RESILIENCE ANALYSIS OF INTERCONNECTED SYSTEMS BY A SET-THEORETIC APPROACH

Xing Liu, Ionela Prodan, Enrico Zio

ANALYSE DE RÉSILIENCE DES SYSTÈMES INTERCONNECTÉS PAR UNE MÉTHODE DE LA THÉORIE DES EMSEMBLES

RESILIENCE ANALYSIS OF INTERCONNECTED SYSTEMS BY A SET-THEORETIC APPROACH

LIU X. and Prodan I.
Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy - Electricité de France, at École Centrale Paris - Supélec, France
Xing.liu@ecp.fr
Ionela.Prodan@ecp.fr

Zio E.
Chair on Systems Science and the Energetic Challenge, European Foundation for New Energy - Electricité de France, at École Centrale Paris - Supélec, France
enrico.zio@ecp.fr, enrico.zio@supelec.fr

Department of Energy, Politecnico di Milano, Italy

enrico.zio@polimi.it

Résumé

Cet article traite de l'analyse de la résilience des systèmes d'infrastructures critiques. Un système d'infrastructure est un réseau de sous-systèmes, qui interagissent par les dépendances de divers types. L'interaction et la dépendance entre les sous-systèmes rendent le système d'infrastructure entier plus complexe et parfois vulnérable. Nous interprétons la résilience comme une propriété de système liés à la prévention, la robustesse et le rétablissement des perturbations et des événements indésirables. Une telle propriété de résistance des systèmes interconnectés dépend également de leur structure et de leurs paramètres de conception. Dans cet article, nous modélisons la structure du système par un graphe orienté. Une dynamique de l'état est associée à chacun des sous-systèmes, avec des termes interdépendants qui peuvent représenter différents types d'interdépendances. La réponse du système aux perturbations et aux événements indésirables peut, alors, être analysée en utilisant des notions de la théorie des ensembles, pour identifier les régions de fonctionnement et les conditions récupérables ou non récupérables. En outre, une caractéristique de la résilience du système en fonction des paramètres de conception est fournie, ce qui est utile pour la conception et le fonctionnement des systèmes résilients. Les avantages de l'approche proposée sont mis en évidence par une application numérique illustrative. Finalement, les différentes topologies des systèmes sont également prises en compte pour discuter de leurs effets au système.

Abstract

This work addresses the resilience analysis of critical infrastructure systems. An infrastructure system is a network of subsystems, which interoperate through dependencies of various types. The interaction and dependency among the subsystems make the entire infrastructure system more complex and possibly vulnerable. Resilience is interpreted here as a system property related to the prevention of, robustness to and recovery from undesired disturbances and events. Such resilience property of interconnected systems depends also on their structure and design parameters. In this paper, the structure of the system is abstracted by a directed graph. A state dynamics is associated to each of the subsystems, with interdependent terms that can represent different types of interdependencies. The system response to undesired disturbances and events can, then, be analyzed using notions from set theory, to identify regions of operation and recoverable or non-recoverable conditions. Moreover, a characterization of the system resilience as a function of the design parameters can be provided, which is useful for resilient design and operation purposes. The benefits of the proposed approach are highlighted through an illustrative, numerical application. Finally, discussions on how the system's topology will influence its resilience are presented.

Introduction

Critical infrastructure systems like electric power grids, telecommunication systems, transportation systems are essential assets in today's modern societies (Carlyle et al. 2006, O'Rourke 2007, Murray & Grubesic 2007). The modern infrastructure systems can have a very complex structure and be composed of different subsystems with specific functionalities.

The interdependencies and the interactions among the subsystems are the force and the weakness of the critical infrastructures. This is because these critical infrastructures are exposed to hazardous natural and artificial incidents, such as earthquakes, hurricanes, random failures and sabotages etc., therefore, a disruption to one of the subsystems can have dire consequences across others, then global system will lose its functionality and becomes unstable.

Such a critical infrastructure has to be resilient, in the sense that it has to provide services under disturbances and be capable to recover to nominal functioning after fault occurrences. In the present paper we interpret resilience as a system property related to the prevention of, robustness to and recovery from undesired disturbances and events.

The modeling of failure propagation dynamics to analyze the resilience of critical infrastructures represents a challenging task (Buldyrev et al. 2010, Dobson 2008, Pederson et al. 2006). Several scientific and technical concentrate their attention to achieve

this goal using different approaches. Some of them are related to Markov random process and probabilistic methods (Nozick et al. 2005), stochastic Petri Net modeling approach (Faraji & Kiyono 2012), a stochastic model whereby each component is modeled as a random process with a probability to switch between two states (Bloomfield et al. 2010). A System Dynamics (SD) infrastructure vulnerability assessment framework is proposed in (Tonmoy & El-Zein 2014) to simulate the dependent behaviors of the infrastructure subsystems, and a measure of system performance is provided. Next, (Svendsen & Wolthusen 2007) provide an extensible graph-theoretical model for investigating the interdependencies among critical infrastructures. The interactions between their components are modeled through a set of response functions on the graph edges and resources on the nodes.

Furthermore, (Filippini & Zio 2013, Angelo & Filippini 2013) represent the infrastructure systems in a directed graph and a state dynamics is associated to each subsystem for describing the failure and recovery processes and their interdependent effects. A first attempt of resilience analysis is proposed based on invariance concepts and asymptotic stability. However, a thorough characterization of the resilience and a metric of the system resilience are not provided.

In the present paper, we consider a similar approach as in (Angelo & Filippini 2013). That is, we consider a topological model of the infrastructure systems described by a directed graph, with nodes and edges representing the subsystems and the dependencies between the subsystems, respectively. Next, we proceed with the modeling of the dynamics of each subsystem and the related interdependencies. More precisely, we use a state-space model with specific dynamics governed by parameters characteristic of the failure and recovery processes. The analysis of the interconnected systems dynamics is performed with the objective of identifying the resilience region for which the system state converges to the operation mode, no matter the disturbances affecting the system. Each mode of the switched system is characterized (if the mode is stable) by an invariant region. These resulting regions can be then used to describe the (un)resilient regions. Some interesting behaviors of the system are highlighted, e.g. a chattering behavior. Also, discussions on how the system's topology will influence its resilience are presented.

The rest of the paper is organized as follows. Section "System modeling and parameters" introduces the topological description of the interdependent systems, and their associated dynamic model. Section "Resilience region identification" presents the conditions on the design parameters, which ensure the existence of a resilience region. Discussions based on simulation results are presented in 'Illustrative examples' Section. Finally, the last Section draws the conclusions and presents the future work.

System modeling and parameters

1 System modeling

In the present work, directed graphs are used to describe to describe the topological model of an infrastructure system where the nodes and the edges represent the subsystems and the functional dependencies between the subsystems, respectively, as illustrated in Figure 1.

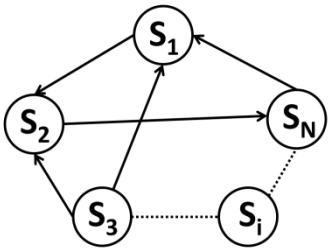

Figure 1. Interconnected system.

To analyze the interoperations and the interdependencies between the subsystems, we take into account the dynamics of the entire system. As the system has the capacities of buffering and recovery, we use a switched Linear Time-Invariant (LTI) dynamic equation to describe system behavior:

$$\dot{x}(t) = A_m x(t) + b_m \quad , \qquad \{1\}$$

where, $x(t) = [x_1^T(t), \dots, x_N^T(t)]^T$represents the state vector of the interconnected system, and matrices $A_m \in \mathrm{R}^{\mathrm{N}\times\mathrm{N}}$ and $b_m \in R^{N\times 1}$ are the characteristic matrices for m^{th} mode, where $m = 1, \dots, 2^N$ representing the dynamic modes of the entire system.

More precisely, we proceed with the modeling of the dynamics of each subsystem and the related interdependencies. For subsystem S_i, i=1,2,…,N, its state is denoted as x_i i=1,2,…,N. The dynamic model for any subsystem S_i is given by the switching dynamical equations below:

$$\dot{x}_i(t) = \begin{cases} -\mu_i(x_i(t) - \sum_{j\in I_i}\alpha_{ji}x_j(t)) + d_i, for\ x_j \le \sigma_j, \forall j \in I_i \\ \lambda_i(1 - x_i(t)), \qquad\qquad for\ x_j \ge \sigma_j, \exists j \in I_i \end{cases} \quad , \qquad \{2\}$$

where I_i is the set of input subsystems of S_i. In the proposed dynamical equations, the design parameters include: i) a threshold μ_i for the state variable, which allows to evaluate if the subsystem can provide the output required for the functioning of its connected subsystems; ii) a perturbation d_i, which affects the behavior of the system in nominal operation; iii) a buffering rate λ_i, which is decided by the threshold and the time to failure of corresponding subsystem; iv) a recovery rate μ_i, obtained from the relation between the threshold and the time to recover; v) a coupling factor α_{ji} representing the dependency between subsystems.

Equation {2} represents a switched dynamics in the sense that the value of $\dot{x}_i$ alternates between an operation and a failure mode, depending on the value taken by the current state x_i and the state x_j of all of its input subsystems S_j. Subsystem S_i is in a nominal operation state if all the states of its input subsystems are within their corresponding thresholds σ_j, as described by the first equation in {2}. Conversely, if one of its input subsystems fails, the subsystem is in an off-operation state and its dynamical behavior is described by the second equation as a failure process.

Note that for N subsystems we have a total of 2^N modes of functioning for the interconnected system, depending where each of the states x_i resides.

2 System parameters

In equation (1) we identify the following parameters:

- $\sigma_i \in [0,1]$ indicates the threshold for state variable $x_i(t)$, which allows evaluating if the subsystem S_i can provide the output required for the functioning of its connected subsystems; in other words, it represents the tolerance of system S_i for the percentage of loss of service: if $x_i(t) > \sigma_i$, then the output is insufficient.
- $d_i(t) \in [0,1]$ represents both external and internal perturbations, which affect the behavior of the system in nominal operation. It can be instantaneous and more or less strong (e.g. caused by natural disasters, such as earthquake, hurricane or a random fault) or continuous and relatively mild (such as sustained wind, electromagnetic interference, degradation etc.). In some situations, instantaneous and continuous perturbations can co-exist.
- $\alpha_{ij} \in [0,1]$ is the coupling factor representing the dependency of the subsystem S_i on the subsystem S_j. The term associated to it in the equation {1} represents the rate of the loss of service that the j^{th} subsystem contributes to the i^{th} subsystem due to the logical dependencies between them.
- $\lambda_i \in [0,1]$ represents the buffering rate for the i^{th} subsystem S_i. The time for the state x_i of S_i to reach the tolerance is the time to failure $\mathrm{TTF_i}$, introduced in the following equation:

$$\int_0^{TTF_i} \lambda_i e^{-\lambda_i t} = \sigma_i. \quad \{3\}$$

From equation {3}, we obtain:

$$\lambda_i = -\frac{log(1-\sigma_i)}{TTF_i}. \quad \{4\}$$

- $\mu_i \in [0,1]$ represents the recovery rate for subsystem S_i. The time to recovery (TTR_i) is the time that subsystem S_i takes to recover from the failed state to the threshold:

$$\int_0^{TTR_i} \mu_i e^{-\mu_i t} = 1 - \sigma_i. \quad \{5\}$$

From equation {5}, the recovery rate is obtained as:

$$\mu_i = -\frac{log(\sigma_i)}{TTR_i}. \quad \{6\}$$

The buffering rate and recovery rate are two important design parameters for the interconnected system. They can represent the capacity of resistance to/ recovery from undesired disturbances affecting the system. However, for the interconnected system, the interdependencies and interaction of the subsystems must be taken into consideration. Even though the buffering rates and recovery rates are no longer directly characterizing the resilience of the global system, they will play a significant role when the overall resilience is measured.

The dependency relationships among the subsystems represent the logics between producer and user, supplier and consumer, controller and controlled, etc. In these functional relationships, physical quantities and information are produced, consumed or/and transmitted among the subsystems to ensure their functionality. The threshold for one subsystem state is set with respect to all its downstream or output subsystems controlled by it. The value of the threshold indicates the level of tolerance for the downstream subsystems with respect to the acceptable percentage of lost input from the controlling subsystem.

The proposed model not only captures the functional relationship between the subsystems (e.g. due to physical and cyber dependencies) but also takes into account the logical dependency among the subsystems. These are originated from human decisions and actions. The coupling factor allows considering the degree of logical interdependencies in the dynamic process of system evolution.

Determination of resilience region

1 Invariance notions

Some basic invariance concepts are introduced in the following.

Definition 1 (Equilibrium point). The point $x_f \in R^n$ is an equilibrium point (or fixed point) for the differential equation,

$$\dot{x}(t) = f(x(t)).$$

If $f(x_f) = 0$.

Definition 2 (Positive invariance). (Blanchini, 1999) A set $P \subset R^n$ is said to be positively invariant for a system of the form

$$\dot{x}(t) = f(x(t)).$$

If every solution of the equation with initial condition $x(0) \in P$ verifies $x(t) \in P$ for $t > 0$.

Definition 3 (Robust positive invariance, RPI). (Blanchini, 1999) A set $P \subset R^n$ is said to be robustly positively invariant for a system of the form

$$\dot{x}(t) = f(x(t), w(t)),$$

where $w(t) \in W$ is an exogenous input. If for all $x(0) \in P$ and $w(t) \in W$, the condition $x(t) \in P$ holds for all $t \geq 0$.

2 Resilience region

The resilience region can be identified using the invariance concepts previously introduced. Moreover, the necessary conditions on the design parameters for the existence of a resilience region are provided.

In any functioning mode of the system described as in {2}, the dynamic equation of each subsystem is an affine equation. Also, note that the eigenvalues λ_A of matrix A satisfy $Re(\lambda_A) \leq 0$, according to the setting of the parameters. Hence, the system given by {1} is asymptotically stable.

Assuming that x_f is an equilibrium point for one mode of the switched system, then the following equation is verified:

$$0 = A_m \cdot x_f + b_m. \quad \{7\}$$

In this particular case, the equilibrium point for each operation mode is:

$$x_f = (I - A_m)^{-1} \cdot b_m. \quad \{8\}$$

If for a certain dynamic mode, the initial set $O \in R^N$ is a convex and compact defining by the thresholds of all the subsystems, and the equilibrium point is inside the initial set. Therefore, $O \in R^N$ is a domain of attraction and we can say that all initial states entering in set O will remain within the set at all future instances, thus O is an invariant set.

For a system with N subsystems, there are 2^N dynamic modes and the system switches from one to another depending on the states of each subsystem. The state space of the entire system is a hyper-cube $[0,1]^N$, a set divided into 3 main parts: operation region, failure-recovery region and out-of-operation region. In the operation region, all the trajectories of the systems lie in the set $O := [0, \sigma_1] \times [0, \sigma_2] \times \ldots \times [0, \sigma_N]$. The out-of-operation region is the opposite, $\bar{O} := [\sigma_1, 1] \times [\sigma_2, 1] \times \ldots \times [\sigma_N, 1]$, whereby all the states of all subsystems are of failure and the trajectories converge to an equilibrium point inside this failure region. In the proposed model, the equilibrium points may exist in the operation and out-of-operation regions.

For the operation mode, all the subsystems take the first differential equation:

$$\begin{cases} \dot{x}_1 = -\mu_1\left(x_1 - \sum_{j \in I_1} \alpha_{j1} x_j\right) + d_1 \\ \vdots \\ \dot{x}_i = -\mu_i\left(x_i - \sum_{j \in I_i} \alpha_{ji} x_j\right) + d_i \\ \vdots \\ \dot{x}_N = -\mu_N\left(x_N - \sum_{j \in I_N} \alpha_{jN} x_j\right) + d_N \end{cases}, \quad \{9\}$$

So the equilibrium point of the operation mode is

$$x_O = (I - A_O)^{-1} \cdot b_O \ , \quad \{10\}$$

where, A_O and b_O are matrices with appropriate dimensions.

If the equilibrium point is situated inside the operation region we can say that it is invariant: $x_O \in O$. Thus, one of the conditions on the design parameters for the existence of a resilience region is:

$$[0, \ldots, 0]^T \leq x_O \leq [\sigma_1, \ldots, \sigma_N]^T. \quad \{11\}$$

For all the initial states in the operation region, the trajectories of system dynamics remain inside the operation region and converge to x_O.

Similarly, the out-of-operation region has the dynamics:

$$\begin{cases} \dot{x}_1 = \lambda_1(1 - x_1) \\ \vdots \\ \dot{x}_i = \lambda_i(1 - x_i) \\ \vdots \\ \dot{x}_N = \lambda_N(1 - x_N) \end{cases}. \quad \{12\}$$

If there is an equilibrium point,

$$x_{\bar{O}} = (I - A_{\bar{O}})^{-1} \cdot b_{\bar{O}}\,, \quad \{13\}$$

it satisfies $x_{\bar{O}} \in \bar{O}$:

$$[\sigma_1, \ldots, \sigma_N]^T \leq x_{\bar{O}} \leq [1, \ldots, 1]^T. \quad \{14\}$$

Once the state of the system enters the out-of-operation mode, the system cannot recover to the operation region.

We denote the region outside the operation and out-of-operation regions as the failure-recovery region. For initial states inside this region, they may converge either to the operation region or to the out-of-operation region in a finite time. We denote by reachable regions all those regions composed by the system initial states, which converge to the operation region in a finite time. Consequently, the overall resilience region is represented by the union of the operation region and the reachable regions. In other words, the resilience region is defined as the set of all initial states of the system that eventually will reside into the operation region in finite time (i.e. it is composed by the operation region itself plus the reachable regions situated within the failure-recovery region). Figure 2 illustrates the steps for describing the resilience region.

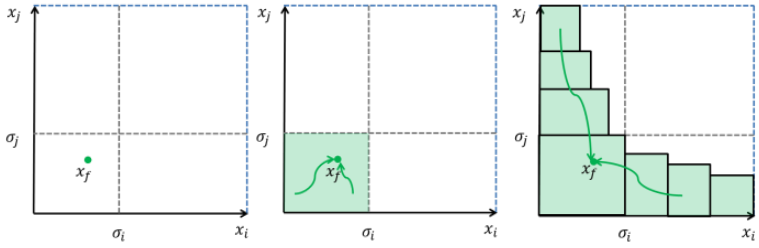

Figure 2. Steps for describing the resilience region.

Up to this point we can describe the resilience regions as they appear from the interdependencies relationships and the subsystems' characteristics. Indeed, the maximization of the system resilience region is the final design, operation and maintenance goal. We exemplify this by analyzing the response of the system as a function of its parameters, adding an element of control in the dynamics such that a supervisor can actively counteract failure modes and steer the overall system towards the operational functioning region.

Illustrative examples

1 Resilience analysis for two interconnected systems

In order to characterize the system resilience as a function of the design parameters and study the interdependencies among the subsystems and their dynamical behavior in a direct way, we consider an illustrative example of an interconnected system composed by two subsystems as in Figure 3. The interconnected system in Figure 3 could represent a power system composed of a power grid and its SCADA system, whereby the components of the SCADA system depend on the power supplied by the power supply system which, in turn, for its functioning makes use of the control and monitoring signals provided by the

telecommunication system. A theoretical analysis of system resilience is performed and the results are collected into a Table which reports the parameters values of different scenarios of system evolution.

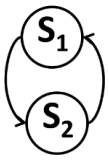

Figure 3. Interconnected system composed by two subsystems.

Consider each subsystem in Figure 3 described by the dynamic equation given in {2}. There are four operation modes for the interconnected system, in which the dynamics is represented by the following equations:
Operation mode, where $x(t) \in O \coloneqq [0, \sigma_1] \times [0, \sigma_2]$

$$\begin{cases} \dot{x}_1(t) = -\mu_1(x_1(t) - \alpha_{21}x_2(t)) + d_1 \\ \dot{x}_2(t) = -\mu_2(x_2(t) - \alpha_{12}x_1(t)) + d_2 \end{cases}, \quad \{15\}$$

Failure-recovery mode 1, where$x(t) \in R_1 \coloneqq [0, \sigma_1] \times [\sigma_2, 1]$

$$\begin{cases} \dot{x}_1(t) = \lambda_1(1 - x_1(t)) \\ \dot{x}_2(t) = -\mu_2(x_2(t) - \alpha_{12}x_1(t)) \end{cases}; \quad \{16\}$$

Failure-recovery mode 2, where $x(t) \in R_2 \coloneqq [\sigma_1, 1] \times [0, \sigma_2]$

$$\begin{cases} \dot{x}_1(t) = -\mu_1(x_1(t) - \alpha_{21}x_2(t)) \\ \dot{x}_2(t) = \lambda_2(1 - x_1(t)) \end{cases}; \quad \{17\}$$

Out-of-operation mode, where $x(t) \in \bar{O} \coloneqq [\sigma_1, 1] \times [\sigma_2, 1]$

$$\begin{cases} \dot{x}_1(t) = \lambda_1(1 - x_2(t)) \\ \dot{x}_2(t) = \lambda_2(1 - x_1(t)) \end{cases}. \quad \{18\}$$

Following the procedure described in previous section, the equilibrium states for the operation mode and the out-of-operation mode are identified:

$$x_O = [\frac{\mu_2 d_1 + \alpha_{21}\mu_1 d_2}{(1 - \alpha_{12}\alpha_{21})\mu_1\mu_2} \; \frac{\mu_1 d_2 + \alpha_{12}\mu_2 d_1}{(1 - \alpha_{12}\alpha_{21})\mu_1\mu_2}]^T$$

and $x_{\bar{O}} = [1\ 1]^T$.
If x_O is inside the operation region, there exists an invariant set and the equilibrium point locus is the location where all the states in the invariant set will converge. In this case, the invariant set is the operation region itself.
A similar result is found for the out-of operation region, which is also an invariant set with the equilibrium point (1,1) being the attractor in this region.
The conditions for the equilibrium point to be inside the operation region are the following:

$$\begin{cases} 0 \le \frac{\mu_2 d_1 + \alpha_{21}\mu_1 d_2}{(1 - \alpha_{12}\alpha_{21})\mu_1\mu_2} \le \sigma_1 \\ 0 \le \frac{\mu_1 d_2 + \alpha_{12}\mu_2 d_1}{(1 - \alpha_{12}\alpha_{21})\mu_1\mu_2} \le \sigma_2 \end{cases}. \quad \{19\}$$

In order to analyze the intrinsic characteristics of the equilibrium point, we simplify by neglecting the logical interdependencies between the subsystems, i.e., $\alpha_{12} = \alpha_{21} = 0$. In this case, the above conditions become:

$$\begin{cases} 0 \le \frac{d_1}{\mu_1} \le \sigma_1 \\ 0 \le \frac{d_2}{\mu_2} \le \sigma_2 \end{cases}. \quad \{20\}$$

Replacing relation {6} in the above equations, we obtain:

$$\begin{cases} TTR_1 \le -\frac{\log(\sigma_1)}{d_1}\sigma_1 \\ TTR_2 \le -\frac{\log(\sigma_2)}{d_2}\sigma_2 \end{cases}. \quad \{21\}$$

This allows highlighting directly the dependence of the time to recovery from the threshold and disturbance values (Figure 4).
If we fix the disturbance d, we can observe the invariance of TTR with the threshold: in the space of parameters (see Figure 3), the time to recovery reaches its maximal value when the threshold is around 0.36.
The next step is the computation of the resilience regions within the two failure-recovery regions, as described in previous section.

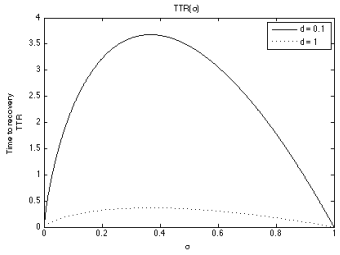

Figure 4. TTR(σ) with fixed disturbance.

Once the states x_1, x_2 enter the out-of-operation region $\bar{O}$ at a certain finite time, the system cannot recover back to the operation region O. But in the two failure-recovery regions R_1 and R_2, it is possible for the system to return to the operation region.
To find the specific resilience region, we compute a resilience curve to separate the end-to-failure and end-to-recovery parts in the failure-recovery region. The situation in R_1 is considered first, whose dynamic equations are (the coupling factors are neglected at first):

$$\begin{cases}\dot{x}_1(t) = \lambda_1(1 - x_1(t)) \\ \dot{x}_2(t) = -\mu_2 x_2(t)\end{cases}. \quad \{22\}$$

After integration, we obtain:

$$\begin{cases}x_1(t) = 1 + (x_1(0) - 1)e^{-\lambda_1 t} \\ x_2(t) = x_2(0)e^{-\mu_2 t}\end{cases}. \quad \{23\}$$

From the equations above, we observe that state x_1 tends to diverge to 1 whereas state x_2 converges exponentially to 0. Therefore, there exists a set of states $M \in R_1$ which pass the point (σ_1, σ_2) at a certain time *t*=*T*. The set *M* is represented by the following state equations, with initial conditions $x_1(0)$ and $x_2(0)$:

$$\begin{cases}x_1(T) = 1 + (x_1(0) - 1)e^{-\lambda_1 T} = \sigma_1 \\ x_2(T) = x_2(0)e^{-\mu_2 T} = \sigma_2\end{cases}. \quad \{24\}$$

The set of the initial states which pass the point (σ_1, σ_2) at time T is the curve described by:

$$x_1(0) = 1 + (\sigma_1 + 1)\left(\frac{x_2(0)}{\sigma_2}\right)^{\frac{\lambda_1}{\mu_2}}, \quad \{25\}$$

where $x_1(0) \in [0, \sigma_1]$ and $x_2(0) \in [\sigma_2, 1]$.

In R_2 where the failure is generated in S_1, the set of initial states who pass the point (σ_1, σ_2) can be identified similarly, and we have the curve:

$$x_2(0) = 1 + (\sigma_2 + 1)\left(\frac{x_1(0)}{\sigma_1}\right)^{\frac{\lambda_2}{\mu_1}}, \quad \{26\}$$

where $x_1(0) \in [\sigma_1, 1]$ and $x_2(0) \in [0, \sigma_2]$.

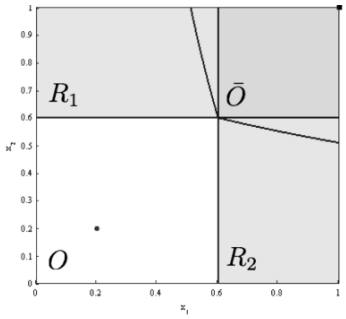

Figure 5. Four operation regions and the curves separating the resilience region and non-resilience region.

Figure 5 illustrates the resilience curves, which separate the resilience regions from the non-resilience regions within the failure-recovery region, as described by the equations {25} and {26}.

Figure 6 depicts several state trajectories for different initial conditions of the system. We observe that as long as the equilibrium point (denoted as the black dot) is inside the operation region (denoted in white) the system trajectories reside at all times in the resilience region. This means that for the design parameters fulfilling conditions {19} the system will always recover from unexpected events.

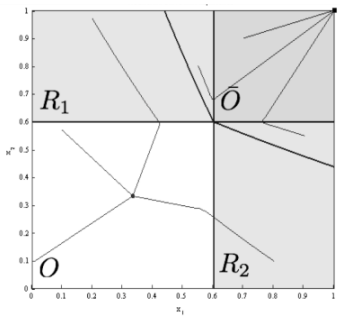

Figure 6. Resilience curve and system trajectories with different initial conditions.

When the design parameters are outside the bounds imposed by conditions {19}, the system will not recover i.e., the state trajectories will always converge to the (1,1) equilibrium point outside the (white) operation region as in Figure 6.

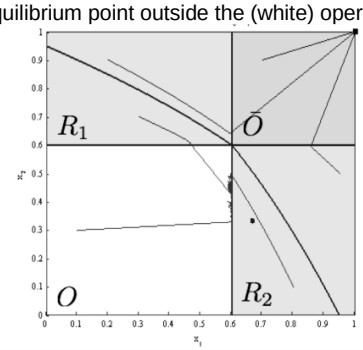

Figure 7. Chattering behavior for the system trajectories with different initial conditions.

The equilibrium point locus is another important aspect for the system resilience. For example, if the equilibrium point of the operation mode resides in the failure-recovery region, we can observe a chattering behavior like the one shown in Figure 7.
Similarly with the previous case, we can determine some conditions on the model parameters such that we can a priori identify the chattering behavior:
In $R_1 \coloneqq [\sigma_1, 1] \times [0, \sigma_2]$
If the equilibrium point is located in the resilience region of R_1, then:

$$\begin{cases} x_{f_1} = \frac{d_1}{\mu_1} \\ x_{f_2} = \frac{d_2}{\mu_2} \end{cases}. \quad \{27\}$$

Then, we get the inequalities:

$$\begin{cases} 0 \le \frac{d_1}{\mu_1} \le 1 + (\sigma_1 - 1)\left(\frac{d_2}{\sigma_2 \mu_2}\right)^{\frac{\lambda_1}{\mu_2}} \\ \sigma_2 < \frac{d_2}{\mu_2} \le 1 \end{cases}. \quad \{28\}$$

In $R_2 \coloneqq [\sigma_1, 1] \times [0, \sigma_2]$
We get similar results:

$$\begin{cases} \sigma_1 < \frac{d_1}{\mu_1} \le 1 \\ 0 \le \frac{d_2}{\mu_2} \le 1 + (\sigma_2 - 1)\left(\frac{d_1}{\sigma_1 \mu_1}\right)^{\frac{\lambda_2}{\mu_1}} \end{cases}. \quad \{29\}$$

The conditions {20}, {28}, {29} allow steering the parameters values in a way to get different scenarios of system evolution, as in Table 1. Note that in the present paper we choose arbitrarily values in [0,1] for the design parameters. At the authors knowledge there are few papers in the literature which provided insightful discussions on the appropriate choosing of the failure rates and recovery rates parameters. This is an issue of greatest importance and highly depends on the system model.

Parameters	Resilience Scenario	Chattering Scenario 1	Chattering Scenario 2
σ_1	0.6	0.6	0.6
σ_2	0.7	0.7	0.7
d_1	0.3	0.3	0.3
d_2	0.4	0.4	0.4
λ_1	0.1	0.1	0.1
λ_2	0.2	0.2	0.2
μ_1	[0.5,1]	0.7	[0.49,1]
μ_2	[0.57,1]	[0.55,1]	0.8

Table 1. Parameters values for two interconnected systems.

2 Resilience analysis for more than two interconnected systems

In the previous example, the resilience region of two interconnected system has been identified and analyzed. It is important to note that the computational complexity of the problem increases exponentially with the number of subsystems.
In the following, higher dimension systems are considered. Simulations are carried out to emphasize the influence of the systems' topology over the resilience properties.
Consider 4 interconnected systems as in Figure 10. Note that the graph is fully connected. The following steps are performed based on Monte Carlo simulations.
1) Randomly choose N_p initial states of the system;
2) For each set of initial states, apply corresponding dynamic equation from {2} for time T;
3) Compute the number of final states, which remain in or recover to functional state (converge to the operation region), calculate the fraction over the number of all initial states N_p;
4) Repeat the steps 1 to 3 N_i times, obtain a distribution of fraction of the resilient cases where the most frequent value is the estimated resilience of system.

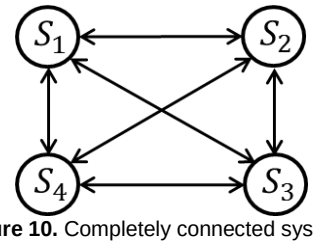

Figure 10. Completely connected systems.

The distribution of fraction of states sets, which remain in or recover to the resilience region, represents an estimation of system resilience. With Monte Carlo simulation, the analysis of resilience of high dimension system also can be realized.
For example, we take into account a system composed of 4 subsystems that are completely interconnected that is to say each subsystem is the input and also the output system for all other subsystems. The system structure is shown in Figure 10.
As Table 2 shows, the design parameters are a priori given determined and all 4 subsystems have the same values. We consider 500 initial states and 100 iterations. By Monte Carlo simulations we obtain that the estimated system resilience is 0.78.

Parameters	Values
N_p: the number of initial states	500
N_i: the number of repetition	100
$\sigma_i \in [0,1]$	0.8
$d_i \in [0,1]$	0.1
$\lambda_i \in [0,1]$	0.3
$\mu_i \in [0,1]$	0.4

Table 2. Parameters values for multi-interconnected systems.

Furthermore, we can analyze the behavior of the system by simulating the operation and failure scenarios.
Firstly, the case where all the systems are in operation mode is studied. The transient behavior of the system can be illustrated by simulation. The left plot of Figure 11 illustrates the initial states of the subsystems, in this case the initial states are supposed to be (0, 0, 0, 0), i.e., the subsystem are in functional mode. The middle plot of Figure 11 illustrates the evolution of each system states, we can observe that the state of each subsystem converges to an equilibrium position and remains on a fixed level under the threshold. The last figure of Figure 11 illustrates the evolution of the behavior of each subsystem over time and all the states converge to an equilibrium position under the thresholds. Thus, the global system continues providing services by the functionality of each subsystem.

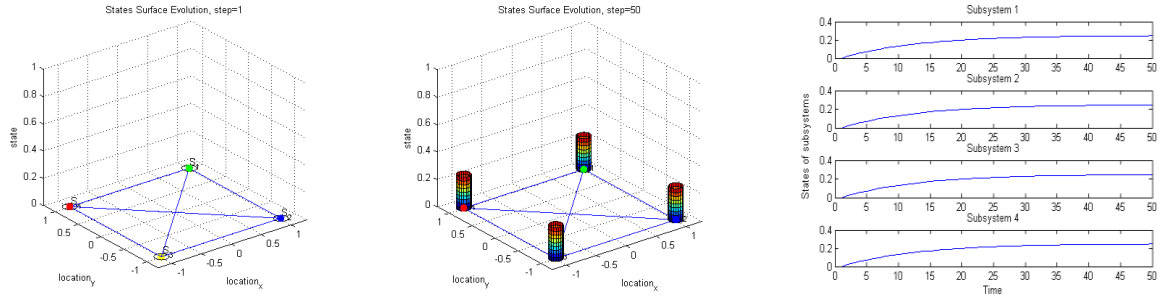

Figure 11. Operation scenario for fully connected systems.

In the next scenario, we consider that the subsystems states are in failure mode and observe the behavior of system with the corresponding design parameters indicated in Table 2.
We consider a sudden perturbation affecting the system. This results in the failure of two subsystems. Figure 12 shows that the entire system fails after a certain time. The left plot of Figure 12 shows the initial states of the subsystems (0, 0.8, 0, 1), i.e., one of the subsystems states is over the threshold and another one reaches the threshold (i.e. it's on the edge of failure). The middle plot of Figure 12 illustrates the final state of the system, and we notice that the state of each subsystem converges to the failure position. The evolution of each subsystem over time is shown on the right plot of Figure 12. We notice that the forth subsystem is in failure state after the incident and it has the tendency towards the operation mode and starts to recover. However, after a short process of recovery it turns back to the failure region under the influence of other connected subsystems. This is because the second subsystem is connected to the forth subsystem and the former turned to failure immediately, and then the failure propagates to the latter. Next, all the subsystems fail eventually due to the interdependencies between each other.

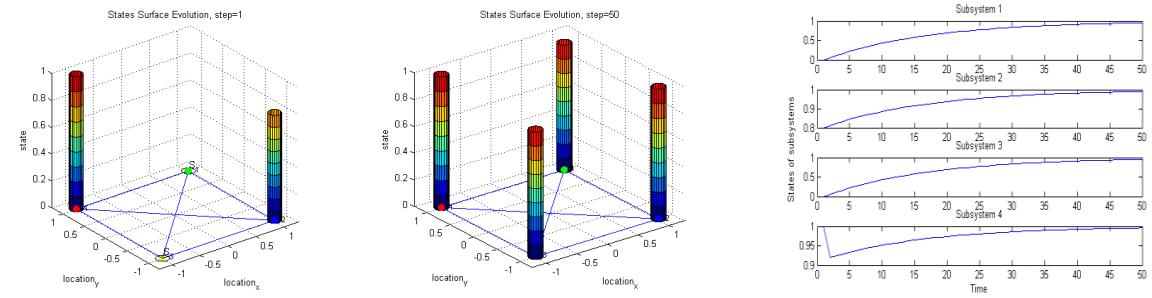

Figure 12. Failure scenario for fully connected systems.

Next, we consider another topological structure for the system, as shown in Figures 13. We keep the same values for their design parameters and apply the Monte Carlo simulation to estimate the size of resilience region. In this case, the estimated resilience for this system is 0.83 which is higher than the fully connected system presented above.

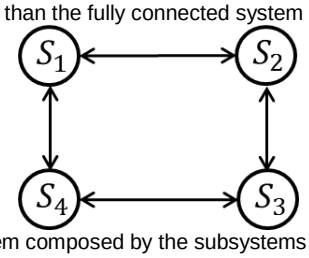

Figure 13. A system composed by the subsystems with loop structure.

The operation scenario of this system is similar with the previous case. However, when we consider the failure scenario, the high resilience for this topological structure can be observed.
In the Figure 14, the middle plot shows that the state of each subsystem converges finally to the equilibrium point inside the resilience region. Both subsystems recover from the beginning and then reach the stable state which is under the threshold the threshold. As previously mentioned, the dependency relationship between the subsystems influences its recovery process.

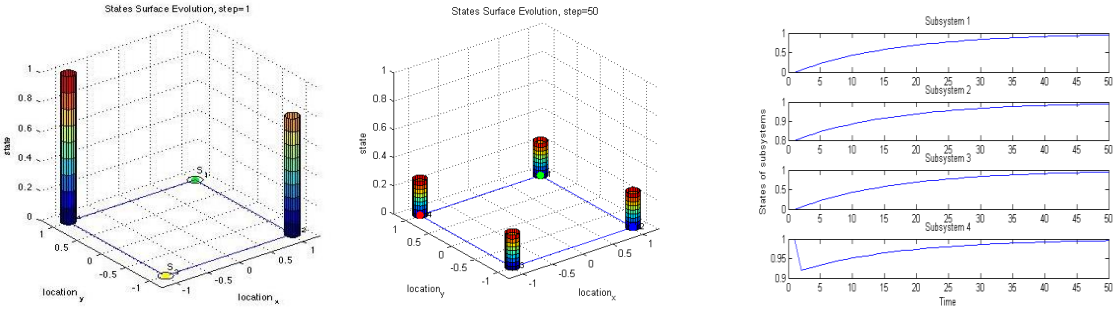

Figure 14. Simulation of failure scenario for system with loop structure.

The above analysis implies that the reduction of the links between the subsystems can increase system resilience. This provides us more insights about the protection measures for the interconnected system.

Conclusion

This paper adopts a control theory framework for the resilience analysis of interconnected infrastructure systems. The system dynamics is described by a switching dynamic model and a resilience region is defined and identified based on invariance concepts. This allows controlling the characteristics of the system resilience properties by design, operation and maintenance properties as represented by the values of the related parameters. Simulations results over two interconnected systems case study are provided in order to validate the proposed approach. Not in the least, higher dimension systems are also taken into account. Simulations are carried out to emphasize the influence of the systems' topology over the resilience properties.

7 References

Angelo, A. & Filippini, R. 2013. "Evaluation of Resilience of Interconnected Systems Based on Stability Analysis." Critical Information Infrastructures Security. Springer Berlin Heidelberg, 180-190.
Bloomfield, R. Buzna, L. Popov, P. Salako, K. & Wright, D. 2010, “Stochastic modelling of the effects of interdependencies between critical infrastructure,” in Critical Information Infrastructures Security. Springer, pp. 201–212.
Buldyrev, S. V. Parshani, R. Paul, G. Stanley, H. E. & Havlin, S. 2010. “Catastrophic cascade of failures in interdependent networks,” Nature, vol. 464, no. 7291, pp. 1025–1028.
Carlyle, G. Salmeron, M. J. & Wood, K. 2006. “Defending critical infrastructure,” Interfaces, vol. 36, no. 6, pp. 530–544.
Dobson, I. 2008. “Analysis of cascading infrastructure fail-ures,” Wiley Hand-book of Science and Technology for Homeland Security.
Faraji, M. & Kiyono, J. 2012. “Infrastructure performance oriented reliability using assessment using weighed stochastic petri net,” 15WCEE, Lisboa.
Filippini, R. & Zio, E. 2013. "integrated resilience and risk analysis framework for critical infrastructures", in Proceeding of ESREL conference, pp. 2001-2008.
Murray, A. T. & Grubesic, T. H. 2007. Critical infrastructure: reliability and vulnerability. Springer Berlin, vol. 16.
Nozick, L. K. Turnquist, M. A. Jones, D. A. & Davis, J. R. 2005. “Assessing the performance of interdependent infrastructures and optimising investments,” International journal of critical infrastructures, vol. 1, no. 2, pp.144–154.
O’Rourke, T. D. 2007. “Critical infrastructure, interdependencies, and resilience,” Bridge-Washington-National Academy of Engineering, vol. 37, no. 1, p. 22.
Pederson, P. Dudenhoeffer, D. Hartley, S. & Permann, M. 2006. “Critical infrastructure interdependency modeling: a survey of us and international research,” Idaho National Laboratory, pp. 1–20.
Reed, D. A. Kapur, K. C. & Christie, R. D. 2009. “Methodology for assessing the resilience of networked infrastructure,” Systems Journal, IEEE, vol. 3, no. 2, pp. 174–180.
Rinaldi, S. M. Peerenboom, J. P. & Kelly, T. K. 2001. “Identifying, understanding, and analyzing critical infrastructure interdependencies,” Control Systems, IEEE, vol. 21, no. 6, pp. 11–25.
Rinaldi, S. M. 2004. “Modeling and simulating critical infrastructures and their interdependencies,” in System sciences, 2004. Proceedings of the 37th annual Hawaii international conference on. IEEE, pp. 54–61.
Svendsen, N. K. & Wolthusen, S. D. 2007. “Connectivity mod-els of inter-dependency in mixed-type critical infrastructure networks,”Information Security Technical Report, vol. 12, no. 1, pp. 44–55.
Tonmoy, F. & El-Zein, A. 2014. “Vulnerability of infrastructure to sea level rise: A combined outranking and system-dynamics approach,” in Safety, Reliability and Risk Analysis: Beyond the Horizon. CRC Press.
Wolfgang, K. & Zio, E. 2011. Vulnerable systems. Springer.