Berg Heinz-Peter
Bundesamt für Strahlenschutz, Salzgitter, Germany

Critical infrastructure and resilience goals

Keywords

critical infrastructure, reliability, resilience, robustness

Abstract

Critical infrastructure risks pose a special problem for all countries. The companies that own these infrastructures operate in competitive and regulated environments. However, it is neither practical nor possible to protect critical infrastructures from all hazards. For the government, the continuity of these infrastructures is critical to many of its fundamental missions: economic stability and growth, national security, public safety, and quality of life. In that context resilience has become an important factor to fulfil the task of the critical infrastructure protection. Thus, the development of a framework to establish resilience goals could be helpful.

1. Introduction

The global supply chain, consisting of multiple activities, which cover design, procurement, manufacturing, distribution, and consumption of goods, repeatedly demonstrates the co-existence of operational optimization with operational vulnerability.
This was dramatically demonstrated in the aftermath of the earthquake and the consequential tsunami which devastated the northern coastal region of Japan and leading to the nuclear accident in Fukushima-Daiichi in March 2011 [9].
Infrastructures in general and critical infrastructures in particular are the heart of modern and efficient societies. Therefore, ensuring the protection of this infrastructure is a key function of security-related preparedness measures taken by industry and government agencies, and is a central issue of our country's security policy.
Germany has, both nationally and internationally, actively addressed matters of critical infrastructure protection and is guided by the principle of joint action by the state, society, and business and industry [4].
Resilience helps to mitigate risk to communities, enhance recovery capabilities, and ensure continuity of essential services and functions. Accordingly, two core resilience objectives are established:

- Broad-based resilience to improve capabilities of families, communities, private-sector organizations, and all levels of government to sustain essential services and functions.
- Infrastructure resilience to enhance the ability of critical infrastructure systems, networks, and functions to withstand and rapidly recover from damage and disruption and adapt to changing conditions.

2. Definition of critical infrastructure

Infrastructure can be categorized into hard infrastructure and soft infrastructure. The former refers to physical structures or facilities that support the society and economy, such as transport (e.g., ports, roads, railways); energy (e.g., electricity generation electrical grids, gas and oil pipelines); telecommunications (e.g., telephone and internet); and basic utilities (e.g., drinking water supply, hospitals and health clinics, schools, irrigation, etc.). The latter refers to non-tangibles supporting the development and operation of hard infrastructure, such as policy, regulatory, and institutional frameworks; governance mechanisms; systems and procedures; social networks; and transparency and accountability of financing and procurement systems [1].
Several definitions of critical infrastructure exist in the literature and in official policy documents. The European Union [2] defines critical infrastructures as:

"An asset, system or part thereof, located in member states, that is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact on a member state as a result of the failure to maintain those functions."

The OECD has given two definitions of the term "critical" and "infrastructure" [13] which attempt to reconcile the various definitions given in the OECD member states. According to this definition:

- The term "critical" refers to infrastructure that provides an essential support for economic and social well-being, for public safety and for the functioning of key government responsibilities, such that disruption or destruction of the infrastructure would result in catastrophic and far-reaching damage.
- National definitions of "infrastructure" refer to physical infrastructure and often also intangible assets and/or to production or communications networks. These definitions are very broad, certainly broader than the notion of infrastructure commonly used in other fields of policy (e.g. the "essential facility" notion in competition law) and end up including not only the tangible assets, but also the intangibles that run with them (e.g. software, services, etc.).

Critical infrastructure protection is a task of society as a whole, which calls for co-ordinated action supported by all players – government, business and industry, and the general public. The importance of this task derives directly from the definition of the term "critical infrastructure" as used by the Federal Administration [4]:

"Critical infrastructures are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences."

Infrastructure is considered "critical" whenever it is of major importance to the functioning of modern societies and any failure or degradation would result in sustained disruptions in the overall system. An important criterion for this assessment is criticality as a relative measure of the importance of a given infrastructure in terms of the impact of its disruption or functional failure on the security of supply, i.e. providing society with important goods and services.

Such criticality may be of a systemic or symbolic nature or include both elements. An infrastructure will, in particular, be of *systemic criticality* whenever - due to its structural, functional and technical position within the overall system of infrastructure sectors - it is highly relevant as regards interdependencies.

Examples are the electricity and information and telecommunication infrastructures which, on account of the size and density of their respective networks, are of particular relevance and where a large-area and prolonged outage may lead to serious disruptions of community life and processes and of public safety and security.

Critical infrastructure may be exposed to various threats which must be included both in risk and threat analyses and in the selection of options for action (all hazards approach). The overall spectrum of threats may be described as provided in Table 1.

Table 1. Overall spectrum of threats

Natural events	Technical failure/ human error	Terrorism, crime, war
Extreme weather events inter alia, storms, heavy precipitation, drops in temperature, floods, heat waves, droughts	System failure inter alia, insufficient or excessive complexity of planning, defective hardware and/or software bugs	Terrorism
Forest and heathland fires	Negligence	Sabotage
Seismic events	Accidents and emergencies	Other forms of crime
Epidemics and pandemics in man, animals and plants	Failures in organization inter alia, shortcomings in risk and crisis management, inadequate co-ordination and co-operation	Civil wars and wars
Cosmic events inter alia, energy storms, meteorites and comets		

These events and incidents - which are due to very different causes - may cause massive damage to, or destroy the infrastructure facilities which are vital to society and the population in general. Due to the great dependence on infrastructure services, society has become very vulnerable; and this vulnerability has greatly increased not only on account of *external* hazards and risks but also because of the important interdependencies among the various infrastructures *within* the relevant systems. Disruptions or failures may entail so-called domino effects and cascade effects which potentially can paralyze sectors of society and, in addition to the immediate damage caused to affected persons, can result in enormous damage to the national economy and in loss of confidence in a society's political leadership.

Apart from the risks resulting from intentional - especially terrorist - acts, consideration must also be given to possible and, in instances, immense damage caused to infrastructure by extreme natural occurrences. In Germany, severe damage to infrastructure facilities and to supply services may be caused, above all, by extreme weather events such as violent storms or heavy precipitation [4].

Resilience is an important strategy for managing all-hazard risks in critical infrastructures. A common definition of resilience is provided in [12] and it is observed that each sector applies resilience strategies and practices in different ways based on its sector structure, asset configuration, risk profile, and business conditions.
It is necessary to develop in each sector a commonly agreed-upon set of outcome-focused goals for each sector. Once established, these goals can provide the basis for guiding industry and government resources to improve infrastructure resilience and outlining policy initiatives that can address potential gaps.
In general, it is also noted that "resilience policy cannot be applied equally to all sectors but rather understood and analyzed on a sector-by-sector basis, taking into consideration the complexity of existing regulatory and voluntary protection programs, the fundamental nature of the sector, and the cost and benefit of potential resilience programs." [11].
Though infrastructure protection and infrastructure resilience represent complementary elements of a comprehensive risk management strategy, the two concepts are distinct.
Infrastructure protection is the ability to prevent or reduce the effect of an adverse event whereas infrastructure resilience is defined in [11] as the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.

3. Relationships between resilience and robustness, reliability, redundancy, sustainability and repairing

In recent years, the complexity of "systems" has generally increased; this has been accompanied by a tendency for increased interactions between subsystems. As a consequence, details of the system behaviour and subsystem interactions cannot be readily observed or controlled by a single operator. Therefore, some systems' behaviour can be unpredictable resulting in catastrophic failures. Building a system which can recover from a failure and re-establish the original system function is a desirable goal. This recovery action is part of a concept which is defined as resilience and the process of designing or analyzing the system is called resilient engineering.
According to [17] resilience is a property of a system which measures how the system can still function to a required level by means of its own after the system has experienced partial damage. Resilience engineering is about modelling, analysis, and design of a system for achieving a desired resilience property of the system.
With this definition, it is possible to distinguish resilience from robustness, reliability, redundancy, sustainability, and repairing [5]. The distinctions are presented in the following.
Resilience engineering stems from the basic philosophy of making a complex system safer. It is related to well-known existing concepts such as reliability and robustness with systems.
At first glance, it can be difficult to distinguish between resilience and these existing concepts. But in fact resilience is unique and the following will first attempt to point out the implicit differences as well as define explicitly, what resilience is.
The five terms (robustness, reliability, redundancy, sustainability and repairing) are chosen to help explain the meaning of resilience. The reason for selecting them is because the five terms are all used to describe system properties. Moreover, some of the five terms are very close to the meaning of resilience. Consequently, many researchers in this area do not clearly define the differences in their meaning. The following will endeavour to define both the differences and overlaps in the definitions.
In *Figure 1* the relationships between the five terms and resilience are illustrated [5].

Figure 1. Relationship between five terms and resilience

The resilience is drawn in the centre of *Figure 1* with the other five terms surrounding it. It can be seen that resilience has intersections with repairing, robustness, and redundancy which implies that these terms do have some common ground in terms of how they are interpreted.
Consider first the relationship between robustness and resilience; both terms are related to the ability of a system to keep functioning under disturbances (where in this interpretation, disturbance is the alternation or influence to a system).

Both a resilient system and a robust system can function in the presence of disturbances. However, for a robust system, the physical structure of the system is still intact whereas for a resilient system, the physical structure is damaged. In essence, a resilient system contains characteristics of a robust system in that it is the magnitude of the disturbance that differentiates between the two properties.

There can be overlaps among the five terms themselves. But these overlaps will not change the relationships between resilience and the five terms.

Consider the relationship between repairing and resilience, both are related to the process of "system recovery". Resilience focuses on the recovery process of internal means as the priority (e.g. resource relocation and system reconfiguration) whereas repairing emphasizes the recovery process using external means as the priority (e.g. bringing in new components to "heal" the damage). As with robustness, a resilient system has characteristics of repairing because the "end result" is the same.

For the relationship between redundancy and resilience, redundancy can be further classified into two types: physical duplication and function duplication [7]. The physical duplication means that there are two or more completely similar components or subsystems in an entire system (e.g., duplication of engines in aircraft). The function duplication means that there are two or more different components which enable the same function. In both types of redundancy, two or more redundant components may perform at the same time or may be such that some of them stay spare or idle, while the other functions. Redundancy in a system will improve the system's resilience; when one component is damaged, its completely duplicated component or partially duplicated component can replace the damaged component to make the system still functional. Redundancy, thus, is a means to improve the resilience of a system.

A more difficult property to consider is that of reliability. Reliability implies that the system does not fail in a certain time period. The longer the period the more reliable the system will be. A system can be unreliable yet very resilient given the characteristics associated with resilience discussed above (e.g. redundancy).

The last property is sustainability. Sustainability considers the equilibrium between the system and nature [6]. Although all systems should be sustainable, the overlap between the two properties is assumed minimal given that the characteristic of "recovery" is the area of concern.

There are almost as many definitions of resilience as there are people defining it. Most definitions, if not all, assume a change in the system's normal operating environment that has the potential, if not the effect, of disrupting normal system performance. Many definitions of resilience assume a momentary disruption or loss in performance followed by a quick recovery to normal system performance. Some definitions also include the ability of a system to continue operating during changing conditions, if only at a diminished level or where system performance drops gradually as opposed to precipitously. Still other definitions include the ability of a system to adapt to changed conditions. In other words, the change in the operating environment may be long lasting and the system has adapted to perform at an acceptable or sustainable level [10]. Resilience can be depicted as in the *Figures 2* to *4*.

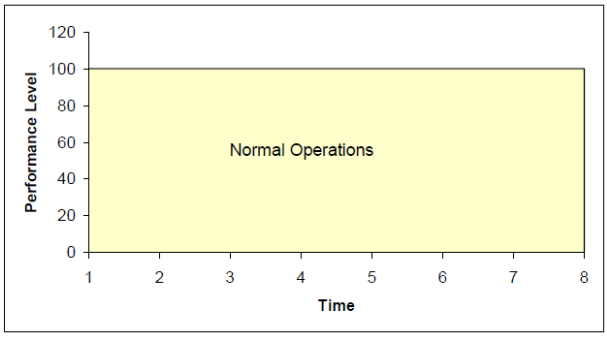

Figure 2. Generic system operations under normal conditions

Figure 2 depicts the normal operation of a system A. System A could be a community's public drinking water system, a regional electric power grid, or, perhaps, the national railroad system. Performance can be measured in many different ways. For example, it could be measured in terms of the number of households beings served, the power being generated within an electric grid, the tonnage of freight moving through the rail system, or the revenue generated by normal system operations. Time can be measured in terms of seconds, or less; years, or longer. For illustrative purposes, the performance of system A in *Figure 2* is measured in dimensionless units over some dimensionless time period. In this case, System A performs at a constant 100 units over the entire time period during normal operations.

The darker area in *Figure 3* depicts the performance of system A resulting from a disrupting event, say a flood, at time = 2.

Performance drops steadily over time, levels off at 60 units, and then, say through recovery efforts, regains normal performance of 100 by time = 7. The lighter area represents the loss of operations during that time.

Figure 4 could depict the performance of system A resulting from a different disrupting event, say an earthquake or terrorist truck bomb, or it could represent the reaction of a different system, system B, to the same event assumed in *Figure 3*.
In either case, the system fails immediately; performance drops to 0, gradually recovers some of its performance, but does not return to the original performance level in the time recorded.

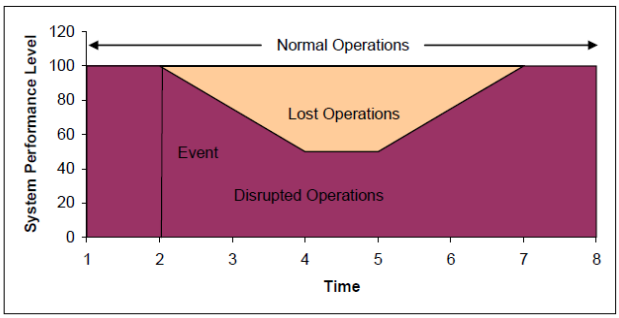

Figure 3. Generic system operations after an event, Scenario A

By most definitions, the system in scenario B (*Figure 4*) would be considered as less resilient than the system in scenario A (*Figure 3*).

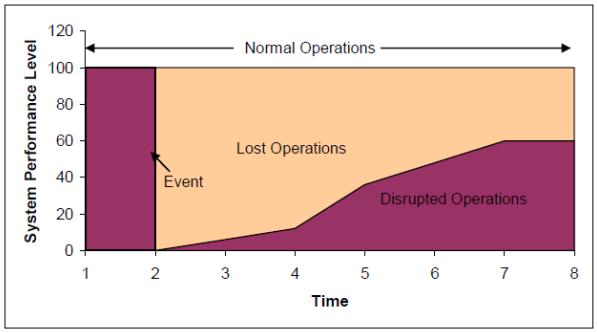

Figure 4. Generic system operations after an event, Scenario B

Just as there is no standard definition of resilience, there is no standard measure of resilience. One measure could be the amount of time it takes to recover fully to normal operations. The quicker the recovery, the more resilient is the system. Another measure could be in terms of total loss of performance.
For example, in *Figures 3* and *Figure 4*, the difference between normal operations and the interrupted performance equals the loss of performance during the disruption. The reduction of the total loss of performance increases resilience.
This approach not only captures the amount of time it takes to recover, but also the initial reaction to the disrupting event, including whether the initial reaction was a precipitous drop in performance or a gradual one, and whether the system continued to function at some level or was put out of operation completely.
How resilience is measured may depend on what decision makers consider most relevant. If monetary losses are important, it may be more appropriate to measure the total (or net) loss of revenue associated with the disruption. If, however, decision makers are more concerned about how long it takes to get their constituents' power back on, then simply measuring time to full recovery may be appropriate.

4. Establishing resilience goals

However, specific definitions of resilience are less important than the fundamental concepts of resilience. Research work identified an impressive array of risk management practices that are commonly used throughout the sector.
To organize and describe these practices the following resilience construct was chosen based on four features [12]:

- robustness – the ability to keep operating or to stay standing in the face of disaster. In some cases, it translates into designing structures or systems to be strong enough to take a foreseeable punch. In others, robustness requires devising substitute or redundant systems that can be brought to bear should something important break or stop working [8]. Robustness also entails investing in and maintaining elements of critical infrastructure so that they can withstand low-probability events but which have high-consequences.
- resourcefulness – the ability to skilfully manage a disaster as it unfolds. It includes identifying options, prioritizing what should be done both to control damage and to begin mitigating it, and communicating decisions to the people who will implement them. Resourcefulness depends primarily on people and not technology.
- rapid recovery – the capacity to get things back to normal as quickly as possible after a disaster. Carefully drafted contingency plans, competent emergency operations, and the means to get the right people and resources to the right places are crucial.
- adaptability – the means to absorb new lessons that can be drawn from a catastrophe. It involves revising plans, modifying procedures, and introducing new tools and technologies needed to improve robustness, resourcefulness, and recovery capabilities before the next crisis.

These features are then organized into a sequence of events as shown in *Figure 5*.

Robustness includes the measures put in place prior to an event [8]; resourcefulness includes the measures taken as a crisis unfolds; rapid recovery includes the measures taken immediately after an event to bring things back to normal; adaptability includes the post-incident measures and lessons learned that are absorbed throughout the system.

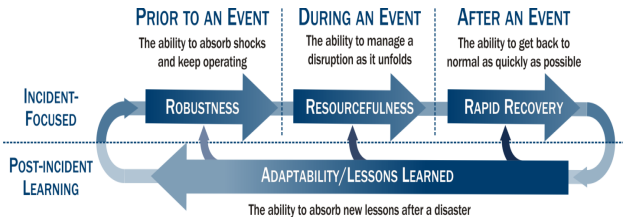

Figure 5. The sequence of the resilience construct according to [10]

Another dimension of resilience is time. The electricity system consists of massive amounts of expensive, long-lived capital assets that have relatively slow turnover. In the near term, system infrastructure and assets are fixed and utilities rely on practices that involve people, plans, processes, and procedures to improve resilience.

In the long term, however, utilities can introduce new technology and alter the design of the electric system to increase resilience. These measures are typically more expensive and require longer lead times, but may offer more enduring resilience because the security is "built into" the infrastructure. Based on these distinctions, each of the four resilience categories can be divided into those practices involving people and processes and those involving infrastructure and assets.

Finally, it has to be recognized that not all threats are addressed in the same way. Unintentional acts, such as storms, floods, earthquakes, and equipment failure, are a part of everyday operations that utilities can prepare for through plans, drills, and direct experience.

Intentional acts, such as theft and targeted physical attacks, are harder to plan for and require different practices and strategies. Cyber acts, which can be accidental or malicious, represent a newer form of disruption that requires a special set of resilience practices.

Through interviews and research more than 100 examples of electricity sector resilience practices have been identified [12]. A summary of representative practices is shown in Table 2.

Developing a commonly agreed-upon set of outcome-focused goals for each sector is challenging. Each subsector, industry segment, owner, and operator has particular business, security, and operational needs.

Table 2. Summary of resilience practices from NIAC resilience matrix of the electricity sector

	Robustness	Resourcefulness	Rapid Recovery	Adaptability
People and Processes	▪ Announced and unannounced emergency drills for control centers ▪ Extensive continuity of operation plans	▪ Highly trained and drilled transmission operators ▪ RTOs prevent cascading failures	▪ Mutual aid agreements ▪ Priority recovery of electricity services for customers (e.g., hospitals, fire, police)	▪ Revising emergency response plan after Hurricane Katrina ▪ Revised industry standards after 2003 blackout
Infrastructure and Assets	▪ Interconnected grid provides enormous absorptive capacity ▪ Double-redundant transmission sections to handle N-2 failures	▪ "State estimators" enable real-time monitoring of transmission ▪ Automatic system transfer for N-1 failure	▪ Shared inventory of spare extra-high-voltage transformers ▪ Spare transmission towers for rapid reconstructions (24 hr)	▪ Substations placed on stilts after major floods ▪ Derated underground power line based on reported failure in another utility

Sector goals that are too specific may not be appropriate for all businesses, while high-level sector goals may be too broad to be meaningful in guiding the development of resilience strategies for individual business. Many sectors also do not have a single organization or body that has the authority or convening power to develop appropriate goals for the entire sector.

Despite these challenges, it is possible to develop a common framework and process for discerning sector resilience goals based on the approach of the electricity sector [12] as depicted in *Figure 6*.

This framework can serve as a model for adoption by other critical infrastructure and key resources sectors.

The first step is to establish a baseline of current resilience practices. In the case study in [9], the electricity sector, hundreds of specific planning, security, business, and operational practices were documented that contribute to the resilience of individual companies and of the sector as a whole.

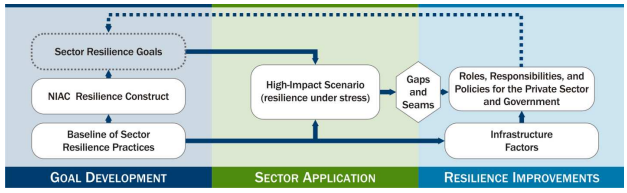

Figure 6. Framework for establishing resilience goals

Practices were examined which are designed to address a variety of potential physical and cyber risks caused by natural weather events, accidents, aging equipment, malicious acts, and supply chain disruptions. A full range of practices from company-specific procedures and practices to sector-wide planning as well as the architecture of infrastructure assets were investigated. Collectively, these practices define the current situation of resilience within the specific sector.

The second step is to describe and organize these practices according to the type of resilience capability it provides using resilience construct depicted in *Figure 5*. The four main organizing principles as described earlier include robustness, resourcefulness, rapid recovery and adaptability.
In the specific case it was distinguished between those practices related to people and processes and those related to the structure of infrastructure and assets for each of the four categories. Additional distinctions were made for practices related to unintentional acts, intentional acts, and cyber events.
The third step is to discern a set of prospective sector resilience goals that are implied by these practices. The purpose of this effort is not to establish final sector resilience goals but rather to propose potential resilience goals that align with the current practices of the sector. For the electricity sector, a set of high-level goals have been derived [12] that aligned well with the way the sector plans and manages reliability for the electric grid. They are:

- Withstand a shock from any hazard with no loss of critical functions.
- Prevent a power disruption from cascading into interconnected systems.
- Minimize the duration and magnitude of power outages through rapid recovery strategies.
- Mitigate future risks by incorporating lessons from past disruptions, simulations and exercises, and sound risk assessment processes.

One important input to this process is an analysis of infrastructure factors that reflect the conditions and circumstances that affect the ability of the sector to resource and implement solutions.
For example, the ability of the nuclear sector - with 104 total plants operated by 32 companies in the U.S. - to implement security solutions is much different from that of the commercial facilities sector, which has thousands of owners and operators of facilities as diverse as office buildings, casinos, malls, and sports stadiums. Several key infrastructure factors were identified and discussed during interviews and weekly conferences.
The final step in the framework is the development or modification of sector resilience goals that are informed by the public-private dialogue. Prospective goals can be modified to reflect specific risks and circumstances. In this way, both government and industry can clarify public and private responsibilities to address infrastructure risks for which there is little precedent and improve the overall resilience of national infrastructures.

5. Concluding remarks

The United States Government Accountability Office has provided a lot of reports to congressional requesters regarding development of a resilience policy and an implementing strategy as a key next step that could strengthen resilience efforts in several critical infrastructure areas ([5], [15], [16]).
Sector-specific agencies (SSAs) are encouraged to emphasize resiliency in their 2010 sector-specific plans (SSPs) and to discuss how resilient these sectors are by design, for example the sectors banking and finance, communications, but also the chemical and nuclear sector [14] as addressed below.
In the chemical sector the SSAs underline that the sector has long recognized that "resilient operations and effective loss prevention are a part of managing risk. These concepts, when woven together, support the umbrella of resiliency." Resiliency, in terms of prevention, protection, response, and recovery along the preparedness spectrum was already covered since 2007 when the SSPs and the SSAs anticipate highlighting and framing the discussion of these items.
In the nuclear sector the SSAs underline that resiliency is an important goal for some aspects of the nuclear sector. Therefore, most nuclear sector programs focus on protection – physical hardening, in additional to other protective strategies – as the underlying goal because of the relatively serious consequences of a successful attack on some nuclear sites.
In Germany, critical infrastructure protection is a task to be performed jointly by government, companies and/or operators and also by civil society. The guiding principles regarding critical infrastructure protection are, in particular [4]:

- trusting co-operation between the state and business and industry at all levels; and
- requirement for, and suitability and proportionality of, the measures taken and the use of resources made for increasing the level of protection.

Consistent implementation of these objectives in the form of a risk management cycle as shown in *Figure 7* for critical infrastructure will offer the necessary guarantee of a consistent protective system of sustained effectiveness, which enhances the German security competencies that are also utilized in the international exchange of experience.

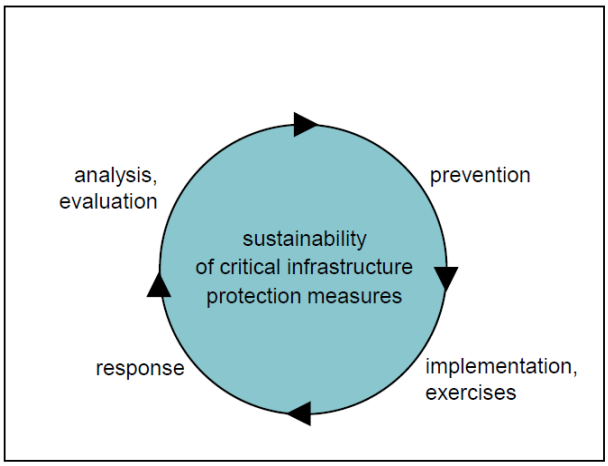

Figure 7. Risk management cycle for critical infrastructure

References

[1] Bhattacharyay, B.N. (2009). *Infrastructure Development for ASEAN Economic Integration*. ADBI Working Paper 138. Tokyo: Asian Development Bank Institute.

[2] European Committee of Manufacturers of Electrical Machines and Power Electronics – CEMEP (2008). *Uninterruptible power supplies*, February 2008.

[3] European Union – EU (2008). *Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, Official Journal of the European Union L 345/75.

[4] Federal Ministry of the Interior – BMI (2009). *National strategy for critical infrastructure protection (CIP strategy)*, Berlin, June 17th, 2009.

[5] Gao, F. (2010). *The proposed resilience analysis methodology and its application to the saskwater pumping station*. PhD Thesis, Department Mechanical Engineering, University of Saskatchewan, Canada, April 2010.

[6] Harris, C.E., Pritchard, M.S. & Rabins, M.J. (2005). *Engineering ethics-concepts and cases, 3rd edition*. Thompson Wadsworth.

[7] He, Y. (2008). *A novel approach to emergency management of wireless telecommunication system*. Master Thesis, Department Mechanical Engineering, University of Saskatchewan, Canada.

[8] Krauß, M. & Berg, H.P. (2012). A generic framework for risk management for critical infrastructure. *Proc. of the 11th International Probabilistic Safety Assessment and Management Conference & The Annual European Safety and Reliability Conference*, Helsinki, Finland 25–29 June 2012, Curran Associates, Inc., Red Hook, NY, Vol. 6, 2189 - 2198.

[9] Krauß, M. & Berg, H.P. (2013). External hazards - in focus after the Fukushima accident, *Kerntechnik*, Vol. 78, Issue 2, in press.

[10] Moteff, J.D. (2012). Critical infrastructure resilience: the evolution of policy and programs and issues for congress. *Congressional Research Service*, R42683, August 23rd, 2012.

[11] National Infrastructure Advisory Council – NIAC (2009). *Critical infrastructure resilience final report and recommendations*, September 8th, 2009.

[12] National Infrastructure Advisory Council – NIAC (2010). *A framework for establishing critical infrastructure resilience goals*, October 19th, 2010.

[13] Organization for Economic Co-operation and Development – OECD (2008) *Protection of 'critical infrastructure' and the role of investment policies relating to national security*. May 2008.

[14] United States Government Accountability Office – GAO (2010). *Critical infrastructure protection, Update to national infrastructure protection plan includes increased emphasis on risk management and resilience*, GAO-10-296, March 2010.

[15] United States Government Accountability Office – GAO (2012). *Critical infrastructure protection, DHS could better manage security surveys and vulnerability assessment*, GAO-12-378, May 2012.

[16] United States Government Accountability Office – GAO (2012). *Critical infrastructure protection, an implementation strategy could advance DHS's coordination of resilience efforts across ports and other infrastructure*, GAO-13-11, October 2012.

[17] Zhang, W.J. (2008). *Resilience engineering presentation material for Hong Kong Poly University*. University of Saskatchewan, Saskatoon, Canada. Http://homepage.usask.ca/~wjz485/PPT%20download/resilience%20engineering%20CNSF%20