Eid Mohamed
CEA DANS/DM2S/SERMA, Saclay Bât, Gif sur Yvette Cedex, France

Serafin Dominique

Yohan Barbarin
CEA Gramat, Gramat, France

Lionel Estel

Souza de Cursi Eduardo

El Hami Abdelkhalak
INSA-Rouen, Saint-Etienne du Rouvray, France

Critical Infrastructures Protection (CIP) – contribution to EU research on resilience & preparedness

Keywords

CIP, resilience, robustness, failure, preparedness, cascading effect

Abstract

Critical Infrastructure (CI) Preparedness and Resilience modelling, simulation & analysis (MS&A) receive a strong interest from systems safety and risk management engineering and research communities. This technical and scientific interest responds to the rapid growth of the use of the smart technology in the modern society activities. The concept of resilience in CIP is not yet clearly defined. However, a probabilistic model is proposed describing the robustness and the resilience of a well-defined infrastructure facing a given threat.

1. Introduction

Critical Infrastructure (CI) Preparedness and Resilience modelling, simulation & analysis (MS&A) receive a strong interest from systems safety and risk management engineering and research communities. This technical and scientific interest responds to the rapid growth of the use of the smart technology in the modern society activities.
The major concerns of the engineers and the scientists involved in the design, the construction and the operation of such systems are to assess the risks and the associated hazards in normal operations and accidental situations. Risk management is almost the major concern.
Recently, Critical Infrastructure Protection (CIP) is identified as a major societal concern, especially after September 11th terrorist action. Under the impulsion of the Homeland Security Act [8], risk management has followed a significant mutation. Some existing taxonomies evolved and has been extended to a wider range of corresponding concepts, such as: resilience, robustness, complex environment, cascading effect, complex system and system of systems.

All these cultural mutations are new and many used taxonomies and concepts are not yet definitively defined. The concept of the CI itself is the 1st of these.

2. Critical infrastructures protection-CIP

The growing societal interest in CIP issues motivates the R&D efforts in MS&A of complex systems preparedness & resilience.
Amongst the corresponding concepts, resilience is gaining a specific interest.
Some recent work promotes even the “promulgation of Critical Infrastructure Resilience (CIR) as the top-level strategic objective in order to drive

national policy and planning" [1], in CIs risk management.

In the same report, [1], of the Centre for Security Studies (CSS), the Risk and Resilience Research Group identifies 3 competing perspectives in risk-resilience relationship: resilience as a goal of risk management, comprehensive risk-resilience management, and (even) resilience as alternative to risk management.

Whatever perspective could take the lead in the future CIs risk management, we can't but notice the strong and invariant relation between: CI, risk management and resilience.

Subsequently, it may be useful to present rapidly the CI concept and its context before treating the resilience concept which is the main topic of the paper.

As far as the author can tell, the 1st use of the concept CI in a strategic official document could be tracked back to the Executive Order EO-13010 [7].

On July 15, 1996, President Clinton signed the EO-13010 establishing the President's Commission on Critical Infrastructure Protection (PC-CIP).

In response to the findings and recommendations of the PC-CIP, the President Directive Decision, PDD-63, on CIP was approved on 22 May 1998.

CIP issue has then been pushed again once more on the scene by the release of the Homeland Security Act, [8], that has been translated in some Presidential Decision Directives such as in [9]. More details about USA strategy in CIP can also be found in [11].

In parallel, the EU launched appropriate actions to identify and designate European CIs (ECIs).

The 1st official mention of the ECI concept is the European Council Directive 2008/114/EC of 8 December 2008, [6], which is based on a report elaborated by a commission of experts and proposed in 2006, [4].

The definition of the ECI is given by in ECD 2008/114/EC, [6].

The EC underlines that "this Directive constituted a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. In the same time it recalls that the primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures".

After the directive, a "critical infrastructure" means "an asset, system or part thereof located in Member States which 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 in a Member State as a result of the failure to maintain those functions".

Regarding the European CIs, the directive, [6], defines the ECIs such as: "infrastructures whose disruption or destruction would have significant cross-border impacts. This may include trans-boundary cross-sector effects resulting from interdependencies between interconnected infrastructures".

The directive underlines that: "the identification by the Member States of critical infrastructures which may be designated as ECIs is undertaken pursuant to Article 3. Therefore the list of ECI sectors in itself does not generate a generic obligation to designate an EC".

Once the basic definitions have been clearly cited, the directive, [6], identifies and designates the sectors as in *Table 1*.

Table 1. List of ECI sectors

Sector	subsectors	
I Energy	1. Electricity	Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity
	2. Oil	Oil production, refining, treatment, storage and transmission by pipelines
	3. Gas	Gas production, refining, treatment, storage and transmission by pipelines LNG terminals
II Transport	4. Road transport 5. Rail transport 6. Air transport 7. Inland waterways transport 8. Ocean and short-sea shipping and ports	

3. Robustness-resilience model

"Resilience" is becoming a very important concept in CIP-MS&A. The ideal situation is to integrate "resilience" and "protection" in one comprehensive risk management strategy. One underlines even attempts to promulgate Critical Infrastructure Resilience (CIR) as the top-level strategic objective.

Unfortunately, unlike protection and risk management, resilience is not yet a specific, easily definable term across all infrastructures, nor is it easily measurable. What is resilience and how to measure it?

Almost, all involved stakeholders agree on the preceding notice. Despite this agreement, consensus regarding important issues, such as how resilience should be defined, assessed, and measured, is still lacking, [3], [10].

The authors would be in favour of a definition looks like:
"Resilience is *the ability of an entity (asset, organization, community, region) to anticipate, resist, absorb, respond to, adapt to, and recover from a disturbance*" [2].
Generally speaking, the term "resilience" in most of its variants refers to: ability, prepare for, adapt to changing conditions, withstand and recover rapidly from disruptions. That covers disruptions induced by deliberate actions, or natural threats or systemic failures. In this paper, the authors will use the generic term threat.
Two conceptual perceptions of resilience are often competing:

- Resilience describes the system after the threat happening.
- Resilience describes the system before and after the threat happening.

The authors' intimate feeling is in favor of associating "resilience" to the system response after "threat happening". The concept "robustness" will be used to describe the system response before and during the threat happening.
Then, the authors opt for the following definition: "Resilience" is the ability of a system/structure/organisation to reduce the duration of a disruption resultant from a given threat.
Subsequently, the authors conceive "resilience" as an after-event dynamic quality and a function of the threat.
The authors should then complete the "resilience" concept by integrating the "robustness" concept. That should allow a complete description of the system functional quality before and after the threat happening, in a dynamic manner.
In the following, the authors will propose a model based on this robustness-resilience concept.

Robustness & Resilience Concept
Regarding the conceptual perception of the authors, they propose the following robustness-resilience concept (RRC).
The functional quality of a system/structure/ organization can be measured using different kind of metrics. Our unique concern is the CIs risk management. Accordingly, we propose to use a probabilistic metric. It could be the "availability", $A(t)$, i.e., the probability that a given functionality is available at its nominal level, at instant "t".
The system/structure/organization is said to be available if the availability magnitude, $A(t)$, is higher than a well-defined critical limit A_0. The system/structure/organization is disrupted if the availability magnitude, $A(t)$, reaches the limit A_∞.
Before the critical limit A_0, no irreversible degradation is observed. Between A_0 and A_∞ a system shows irreversible degradations with time if the threat continue. The limits A_0 and A_∞ are based on probabilistic rationales dependent on the societal risk perception corresponding to the threat.
Our metrics are then the system availability versus time. The proposed RRC is by essence dynamic.
Five characteristic time intervals describe the system life-cycle, *Figure 1*, given that the threat occurred at t_0:

Δ_1 : where $(\Delta_1 = t_1 - t_0)$ is the interval of time during which the system continues providing its normal function and shows no irreversible degradation in spite of the action of the threat. This is the phase of the elastic degradation. If the threat's action stops, the system recovers immediately its full functionality, with no residual degradations. This is a measure of the CI ability to absorb the energy of the threat within its elastic limit (hardness).

Δ_2 : where $(\Delta_2 = t_2 - t_1)$ is the interval of time during which the system shows irreversible degradations. This is the phase of the plastic degradation. If the aggression stops, the system would not be able to recover its full functionality without reparation. This is a measure of the CI ability to mitigate the energy of the threat and tolerate the plastic degradation (toughness).

Δ_3 : where $(\Delta_3 = t_3 - t_2)$ is the interval of time during which the degradation of the system is stabilized. No additional degradation is observed but the recuperation of the functionality is not observed either. That could be because the threat is neutralized or because the system is ultimately disrupted. This is a measure of the CI ability to be maintained or replaced (maintainability).

Δ_4 : where $(\Delta_4 = t_4 - t_3)$ is the interval of time during which the healing actions are progressively and successfully undertaken. The system is repaired but not yet available to facing the threat. This is a measure of the CI ability to be restarted up and reconnected with its operational environment. (convalescence / relapse phase).

Δ_5 : where $(\Delta_5 = t_5 - t_4)$ is the interval of time during which the system is operational and available (in-service). It operates at its nominal level (active resilience). The system recovers its robustness. (robust again)

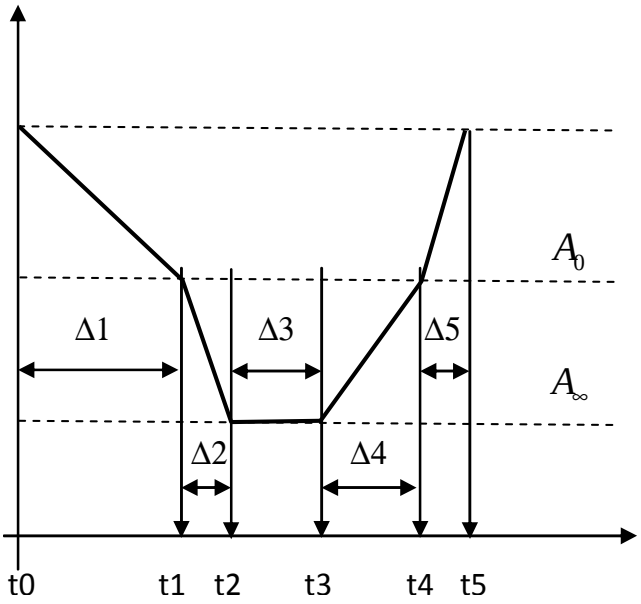

Figure 1. Schematic representation of the CI behavior during and after the threat occurrence

Robustness

In this RRC, robustness is perceived as a "resistance" quality (with/without degradation). One may then distinguish between two types of robustness:

- Robustness-H (hardness): longer is Δ_1, higher is the hardness. No degradation.
- Robustness-T (toughness): longer is Δ_2, higher is the toughness. With degradation.

Longer is $(\Delta_1 + \Delta_2)$, more robust is the CI.

But, one should generally aim at designing and operating CIs such that:

$$\frac{\Delta_1}{\Delta_1 + \Delta_2} \to 1,$$

Under the conditions $\Delta_2 < \Delta_1$ and $\Delta_3 \to 0$.

A CI is robust when it shows high hardness and toughness levels, facing a given threat. Robustness could include the maintainability interval, Δ_3, as well.

Resilience

One may equally distinguish between two types of resilience:

- Resilience-H (healing phase): shorter is Δ_4, higher is the Resilience-H.
- Resilience-O (Operational phase): shorter is Δ_5, higher is the Operational Resilience.

One should generally aim at designing and operating CI out of threat such that:

$$\frac{\Delta_5}{\Delta_5 + \Delta_4} \to 1,$$

Under the conditions: $\Delta_4 < \Delta_5$, $\Delta_4 < \Delta_2$ and $\Delta_3 \to 0$

A CI is resilient when it shows high healing and operational resilience levels, facing a given threat. Resilience could include the maintainability interval, Δ_3, if it is not included in the robustness.

Robustness vs Resilience

In order to measure the relative robustness of a well-defined CI facing a threat, one may propose the following relative robustness indicator, κ_{robust}:

$$\kappa_{robust} = \frac{\Delta_1}{\Delta_1 + (\Delta_2 + \Delta_3 + \Delta_4)}$$

In order to measure the relative resilience of a well-defined CI facing a threat, one may propose the following relative resilience indicator, $\kappa_{resilient}$:

$$\kappa_{resilient} = \frac{\Delta_5}{\Delta_5 + (\Delta_2 + \Delta_3 + \Delta_4)}$$

One may then propose the following metric, ε_{robust}, in order to measure how relatively robust a CI is:

$$\varepsilon_{robust} = \frac{\kappa_{robust}}{\kappa_{robust} + \kappa_{resilient}} = \frac{\Delta_1}{\Delta_1 + \Delta_5}$$

Or the following metric, $\varepsilon_{resilient}$, in order to measure how relatively resilient a CI is:

$$\varepsilon_{resilient} = \frac{\kappa_{resilient}}{\kappa_{robust} + \kappa_{resilient}} = \frac{\Delta_5}{\Delta_1 + \Delta_5}$$

If $\varepsilon_{robust} > 0.50$, the CI is relatively more robust than resilient

If $\varepsilon_{resilient} > 0.50$, the CI is relatively more robust than resilient

Notice that κ_{robust}, $\kappa_{resilient}$, $\varepsilon_{resilient}$ and ε_{robust} are all static quantities.

4. Threat characterization

In spite of the preceding developed metrics, one has not yet assessed the protection level of a given CI, facing a well-defined threat.
In order to be able to carry on this assessment, one should characterize threats in probabilistic terms, as well. One can, then, characterize a given threat by:

- τ_a : the mean action-time of the threat if it occurs,
- τ_c : the mean cycle-time of the threat occurrence, and
- τ_{off} : is the mean off-time per threat occurrence ($\tau_{off} = \tau_c - \tau_a$).

There is no generic and universal model to predict the activation and the deactivation of threats. However, a tentative effort to make a 1st approximation based on the previous characterization could be the following.
Having laid down the hypothesis that τ_a and τ_{off} are *constant with time*, one could proceed to using the hypothesis that threats with constant τ_a and τ_{off} are driven by Stochastic Poisson's Processes (SPP). Subsequently, they occur at constant rates, such as:

- α : is the threat activation rate (h^{-1}) that is equal to (τ_{off}^{-1}), and
- β : is the threat deactivation rate (h^{-1}) that is equal to (τ_a^{-1}).

Threat activation model
Having established the assumption of a SPP, the threat activation probability density function (pdf), $h(t)$ is given by

$$h(t) = \alpha e^{-\alpha t}$$

Leading to a mean off-time $\tau_{off} = \alpha^{-1}$

This is the mean time between two successive threat's actions.

Threat deactivation model
Having established the assumption of a SPP, the threat deactivation probability density function (pdf), $g(t)$ is given by:

$$g(t) = \beta e^{-\beta t}$$

Leading to a mean action-time $\tau_a = \beta^{-1}$

This is the mean duration of a given threat.

Threat recurrence probability
Once a given threat is modelled as a cycle of alternating activation/deactivation periods which is driven by a well-defined SPP, one will be interested in determining the recurrence of a finite number of cycles in a given interval of time T.
One can show, Eid (2011), that the Probability Distribution Function (PDF), $P_k(T)$, describing the k^{th} occurrence of the threat within a given time interval T is given by:

$$P_k(T) = \Psi_k(T).e^{-\beta T} - \Phi_k(T).e^{-\alpha T} \quad (1)$$

where

$$\Psi_k(\sigma T) = \left(\frac{\alpha\beta}{\sigma^2}\right)^k . \left[\sum_{j=0}^{k} (-1)^j . C_j^k \frac{(\sigma T)^{k-j}}{k-j!}\right]$$

$$\Phi_k(\sigma T) = (-1)^k . \left(\frac{\alpha\beta}{\sigma^2}\right)^k . \left[\sum_{j=0}^{k} B_j^k \frac{(\sigma T)^{k-j}}{k-j!}\right]$$

$$\sigma = \alpha - \beta,$$

where,
α: is the threat activation rate (h^{-1})
β: is the threat deactivation rate (h^{-1})
k: is number the threat occurrence cycles within a given time interval T.

The definitions of B and C coefficients are given in *Table 2*. One will be interested in two cases for $k = 1$ and 2, see *Table 3*.

Table 2. definitions of B and C coefficients

C_0^k	$= 1,$	$B_0^k = 0$	$k \geq 0$
C_k^k	$= B_k^k,$		
B_k^k	$= C_{k-1}^k + B_{k-1}^k,$		$k \geq 1$
C_{j-1}^k	$= C_{j-2}^k + C_{j-1}^{k-1},$		
B_{j-1}^k	$= B_{j-2}^k + B_{j-1}^{k-1}$,		$k \geq j \geq 2$

Table 3. The PDFs for k = 1, 2

$P_1(T) = \frac{\alpha\beta}{\sigma^2}\left((\sigma T - 1)e^{-\beta T} + e^{-\alpha T}\right)$
$P_2(T) = (\frac{\alpha\beta}{\sigma^2})^2((\frac{(\sigma T)^2}{2} - 2\sigma T + 3)e^{-\beta T} - (\sigma T + 3)e^{-\alpha T})$

5. CI's protection assessment

Having characterized the threat, it is possible now to assess the protection level of a well-defined CI facing a given threat.
The CI protection assessment can be carried on using different ways. The following is one possible way, based on the length of the threat cycle:

Threat with long cycle
A threat is said to have a long cycle, if:

$$\frac{1}{\alpha} + \frac{1}{\beta} >> \sum_{i=1}^{5} \Delta_i$$

In that case, one faces two possible situations:
Situation #1 is characterized by its relatively long active period with respect to Δ_1, i.e.:

$$\frac{1}{\beta} >> \Delta_1$$

The CI robustness indicator I_{robust} facing a given thread, can, then, be determined such as:

$$I_{robust} = \frac{\Delta_1}{\Delta_1 + \beta^{-1}}$$

In that situation I_{robust} is very low which means that the CI robustness is not sufficient and improving the system resilience (shorten Δ_5) is useless, anyway. The only possibility to qualify this situation as acceptable if the occurrence probability $P_1(\Delta_1)$ is lower than some acceptable limit. This acceptable probabilistic limit could be defined through good practice or through directive decisions of a responsible authority.
Situation #2 is characterized by its relatively short active period with respect to Δ_1 and a very long off-period, i.e.:

$$\frac{1}{\beta} << \Delta_1, \text{ and}$$

$$\frac{1}{\alpha} >> \sum_{i=2}^{5} \Delta_i .$$

The CI robustness indicator I_{robust} facing a given thread, is determined such as:

$$I_{robust} = \frac{\Delta_1}{\Delta_1 + \beta^{-1}}$$

In that situation the CI is robust facing the identified threat and acceptable.

Threads with short cycle
A thread is said to have a short cycle, if:

$$\frac{1}{\alpha} + \frac{1}{\beta} << \sum_{i=1}^{5} \Delta_i$$

In that case, one faces two possible situations:
Situation #3 is characterized by its relatively long active period with respect to Δ_1, i.e.:

$$\frac{1}{\beta} >> \Delta_1$$

The CI robustness indicator I_{robust} facing a given threat is determined such as:

$$I_{robust} = \frac{\Delta_1}{\Delta_1 + \beta^{-1}}$$

In that situation, I_{robust} is very low which means that the CI robustness is not sufficient. The situation is unacceptable even if the occurrence probability $P_1(\Delta_1)$ is lower than some acceptable limit. This is because many threat cycles are possible, with mean number of cycles equal to:

$$\hat{n} = \frac{\sum_{i=1}^{5} \Delta_i}{\frac{1}{\alpha} + \frac{1}{\beta}}$$

The toughness, the maintainability, the operability and the resilience of the CI should be improved, such that:

$\sum_{i=2}^{4}\Delta_i \Rightarrow 0$, and $\Delta_1 + \Delta_5 \Rightarrow \hat{n}(\frac{1}{\alpha}+\frac{1}{\beta})$

The probabilistic condition to accept this situation should be verified as well :

$$\sum_{n=1}^{\hat{n}} P_{\hat{n}}(\sum_{i}^{5}\Delta_i) \leq P_{accept},$$

with the condition;

$\sum_{i=2}^{4}\Delta_i \Rightarrow 0$, and $\Delta_1 + \Delta_5 \Rightarrow \hat{n}(\frac{1}{\alpha}+\frac{1}{\beta})$

The PDF $P_n(\sum_{i}^{5}\Delta_i)$ can be determined using Equation (1).

Situation #4 is characterized by its relatively short active period with respect to Δ_1, i.e.:

$$\frac{1}{\beta} << \Delta_1$$

The CI robustness indicator I_{robust} facing a given thread, is determined such as:

$$I_{robust} = \frac{\Delta_1}{\Delta_1 + \beta^{-1}}$$

In that situation, I_{robust} is very good for only one occurrence of the threat. But the threat is could be very frequent within the interval τ ($\tau = \sum_{i=1}^{5}\Delta_i$). The situation could be unacceptable if the occurrence probability $P_1(\Delta_1)$ is higher than some acceptable limit. In that case the protection of the CI will depend on its resilience.

6. Interdependence

In the previous chapter we proposed a robustness-resilience model for only one CI. One of many still open questions in our model is how to develop a model of robustness-resilience for higher order systems (systems of systems) that may be composed of many interdependent CIs facing many independent given threats [3].

We do not presently have the answer. Despite of this, we believe that the "robustness-resilience concept" would have its full interest in risk management of complex systems that include many interdependent CIs.

7. Application

In order to fix up the main aspects in the proposed robustness-resilience concept model, the authors plotted in *Figure 2* the probability (surfaces) of the first occurrence of a given threat as a function of both: αT and βT, where T is the interval of interest. Four groups of robust-resilient CI could be identified regarding a given threat, such as:

A) The threat is characterized by a short period of action compared to T and a long off-period (low frequency). If T describes the mean time before failure of the CI corresponding to this threat ($T = \Delta_1 + \Delta_2$), one would conclude that CI's facing these conditions shout be robust enough if the threat occurrence probability is low enough.

B) The threat is characterized by a long period of action compared to T and a long period off (low frequency). If T describes the mean time before failure of the CI corresponding to this threat ($T = \Delta_1 + \Delta_2$), one would advise to design CIs with higher robustness even at significantly low threat occurrence probability. If T describes the mean life-cycle of the CI corresponding to this threat ($T = \tau = \sum_{1}^{5}\Delta_i$), one would consider CI's robust-resilience satisfactory, if the threat occurrence probability is low enough.

C) The threat is characterized by a short action-period (compared to Δ_1) and a short off-period (compared to Δ_5). The CI should be robust and resilient enough if the threat occurrence probability is not low enough.

D) The threat is characterized by a long period of action compared to T and a short period off (high frequency). The CI should be resilient enough if the threat occurrence probability is low.

It would be interested as well to underline the fact that a well-determined occurrence probability within a given T of interest could be attended at different combinations of activation-periods (β^{-1}) and off-periods (α^{-1}). In *Figure 2*, we demonstrate the case for $P_1(\sigma T)$, the probability of only one occurrence within T. The same can be illustrated for occurrence probability distribution functions at higher orders.

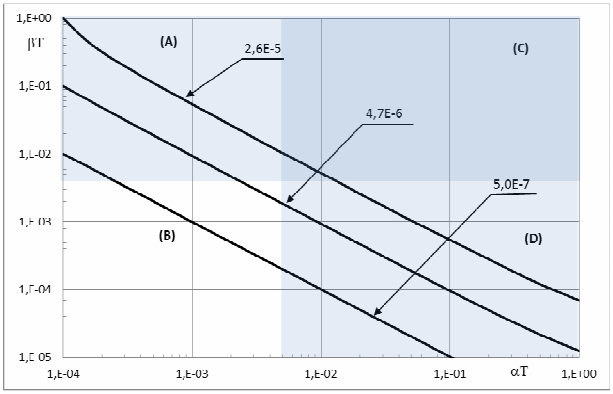

Figure 2. Equi-probable surfaces representing $P_1(\sigma T)$ at 3-values; 2.6E-5, 4.7E-6, 5.0E-7

In *Table 4*, one gives the details of the dependence of the probability $P_2(\sigma T)$, the occurrence of two successive cycles of the threat within T, for threats that occurs once within T at the fixed probability $P_1 = 4.7E-06$.

That is to show that

- threats could be grouped in families according to their occurrence probability of only once in a given interval of time.
- CI's robustness and resilience qualities depend on the threat characteristics (α, β).
- CIs maybe either robust or resilient to be satisfactory protected, facing some families of threats.
- But CIs should be robust or should be resilient, facing some other families of threats.

8. Conclusions

"Resilience" is becoming a very important concept in CIP-MS&A. The ideal situation is to integrate "resilience" and "protection" in one comprehensive risk management strategy.

In the proposed model, "resilience" is associated to the system response after "threat occurrence" and "robustness" to the system response before and during the threat occurrence.

In that model the CI behavior during and after the threat occurrence is characterized by a model which could schematically be described as in *Figure 1*. In parallel the threat occurrence is described in probabilistic terms by , which is the probability that the given threat occurs k times with a given interval T.

The proposed model does not allow yet describing the robustness-resilience for systems of higher orders (systems of systems) composed of many interdependent CIs facing many independent given threats.

Table 4. the equi-probable surface for P_1 = 4.7E-6

	αT	βT	$P_1(\sigma T)$	$P_2(\sigma T)$
1	1.0E-04	1.0E-01	4.7E-06	3.9E-12
2	1.4E-04	7.1E-02	4.7E-06	3.8E-12
3	1.9E-04	5.1E-02	4.7E-06	3.8E-12
4	2.6E-04	3.7E-02	4.7E-06	3.7E-12
5	3.6E-04	2.7E-02	4.7E-06	3.7E-12
6	4.9E-04	1.9E-02	4.7E-06	3.7E-12
7	6.7E-04	1.4E-02	4.7E-06	3.7E-12
8	9.2E-04	1.0E-02	4.7E-06	3.6E-12
9	1.3E-03	7.4E-03	4.7E-06	3.6E-12
10	1.7E-03	5.4E-03	4.7E-06	3.6E-12
11	2.4E-03	3.9E-03	4.7E-06	3.6E-12
12	3.3E-03	2.8E-03	4.7E-06	3.7E-12
13	4.5E-03	2.1E-03	4.7E-06	3.6E-12
14	6.2E-03	1.5E-03	4.7E-06	3.6E-12
15	8.5E-03	1.1E-03	4.7E-06	3.6E-12
16	1.2E-02	8.0E-04	4.7E-06	3.6E-12
17	1.6E-02	5.8E-04	4.7E-06	3.6E-12
18	2.2E-02	4.2E-04	4.7E-06	3.6E-12
19	3.0E-02	3.1E-04	4.7E-06	3.6E-12
20	4.2E-02	2.3E-04	4.7E-06	3.7E-12
21	5.7E-02	1.7E-04	4.7E-06	3.7E-12
22	7.9E-02	1.2E-04	4.7E-06	3.7E-12
23	1.1E-01	8.9E-05	4.7E-06	3.7E-12
24	1.5E-01	6.6E-05	4.7E-06	3.8E-12
25	2.0E-01	4.9E-05	4.7E-06	3.8E-12
26	2.8E-01	3.6E-05	4.7E-06	3.9E-12
27	3.9E-01	2.7E-05	4.7E-06	4.0E-12
28	5.3E-01	2.1E-05	4.7E-06	4.1E-12
29	7.3E-01	1.6E-05	4.7E-06	4.3E-12
30	1.0E+00	1.3E-05	4.7E-06	4.6E-12

References

[1] 3RG (2011), Focal Report 7: CIP Resilience and Risk Management in Critical Infrastructure Protection Policy: Exploring the Relationship and Comparing its Use, Risk and Resilience Research Group, Center for Security Studies (CSS), ETH Zürich, commissioned by the Federal Office for Civil Protection (FOCP), Zurich. (www.css.ethz.ch)

[2] Argonne National Laboratory, (2012). Resilience: Theory and Application, ANL/DIS-12-1, Decision and Information Division, January 2012.

[3] Bloomflield, R. (2009). *Infrastructure interdependency analysis: Requirements, capabilities and strategy.*

[4] D/418/12101/3. (2006). © Adelard LLP.COM, DIRECTIVE OF THE COUNCIL (Proposal for a), On the identification and designation of

European Critical Infrastructure and the assessment of the need to improve their protection, 2006/0276 (CNS), final. Brussels, 12.12.2006, 787.

[5] Eid, M. (2011). Sequential Events Modelling: A Challenge in Structure Safety & Risk Analysis. *International Journal of Materials & Structural Reliability*, 9, 1, ISSN 1685-6368, 1-25.

[6] ECD (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*, 23/12/2008.

[7] EO (1996), Executive Order 13010—Critical Infrastructure Protection. *Federal Register*, 61, 138, 37347-37350.

[8] HSA (2002), Homeland Security Act of 2002, *Public law*, 116 STAT. 2135, 107–296.

[9] HSPD-7, (2003) Homeland Security Presidential Directive-7.

[10] Moteff, J. (2004). Critical Infrastructure and Key Assets: Definition and Identification, *CRS Report for Congress*, Order Code RL32631 *https://www.fas.org/sgp/crs/RL32631.pdf*

[11] OHS. (2002). U.S. Office of Homeland Security. The National Strategy for Homeland Security, 30