. **Fig. 2** shows a generic risk map, applied to the system of critical infrastructure in the electricity sector. The proposed **interconnected risk map** provides a framework for decision making, since it simplifies risk perception in an integrated way. The method may assist discovering and analysing of different threats on which infrastructures are exposed, including those that may be considered as the most critical. It is also applicable to operating organizations in transmission electric networks. Furthermore, in the interconnected risk map of **Fig. 2** the thickness of the graph lines may indicate an insight on how risks are related among them.

In practical terms, organizations that own or operate electric infrastructures always characterize each risk in form of *components* [17, 33]. Within the scope of this article, the determination of the risk components that are part of the 21 major risks presented in the interconnected risk map of **Fig. 2** is compiled in a set that includes over 142 risk components, classified in four categories that may consulted in [34].

Within a risk management framework, the proposal of using risk maps can be also applied into organizations that are vertically integrated, i.e. the same company maintains the subsystems of generation, transmission, distribution and energy trading.

IV. CONCLUSIONS

Homeland security, economic prosperity and social welfare in any country depend on a complex system of interdependent infrastructures. Particular attention is emphasized on those related to the electrical infrastructures and their value chain, both in organizational and physical assets assembling the infrastructure.

In response to the need to apply infrastructure protection plans, it should be implemented risk management programs in order to ensure the applicability of these protection plans.

For the identification stage, the authors suggest the use of risk mapping techniques, which allow a comprehensive analysis of all threats in the entire environment of the organizations that owns and operate the infrastructure. A greater level of detail in this activity requires the determination of risk components, preferably defining its categorization by clustering risks (operational, environment, financial and compliance of indicators) as well as their impact on the value chain of the infrastructure system.

Activities that give continuity to the stage of risks identification (risk assessment, prioritization of actions, etc), facilitate deploying defense elements in order to mitigate threats.

REFERENCES

[1] EC, "Libro Verde: Sobre un Programa Europeo para la Protección de Infraestructuras Críticas," European Comission, Brussels (Belgium): *Official Journal of the European Communities*, 2005, 28p

[2] CEU, "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection," in *Council Directive December/2008*, Directive 114, Council of the European Communities. Brussels (Belgium): *Official Journal of the European Communities*, 2008, 75p

[3] NIPP, "National Infrastructure Protection Plan", Washington DC (USA): *U.S. Department of Home Security*, 2009, 175 p.

[4] US Dept Home Security, "Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," *U.S. Department of Homeland Security*, 2003

[5] US Dept Home Security, US Dept Energy Office, "Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan (Redacted)," Washington DC (USA): *U.S. Department of Homeland Security & U.S. Department Energy Office*, 2007.

[6] BOE, "Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas.," Madrid (Spain), *Boletín Oficial del Estado del Reino de España*, 2011, 11p.

[7] BOE, "Real Decreto 704/2011, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.," Madrid (Spain), *Boletín Oficial del Estado del Reino de España*, 2011, 18p.

[8] B. Morel, I. Linkov, D. A. Belluck, R. N. Hull, S. L. Benjamin, J. Alcorn, I. Linkov, "Environmental Security, Critical Infrastructure and Risk Assessment: Definitions and Current Trends," *Environmental Security and Environmental Management: The Role of Risk Assessment*. Springer Netherlands, vol. 5, pp. 1-16, 2006.

[9] A. Löschel, U. Moslener, D. Rübbelke, "Indicators of energy security in industrialised countries", *Energy Policy*, pp. 1665-1672, 2010.

[10] US Dept Energy Office, "Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities", Washington DC (USA): *U.S. Department of Energy, Office of Energy Assurance*, 26p, 2002.

[11] T. Consolini, "Regional security assessments: A strategic approach to securing federal facilities," *Master Thesis in Safety*. Naval Postgraduate School, Monterey, CA (USA), 2009, 103p.

[12] J. M. Yusta, G. J. Correa, and R. Lacal-Arántegui, "Methodologies and applications for critical infrastructure protection: State-of-the-art," *Energy Policy*, vol. 39, pp. pp. 6100-6119, 2011.

[13] V. Costantini, F. Graccevaa, A. Markandyaa, G. Vicini, "Security of energy supply: Comparing scenarios from a European perspective," *Energy Policy*, pp 210-226, 2007.

[14] A. Murray, T. Matisziw, and T. Grubesic, "Critical network infrastructure analysis: interdiction and system flow," *Journal of Geographical Systems*, vol. 9, pp. 103-117, 2007.

[15] EC, "European Network and Information Security Agency," European Comission, Brussels (Belgium): *Official Journal of the European Communities*, 2005, 12p.

[16] CSIRO, Informatics and Statistics, "CIPMA: Critical Infrastructure Protection Modeling and Analysis." Clayton (Australia): *CSIRO Mathematics, Informatics and Statistic*s, 2008.

[17] AS/NZS, "Estándar Australiano de Administración del Riesgo," AS/NZS 4360, 1999, 36 p.

[18] H. M. Abdur Rahman, "Modelling and Simulation of Interdependencies between the Communication and Information Technology Infrastructure and other Critical Infrastructures," *Doctoral Thesis in Electrical and Computer Engineering*, University of British Columbia, Vancouver (Canadá), 2009, 163p.

[19] ISO, "Norma ISO 31000, para la Gestión de Riesgos.", *International Standard Organization*, Geneve (Switzerland), 2010.

[20] CERT.br, "Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil", Brasilia (Brasil), 2011.

[21] CERT-CCIT, "Centro de Coordinación Informática Colombia.", Bogotá (Colombia), 2011.

[22] SGDSN, "Secrétariat General de la Défense Nationale.", Paris (France), 2011.

[23] NAVI, "Nationaal Adviescentrum Vitale Infrastructuur.", Amsterdam (Holland), 2011.

[24] CNPIC, "Centro Nacional de Protección de Infraestructuras Críticas en España.", Madrid (Spain), 2010.

[25] P. Donzelli, R. Setola, "Identifying and evaluating risks related to enterprise dependencies: a practical goal-driven risk analysis framework". *International Journal of Risk Assessment and Management*, vol. 8, pp. 1120 - 1137, 2007

[26] CCN-CERT, "Centro de Incidentes del Centro Seguridad de la Información del Centro Criptológico Nacional", Madrid (Spain), 2011.

[27] CPNI, "Centre for the Protection of National Infrastructure" London (United Kingdom), 2011.

[28] ICONTEC, "Norma Técnica Colombiana para 5254 la Gestión de Riesgos," *Instituto Colombiano de Normas Técnicas*, 2004, p. 44p.

[29] EC, "A Reference Security Management Plan for Energy Infrastructure", *Harnser Group for the European Commission*, Norwich (United Kingdom), 2011.

[30] AON, "Global Risk Managemente Survey," Chicago, IL (USA): *Aon Corporation*, 2010.

[31] B. López, D. Arboleda, "Integración del manejo de riesgo e incertidumbre en la planeación financiera de empresas de transmisión de energía.," *Revista CIER*, Montevideo (Uruguay), Vol. 54, pp. 80-88, 2010

[32] J. M. Yusta, "Amenazas a la seguridad del suministro energético español," *Inteligencia y seguridad. Revista de análisis y prospectiva*,, vol. 6, 2009.
[33] JP-Morgan, "Corporate Metrics," *J.P. Morgan and Co Technical Document*, New York, NY (USA), 1999.
[34] G. Correa, "Identificación y Evaluación de Amenazas a la Seguridad de Infraestructuras de Transporte y Distribución de Electricidad," *Doctoral Thesis in Renewable Energy and Energetic Efficiency*, Universidad de Zaragoza, Zaragoza (Spain), 238p, 2012

Gabriel J. Correa received the Electrical Engineer degree in 2001, the M.Sc. degree in Computer Science in 2004, from Universidad Nacional de Colombia, Medellín, Colombia, and the Master degree in business administration in 2007 from Universidad San Pablo, Madrid, Spain. He also received the PhD degree in Renewable Energy and Energetic Efficiency from Universidad de Zaragoza, Spain in 2012.

José M. Yusta (M'01) received a degree in Industrial Engineering (1994) and a PhD. in Electrical Engineering (2000) from the University of Zaragoza, Spain. He is currently a Senior Lecturer at the Department of Electrical Engineering of the University of Zaragoza. From 2004 to 2007 he was Vicedean of the Faculty of Engineering at the University of Zaragoza. His research interests include technical and economic issues in electric distribution systems, power systems security analysis, and demand side of electricity markets.