Emergent Disservices in Interdependent Systems and System-of-Systems

Igor Nai Fovino and Marcelo Masera

Abstract—The assessment and the evaluation of the risk exposure to failures and cyber attacks, is nowadays—in times of pervasive ICT applications—a much required task. However, in some cases, and especially when evaluating an ICT infrastructure (which can be logically and geographically sparse and which can provide services to other systems), the evaluation of system risk is not sufficient. In fact in this context, a failure judged negligible for the life of a system may have not negligible effects on another system which is in someway in relation with the former one. In this paper, we present a formal approach based on the concept of System of System allowing to represent the interdependencies existing among a group of collaborating systems. Moreover we show how such an approach can be integrated in a risk assessment methodology in order to obtain a System of System risk assessment framework.

I. INTRODUCTION

The assessment and management of the security of large-scale systems (as e.g. infrastructures) requires appropriate sources of data, in quantity and quality. These data refer to events, conditions and attributes internal to the system (e.g. vulnerabilities), but also to external elements (e.g. many threat circumstances), and to information that derives from the accumulation and treatment of historical data (e.g. attack patterns). By the analysis of such data and adopting some analysis methodologies [2, 3, 22] we are today able to identify the impact, in term of economical and physical damages, that a failure (accidentally or maliciously caused) causes in a system.

This type of analysis is usually known as risk assessment. However, nowadays, the pervasive use of ICT infrastructure in the modern systems has made the risk assessment scenario more complicated. In fact, by the use of ICT infrastructures, systems geographically far are logically near, allowing then the collaboration and the exchange of information and services. In such a context, it is evident how is not sufficient to evaluate the effects that a failure has in a single system. In fact, in a world in which several systems are connected, a failure judged negligible in a system may have disastrous effects on another system connected in some way with the first one. In other words, a butterfly movement in Asia may cause a tornado in USA.

We believe that, in such a scenario, the modern risk assessment methodologies need to move their attention from the system level to the System-of-Systems level. In fact, as the System-of-Systems paradigm can be used to study the concepts of Emerging Properties and Emerging Algorithms (well representing the idea of independent system providing services that can be used in order to obtain not explicit results), at the same way, it can be used to represent the new concept that we introduce in this paper, of Emerging Disservice. More in details, for Emerging Disservice we intend a not evident disservice in a target system, originated by a disservice or a set of disservices physically or logically localized in another independent system. In a context in which every public infrastructure (like Power grids, Water grids etc.) has increased its complexity reaching the status of System-of-System, such a concept is extremely relevant.

From the security analysis point of view, a crucial element is then the description of the relationship existing between the different systems and the methodology used for deriving useful information from this knowledge.

The problem of the “Infrastructure Modeling” is well known in the scientific literature and different approaches have been suggested in order to model systems, both theoretical and practical. The work presented in [2] by Alberts & Dorofee is a good example of risk assessment methodology based on a system description. However such a description lacks mainly in two points: it is not formal and, more relevant, it is not centered on the concept of System-of-System. Folker den Braber et al. present in [3] another risk assessment approach partially based on a system description. Such a description tries to capture partially the concept of adverse environment by introducing, using an UML style, the concept of “Threat Scenario”. This, of course, represents an advance in the representation of a system that could be adapted in order to represent more than a system interacting in some way; however this was not the intention of the authors and represents only a possible adaptation of the methodology.

In this paper, starting from the results obtained in our previous works [28, 29], we analyze the problem of the risk assessment of interconnected system, paying a particular attention to the inter-system relationship modeling.

The paper is organized as follows: in Section II we give some preliminary definitions, in Section III we describe our modeling approach. Moreover, in Section IV we show how to use the presented approach in order to extend a risk assessment process in the case of system-of-systems analysis, and finally, in section V take out some conclusion presenting
the future works.

II. PRELIMINARY DEFINITIONS

As claimed in the introduction, we are interested in capturing the relationship existing between independent systems in order to study the propagation of the effects caused by failure (accidental or malicious) in a system $X$ on the other interacting systems.

The key point of this study is then the representation of the relationship between the systems under analysis. Intuitively, a collection of systems interconnected by an ICT infrastructure, can be equated to a System–of–Systems. The use of this term implies the existence of a taxonomic grouping. In other words it implies the existence of a classification of different elements which in some way can be identified as separated systems, connected with the others according to some relationship criteria. In the same way, every system can be defined as a collection of entities collaborating to realize a set of objectives [7].

In the scientific literature there exist several definitions of System of Systems. For example, Shenhar [8] define a System Array (that can be equated to a system of systems), as a “Large widespread collection or network of systems functioning together to achieve a common purpose”. In a similar way, Eisner [9] define a system of systems as a geographically distributed set of entities with a centrally directed effort oriented to a target objective. These two definitions, even if extremely interesting, do not capture a wide range of modern “System of Systems”, and mainly the class of Emerging Systems [10], characterized by the absence of a coordinate central management system. In such a class of systems, the concept of central management is substituted by the concept of collaboration. Maler [11] gives a definition that allows to capture this property. More in details, for Maler, a System–of–Systems is an assemblage of components which individually may be regarded as systems, but that possesses two additional properties:

1. Operational Independence of the components
2. Managerial Independence of the components

The first property implies that every component (system) is in relation with the others in a producer/consumer schema. The second property captures the independence of every system in the management of the internal behavior.

This definition of System–of–Systems, from a modeling point of view, is extremely powerful. In fact, when considering complex systems, it helps in concentrating the attention onto the different systems and to their relationships in an abstract and flexible way. Moreover, the possibility to see every system as an independent entity which interacts with the others by a mechanism producer/consumer–like (collaboration), guarantee an high level of scalability – allowing when necessary, to view each single system as a little System–of–Systems that can be then described without taking into consideration the information of the higher levels, in a vision that we can identify as a “Matrioska” view. However, the applications of such decomposition approach in an exhaustive manner, risks causing an information overhead which could prevent a clear analysis. It is then fundamental to identify in a similar decomposition a lower bound which limits the description detail to the minimum needed for a correct assessment.

As claimed before, the glue connecting the systems of a complex “System-of-Systems” (SoS) are the relationships between them. The description of these relationships is very important, especially when evaluating the possible propagation effect of a damage/failure/attack. These relationships can be functional, or physical. However, due to the scalability of their structure, and in the light of our previous modeling experiences [13], we note an analogy with a well known structure usually used to represent social networks: the “Small World Graph” (SWG), introduced for the first time by Korte and Milgram [12]. In their study, they discover that in a social network (even of considerable size), the average number of hops needed to join two human beings chosen randomly is six (see Fig. 1). This phenomena, studied even by others authors [14, 15, 16, 17, 18], is mainly due to two characteristics of the social networks: the clustering (a friend of your friend probably is your friend) and the sparse geographical distribution.

More formally, a small-world network is characterized by the following properties:

1. The local neighborhood is preserved
2. The diameter of the network, quantified by the average shortest distance between two vertices, increases logarithmically with the number of vertices $n$ (as for random graphs)

These properties imply that it is possible to connect two vertices in the network through a few hops; moreover, the local connectivity implies the network to be of finite dimensionality. Anderson in [19] has shown that SWG can be used to model the spread of disease. Moreover, Albert et al. in [20] has even shown that the Internet can be modeled using SWG. This result, together with the results of Watts in [21] (an electric power grid has SWG properties), is, for the scope
of this paper, extremely interesting. In fact, merging the
definition of System-of-Systems presented before, with the
SWG, we obtain our original approach to the relationship
modeling problem. In fact, we sustain that a set of systems
connected by ICT infrastructure is modeled as a
System-of-Systems (i.e. managing every component as an
independent system having the properties described before in
this section), making explicit the relationship among the
different components by means of services and taking care of
their locality property.

III. THE MODELLING APPROACH

In order to study the propagation and the eventual
amplification of the disservices, it is necessary before to
identify and represent the way by which such disservices can
be propagated.

As described previously the SoS paradigm allow us to
represent the systems as independent entities which
communicate with the others adopting a producer/consumer
approach (see Figure 2). This schema is then the unique way
by which two systems interact.

It is then obvious that if a disservice occurs in a system, it
can be modelled by services, which will use the results
provided by the external service in order to make another task
in their system.

Modelling the service chains among the systems of the SoS
is then the key point in the damage propagation analysis.

This preliminary description of our approach lacks in two
points:

1. Not all the services of a system has the same
   relevance
2. Not all external services required by a system has
   the same relevance

We need then to specify the relevance that a certain service
has for the requesting entity. We describe now, more in detail
and in a formal way, our approach.

As explained in the introduction, a SoS is a “collection” of
systems. We describe then every system as grey boxes which
contain internal services and which provide external services
to the other systems. Formally:

\[ \text{Definition 1: we define a service as a tuple } s = \langle \text{Name}, \text{Description} \rangle \text{ where Name identifies the service and Description gives a brief functional description of the service.} \]

\[ \text{Definition 2: a system } S_n = \{ s_1, \ldots, s_n \} \text{ where } s_1, \ldots, s_n \text{ are services provided by } S_n \]

As claimed before, the glue of the SoS (and then the way
by which model the failure propagation), is the
interdependency of the services. Such a dependency must
then be modelled.

\[ \text{Definition 3: Let } S = \{ S_a, S_b, \ldots, S_n \} \text{ be the set of the} \]

![Fig. 2. A logical overview of a SoS approach.](image)
systems in SoS, let $\text{Serv}$ be the set of all the services of $\text{SoS}$, a service dependency record is a tuple $\text{sdr} = (s, \text{sid}, \text{inset}, \text{outset})$ where:

- $s$ is a service.
- $\text{Sid}$ is the identifier of a system $\text{Sa}$ in $\text{SoS}$.
- $\text{Inset} = \{(d, w) | d \in \text{Serv}, w \in \mathbb{R}\}$ represents the collection of the services directly contributing in the realization of the service with the associate relevance $w$. To simplify the next definitions, we call every tuple $\langle d, w \rangle \rightarrow \text{Dep}_\text{rel}$.
- $\text{Outset}$ is the list of services to which directly the service $s$ gives a contribution.

Such a definition allows us to capture at the same time many properties: in fact, every service dependency record, magnify the relation existing between services in the SoS. Moreover, the $\text{Sid}$ allows to capture the locality property (in accordance with the SWG definition); finally, the weight $w$ will allow to the analyst to understand which is the immediate damage caused by a failure in the related service.

In the SoS description task, we are then able to define, for each system, the set of associated services and the relations with the other “nearest” (under some criteria) services.

**Definition 4**: Let $\text{SoS} = \{\text{Sa}, \text{Sb}, \ldots, \text{Sn}\}$ be the set of the systems in $\text{SoS}$, let $\text{Serv}$ be the set of all the services of the $\text{SoS}$, and let $\text{SDR}$ the associated set of service dependency records, for each system $\text{Sa}$ in $\text{SoS}$, we define the associated services set as the set:

$$\text{Sv}_\text{sa} = \{\text{sdr} | \text{sdr} \in \text{SDR}, \text{sdr}.\text{sid} = \text{Sa}\}$$

By the use of the previous definitions in the SoS modelling, we are able to represent every connection existing between the services of the SoS. Moreover, we can easily discover if a disservice on a service $x$ of a system $Z$ may have effects on a service $k$ in a system $Y$. In order to do this, we need to define a particular function.

**Definition 5**: we define as relationship validation function a function $r : \text{SDR} \times \text{SDR} \rightarrow \{0,1\}$ where

$$r(\text{sdr}_j, \text{sdr}_k) = \begin{cases} 0 \iff \text{sdr}_j.\text{inset} \exists \text{dep}_\text{rel} d \in \text{outset} \wedge \text{dep}_\text{rel} \in \text{inset} \\ 1 \iff \exists \text{dep}_\text{rel} d \in \text{outset} \wedge \text{dep}_\text{rel} \in \text{sdr}_j\text{inset} \end{cases}$$

In other words, the function $r$ returns a value 1 only if the service associated to $\text{sdr}_j$ depends in some way from the service $\text{sdr}_k$. Then by using such a function, we can say that:

**Theorem**: with respect to the representation given previously, a damage to a service associated to the dependence record $\text{sdr}_j$ provided by a system $\text{K}$ has an effect on a service associated to a dependence record $\text{sdr}_p$ $\iff \exists a$ sequence $\text{sdr}_j, \text{sdr}_k, \text{sdr}_l, \ldots, \text{sdr}_p | r(\text{sdr}_j, \text{sdr}_k) \cdot r(\text{sdr}_k, \text{sdr}_l) \cdot \ldots \cdot r(\text{sdr}_p, \text{sdr}_p) = 1$

The proof of the theorem is, by construction, self-evident.

**Definition 6**: let $\text{Sb}$ be the set of services of a system $\text{B}$, let be $\text{SK}$ the set of services of a system $\text{K}$, a disservice $D$ is an Emergent Disservice $\iff \exists$ a sequence $\text{sdr}_j, \text{sdr}_b, \text{sdr}_c, \ldots, \text{sdr}_z, \text{sdr}_p | r(\text{sdr}_j, \text{sdr}_b) \cdot r(\text{sdr}_b, \text{sdr}_c) \cdot \ldots \cdot r(\text{sdr}_z, \text{sdr}_p) = 1$, with $j \in \text{Sb}$ and $p \in \text{SK}$ and the fault is originated in $\text{Sb}$.

IV. INTERDEPENDENCY ANALYSIS IN A RISK ASSESSMENT PROCESS

By the use of the formal description presented it is possible to model in an easy way the interaction existing among the different systems of a more complex System of Systems. However, such an approach, in order to result useful must to be integrated in a more complex and exhaustive risk assessment process. In this way, we obtain a double advantage: from one hand, by applying to the proposed approach a risk assessment methodology, we are able to quantify the impact of the disservice propagation. On the other hand, by using this approach in a risk assessment context, we are able to easily model interdependence relationships among systems which are part of a more complex one.

There exist in literature several types of risk assessment methodologies [2,22]. In particular, the work of Masera and Nai [22] presents some suitable characteristics allowing to easily integrate the intersystem dependency description and analysis with the risk assessment process. In such a work, the authors present a risk assessment methodology tailored to the analysis of the ICT infrastructure of complex industrial systems. More in details, this methodology foresees that in order to assess the security of a system, it is necessary firstly to provide a description of the system itself, of its components, of its assets, of the interaction and the relationships among the components, the assets and the external world.

Such a description (expressed analytically by tables) could be used to identify in a systematic way the vulnerabilities affecting the whole system. These vulnerabilities are then described by some significant parameters and used to identify the threat that can be associated to the components and to the whole system. From the analysis of this information, one can derive the evaluation of the possible damages to the components, their propagation to the system and the consequent attack patterns. All these operations are quantified in some risk related indexes that are then employed to perform the evaluation of the security failure risk and the countermeasures.

The approach adopted is based on five main steps:

- **System Description**, in which the system is described in term of components, services, subsystems, assets and flows.
The methodology then can be extended in this way:

- **Vulnerability Assessment**, in which the vulnerabilities affecting the components of the system are identified.
- **Threat Assessment**, in which the threats to the system are described and evaluated (in terms of severity and plausibility).
- **Attack Assessment**, in which the plausible and severe attacks are identified.
- **Risk Assessment**, in which the system exposure and risk are evaluated.

As it is possible to see such an approach have several points in common with what we propose here, especially in terms of the elements described and involved. Moreover, of particular interest is the accent that the authors pose on the relevance of the services as main vehicle of “transmission” of threats and attacks.

It is then possible to extend this methodology in order to allow its application in the context of risk assessment of **System of System**.

In the methodology of Masera and Nai in fact, the entity which represents the external world is the “Stakeholder” which is the entity which take advantage of a service provided by the system. In our context, an external system which requests a service to another system, can be easily equated to a Stakeholder.

The methodology then can be extended in this way:

- **Systems Description**, in which every system of the SoS under analysis is described in terms of components, services, subsystems, assets and flows. In this phase a new sub-phase is introduced: the **intersystem service description**, which, according with the formal approach described previously, is dedicated to the identification of the services which can be requested by external systems (we call these services **Boundary Services**). These services have to be described even in terms of dependencies with the internal service of the owner system.

- **Vulnerability Assessment**, in which the vulnerabilities affecting the components of the system are identified. The evaluation of the severity of these vulnerabilities has to be made taking into account if the vulnerability affects a component which is involved in the realization of a Boundary Service. The concept of **Disservice Chain** (i.e. the chain of disservices caused by a failure in a certain component) is then extended to all the systems having some service relation with the one analyzed.

- **Threat Assessment**, in which the threats to the system are described and evaluated (in terms of severity and plausibility). Even in this case the threat evaluation and rating must take in consideration the new information about the Boundary Services

- **Attack Assessment**, in which the plausible and severe attacks are identified. The validation of the attacks must take into consideration the effects that an attack realized on a system \( X \) has on a service-connected System \( Z \)

- **Risk Assessment**, in which the system exposure and risk are evaluated.

**V. CONCLUSION**

The study of the interdependencies existing among collaborating systems is extremely relevant in the context of risk assessment. This is especially true considering the evaluation of ICT infrastructures, where the effects of a local negligible failure in a system may cause a potential “disaster” on the other side of the world. In this paper we have presented a formal approach to model these interdependencies based on the concept of System of System, and adopting a service oriented analysis. Moreover, we have showed how to integrate such an approach in an existing risk assessment methodology.

Even though, by means of this approach, it would be possible to correctly identify these interdependencies and use the derived knowledge to extend a risk assessment process to the analysis of a SoS, this only a partial view and the methodology need to be improved.

We plan in fact, as future work, to extend the present work in the direction of the study of the interconnection derived by the exchange of Information (Information Asset Exchange).

**REFERENCES**


