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

El Hami Abdelkhalak

Souza de Cursi Eduardo
INSA-Rouen, Saint-Etienne du Rouvray, France

Kołowrocki Krzysztof

Kuligowska Ewa

Soszyńska-Budny Joanna
Maritime University, Gdynia, Poland

Critical Infrastructures Protection (CIP) – coupled modelling for threats and resilience

Keywords

CIP, resilience, robustness, failure, dynamic, model, crisis, management

Abstract

Critical Infrastructure Protection (CIP) requires the development of models and tools able to describe and simulate the threats' and the Critical Infrastructure's (CI) dynamic behaviour. However, these modelling activities are very often carried out separately for threats and for CI behaviour. An effective assessment of the CI's resilience and preparedness requires real coupled models of threats dynamic and CI's one. The authors develop some basic ideas about coupled modelling in the sense of coupling the dynamics of the threat with that of the CIs, within a stochastic modelling approach. Such coupled dynamic models would enhance the effectiveness of our capabilities to assess CI's resilience and to help in decision making for crisis management.

1. Introduction

Critical Infrastructure (CI) preparedness and resilience modelling, simulation & analysis (MS&A) receives an ever increasing interest from systems safety engineers, risk managers and many other related stakeholders. This interest comes in response to the rapid growth of the use of the smart technology in modern societies. The major concerns are related to CI's resilience and to crisis management capabilities.

Critical Infrastructure Protection (CIP) is identified as a major societal concern, especially after September 11th terrorist action [8]-[9]. Some classic safety concepts have been newly revisited and extended to cover a wider range of corresponding concepts, such as: resilience, robustness, cascading failures, connectivity, interdependency and system of systems.

This growing concern about CIP issues motivates the R&D efforts in MS&A of threats and CI's responses to threats' action. Our work focuses on the dynamic modelling of threats and CIs within a probabilistic frame.

2. Resilience M&S

Amongst the relevant concepts, CI's resilience is gaining a specific interest. However, it is still a fuzzy concept, with neither standard definition nor uniform usage. We may say it is still an underdeveloped concept.

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]. However, a national policy in CIP can't exclusively be driven by resilience whatever definition it could have. As far as the open

literature can till, the USA may have the most advanced and coherent national policy in CIP. Details about USA policy and strategic objectives in CIP are published and available in open literature, e.g. [10]-[11].
The EU has, in parallel, launched a series of 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 [5], which is based on a report prepared by a commission of experts and was proposed in 2006 [4].
Similar institutional and (almost) normative activities are multiplied worldwide, as well. Now and then, the use of the concept "resilience" shows a growing inflationary trend in the field of CIP.
This hyper-use and the frequent abuse of the term resilience lead often to develop incoherent MS&A concept and tools, all claiming being resilience oriented objects.
Unlike reliability and risk basic concepts, resilience is not yet a well-defined concept across all CIP domains nor is it easily measurable. The main issue is:
What is resilience and how to measure it?
The authors are in a favour of a resilience concept that is very close to:
"Resilience is *the ability of an entity (asset, organization, community, region) to anticipate, resist, absorb, respond to, adapt to, and recover from a disturbance*", [1].
What we approve in that definition is the following:

- Resilience is not related to the physical being of the entity but to its ability to supply a service.
- Disturbance is when the supply of the required service is disrupted.
- The risk of a service supply disturbance is dependent not only on the nature of the entity but also on the nature of the threat. We will use indifferently both terms "disturbance" and "disruption".
- Resilience is then not an intrinsic propriety of the CI, but it is an extrinsic propriety integrating both the entity nature and its environment (the nature of the menace)

But, what we approve less in the definition above is the following. From our point of view, "resilience" is an extrinsic propriety characterising the CI behaviour under the actions of a given threat. Accordingly, the propriety "resilience" reacts once the threat acts on the CI. One can't observe a resilience reaction, if there is no threat's action. While "anticipation" concerns all preventive actions that may be undertaken before the threat action, by definition. Including "anticipation" in the definition of "resilience" adds additional fuzziness to the "resilience" concept.
We will then maintain only the following 5 aptitudes included the above definition of resilience: resist, absorb, respond to, adapt to, and recover from the disruption.
Having admitted that "resilience" is dependent on both the CI and the threat, a dynamic model describing the resilience should integrate both the threat's dynamic and the CI's one.

3. CI's Resilience & Robustness

Any CI is functionally described by its ability to supply a given well-defined service. The service supply quality of an entity can be described using different conceptual approaches. We propose to use a probabilistic approach.
One may, then, use the "availability" of the service supply, $A(t)$, i.e., the probability that a given service is successfully supplied at its nominal level, at instant "t".
One could also use the "unavailability" of the service supply, $\overline{A}(t)$, i.e., the probability that a given service supply is disrupted, at instant "t".
The expected service is considered to be supplied if the availability, $A(t)$, is higher than a well-defined critical limit A_0. The service supply is disrupted when the availability, $A(t)$, is lower that the limit A_∞. The service supply would be considered as degraded when the availability $A(t)$ is between A_0 and A_∞.
Before the critical limit A_0, no irreversible degradation is observed. Between A_0 and A_∞ a system shows irreversible degradations. The limits A_0 and A_∞ are specified based on probabilistic rationales determined by the societal perception of a given risk.
Five characteristic time intervals, at least, may describe the system life-cycle (resist, absorb, respond to, adapt to, and recover from). These intervals are random variables and schematically presented in *Figure 1*:
Δ_1: ($\Delta_1 = t_1 - t_0$) is the interval of time during which the system continues supplying the required service in spite of the action of the threat. This is the phase of no degradations in spite of the threat's actions. It measures the CI's ability to resist to the threat (hardness).

Δ_2: $(\Delta_2 = t_2 - t_1)$ is the interval of time during which the system shows irreversible degradations. It measures the CI's ability to mitigate the energy of the threat and tolerates the plastic degradation (toughness).

Δ_3: $(\Delta_3 = t_3 - t_2)$ no additional degradation is observed. That could be either because the threat is neutralized or because the system is ultimately destroyed. It measures the CI ability to be maintained or replaced (maintainability).

Δ_4: $(\Delta_4 = t_4 - t_3)$ is the interval of time during which the service is becoming available but it is not supplied yet.

Δ_5: $(\Delta_5 = t_5 - t_4)$ is the interval of time during which the service is gradually supplied. The service supply is at its original quality.

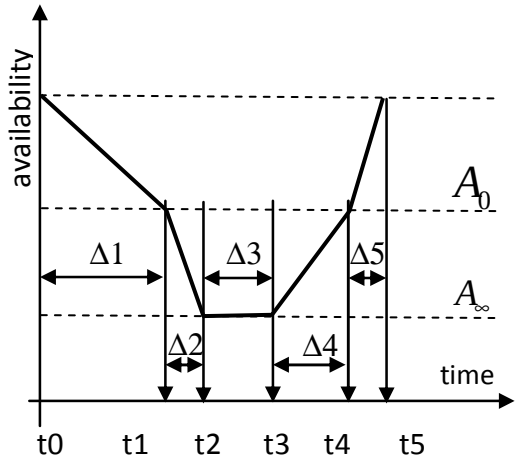

Figure 1. Schematic representation of the CI behavior during and after the threat occurrence

Although we have developed this approach inspired by the definitions of resilience in [1] and [2], we would like to propose an additional slight modification.

We would like to distinguish between the robustness and the resilience. Where "robustness" would cover the resistance quality of the CI to the threat actions and "resilience" would cover the recovery quality of the CI.

3.1. Resilience index

The authors have already expressed some precise ideas that may contribute to the effort of defining, describing and measuring the resilience by proposing a conceptual resilience model [6]. Accordingly, resilience may then be defined using a resilience index $\varepsilon_{resilient}$ defined as following:

$$\varepsilon_{resilient} = \frac{\Delta_5}{\Delta_4 + \Delta_5},$$

But, it can, as well, be defined as:

$$\varepsilon_{resilient} = \frac{\Delta_4 + \Delta_5}{(\Delta_1 + \Delta_2 + \Delta_3) + (\Delta_4 + \Delta_5)},$$

Expressing the resilience index $\varepsilon_{resilient}$ in any of the preceding forms or any other derived forms can be decided thanks to a normative effort. However, this is out of the scope of the paper

3.2. Robustness index

Robustness concept is even fuzzier than the resilience one. The authors conceive "robustness" as the aptitude of the CI to withstand the harmful impact of a given threat. Again, we use time measures in order to figure out an index of robustness. One may propose a robustness index, I_{robust}, such as:

$$I_{robust} = \frac{\Delta_1}{\Delta_1 + \Delta_2}$$

But, it may also be expressed in a different form, such as:

$$I_{robust} = \frac{\Delta_1 + \Delta_2}{(\Delta_1 + \Delta_2) + (\Delta_3 + \Delta_4 + \Delta_5)}$$

3.3. Is that Dynamic Modelling?

This resilience and robustness indices may significantly provide useful measures of the CI's qualities to resist and recover. However, they are still static measures.

4. Resilience Dynamic Modelling

Regarding the development of a dynamic probabilistic model of resilience, the authors have previously proposed some basic ideas in [7]. The backbone of this tentative conceptual model was based on the use of time as a metric to measure the resilience.

This proposed resilience dynamic model distinguishes three phases when a given CI is exposed to a well-defined threat. The model is schematically presented in *Figure 2* with the help of a graph of states. It is fully inspired from the descriptive static model that has been present above.

The states graph contains four states: three service-supply states (availability) and one absorbing state (disruption). These states are described as follows:

State 1: the CI is in its perfect operating state and supplies the expected service at its nominal strength in spite of the threat action. During this phase, the CI may fail to supply the required service and its failure rate is equal to λ_{01}. This is represented by a transition from the 1st service-supply state to the absorbing state.

State 2: the CI is affected and no repair actions have undertaken or no significant repair is carried on, yet. During this phase, the CI may fail to supply the required service and its failure rate is equal to λ_{02}. This is represented by a transition from the 2nd service-supply state to the absorbing state.

Phase 3: the CI is under repair action and provides the expected service at lower strength. During this phase, the CI may fail to supply the required service and its failure rate is equal to. λ_{02}. This is represented by a transition from the 3rd state to the absorbing state.

Transitions between the operating states are governed by the transition rates τ_{ij}. The transitions from the operating states to the "loss of service supply" one (service disruption state) are governed by the transition rates λ_{0i}, ($i, j \in [1,2,3]$). These λ_{0i} transition rates can be called failure rates because they lead to the state of "loss of service supply".
The model can certainly be extended to more than three operating states in order to describe the operating states of the CI under the action of a threat in finer manner.
The model describes the CI behavior in probabilistic terms, i.e., one determines sojourn and transition probabilities. The dynamic of the CI under the action of a threat is perfectly described by these probabilities in [7].

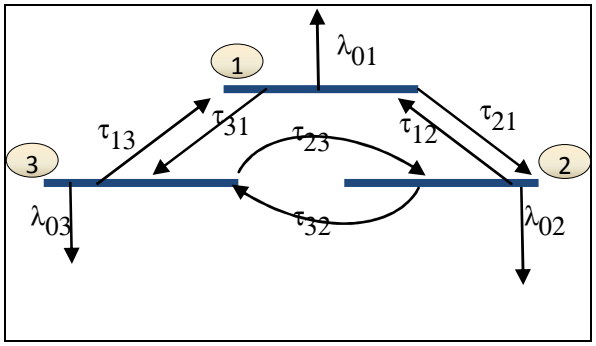

Figure 2. Schematic presentation of the operational phases of a CI under the actions of a threat

The transitions are fully described by a system of differential equations that can analytically be solved if all the transition rates are time independent, using Markov stochastic approach. If not, the system can be approximated using a semi-Markov stochastic approach. It can also be solved without any approximation using Monte-Carlo simulation techniques.
This system of differential equations is described as following:

$$\frac{d}{dt} p_i(t) = \sum_{j=1}^{3} \tau_{ij} p_j(t),$$

$$\frac{d}{dt} q_i(t) = +\lambda_{0i} p_i, \quad i = 1,2,3$$

and

$$\tau_{ii} = -\left(\lambda_{0i} + \sum_{\substack{j=1 \\ j \neq i}}^{3} \tau_{ji} \right),$$

where $p_i(t)$ $(i = 1,2,3)$ are the probabilities to be in one of the operating states and $q_i(t)$ $(i = 1,2,3)$ are the probabilities to be in one of the absorbing states (failure states) and τ_{ij} is the transition rate from state j to i ($\tau_{i \leftarrow j}$).
Solving this system of differential equations will directly result in the different sojourn and transition probabilities corresponding to each operating state.
If the transition rates are supposed to be constant, the solution of this system of differential equations can be written as:

$$p_i(t) = \sum_{l=1}^{n} c_{il} e^{-\omega_l t},$$

$$q_i(t) = \lambda_{0i} \sum_{l=1}^{3} \frac{c_{il}}{\omega_l} (1 - e^{-\omega_l t})$$

Where ω_l and c_{il} are the characteristic parameters that are fully determined [7].
In *Figure 3* and *Figure 4*, we present the time profile of both; the sojourn probabilities and the failures probabilities corresponding to the test-case treated in [7].
The transitory behavior of the CI depends on the initial values of the sojourn probabilities. But the asymptotic behavior is always characterized by time-increasing failure probabilities and time-decreasing sojourn probabilities.

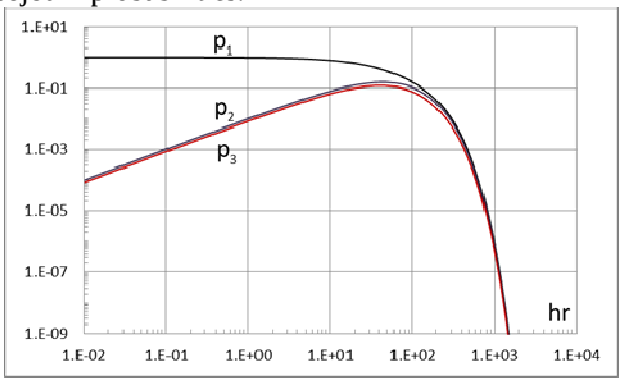

Figure 3. Time profile of the sojourn probabilities

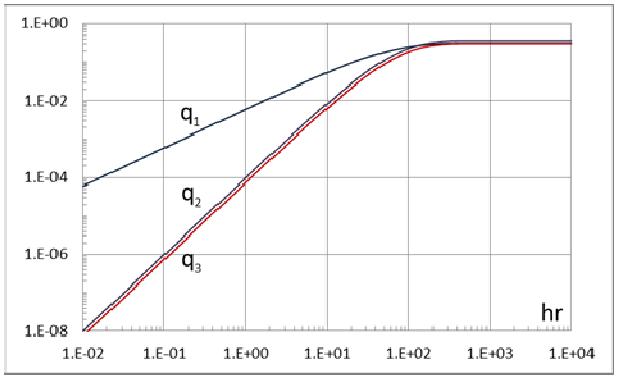

Figure 4. Time profile of the failure probabilities (Loss of Service Probability)

The transition rates τ_{ij} are supposed to be independent, in this model. Accordingly, the proposed model does not allow considering the existing interdependencies between CIs facing many independent given threats. Subsequently, it can describe the robustness-resilience for systems of higher orders (systems of systems) generally characterized by strong dependency and interdependency between there elementary CIs [3].

5. Threat Dynamic Modelling

Similarly, threats dynamic should be modelled 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,
- 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 is proposed in the following.
Generally, both τ_a and τ_{off} can obey to any form of stochastic processes. If τ_a and τ_{off} are supposed constant with time, one can 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}).

Once a given threat is modelled as a cycle of alternating activation/deactivation periods that 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 [6], 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:

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

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 1*. One will be interested in two cases for $k = 1$ and 2, see *Table 2*.

Table 1. definitions of *B*and *C* coefficients

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

Table 2. The PDFs for $k = 1, 2$

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

6. Threat's Dynamic Classification

Now, we have 2 independent dynamic models: one describes the occurrence of the CI under the action of the threat (loss of service) and another describes the threat's occurrence. But they are not coupled.
As we have already mentioned above, a full dynamic description of the resilience requires the development of coupled-dynamic models CI-Threat. In order to approach our main target, let's first distinguish two categories of threats with respect to the CI response functions.

6.1. 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 threat, 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 threat, 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.

6.2. Threat with short cycle

A threat 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:

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

A very low I_{robust} 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:

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

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

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

with the condition;

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

The PDF $P_n(\sum_{i}^{5}\Delta_i)$ can be determined using (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 threat, 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 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 less than some acceptable limit. In that case the protection of the CI will depend on its resilience.
Figure 2 shows the equiprobable surfaces of the first occurrence of a given threat as a function of both: αT and βT, where T represents any interval of interest. Four categories of robust-resilient CI could be identified regarding a given threat, such as:

Cat-A) The threat is characterized by a short period of action and a long off-period (low occurrence frequency), compared to given *T*. 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 should be robust enough if the threat occurrence probability is low enough.

Cat-B) The threat is characterized by a long period of action and a long period off (low occurrence frequency), compared to *T*. 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.

Cat-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.

Cat-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 is worth to underline the fact that a well-determined occurrence probability within a given *T* of interest could be attended at different combinations of activation- and off-periods (β^{-1}, α^{-1}).

In *Figure 2*, we demonstrate the case for $P_1(\sigma T)$, the probability of only one occurrence within *T*.

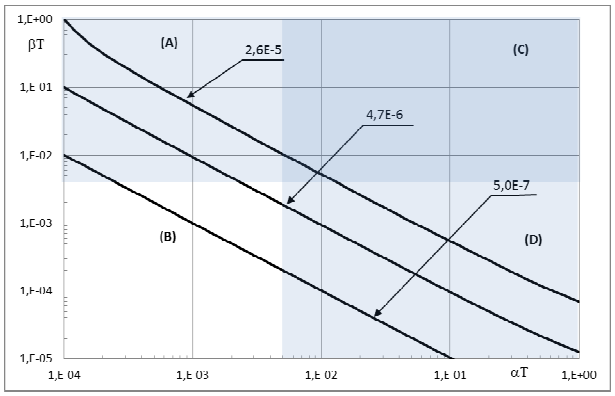

Figure 2. Equi-probable surfaces representing $P_1(\sigma T)$ at 3-values; 2.6E-5, 4.7E-6, 5.0E-7

The same can be illustrated for occurrence probability distribution functions of higher orders.
In *Table 4* [6], the probability $P_2(\sigma T)$ - the occurrence of two successive cycles of the threat within T - is determined for threats that occurs once within T at the fixed probability $P_1 = 4.7E-06$. That is to show the following:

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

7. Resilience Measure

But still - after this tentative effort above to couple resilience (with robustness) to threats – the model is not dynamic yet. It is still a static model using some indicators averaged on time intervals. These indicators are easily calculable and significant. But they need to be completed if we require a real dynamic coupled model of resilience-threat.
A real coupled dynamic model "resilience-threat" would be possible if we can correlate the transition rates τ_{ij}, (§4), and threat's characteristic parameters (α, β), (§5). This required coupling can be through either some advanced model – still to be developed – or data issued from operating experience feedback. It could also be through both paths.
If τ_{ij} can be described as a function of (α, β) [7] proposes to use some measures such as: the mean time before disruption, the meantime to sojourn in any of the operating states, the meantime to recuperate (back to the perfect state), the time-dependent overall failure rate of the CI, the probability to be in any of the availability states,… etc.
Two of these measures seems the more significant and easily usable to describe the CI resilience:

- The probability to be in any of the availability states, $\sum_{i=1}^{3} p_i(t)$, or the probability to be in any of the failure state, $\sum_{i=1}^{3} q_i(t)$.
- The time before failure (loss of service supply), $\overline{T}$.

The determination of $p_i(t)$ and $q_i(t)$ is already described above.
Regarding the "time before failure, $\overline{T}$", it is determined by:

$$\overline{T} = \sum_{i=1}^{3} \int_{\xi=0}^{\infty} \int_{\eta=\xi}^{\infty} \eta . dp_i(\xi) . e^{-\tau_i(\eta-\xi)} . e^{-\lambda_i \eta} . \lambda_i d\eta$$

$$\overline{T} = \sum_{i=1}^{3} \frac{\lambda_i}{(\lambda_i+\tau_i)^2} \sum_{j=1}^{3} \tau_{ij} \sum_{l=1}^{3} \frac{c_{jl}}{(\lambda_i+\omega_l)} \left(\frac{(\lambda_i+\tau_i)}{(\lambda_i+\omega_l)} + 1 \right)$$

8. Conclusions

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

A model is proposed associating "resilience" and "threat". The model tentatively proposes to distinguish between "robustness" and "resilience", distinguishing between two operating phases in CI life-cycle: loss of service and recuperation of service. In that model the CI behavior is probabilistically described during and after the threat occurrence and schematically presented in *Figure 1*. In parallel the threat occurrence is described in probabilistic terms as well, given the number of the threat occurs-cycles, k, within an interval of interest T.

The proposed model does not allow yet describing the robustness-resilience for systems of higher orders (systems of systems) and considering the existing interdependencies between CIs facing many independent given threats.

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, December 2011. (www.css.ethz.ch)

[2] Argonne National Lab. (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*. D/418/12101/3, 2009, © Adelard LLP.

[4] COM (2006), 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). COM (2006) 787 final. Brussels, 12.12.2006.

[5] 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.

[6] Eid, M., et. al. (2014). Critical Infrastructures Protection (CIP) – Contribution to EU Research on Resilience & Preparedness. *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars*, 5, 1.

[7] Eid, M., et. al. (2015). A resilience model based on Stochastic Poison Process. To be published in the Journal of Polish Safety and Reliability Association, 48th ESReDA seminar, 2015.

[8] HSA (2002). Homeland Security Act of 2002. PUBLIC LAW 107–296—November 25, 116 STAT. 2135.

[9] HSPD-7 (2003). Homeland Security Presidential Directive-7. December 17.

[10] Moteff, J. (2004). Critical Infrastructure and Key Assets: Definition and Identification. October 1, 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. July 16, 30