Mohamed Eid,
CEA DANS/DM2S/SERMA, Saclay Bât.470, 91191 Gif sur Yvette Cedex, France

Dominique Serafin

Yohan Barbarin
CEA Gramat, BP 80200, 46500 Gramat, France

Krzysztof Kołowrocki

Ewa Kuligowska

Joanna Soszyńska-Budny
Gdynia Maritime University, Gdynia, Poland

A resilience model based on Stochastic Poison Process

Keywords

critical infrastructure, resilience, protection, modelling, simulation

Abstract

Critical Infrastructure (CI) Preparedness and Resilience modelling, simulation & analysis (MS&A) is a major issue in CI protection (CIP) and crisis management. This is due to the rapid growth of the inference of the smart complex systems in the modern society activities. The concept of resilience in CIP is not yet clearly defined. However, "resilience" is often used as a measure of the system good behaviour facing a given threat. Under a given threat, a CI may evolve within a set of well-defined operating phases. Subsequently, the failure of the CI to provide the expected service will depend not only on the threat nature but also on the operating phase.
A tentative probabilistic model is proposed describing the robustness and the resilience of a well-defined infrastructure facing a given threat.

1. Introduction

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, [7], risk management has followed a significant mutation. Some existing taxonomies evolved and has been extended to a wider range of concepts, such as: resilience, robustness, complex environment, cascading effect, complex system and system of systems.
Amongst these concepts, resilience is receiving a specific interest and a wider use. Some researchers promote even the "promulgation of Critical Infrastructure Resilience (CIR) as the top-level strategic objective in order to drive national policy and planning", [1] . The Risk and Resilience Research Group, [1], identifies 3 competing perspectives in resilience & risk-management.
These 3 competing perspectives are: resilience as a goal of risk management, comprehensive risk-resilience management, and (even) resilience as alternative to risk management. Notably, there is a strong and an invariant relation between: risk management, CI, and resilience.
Risk management concept is well-defined, normalised and with proved practices in almost all engineering fields.
Regarding the CIs, they are generally defined such as: "infrastructures whose disruption or destruction would have significant impacts on the whole society. This may result from interdependencies between interconnected infrastructures". On the national levels, most of the nations have defined their own lists of CI. The EU defines even the European CI in a specific EU-Directive, [4].

However, "resilience" concept is still to be developed for the use in the CIP field. In this paper, a conceptual model is proposed, in this paper, and covering a formal description of the resilience and a definition of its possible metrics.

2. Resilience: Notion & Metric

Unfortunately, unlike risk management and CI, resilience is still neither a specific, easily definable term across all CIP field nor is easily measurable. Simply, the concept of "resilience" is still ambiguous in engineering fields.

Most of the stakeholders agree on the preceding remark. Instead, consensus regarding how resilience should be defined, measured and assessed, has not still emerged [3], [8].

What could resilience be and how to be measured?

Argonne proposes the following definition: "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].

We underline that "resilience" evokes very often notions such as: ability, resistance, adaptability and rapid recovery. It evokes very less often notions such as: anticipation, (active) response (to a threat) or mitigation (of the resultant hazard). "Resilience" is widely used in other fields such as: sociology, biology, ecology and psychology. If one considers these uses as well as the use in engineering, one get the conviction that "resilience is the capacity of survival …" is the minimum common definition between different scientific disciplines.

Thinking the "resilience" and tending to develop metrics to measure it is a big challenge.

The European Network & Information Security Agency (ENSIA) gives high interest to the "resilience" issue. ENISA's program on Networks and Services Resilience and Critical Information Infrastructures Protection (CIIP) has been developed to face that challenge. The goal was to collect information on existing practices and metrics with key experts and stakeholders and to perform a qualitative analysis of the input received. The ENISA's report, [6], identifies the challenges corresponding to the concept of resilience and to its metrics as following:

- The lack of a standardised framework, even for the most basic resilience measurements. There are not that many frameworks available and none of them are globally accepted
- No standard practices were identified within the different organisations for the baseline resilience metrics. Different organisations all use their own specific approaches and means of measuring resilience, if they measure at all. This impedes the usage of those metrics for overall assessment of resilience, or the aggregation and composition towards higher levels (such as a national or a pan-European assessment of resilience)
- Lack of knowledge and awareness of resilience metrics. This results in severe difficulties for organisations when deploying resilience metrics

From the system stand point there is difference between disruptions induced by deliberate actions, or natural threats or systemic failures. In this paper, the authors will use the generic term threat.

Regarding the metric to be used in measuring the resilience, one should first specify which CI's property to be measured?

ENISA report, [6], underlines that "the usefulness and value of metrics is challenged when complexity increases". It draws our intention to the fact that "in cases where relevant measurement data is difficult to collect, or when its analysis becomes too complex and subject to interpretation, the usefulness of resilience or security metrics was severely challenged. Focus on the key issues in resilience measurement is seen as important and there is also a clear need for tools and solutions to rationalise the measurement data overload".

We draw, then, the following guidelines regarding the usefulness and the value of the metric to be developed:

- The searched metric should require data easily collectable (elementary data).
- These data should not require complex analyses and treatments and should not be subject to complex interpretation processes.
- The metric and the required data should be subject to common standardisation, normalisation and collective collection effort.

In this paper, we would like to contribute to the development of useful and valuable answers to the two first challenges: the formal description of resilience and the used metric. Our proposed contribution is based on our past experience in system reliability, availability, maintenance and safety - (RAMS) - analyses and risk management. Our proposal is driven by the requirement to use, when possible, existing proved models and data in order to define and measure the system resilience.

From past experiences in RAMS and risk management, a system is fully defined by its functionalities and missions. In case of CI, these functionalities are often called "services" and the mission of the CI is to supply a well-defined service over a given interval of time. The "service supply"

capability can then be measured using many of CI's intrinsic properties.

Two properties can be measured: the "duration before disruption-DBD" under a given threat or the "duration of a disruption" resultant from a given threat. In one case or in the other, the used metric is the time. One may also be interested in measuring both, or in measuring a third composite property to be clearly defined.

The 1st property, the "duration before disruption" is related to the "robustness" of the CI, while the second to the "recovery" capacity. Robustness and recovery are the two basic elements of the resilience. The authors believe that any useful and valuable resilience model should be able to distinguish between these basic elementary properties of the CI: robustness and recovery capacity.

Another possible metric can be of a probabilistic nature. It can be the "availability", of the service(s) supplied by the CI, i.e., the probability that a given functionality is available at its nominal level, at instant " ". It can also be the complementary property, i.e., the unavailability of the supplied service.

Qualitative Model

The ideal resilience model should allow us measuring both: time (robustness and recovery) and availability/unavailability of the service supply (likelihood).

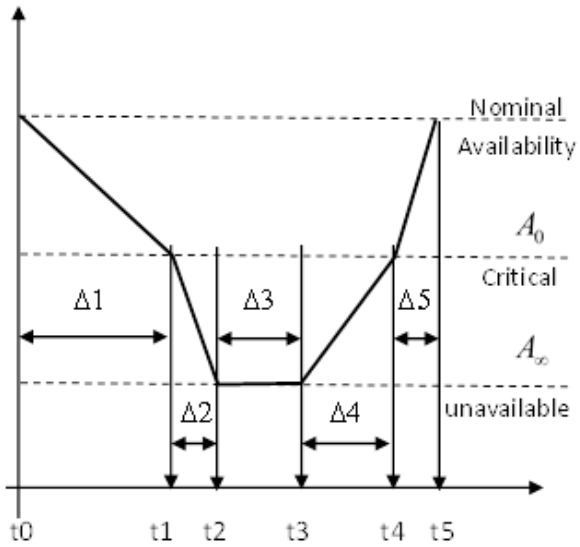

Figure 1. Schematic representation of the CI behavior during and after the threat occurrence

Schematically, one may imagine that the CI behaves as shown in *Figure 1* under a given threat active phase, where:

Δ_1 ($\Delta_1 = t_1 - t_0$): is the interval of time during which the CI continues providing its normal service and shows no irreversible degradation in spite of the action of the threat. This is the phase of the elastic degradation in service-supply. 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 ($\Delta_2 = t_2 - t_1$): is the interval of time during which the system shows irreversible degradations. This is the phase of the plastic degradation in service-supply. 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 ($\Delta_3 = t_3 - t_2$): 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 ($\Delta_4 = t_4 - t_3$): 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 ($\Delta_5 = t_5 - t_4$): 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).

The details of this qualitative model are given in (ENISA, 2010).

As we can see from the schematic description above, one can distinguish 3 intrinsic properties of the CI: robustness (phases 1-2), maintainability (phase 3) and recovery capacity (phases 4-5). If appropriate failure data are available, each of these five service-supply phases can be even subdivided in to finer sub-phases.

Quantitative model

A resilience model is developed to be used in assessing the resistance (robustness) and the recovery capacity of a given CI under the hazardous actions of a well-defined threat, [5]. The CI resilience can't but be dependent on the threat as well as on the intrinsic properties of the CI. A resilience measure which depends on time seems to be the most appropriate one. The principal difficulty comes from the lack of formal models which may describe the behaviour of a given CI under the actions of a threat. We are looking for a functional model that may consider: the perfect service-supply phase of the CI, the degraded phase when repair is not yet active and finally the degrading phase but the repair actions are effective and the CI is healing. The CI may transit from one service-supply phase to another, following some given stochastic patterns that are in principal functions of the threat-CI interacting failure mechanisms.

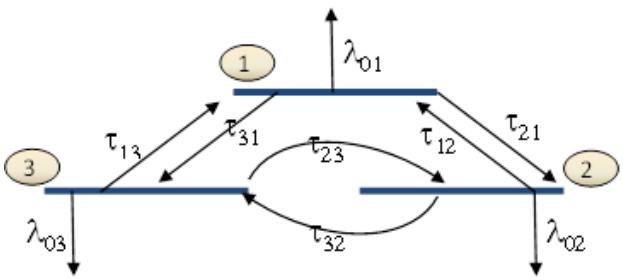

Figure 2. Schematic presentation of the operational phases of a CI under the actions of a threat

The proposed resilience model distinguishes three phases (macro-) when a given CI is exposed to a well-defined threat. These three service-supply phases are described as following, *Figure 2*:

1. Phase 1: the CI is in its perfect operating state and provides the expected vital service at its nominal strength in spite of the threat action. During this phase, the CI may fail to provide 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 an absorbing state "0".

2. Phase 2: the CI is touched and no repair actions have undertaken or no significant repair effect is significant, yet. The CI provides the expected vital service at a decreasing strength with time. During this phase, the CI may fail to provide 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 an absorbing state "0".

3. Phase 3: the CI is under repair action and provides the expected vital service at its lowest strength. During this phase, the CI may fail to provide the required service and its failure rate is equal to. λ_{03}. This is represented by a transition from the 3rd state to an absorbing state "0".

The model is schematically presented in *Figure 2* with the help of a graph of states. Generally speaking, transitions between states may follow any possible stochastic pattern. In this paper, the transitions are supposed to be described by Stochastic Poisson Processes (SPP). The graph of states can then be called Markov's graph. The graph is composed of 3 operating states with different degradation degrees. Transitions between states are governed by the transition rates τ_{ij} and the transitions from the operating states to the absorbing one (service disruption state) are governed by the transition rates λ_{0i}, ($i, j \in [1,2,3]$). The behaviour of the CI under the given threat is fully described by, [5]:

$$\frac{d}{dt} p_i(t) = \sum_{j=1}^{3} \tau_{ij} p_j(t), \qquad \tau_{ii} = -\left(\lambda_{0i} + \sum_{\substack{j=1 \\ j \neq i}}^{3} \tau_{ji} \right), \quad i = 1,2,3 \tag{1}$$

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

$$\sum_{i=1}^{3} p_i(t) + \sum_{i=1}^{3} q_i(t) = 1, \qquad \forall t \in [0, \infty[\tag{3}$$

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 ($\tau_{i \leftarrow j}$).

The differential equations system given in Equations (1)-(3) is general and independent on the considered stochastic pattern.

In the case of Stochastic Poisson Process, this differential equations system shows an analytical solution. In that case, the solution of the differential equations system described above may be expressed by the following, [5]:

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

$$p_i^0 = \sum_{l=1}^{n} c_{il} \text{,} \tag{4}$$

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

$$q_i^0 = 0., \tag{5}$$

p_i^0 and q_i^0 are the initial values.

The exponents ω_i are the solution (3 roots) of the following expression:
And the coefficients c_{il} are determined by:

$$\begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix}^T = \begin{pmatrix} 1 & 1 & 1 \\ -\omega_1 & -\omega_2 & -\omega_3 \\ \omega_1^2 & \omega_2^2 & \omega_3^2 \end{pmatrix}^{-1} * \begin{pmatrix} \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} p_1^0 \\ p_2^0 \\ p_3^0 \end{pmatrix} \right)^T \\ \left(\begin{pmatrix} \tau_{11} & \tau_{12} & \tau_{13} \\ \tau_{21} & \tau_{22} & \tau_{23} \\ \tau_{31} & \tau_{32} & \tau_{33} \end{pmatrix} \begin{pmatrix} p_1^0 \\ p_2^0 \\ p_3^0 \end{pmatrix} \right)^T \\ \left(\begin{pmatrix} \tau_{11} & \tau_{12} & \tau_{13} \\ \tau_{21} & \tau_{22} & \tau_{23} \\ \tau_{31} & \tau_{32} & \tau_{33} \end{pmatrix} \begin{pmatrix} \tau_{11} & \tau_{12} & \tau_{13} \\ \tau_{21} & \tau_{22} & \tau_{23} \\ \tau_{31} & \tau_{32} & \tau_{33} \end{pmatrix} \begin{pmatrix} p_1^0 \\ p_2^0 \\ p_3^0 \end{pmatrix} \right)^T \end{pmatrix} \tag{7}$$

<u>Resilience measure</u>
As mentioned above, two measures will be used to describe the CI resilience:

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

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:

$$\overline{T} = \sum_{i=1}^{3} \int_{\xi=0}^{\infty} \int_{\eta=\xi}^{\infty} \eta . dp_i(\xi) . e^{-\tau_i(\eta-\xi)} . e^{-\lambda_i \eta} . \lambda_i d\eta \tag{8}$$

Whose solution will be given by:

$$\overline{T} = \sum_{i=1}^{3} \frac{\lambda_i}{(\lambda_i + \tau_i)^2} \sum_{j=1}^{3} \tau_{ij} \sum_{l=1}^{3} \frac{c_{jl}}{(\lambda_i + \omega_l)} \left(\frac{(\lambda_i + \tau_i)}{(\lambda_i + \omega_l)} + 1 \right) \tag{9}$$

3. Numerical application

The case presented here is characterized by the following operational state transition probabilities matrix, $H_{k \to l}(t)$:

$$H_{k \to l}(t) = \begin{bmatrix} 0 & 1 - e^{-\frac{t}{100}} & 1 - e^{-\frac{t}{120}} \\ 1 - e^{-\frac{t}{150}} & 0 & 1 - e^{-\frac{t}{150}} \\ 1 - e^{-\frac{t}{100}} & 1 - e^{-\frac{t}{270}} & 0 \end{bmatrix} \tag{10}$$

The failure rates corresponding to the operational phases, are the following:

$$\lambda_{01} = 0.006 h^{-1}, \qquad \lambda_{02} = 0.015 h^{-1},$$
$$\lambda_{03} = 0.024 h^{-1}$$

That reflects the fact that the CI vulnerability is proportional to its degradation level (higher failure rate at higher degradation).
The robustness of the CI is determined by:

$$\tau_{1 \to 2} = \frac{1}{100}, \ \tau_{1 \to 3} = \frac{1}{120}, \ \tau_{2 \to 3} = \frac{1}{150},$$
$$\lambda_{01}, \ \lambda_{02}, \ \lambda_{03}$$

and by their relative values.

While, the recuperation is determined by:

$$\tau_{2 \to 1} = \frac{1}{150}, \ \tau_{3 \to 1} = \frac{1}{100}, \ \tau_{3 \to 2} = \frac{1}{270}$$

and by their relative values.

<u>Determining the exponents</u>
Considering transition data given above, the exponents ω_l (3 roots) are:

$$\omega_1 = 0.0133, \ \omega_2 = 0.0353 \text{ and } \omega_3 = 0.0418.$$

Determining the coefficients

The final step is to determine the coefficients c_{il}. That requires fixing the values of the initial probabilities [p_1^0, p_2^0, p_3^0], see equation(7).

If the initial probabilities are [1,0,0], respectively, then we will have the following coefficient values:

$$\begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} = \begin{pmatrix} 5.46E-01 & 2.93E-01 & 1.61E-01 \\ 4.40E-01 & -3.88E-01 & -5.22E-02 \\ 3.07E-01 & -6.16E-02 & -2.46E-01 \end{pmatrix}$$

Failure probabilities

Finally, we can then express the failure probabilities $q_i(t)$ as following:

$$q_1(t) = \frac{0{,}546}{0{,}0133}(1-e^{-0{,}0133t}) + \frac{0{,}293}{0{,}0353}(1-e^{-0{,}0353t}) + \frac{0{,}161}{0{,}0418}(1-e^{-0{,}0418t})$$

$$q_2(t) = \frac{0{,}440}{0{,}0133}(1-e^{-0{,}0133t}) - \frac{0{,}388}{0{,}0353}(1-e^{-0{,}0353t}) - \frac{0{,}0522}{0{,}0418}(1-e^{-0{,}0418t})$$

$$q_3(t) = \frac{0{,}307}{0{,}0133}(1-e^{-0{,}0133t}) - \frac{0{,}0616}{0{,}0353}(1-e^{-0{,}0353t}) - \frac{0{,}0246}{0{,}0418}(1-e^{-0{,}0418t})$$

As we may expect, the failure probabilities, $q_i(t)$, have asymptotic values and they are equal to: 0.32, 0.31 and 0.37, respectively.
The time profile of the failure probabilities are shown in *Figure 4.*

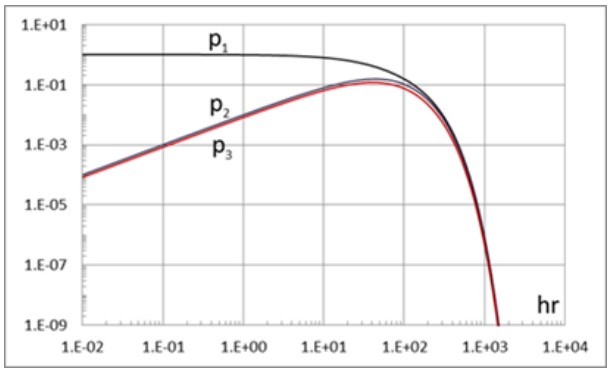

Figure 3. Time profile of the sojourn probabilities

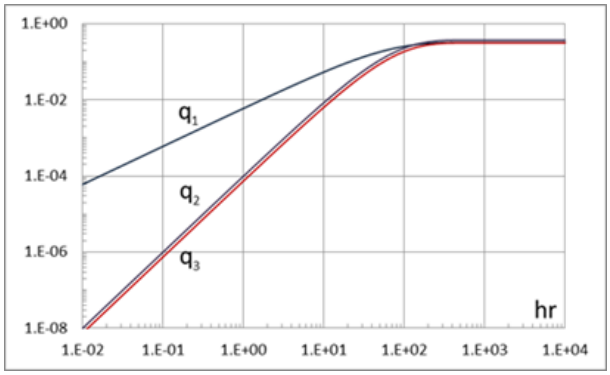

Figure 4. Time profile of the failure probabilities (Loss of Service Probability)

Mean time before failure

Regarding this case and considering its initial conditions, the MTBF was determined using Equation 9. The MTBF is equal to 33.7 hours. This overall value is distributed in that manner:

- 28 hours in the 1st operational phase
- 4.3 hours in the 2nd operational phase
- 1.4 hours in the 3rd operational phase

3. Conclusions

A model is proposed in the paper to describe, when appropriate, the resilience of a given CI under the action of a well-defined threat.
Qualitatively, five service-supply phases can be identified when a given CI is subject to the actions of a well-defined threat, *Figure 1*, such as: service-supply with no degradation, service-supply in degrading modes, out of service, back to service in degrading modes and in-service.
It is worth underlying that "service-supply in degrading modes" and "back to service in degrading modes" may include many distinguished service-supply phases.
In practices, the exact number of degrading operation phases to be considered will be restricted to the availability of the corresponding failure data. The availability of the appropriate data is a serious challenge in CIP.
From a conceptual point of view, these five service-supply phases allow us to distinguish between the two basic properties of the "resilience": the robustness and the recovery. The 1st corresponds to intrinsic resistance of the CI to threats' aggression and the 2nd refers to recovery of the CI in presence of the repair and other possible threat counteractions.

In the model presented in this paper, the number of operating phases was reduced to only three which is the minimal required number to distinguish between: full service supply phase, degrading supply without repair actions (robustness) and degrading supply with repair in action (recovery).
The extension to a five phase or more is straight forward if corresponding failure data are available.

Acknowledgements

This work is a collaborative effort between the EU project PREDICT [SEC-2013.4.1-2, grant agreement 607697] and the Department of Mathematics, Gdynia Maritime University, Poland. It is an explorative effort on the resilience issue in CIP engineering field.

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 (2012). Resilience: Theory and Application". ANL/DIS-12-1, *Argonne National Lab., Decision and Information Division*, January 2012.

[3] Bloomflield (2009). Infrastructure interdependency analysis: Requirements, capabilities and strategy. D/418/12101/3, 2009 , © Adelard LLP.

[4] 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.

[5] 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*, Volume 5, Number 1, 2014, ISSN: 2084-5316.

[6] ENISA (2010). Measurement Frameworks and Metrics for Resilient Networks and Services: Challenges and Recommendations © European Network and Information Security Agency (ENISA), 2010. http://www.enisa.europa.eu/act/res

[7] HAS (2002). Homeland Security Act of 2002. PUBLIC LAW 107–296—NOV. 25, 2002, 116 STAT. 2135.

[8] Moteff, (2004). Critical Infrastructure and Key Assets: Definition and Identification." October 1, 2004, CRS Report for Congress, Order Code RL32631. https://www.fas.org/sgp/crs/RL32631.pdf