Mastering Complexity and Risks in Modern Infrastructures: a Paradigm Shift

FILIPPINI, Roberto
a EBG MedAustron, Wiener Neustadt, Austria, e-mail: rob.filippini@tiscali.it

Abstract – Modern infrastructures are exposed to risks of difficult estimation. One reason is the unique complexity of this class of systems for which the risk assessment frameworks are not easy to apply: in many cases, they are inadequate to meet the needs of decision makers, and overall they cannot estimate if our societies are predictably secure and safe. This paper addresses these limitations and proposes a paradigm shift from a risk-centred to a resilient-centred approach. Arguments in favour of the proposal are discussed by considering the features of modern infrastructures, such as interdependencies, cascading and escalating failures, and emerging behaviours.

Keywords – Critical infrastructures, systems of systems, integrated risk management, resilience

1. Introduction

Technical transformations are profoundly innovating the functioning of modern infrastructures, with industry and economy as the main drivers. At the same time, concerns are growing with respect to security and vulnerability issues related to these transformations, which overall contribute to the exposure to new risks. In the book of Perrow, 1999 the author exemplifies why accidents in modern societies are expected to increase in size, they are hard to predict and, to some extent, unavoidable. These concerns and the related risks to our societies are taken in due consideration, for example in the programs for the protection of critical infrastructures prepared by the European Council [EC, 2008] and the US Department of Homeland Security [DHS, 2003]. The performance of integrated risk management, with resilience as key attribute, is recommended; nonetheless the way to achieve these objectives is still largely unclear.

This paper critically reviews risk management for modern infrastructures and suggests a new approach, starting from the specificities of the technical transformations in place. The groundwork is inspired by a simple intuition, based on the way modern infrastructures interoperate, which is explained in Figure 1. The figure shows the distance from the provider of a service (i.e. the base platform at the physical level) and the final user/consumer. Three levels are identified. In between, communications support the integration at a large scale, and have a major role in the so called “virtualization of services”. The virtualization enlarges the plateau of users, which can be reached by a larger number of service providers. In addition, it rationalizes resources, so that for example an energy public utility may use the communication from an external provider, instead of implementing its proprietary network. The result is a huge number of heterogeneous systems and organizations that are tightly-coupled together in what is called a “system of systems” [Maier]. In spite of the benefits, virtualization artificially hides complexity to the users, thus giving a dangerous feeling of simplification. A service is defined as virtual if its implementation is transparent to the user and may change, provided that functionalities at the interface are maintained. As a consequence, the direct connection between the physical level and the user is lost. This complicates the accountability of risks to a specific service provider, as well as the traceability of the causes that lead to an accident. Risk control measures may be poorly effective so that accidents will occur by surprise. There are several papers in literature that address risks for complex systems and infrastructures. A solid reference for understanding interdependency is [Rinaldi, 2001]. Uncertainty in risk analysis for complex systems is addressed in [Cox, 2012]. [Haimes, 2008] develops a theoretical framework for integrated risk management of infrastructures, while [Kroeger, 2009] outlines the issues related to the current modelling and simulation techniques in face of the increasing system complexity. They are all very inspiring papers. Like several other scientific contributions in this field, more advanced tools are suggested to fill the gap, which is correct provided that the mathematical effort avoids an unnecessary focus to an already very complex reality. The parsimony problem-solving principle (or Occam’s razor) must rule. In the specific case, the under-
understanding of needs and objectives of decision makers and operators is crucial. In order to take decisions in real time and control risks the “global picture” of the infrastructure with its vulnerability is necessary. These sensible principles have inspired the realization of this work.

The paper is structured in 5 sections. Section 2 presents the integrated risk management as applied to modern infrastructures, with its limitations and challenges. Section 3 departs from the discovered limitations and formalizes the paradigm shift. The models of reference for the resilience analysis are explained in Section 4 and exemplified for a case study. A few concluding remarks will end the paper.

2. Integrated Risk Management for Modern Infrastructures

Integrated risk management (IRM) has solid theoretical foundations (e.g. finance and economy, socio-technical organizations) though its application is not trivial especially for technical systems of significant complexity. The following are the constituent elements:

1. Definition of problems in scope and their boundaries;
2. Identification of hazards;
3. Identification of the categories at risk (stakeholders) with risk acceptability criteria;
4. Estimation and evaluation of risks;
5. Identification of the risk control measures (technical, organizational) that contribute to reducing the risks in accordance with the acceptability criteria.

The above steps are performed over the entire lifetime, which includes the conceptual realization, implementation, commissioning, operation, development, and decommissioning. Changes must be documented and new risks have to be analysed. This is a time consuming activity and prone to errors. Risk management admits a fraction of unknowns, which is unavoidable. Nonetheless, these unknowns are expected to be negligible, if an accurate description and analysis of the concerned systems have been performed. Eventually, the remaining unknown risks are traded off against the benefits of using the system.

2.1. Risk analysis rationale

Figure 2 sketches the development of an accident scenario triggered by a hazard i.e. the initiating event, that escalates across three domains: control, risk and emergency. The first domain affected is the control domain. The system must be able to operate with adequate margins to tolerate out-of-normal conditions, up to a certain extent. Fault tolerance and robustness are the measures applied. When controls are overdone, the developed hazard falls into the risk domain. The risk controls measures are reaction chains, triggered on demand if deviations in the system behavior and in the surrounding environment are detected. Such measures either provide an alternative mean to continue operation (e.g. switching on back up systems) or they guarantee that a safe state is reached (by stopping the operation). The risk domain differs from controls as it does not interfere with the nominal functioning. Because of that, a risk control measure is expected to be triggered at a much lower frequency. Emergency is the last concerned domain, which comes into play if the accident develops in spite of the existing control and risk measures. Emergency measures are very diverse: for example they alleviate the consequences to population, facilitate rescue operation, and try to restore infrastructure at a minimal acceptable service.

In the presented framework, the emergency domain must intervene as the last resort and in very rare circumstances. Measures applied in the control domain are less effective for the risk reduction. Actually, they are almost never considered to prevent and reduce risks, especially if a rigorous risk certification process is in place. Risk con-
trol measures are therefore predominant, and the overall framework can be said as risk-centered.

### Table 1: Domains of concern for risk evaluation

<table>
<thead>
<tr>
<th>Domain of concern</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain of hazard</td>
<td>Exposure and occurrence of hazards</td>
</tr>
<tr>
<td>Domain of control</td>
<td>Fault-avoidance, fault-tolerance, operation safety margins</td>
</tr>
<tr>
<td>Domain of risk</td>
<td>Reaction chains: monitor-evaluate-actuate</td>
</tr>
<tr>
<td>Domain of emergency</td>
<td>Emergency plans</td>
</tr>
</tbody>
</table>

#### 2.2. Risk evaluation

Risk evaluation has a relatively simple onset and assumptions. The hazards must be known, with the initiating events and the circumstances that contribute to their occurrence. The risks (i.e., the product of the consequence by the likelihood) are evaluated after the application of the risk control measures. Several possible end states may exist, depending on the successful or unsuccessful performance of the risk control measures.

The risk evaluation is sketched in Figure 3, using the conceptual representation in domains of Fig 2. Every domain counteracts (probabilistically) the development of the accident. If the action is successful, then the end state “green” is reached, which means “no risk or acceptable residual risk”. The column to the right of Figure 3 describes the ideal case with no sources of uncertainties and unknown. In this case, the residual risk is the product of the hazard exposure $E$, the hazard frequency $F$, the probability of failure of the system response (or susceptibility to the hazard) $P_c$ and the probability of failure of the risk control measures $P_r$. The columns to the left take into account all possible sources of uncertainties and unknowns during the risk assessment process such as the incomplete identification of hazards or unforeseen system behavior that may lead to underestimated risks. In this case, the final evaluation of risks will be biased by an additional unknown/uncertain contribution, which makes it impossible to perform a cost–benefit analysis, and finally to justify the investments in the protection measures.

The above description, with residual risks due to uncertainties and unknowns, applies to a modern infrastructure. The following are the main concerns:

- Definition of systems and operation scenarios: the definition of a modern infrastructure can only get close to a fair picture, based on the present knowledge, which is expected to evolve in time. This is a source of uncertainty and unknown.
- Identification of hazards: they are identified on the intended behaviour and misbehaviour of the single system, while interplaying with the other systems. A too low-grained description of the infrastructure will not be able to identify all hazards and the way they propagate. This is a source of unknown.
- Evaluation of the residual risk: many stakeholders are involved, and there is not one single responsible for the risk reduction. If the risk analysis is conducted separately (and not integrated) and acceptability crite-
ria are not harmonized, then the overall residual risk cannot be correctly evaluated. This is a source of uncertainty.

- Effectiveness of risk control measures: the effectiveness of the risk control measures cannot be tested in the single system, in isolation. The measure must be effective at a larger scale, when demanded for counteracting the accident scenario. For example, this is the case of a transfer of risks among systems, e.g. a system has to be aware and prepared to control risks that are generated elsewhere. The lack of risk awareness is both source of uncertainties and unknowns.

Uncertainties and unknowns cannot be avoided if the presented risk management framework is applied as it is to modern infrastructures. This is not a surprise, as the framework is conceived for systems well defined in their constituent elements and borders, and with a long lifetime during which very few changes are considered. All these features hardly apply to modern infrastructures.

### 3. Changing the Paradigm

The previous section proved, by reasoning and evidences, that this risk-centered approach is inadequate when applied to complex interconnected systems such as modern infrastructures. The methodologies for the assessment and evaluation of risks as well as the design of risk control measures need to be rethought. The starting point is the review of an important assumption on which the risk methodology relies. As stressed in the previous section, the domain of control has a little involvement in the response to hazards and failures, which therefore are within the big umbrella of the risk domain. The question is: what if this assumption is relaxed? The following idea is at the basis of the paradigm shift:

“The control domain shall be extended in order to overlap in part the risk domain and some of the risk control measures”

This idea is simple and revolving at the same time. The paradigm shift suggests leaving the risk-centered approach and allowing hazards to be counteracted in the control domain. This idea was first proposed in the field of safety engineering, see [Hollnagel, 2006] and [Leveson, 2004]. The implications are relevant. If controls are central in counteraction malfunctioning and failures, then resilience becomes the attribute of interest. Moreover, the entire accident development is in scope, including the restoration to operation. In order to support the paradigm shift, a holistic (systemic) description is very much needed. A functional description responds to these needs because of the neutrality with respect to the systems and domains so that all interdependencies of concern can be represented in the same model.

The implications of the paradigm shift are shown in Figure 4. The functional description is a network arranged as directed graph, where the nodes are the systems and the arcs account for functional dependencies of type provider/consumer (if a resource is consumed) and provider/user (if a service is exchanged). In order to analyze the network resilience, four phases are identified:

- Phase 1: the hazard develops in the system;
- Phase 2: the hazard propagates to the systems that depend either directly or indirectly from the source of the hazard, i.e. the vulnerable set;
- Phase 3: the initial hazard is resolved, and recovery may start;
- Phase 4: the recovery is completed and operation is restored.

The four phases account for the accident dynamics in complex networks. The hazard occurs in a single node-system (but it may also affect more nodes at a time). The ability of the system to counteract the hazard are within the implemented resilience measures. Then it propagates to the dependent nodes that in their turn apply their resilience measures, for example by retarding the accident propagation. The final phase is the restoration to operation when circumstances permit.

With respect to the risk-centred approach, the paradigm shift gives more relevance to resilience than to the risk. While a risk-centered approach resolves the hazardous situation by assuring that the residual risk is acceptable, a resilience-centered approach always guarantees that the network is restored to the initial condition. In order to get these goals, also the applied measures are significantly different. The risk-centered paradigm may recommend aborting the operation, if this measure is safe and for example preserves a system from undesired consequences. This would not be a suitable strategy for resilience, which instead tries to minimize the service outage. In one hand, resilience is more encompassing than risk. On the other hand, risk is necessary for evaluating the consequences and the related costs associated to an accident. Resilience and risk are therefore complementary.

The paradigm shift lead to a model for the representation of structural, and dynamical properties of the analysed systems, as well as the evaluation of risks. The structural properties of the model are:

- S1: modeling (inter)dependencies among systems, which exchange services and quantities;
- S2: identification of vulnerabilities.

The concept of vulnerability is based on the definition of functional proximity among systems e.g. how far the client system from a provided service is. Therefore, a system is vulnerable from another system if this latter contributes to provide its input services either directly or indirectly. By visiting the graph, it is possible to identify those systems that directly or indirectly are reachable and therefore depend on a chosen node-system, say the node N of the graph. These systems belong to the vulnerability set V(N). A special vulnerability set is the one that forms a loop. In this case, all systems in the loop are mutually dependent and vulnerable. The analysis of vulnerability improves the awareness of every system to be either exposed to external hazards or a potential source of hazards.
to other systems. It also provides the size of propagation of an accident if the hazard is left free to develop across the network. More details are in [Filippini and Silva, RESS, 2014] and [Filippini and Silva, IEEE, 2014].

The dynamic properties of the model are:

- **D1:** system reaction to an input hazard;
- **D2:** system recovery from a failure caused by an input hazard;
- **D3:** system preparedness to a developing accident;
- **D4:** ability to coordinate with other systems in response to a developing accident;
- **D5:** learning from experience;

The system reaction (D1) consists of two stages: 1) an overhead, which is the time necessary in order to set up and allocate resources and 2) the activation of the resources and the execution of predefined procedures. The set-up time can be shortened if the system is informed about the incoming hazard (D3). Once the hazard is resolved at the source, the affected systems can recover (D2), starting from the one that was affected first. In case of a functional loop, the recovery from an accident scenario might be impossible, for example if all systems in the loop have failed. In such case, the network resilience is overridden, and the unresolved accident will have to be managed in the emergency domain.

The risk related properties of the model are:

- **R1:** risk consequences are based on the service downtime, w.r.t. systems and users;
- **R2:** risk accountability;
- **R3:** risk traceability;
- **R4:** assessment of residual risks with respect to acceptability criteria of every stakeholder.

The estimation of the consequences during the development of an accident has to be compared against the risk acceptability criteria of every stakeholder (i.e. the owner of the system and the user). For instance, an interruption of services may cause damages to systems, and therefore cost for the reparation. As well as it causes costs (directly or indirectly) to the users. The consequences are proportional to the downtime, i.e. the time interval during which a service or quantity is not available, which can be calculated by simulating the accident dynamics in the presented model. In addition, it is possible to trace all risks and account them to the initial cause of the accident. The risk likelihood is estimated on the same model of Fig 4 by combining the hazard, with its frequency and duration, and the applied resilience measures (preparedness, reaction and recovery). The resilience measures are performed on demand, which means that probability figures (i.e. availability) can be assigned to the deployed resources that implement the measures themselves. The combination of resilience and risk in the same model is at the basis of the integrated resilience and risk assessment framework, which is presented in more details in [Filippini & Zio, 2013].

4. Models for Resilience Analysis

They make it possible to analyze the resilience of interconnected systems by progressively meeting the properties D1-D5 outlined in section 3 (i.e. from a base model to more sophisticated models).

The first model is the "base model", and describes the internal failure-recovery dynamics of the single system-node. An internal state variable $x$ in $[0, 1]$ associated to every system and represents the integrity of the provided service/function: it holds 1 if the service is available and 0 if it has failed. Values between 1 and 0 account for degraded states. The internal state dynamics is governed by two distinct modes, which are the failure mode and the recovery mode. The two modes are switched when a state threshold is reached, which represents the minimum acceptable Service Level Agreement among clients and providers. The system failure mode dynamic is triggered by an input hazard, which corresponds to the loss of an input service from a provider. If the state $x$ falls below the SLA threshold then the client-system will suffer from an interruption of service, and as a consequence it will activate its resilience measures, e.g. buffering resources to mitigate the absence of service. The more the threshold is close to $x = 1$, the higher the required SLA is, which means a higher sensitivity to degradation of the input service. The recovery is based on the same principle, but reversed: if the state $x$ overdoes the threshold, then the system will see again the service available at its input. In general the resilience measures, either buffering or recovery, can be modelled as sensitive to the input hazards, so to represent more accurately the accident dynamics.

In order to mathematically model the switching between failure and recovery modes, every base model of a system has an internal representation of the state of the system(s) at the input interface, which is called "external state". This is a binary variable $X$ which is equal to 1, if the system is available and provides the service as expected (i.e. above the threshold), otherwise it is 0. Because the SLA can be negotiated among systems, the external state of the same system can be different at a time $t$, depending on the client-systems to which it provides its service. In order to account for this property, a system $j$ will represent the external state of the system $i$ at its input interface.
as \( Xi/j \).

The following differential equations describe the internal and external state dynamics for the base model of a system \( k \), which depends on system \( i \) and \( j \) at its input interface. The parameters are the failure rate \( \lambda \), the recovery rate \( \mu \) and the state threshold \( x_{th} \), which serves to calculate the external state. The equations are the following:

1. Failure mode:
   \[
   \frac{dx_k}{dx} = -f(X_i, X_j, \lambda)x_k, \quad \text{triggered if } X_i \lor X_j = 0
   \]

2. Recovery mode:
   \[
   \frac{dx_k}{dx} = g(X_i, X_j, \mu)(1 - x_k), \quad \text{triggered if } X_i \land X_j = 1
   \]

3. External state of the system \( k \):
   \[
   x_k = 1(x_k - x_{th}) = \begin{cases} 
   1 \text{ if } x \geq x_{th} \\ 
   0 \text{ if } x < x_{th} 
   \end{cases}
   \]

The initial conditions correspond to

\[
X_k = 1, X_i = X_j = X_k = 1
\]

The function \( 1(.) \) is the step function.

Model 1.0 extends the base model in order to describe the failure propagation (and recovery) from the single system throughout the entire network. The mechanisms that trigger the failure propagation and recovery at the systems’ interface are introduced. These mechanisms depend on the SLAs between a system provider and the users. If the level of an input service decreases below the SLA then the failure propagates to the client-system. The recovery follows the same principles, but reversed: if the service level returns to SLA, then the recovery may start.

Model 2.0 encompasses model 1.0, plus it adds the possibility for a system to be aware of the neighbors’ state. The original base model is modified by introducing a “state observer” of the external systems, on the basis of which, in case a failure is observed, it is possible to anticipate the activation of the internal resilience measures. This reduces the overhead (e.g. during the set-up of the buffering resources) and avoids that a system is not prepared to face the accident.

Model 3.0 encompasses model 2.0 plus it adds the possibility of coordinating the systems’ reactions, during the development of the accident. This resilience feature applies to clusters of systems or the entire network. It makes it possible to manage accident during the reaction to hazards and the recovery, with the objective of containing the consequences and minimizing costs. A further feature accounts for the possibility of the network to perform a dynamic reconfiguration, for example by disconnecting systems before these are reached by the hazard. This strategy is applicable if alternative service providers are available as back-ups.

Model 4.0 is the last and most advanced model. It implements the ability of every system, and the network, to learn from experience. Any deviation from the nominal functioning is considered to be an “experience” to learn from. This can be a failure event, but near misses are also in scope. This additional feature makes it possible that resilience for interconnected systems is designed by a continuous improvement process. The so called “evolutionary behavior” of the network is a genuine attribute of modern infrastructures.

### Table 2: Model of references versus resilience features

<table>
<thead>
<tr>
<th>Feature</th>
<th>M 1.0</th>
<th>M 2.0</th>
<th>M 3.0</th>
<th>M 4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response (Buffering)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Recovery</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Failure propagation</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Preparedness</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Coordination</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Reconfiguration</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Adaptive learning</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4.1. Example

The case study is a proof of concept for the Model 1.0, and as such its size and the level of description are intentionally simplified. The considered network of interconnected systems is a simplified energy infrastructure with five systems: production, transmission and distribution, plus power grid controls and communications, see Figure 5. Every system is associated a base model. In total, 5 internal state variables \( \{x_1; x_2; x_3; x_4; x_5\} \) and 6 external state variables \( \{Xi_1; Xi_2; Xi_3; Xi_4; Xi_5\} \) are defined. The parameters (failure and recovery rates, and state threshold for the SLA) are set purely demonstrative values, for testing the potentiality of the model.

The analysed accident scenario considers that the power plant (Node 1) stops functioning for a time \( T \) before it can put in place the resilience measures and restore to operation. During this interval, the hazard propagates to the dependent systems. The result is shown in Figure 6. The left plot represents the internal state dynamics of one of the system, the transmission, while the entire accident scenario is shown in the right plot. The dynamics of the internal and external states of the transmission system is can be split in three phases, a, b and c, see Figure 6 (left). Phase (a) is governed by the failure mode dynamics, and it lasts until the power plant restores its service. Phase (c) is governed by the recovery mode dynamics, and starts after the power plan has restored the service. Phase (b) is the phase in between and it shows the service downtime, which causes the failure propagation from the transmission system to the distribution system, as soon as the state
threshold is overdone. Figure 6 (right) shows the sum of the states of the systems that depend on the power plant (Node 1 of the network), which define the vulnerability set \( V(1) = [2, 3, 4, 5] \). The accident dynamics depends on the time to recover of the power plant and the effectiveness of the resilience measures of the systems that are affected. Again the recovery phase follows the failure phase. In the example, the vulnerability set forms a loop so that a maximum downtime of the power plant exists, after which all systems in the loop will fail.

![Figure 6: Internal and external state (left) and accident scenario (right)](image)

Figure 6 shows the result of the sensitivity analysis with respect to the downtime of the power plant, i.e. the length of phase (b). Four accident scenarios are analyzed, each one corresponding to a bigger service downtime of the power plant. In the last plot the resolution of the accident scenario is not possible; a “structural deadlock” is reached. The last accident scenario cannot be resolved with the existing resilience measures (i.e. buffering and recovery) and has to be managed in the emergency domain.

![Figure 7: Sensitivity to duration of the downtime in the power plant](image)

The sensitivity analysis can also be performed for the resilience measures. Every resilience measure is associated an interval of values (i.e. a distribution) that account for their uncertainty. The model is simulated by Monte Carlo for a fixed power plan downtime. The result of the simulation is shown in Fig. 8, and represents the density distribution (fitting a lognormal curve) of the time of recovery of the infrastructure to its initial state, i.e. the overall accident duration (i.e. the transient response of the network). Only a small fraction of accident scenarios (3%), corresponding to specific settings of the resilience measures, ends into a non-recoverable deadlock condition for the infrastructure, which has to be managed in the emergency domain.

More details can be found in Alessandri and Filippini, 2012 and Filippini and Zio, 2013.

![Figure 8: Distribution of the duration of the accident scenario for a fixed power plant downtime.](image)

5. Concluding Remarks

This paper addressed the applicability and limitations of existing risk management frameworks for modern infrastructures and it proposed an improvement, which is based on a paradigm shift: failure and accidents have to be treated in the control domain, and resilience is the attribute of interest. In order to implement the paradigm shift, a model based on the functional representation of the (inter)dependencies among systems was developed. The model makes it possible to analyze the response to accident scenarios of every system and throughout the infrastructure. The advantages of the presented paradigm shift are summarized as it follows:

1. The accident dynamics (state-based, event-driven) can be analysed as the combination of a developing hazard and system response, which consists of the resilience measures in place: reaction and recovery, detection/anticipation of precursors of failures, coordination and learning from experience.

2. Accident scenarios that cannot be governed with the existing resilience measures (and therefore calls for emergency measures) are identified.

3. The risks can be evaluated in the same model. This guarantees the consistency of the results and acceptability of risk, as harmonized among the several stakeholders. Accountability and traceability of risks is possible because the accident dynamics is known and can be tracked back to the initial cause.

4. The outcomes of the resilience analysis are useful to screen the response to hazards of various natures that affect the infrastructures. This information is valuable both for operators and decision makers.

5. The frequent changes of the infrastructure over the life-cycle do not present a problem. Indeed, the model is at high level and functional, and it can be updated so to cope with the introduced changes.

Some of the ideas presented in this paper are still research challenges, such as for example the implications existing between system resilience and system stability when analysing the accident dynamics. From a more abstract reasoning point of view, the reaction to a haz-
ard and the recovery (literally bouncing back to the initial state) suggests the existence of a region in the state space where the network performs as expected, and a region where it does not perform but can be recovered. This requires to study the state transitions among stable/predictable behaviors (i.e. under the control domain), unstable/predictable (i.e. under the risk domain) and eventually unstable/unpredictable (i.e. under the emergency domain). These advanced theoretical concepts are introduced and investigated in the paper of [Alessandri and Filippini, 2012]. The results are promising and lead towards a better understanding of decentralized control issues of systems of systems at the functional level.

In conclusion, resilience is an attribute that can be "designed" around systems of systems and more specifically infrastructures, and this paper has demonstrated that this is possible and how. These ideas have been developed for research purposes, but they are neither speculative or too innovative. For example, the so called smart infrastructures already embed many of the presented resilience features, such as distributed real time controls and state feedback. In this respect, it is possible to state that the new technologies will facilitate and contribute to the implementation the paradigm shift.

References


Citation