Availability of healthcare services in a network-based scenario

Roberto Setola

Complex Systems & Security Lab
Università Campus Bio-Medico di Roma
via E. Longoni 83, 00155 Roma, Italy
E-mail: r.setola@unicampus.it

Abstract: In this paper, we illustrate how the third millennium healthcare system is strongly related to many networked infrastructures. This contributes to improving its efficiency and efficacy but, at the same time, introduces new and very dangerous elements of vulnerability that should be carefully taken into account. These vulnerabilities are mainly induced by the presence of different, and many times hidden or poorly known, dependencies and interdependencies existing among the different infrastructures. These interdependencies induce an augmentation of possible threats and the occurrence that negative consequences of a failure might be largely amplified owing to the presence of the cascade and/or feedback phenomena. To better illustrate the possible catastrophic scenarios induced by this framework, the Input-output Inoperability Model (IIM) has been applied on a modern hospital to compare its behaviour, in the presence of a failure in the IP network, with that of a more classical structure.

Keywords: interdependencies; complex network; e-health; critical infrastructures; Input-output Inoperability Model; IIM.

Reference to this paper should be made as follows: Setola, R. (2007) 'Availability of healthcare services in a network-based scenario', *Int. J. Networking and Virtual Organisations*, Vol. 4, No. 2, pp.130–144.

Biographical notes: Roberto Setola received his Laurea degree in Electronic Engineering (1992) and Research Doctorate in Electronic Engineering and Computer Science (1996) from the University of Naples. From 1999 to 2004, he worked at the Italian Prime Minister's Office. At present, he is Assistant Professor of Automatic Control at the University CAMPUS Bio-Medico di Roma. He is the Technical Representative of the Italian Government Working Group on Critical Infrastructure Protection, and a member of the G8 Senior Experts' group for Critical Information Infrastructure Protection. He wrote three books about the simulation of dynamic systems and more than 80 scientific papers related to the modelling and control of complex systems (electro-mechanical, biological and social) and about critical infrastructures.

1 Introduction

In recent years, healthcare systems have largely changed the way in which their services are produced and supplied to improve the quality (*e.g.*, better diagnosis and treatments), to guarantee more comfort to the patients, to increase the efficiency of the systems (*e.g.*, reducing time-in-hospital, and generally, any type of side effects), and to have a more rational use of money.

A key component of this revolution is the spread of Information and Communication Technologies (ICT) at all levels and in any field of the healthcare systems. Indeed, because of the power of ICT to make interoperable the different elements and actors, useful synergies have been exploited to better use these resources.

To fully achieve these results, however, the different apparatuses, components and systems (once autonomous and insulated entities) began to be integrated into networks. In this framework, even if each component still performs its specific task, any service (see Box 1) is provided by the concurrent activities of many actors and elements of the network.

Box 1 Assets versus Infrastructures

In a network-based organisation, the importance of infrastructures is increased with respect to that of assets, the focus being on *services* rather than on (physical) products

Asset: element able to supply a specific service to an easily identifiable set of users (generally located in the proximity of the asset itself)

Infrastructure: system composed of many interoperable elements, geographically dispersed, able to supply generalist products (that have to be specialised by the end-user) to an unforeseen set of users, difficult to identify and estimate

Service: any activity identifiable by a tangible benefit for the end-user.

Indeed, the customer (in our case the patient) is put into the centre of a technological web that supplies services highly customised and able to satisfy the specific requirements of the customer in terms of quality and costs, also taking into account other attributes, such as availability and accessibility. In this framework, from the patient's point of view, any single element of the system is less and less important because the network, as a whole, provides the services. Indeed, these are more and more available via a multitude of channels (from hospital to telecare) and in a fashion that hides the activities performed by any single element of the network. This is obtained by integrating multichannels delivery strategies into the front-ends and making interoperable the different back-end elements.

Implicit in this change of paradigm is the increased role played by technological infrastructures in the healthcare systems. These infrastructures, which until a few years ago were confined to complementary activities, are today becoming the backbone of any healthcare system.

Unfortunately, this introduces many *dependencies* and *interdependencies* links (see Box 2) among the different components. This represents the real weakness of this scenario. Indeed, even if a network-based healthcare system is more robust than a model composed of many single 'assets' with respect to components' failure, it appears to be more fragile to 'catastrophic' events. The presence of these interdependencies (many of them neither designed nor considered at implementation time and actually poorly known or even completely hidden) exposes the system from one side to a huge variety of threats and makes it susceptible, because of the domino and cascade effects, to simultaneous failures of many services, as dramatically emphasised in healthcare and other sectors by the blackouts of 2003 (Italian Government Working Group on Critical Information Infrastructure Protection, 2004).

Box 2 Dependency and Interdependency

Dependency: is the capability of an infrastructure to influence the state of an other infrastructure. It is a *unidirectional* relationship.

Interdependency: is a *bidirectional* relationship between two infrastructures through which the state of each infrastructure is influenced, or is correlated to the state of the other.

Then, moving from a traditional heathcare scenario to a highly network-centred framework, we improve the capability to provide efficient, effective and economic services, but at the same time, we have to carefully consider also the other side of the coin. This paper is devoted specifically to pinning down some of them and to stimulate great attention to this topic.

The paper is organised as follows: Section 2 illustrates the role of networks inside the healthcare system. The Input-output Inoperability Model (IIM) is used in Section 3 to emphasise the fragility of this new paradigm, while some conclusive comments are collected in Section 4.

2 Healthcare in a networked framework

Until some decades ago, healthcare services were primarily supplied inside hospitals. The patient had to move from his/her home to the hospital, where different diagnostic and therapeutic treatments were provided. Moreover, inside the same hospital, the different tools and processes were insulated and autonomous. Patients, and also doctors, had to move from one tool to another, often placed in different areas, to acquire the different resources. Information provided by these tools was generally collected via paper records. These records were then physically moved (generally in a very inefficient way) from one side to the other in order to exchange information. In many situations, these records represented the most critical element in the healthcare system because of misunderstanding, errors and loss of information caused by their use. Nevertheless, its main drawback was the difficulty, or even impossibility, to retrieve information from paper records when these were needed in the future and/or outside the hospital.

This situation was largely inefficient, especially from the patient's point of view. Indeed, he/she had to spend a lot of time to move to and from hospital, had to suffer a great deal of stress supplying the same information over and over (very often in an incomplete, vague or erroneous manner) and eventually to suffer for errors and/or unavailability of information previously stored in some other records.

Thus we observed, as happened also in many other business sectors, a major change: the customer (*i.e.*, the patient) has been posed at the centre of a networked system. He/She has no more need to 'physically' move to reach the different providers; the services themselves are made available 'at any time, in any place', suitably customised via a multitude of channels to facilitate their use by the customer.

Obviously, in the healthcare framework, the *ubiquitous* concepts will never be completely possible nor desirable, but even in this sector we observe the consequences of these changes.

This implies an increased relevance, at least for the end-user, of the *service* with respect to that of the *asset* able to provide it (see Box 1). Indeed, in many cases, the user has no information on who actually provides the service (and from where). This contributes to improving the quality of the services (I am able to offer more qualified and specialised services in spite of geographical location) and, at the same time, to improving efficiency (because it is possible to better distribute loads, and to exploit synergy and scale economy).

This revolution is possible because the different elements are no longer insulated, but they are components of a network that allows one to share information, to support cooperation, to exploit redundancy and to implement supplementary strategies.

This new paradigm, however, imposes assigning a different role for the technological infrastructures.

In classical hospitals, these infrastructures were not strictly related with the core business (*i.e.*, supply care), but represented only complementary services. Indeed, each medical tool was able to autonomously operate without the support of any kind of infrastructure, eventually, with the help of some battery or auxiliary energy power.

On the other side, in a modern hospital, some *infrastructures*, *e.g.*, the IT network, represent important and irreplaceable components of the system.

To better understand the actual role played by technological infrastructures inside the healthcare system, we have to consider, as emphasised in Figure 1, at least three, not completely disjointed, types of networks:

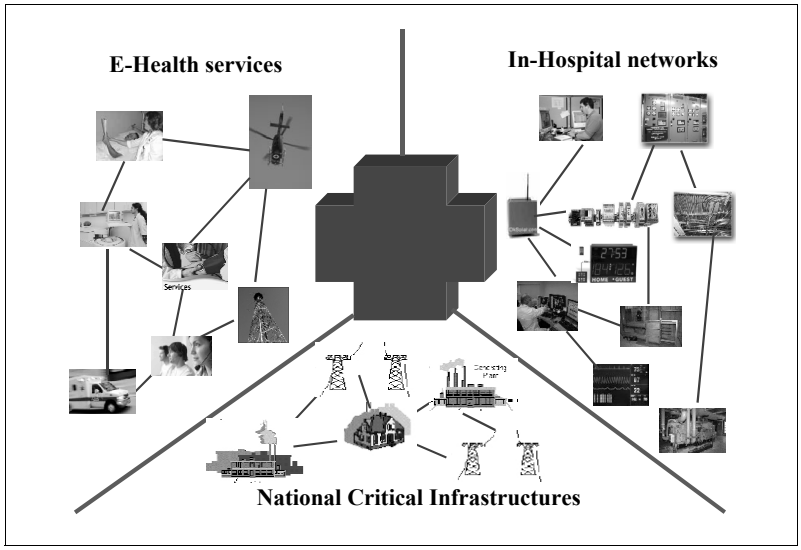
1 In-hospital network

2 e-health services

3 National critical infrastructures.

The first one represents the different networks exploited within the hospital; the second one, those needed to provide service in a remote fashion; the last one, the set of technological infrastructures at the base of every developed country.

Figure 1 The most relevant networks in the healthcare system



Considering the in-hospital networks, especially with the introduction of electronic case history, we observe that the different autonomous and isolated devices have been strongly integrated into a network. This has been obtained by exploiting the capabilities of ICT and IP-based connectivity. Moreover, in modern hospitals we observe that even environmental parameters (*e.g.*, temperature, humidity), bio-medical devices and infrastructures' status are monitored, and in some cases actuated, via an IP-based network. Nevertheless, an IP network, to correctly operate, needs the presence of other technological infrastructures, such as electric energy and air-conditioning (just to cite two). Even if each one of these infrastructures has been designed with a tree-like structure (which simplify management and failure impact analysis), because of the presence of many functional relations, the global system appears to be an intricate and complex graph. In this scenario, the presence of feedback mechanisms and cascade phenomenon, as illustrated in the next section, largely modifies the behaviour of any component.

In addition to in-hospital networks, we have to consider that more and more hospitals are supplying e-health services. Moreover, some in-hospital services are also provided in cooperation with remote structures (*e.g.*, teleconsulting or outsourcing diagnosis). This configures the second type of network, where the hospital represents a node of a huge and geographically dispersed system. Notice that, unlike the previous one, this network is only partially under the control of the hospital and largely depends on external providers. This introduces some new elements generally poorly considered in the management procedures (especially that for emergency): Which should guarantee redundancy connections from the hospital to the patient's home? In the presence of failure in the connection link, how should the hospital provide alternative service to e-health ones? How should the responsibility for onsite assistance be allocated: with a geographical distribution or with other criteria? Not only these and many other questions are without any answer, but in many hospitals, no one has posed these kinds of questions yet, even if they provide remote assistance.

These networks base their operativeness on the existence of the national *critical infrastructures*; *e.g.*, energy, telecommunications, water, transportation, banking and financial services (Dunn *et al*., 2006).

In recent years, for a lot of economical, social, political and technological reasons, we observed a rapid change in the organisational, operational and technical structures of these critical infrastructures. Indeed, for the same reasons that drive the changes in the healthcare system, critical infrastructures have become more and more interoperable and have extensively adopted off-the-shelf and open ICT solutions. Moreover, to effectively and profitably operate in the global market in the absence of monopolistic privileges, infrastructures' stakeholders have started to focus on their core business and to largely use outsourcing strategies (Donzelli and Setola, 2007).

Then, although designed as logically separated systems delivering different services, these infrastructures have become interdependent, each one relying (directly or indirectly) on the services provided by the others. This contributes to creating a very huge and complex system of systems that appears prone to cascade failures.

The criticality and the 'unpredictability' of the consequences of a failure inside one of these infrastructures have been emphasised by different episodes, as, for example, the communication blackout that occurred in Rome, Italy, at the beginning of 2004. In this case, the air-conditioning failure of a major node of the telecommunication network resulted in a five-hour blackout of land and wireless telecommunications (affecting almost all the telecom providers), malfunctions of the financial circuits, and problems at the Rome International Airport, where 70% of the check-in desks became unavailable (Italian Government Working Group on Critical Information Infrastructure Protection, 2004).

In addition to vulnerability to accidental and natural failures, critical infrastructures (also including healthcare systems) are becoming targets for terrorist and criminal actions (US Government, 2003a). Indeed, attacks could be carried out against critical infrastructures to create damage, panic and/or mistrust, or to increase the effects of more traditional acts of terrorism, *e.g.*, slowing down emergency services and delaying rescue operations (US General Accounting Office, 2003). In this context, cyber attacks represent very dangerous threats (US Government, 2003b).

Owing to the huge relevance of health services, and to be able to supply these services even in the presence of negative events, it is mandatory to understand how the presence of interdependencies may undermine the robustness of the whole system.

To better stress how a networked system is prone to large and catastrophic failures, in the next section we use the IIM to qualitatively analyse the consequences of a failure inside a modern (highly networked) hospital, comparing the results with that of a more traditional (not network-oriented) one.

3 Input-output inoperability analysis

In this section, to simplify the analysis, we focus only on the 'in-hospital network' and show that, even considering only this subset, a 'small' failure may induce generalised consequences able to concretely affect the capability of the whole hospital to provide health services.

To this end, we use the IIM proposed by Haimes and Jiang (2001). IIM is a simple tool able to emphasise how the presence of dependencies and interdependencies among the different components of a complex system may facilitate the spreading of degradation.

Haimes and Jiang (2001) set up this model building on the well-known theory on market equilibrium of the economy by Nobel Prize awarded Wassily Leontief. The IIM uses the same framework proposed by Leontief, but instead of considering how the production of goods or services of a firm influences the level of production of the other firms, it focuses its attention on the spreading of 'degradation' into a networked system. To this end, the authors introduce the concept of *inoperability*, defined as the inability of a system to perform its intended functions, and analyse how a given amount of inoperability inside one element influences the other components of the network.

In Haimes *et al.* (2005), the authors use this approach to analyse how inoperability induced by a High Altitude Electromagnetic Pulse (HEMP) affects the different sectors of the US economy and to estimate the recovery time under different hypotheses, while in Panzieri and Setola (2007), the approach is modified to explicitly consider also the spreading of failures.

The great interest in this approach is related to its simplicity, even if the results that it provides are, for many aspects, largely qualitative and oversimplified.

We use IIM to analyse what should be the negative consequence of a failure in the *IP network* of an hospital. To this end, we adopt a very crude approximation, modelling each technological infrastructure present within the hospital as an entity in which the level of operability depends, further to external causes, on the availability of 'resources' supplied by other infrastructures.

Then, an event (*e.g.*, a failure) that reduces the capability of the *i*-th infrastructure induces degradation also in other infrastructures that need the services or goods produced by the *i*-th infrastructure. This degradation may propagate, involving other infrastructures (cascade), or even exacerbate the negative consequences in the *i*-th one (feedback).

Mathematically, IIM describes these phenomena on the base of the level of inoperability associated with the different infrastructures. Specifically, the inoperability of the *i*-th infrastructure is coded via the variable x_i defined in the range [0, 1]. Specifically, $x_i = 0$ means that the infrastructure is fully operative, while $x_i = 1$ means that the infrastructure is completely inoperable.

The inoperability induced on the system by external causes u_i, also taking into account the presence of dependencies and interdependencies among the different components, is calculated via the following dynamic equation:

$$\mathbf{X}(k+1) = \max\left\{\mathbf{A}\,\mathbf{X}(k) + \mathbf{U}, \mathbf{1}\right\} \tag{1}$$

where $\mathbf{X} \in \mathbb{R}^n$ and $\mathbf{U} \in \mathbb{R}^n$ are vectors composed, respectively, of the level of inoperability and external failure associated with each one of the n different infrastructures considered in the scenario. $\mathbf{A} \in \mathbb{R}^{n \times n}$ is the Leontief matrix, in which entry a_{ij} represents the level of influence that the inoperability of the *j*-th infrastructure has on the *i*-th one.

We impose that $a_{ii} = 0 \ \forall i$ because we do not consider any recovery phenomenon. Notice that in the model, $a_{ij} = 1$ means that the *i*-th infrastructure is completely dependent on the *j*-th one, because a given amount of failure in the latter will directly induce an equal level of degradation into the *i*-th one.

In order to evaluate the level of dependencies of an infrastructure, we introduce the *dependency index*, defined as the sum of the Leontief coefficient along a single row:

$$\delta_i = \sum_j a_{ij} \qquad \text{(row summation)}. \tag{2}$$

This index represents a measurement of the robustness of the corresponding infrastructure with respect to the inoperability of the others. If this quantity is less than 1, *i.e.*, $\Sigma_j a_{ij} < 1$, then the *i*-th infrastructure preserves some working capabilities (*e.g.*, thanks to the presence of buffers, UPS, *etc*.) in spite of the level of inoperability of its suppliers. On the other side, when $\delta_i = \Sigma_j a_{ij} > 1$ the operability of the *i*-th infrastructure may be completely nullified even if the supplier infrastructures show some residual capabilities.

The influence that a specific infrastructure has on the global system may be evaluated considering the *influence gain*, *i.e.*, the sum along a column of the Leontief coefficients:

$$\rho_j = \sum_i a_{ij} \qquad \text{(column summation)}. \tag{3}$$

A large value for this index means that the inoperability of the *j*-th infrastructure will induce significant degradation into the whole system. Specifically, when $\rho_j = \Sigma_i a_{ij} > 1$, the negative effects induced by cascade phenomena on the other infrastructures are more relevant, in terms of inoperabilities, than those affecting the *j*-th infrastructure. The opposite happens when $\rho_j < 1$.

The hardest task to be performed in order to apply IIM is the estimation of the Leontief matrix **A**. In Haimes *et al.* (2005) this quantity is evaluated using the economic statistical data provided by the Bureau of Economic Analysis (BEA). In this paper, we follow a different strategy, evaluating these coefficients, as better explained later, on the basis of information collected directly on the field.

We applied this model to the actual and to the in-building hospital of our university. Indeed, actually the CAMPUS has a traditional hospital, but it is building a new one with a highly modern idea. The technological infrastructures on which we focus our analysis are reported in Table 1.

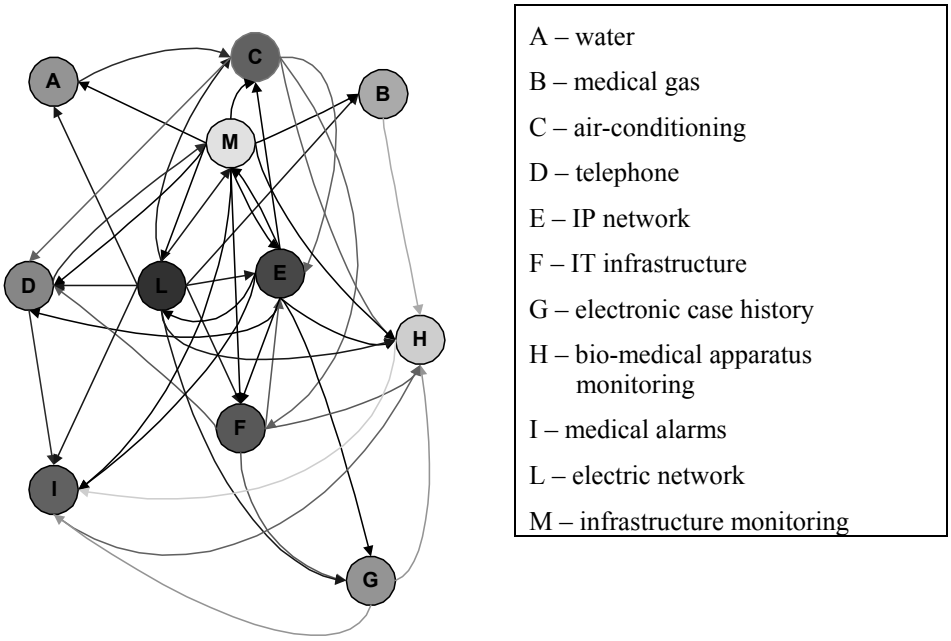
Table 1 Technological infrastructures considered in the analysis

Technological infrastructures
A – water
B – medical gas
C – air-conditioning
D – telephone
E – IP network
F – IT infrastructure
G – (electronic) case history
H – bio-medical apparatus monitoring
I – medical alarms
L – electric network
M – infrastructure monitoring (SCADA)

In a modern hospital, as reported in Figure 2, analysing the different infrastructures, we record a very complicated web of reciprocal influences. Inside this web, *Electric network* (L), *IP network* (E) and *Infrastructure monitoring* (M) represent hubs with a higher out-degree (*i.e.*, number of outgoing links). This means that these infrastructures have a large influence on the others (they have many non-null terms in the influence gain). On the other side, *Bio-medical apparatus monitoring* (H) has a higher in-degree (*i.e.*, number of incoming links). Then the capability of this infrastructure to correctly operate largely depends on the operability of the other infrastructures. Consequently, in the corresponding row of the Leontief matrix, many elements will be different from zero and this suggests that the corresponding *dependency index*, *i.e.*, δ_H, should be quite large, making more 'concrete' the risk that this infrastructure would exhibit large degradations owing to failures in the other infrastructures.

However, to better understand the role played by the different infrastructures and to identify their most critical elements, we have to consider also the degree of influence that characterises the different links.

Figure 2 Inoperability influence graph for the modern hospital



To this end, the Leontief coefficients associated with traditional and modern hospitals have been estimated via interviews, both with the managers of the different infrastructures, and with architects, engineers and technicians involved in the design of the new hospital. This information has been merged with 'experiences' coming from doctors and medical assistants. Moreover, as proposed in Panzieri and Setola (2007), we also used schemas and maps of all the infrastructures to evaluate physical, geographical and cyber interdependencies (for more information on this taxonomy, see Rinaldi *et al.*, 2001).

Comparing the Leontief matrices of Tables 2 and 3, one can notice that (except for the relevance of the telephone network) there is a generalised augmentation of the influence coefficients in the modern hospital.

Table 2 Leontief matrix for a traditional hospital. Notice that in this case, *G* represents paper-based case history. The matrix has been bordered with the dependency δ_i and influence ρ_j indexes.

	A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*L*	*M*	$\delta_i = \sum_j a_{ij}$
A	0	0	0	0	0	0	0	0	0	0	0,03	0,03
B	0	0	0	0	0	0	0	0	0	0,3	0,1	0,40
C	0,03	0	0	0	0	0	0	0	0	0,6	0,05	0,68
D	0	0	0,10	0	0	0,01	0	0	0	0,15	0,03	0,29
E	0	0	0,15	0	0	0,10	0	0	0	0,3	0,05	0,60
F	0	0	0,20	0	0,25	0	0	0	0	0,2	0,05	0,70
G	0	0	0	0	0	0	0	0	0	0,05	0	0,05
H	0,05	0,15	0,20	0	0,10	0,05	0	0	0,05	0,3	0,05	0,95
I	0	0	0	0,10	0,05	0	0	0	0	0,25	0,20	0,60
L	0	0	0	0	0	0	0	0	0	0	0,07	0,07
M	0	0	0	0	0,03	0	0	0	0	0,08	0	0,09
$\rho_j = \sum_i a_{ij}$	0,08	0,15	0,65	0,10	0,43	0,16	0	0	0,05	2,23	0,63	

Table 3 The Leontief matrix for a modern hospital. Notice that in this case, *G* represents electronic case history. The matrix has been bordered with the dependency δ_i and influence ρ_j indexes.

	A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*L*	*M*	$\delta_i = \sum_j a_{ij}$
A	0	0	0	0	0	0	0	0	0	0,05	0,06	0,11
B	0	0	0	0	0	0	0	0	0	0,30	0,13	0,43
C	0,03	0	0	0	0,08	0	0	0	0	0,60	0,08	0,79
D	0	0	0,10	0	0,40	0,10	0	0	0	0,15	0,04	0,79
E	0	0	0,15	0	0	0,18	0	0	0	0,35	0,09	0,77
F	0	0	0,20	0	0,43	0	0	0	0	0,23	0,06	0,92
G	0	0	0	0	0,63	0,87	0	0	0	0,39	0	1,89
H	0,05	0,15	0,20	0	0,24	0,19	0,31	0	0,05	0,42	0,08	1,69
I	0	0	0	0,08	0,09	0	0,02	0,02	0	0,29	0,21	0,71
L	0	0	0	0	0,02	0	0	0	0	0	0,09	0,11
M	0	0	0	0,14	0,04	0	0	0	0	0,22	0	0,40
$\rho_j = \sum_i a_{ij}$	0,08	0,15	0,65	0,22	1,93	1,34	0,32	0,02	0,05	3,00	0,84	

In Table 2, the *dependency index* δ_i, which represents a measurement of the robustness of the corresponding infrastructure with respect to the inoperability of the others, varies from 0,05 (associated with the paper-based *Case history* (G)) to 0,95 (of the *Bio-medical apparatus monitoring* (H)). Because this quantity is considerably less than 1 unit for

almost all the infrastructures, we may infer that in a traditional hospital, the different infrastructures were substantially autonomously and able to correctly supply their services without the need for the resources provided by the other infrastructures.

On the other side, in a modern hospital (Table 3), this quantity varies from 0,11, (corresponding to *Water infrastructure* (A)), to 1,89 (related with the *Electronic case history* (G)). Moreover, *Bio-medical apparatus monitoring* (H) shows a very high value (1,69). This means that there is a generalised increase of interdependencies but also an augmentation of fragility because the failure of any infrastructure has a direct influence on the capability of the other infrastructures to correctly perform their own work.

Curiously, the case history infrastructure, which in the traditional hospital is one of the less sensitive elements with respect to infrastructures' failures, becomes one of the most sensitive one in the modern hospital (where the electronic version is adopted).

The level of influence that the different infrastructures exercise (*i.e.*, the influence gain, defined as the sum for the columns of the Leontief matrix $\rho_j = \Sigma_i a_{ij}$) varies, for the traditional hospital, from 0 (*Case history* (G) and *Bio-medical apparatus monitoring* (H) infrastructures have practically no impact on the other infrastructures) to the 2,23 of the *Electric network* (L). The large value of this last coefficient emphasises the cornerstone role played by electricity in a traditional hospital.

If we look at the modern hospital, we see that the influence gain varies from 0,02 (associated with the *Bio-medical apparatus monitoring* (H)) to the value 3 of the *Electric network* (L). In this configuration, however, the influence gains associated with the *IP network* (E) and that of the *IT infrastructure* (F) are greater than 1 and equal to 1,93 and 1,34, respectively. This illustrates two elements. First, the importance of the electric network is increased and it is still the most critical infrastructure within the hospital. Second, as mentioned before, the capability of each single infrastructure to autonomously operate has been reduced because of the need to use the services provided by the others. Obviously, this makes the whole system more prone to amplifying negative consequences owing to the cascade phenomenon.

To compare the behaviour of the two configurations, we analyse the overall consequences induced by a failure that reduces by 10% the operability of the *IP network* (E).

Figure 3 shows the behaviour of the traditional hospital. The overall levels of inoperability, *i.e.*, the steady-state solution of Equation (2), are reported in Table 4.

In this scenario, we observe that the other infrastructures are only marginally influenced by the failure in the *IP network* (E). Only *IT Infrastructure* (F) and *Bio-medical apparatus monitoring* (H) show a degradation greater than 1%.

The consequences of the same failure in the modern hospital, as shown in Figure 4, are more relevant (see Table 5).

It is evident that in this case, there is an increment in the *IP network* inoperability (due to feedback) but also a generalised diffusion of inoperability. Indeed, except for *Water* (A), *Medical gas* (B) and *Electricity* (L), all the infrastructures show an inoperability level greater than 1%. The highest rate of inoperability is shown by the *Electronic case history* infrastructure (G). It reaches a degradation of about 12%.

Figure 3 Impact scenario induced by a failure that reduces by 10% the operability of the IP network (E) in a traditional hospital. Notice that in the steady state, there is a limited increment in the inoperability of the IP network, while the other infrastructures are quite unaffected (only IT infrastructure (F) show a degradation higher than 2%).

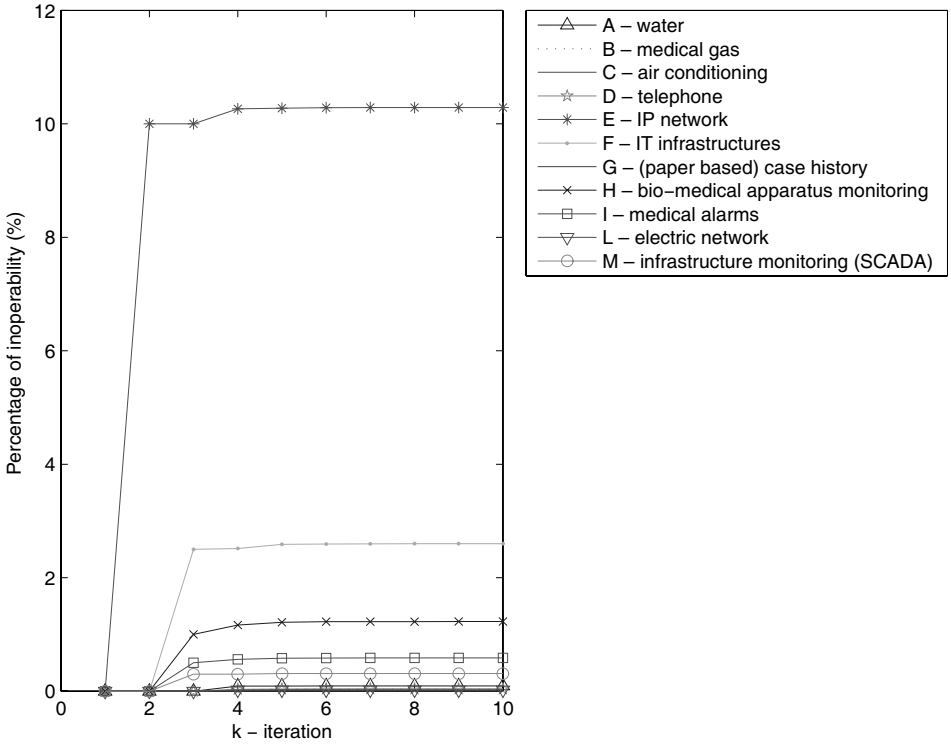
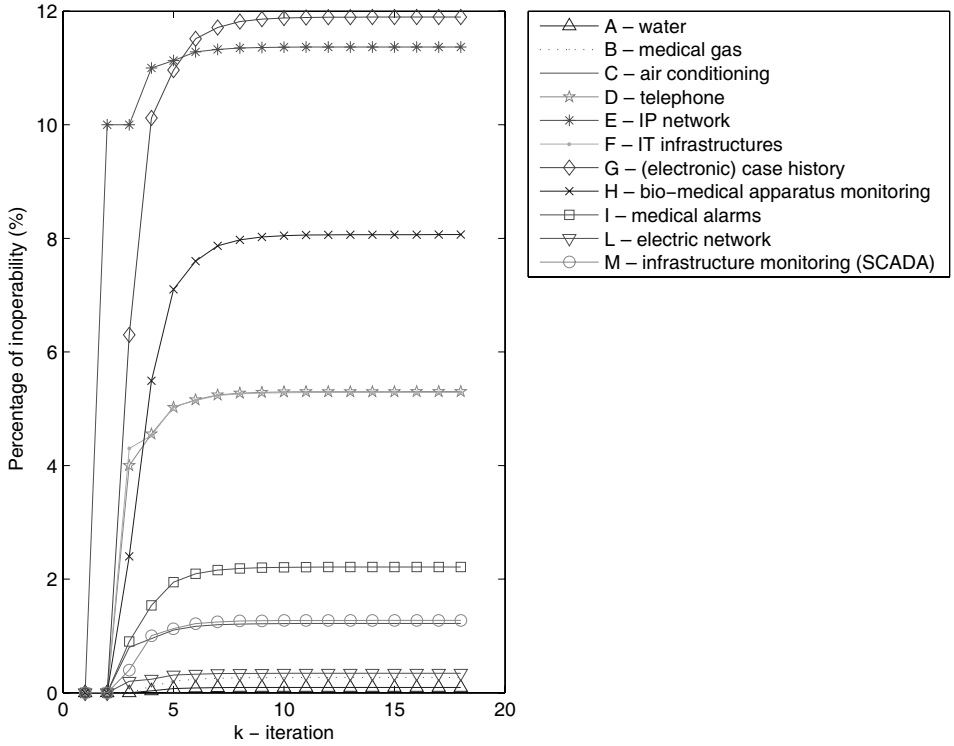


Table 4 Steady-state level of inoperability associated with the different infrastructures for a traditional hospital in the presence of a 10% failure in the IP network

Hospital infrastructures	*Steady-state level of inoperability (%)*
A – water	0,09
B – medical gas	0,04
C – air conditioning	0,03
D – telephone	0,04
E – IP network	10,29
F – IT infrastructures	2,60
G – paper-based case history	0,001
H – bio-medical apparatus monitoring	1,23
I – medical alarms	0,59
L – electric network	0,02
M – infrastructure monitoring	0,31

Looking at Table 3, one can recognise that the direct influence of the *IP network* (E) on the *Electronic case history* (G) is $a_{GE} = 0{,}63$. Then, neglecting interdependency phenomena, we should have predicted a degradation of about 6%. Nevertheless, as shown, the presence of the interdependencies amplifies the consequences of the failure producing an inoperability level that is quite the double of that foreseen in an atomistic analysis.

Figure 4 Impact scenario induced by a failure that reduces by 10% the operability of the IP network (E) in a modern hospital. Notice that almost all the infrastructures show a significant degradation and that the worst condition is that of the electronic case history system (G), which is affected by an inoperability of about 12%.



Obviously, because of the importance (and thanks to technological improvements) of the different infrastructures within the modern hospital, they are designed, conducted and managed with higher standards in order to improve their efficiency, robustness and business continuity. Thus, it is very difficult that 'normal accident' may induce serious degradation in any modern infrastructure. Indeed, in everyday activities, we observe that in a modern hospital, almost all the consequences of any negative events that affect, as in our example, IP networks are absorbed without any appreciable degradation (thanks to redundancy, back-up elements, *etc*.). However, as our analysis and different real-world episodes show, if an event is able to induce tangible degradation into a single infrastructure, it is largely amplified owing to interdependencies and domino effects, to the point that it may induce generalised inoperability in the whole system.

Table 5 Steady-state level of inoperability associated with the different infrastructures for a modern hospital in the presence of a 10% failure in the IP network

Hospital infrastructures	*Steady-state level of inoperability (%)*
A – water	0,09
B – medical gas	0,27
C – air-conditioning	1,22
D – telephone	5,30
E – IP network	11,37
F – IT infrastructure	5,29
G – electronic case history	11,89
H – bio-medical apparatus monitoring	8,06
I – medical alarms	2,21
L – electric network	0,34
M – infrastructure monitoring (SCADA)	1,27

4 Conclusion

An emergent paradigm in the developed countries is the increased relevance of networked systems in many sectors. Indeed, technological, economical, sociological and political reasons suggest, or even impose, adopting a service-oriented paradigm where the customer (the patient) is collocated into the centre of a complex web of technological infrastructures.

This largely contributes to improving the quality of our life.

Specifically in the healthcare framework, exploiting the facilities provided by this new paradigm, it is possible to supply health services with very high quality and better comfort for the patient; at the same time, we are able to reduce their costs.

This scenario, however, which is mainly dominated by the interdependencies phenomenon, has to be carefully understood in order to also manage its side effects.

Indeed, even if this framework appears very robust with respect to 'normal' accidents, it is globally vulnerable to some events. Nearly all failures are absorbed with practically no consequences to the end-users, but in the presence of some 'rare' events (actually neither identifiable nor predictable), the whole system appears incredibly fragile.

References

Donzelli, P. and Setola, R. (2007) 'Identifying and evaluating risks related to external dependencies: a practical goal-driven risk analysis framework', *Int. Journal of Risk Assessment and Management (IJRAM)*.

Dunn, M., Wigert, I., Wenger, A. and Metzger, J. (2006) *CIIP Handbook 2006*, ETH, Zürich, Switzerland.

Haimes, Y. and Jiang, P. (2001) 'Leontief-based model of risk in complex interconnected infrastructures', *Journal of Infrastructure Systems*, pp.1–12.

Haimes, Y., Horowotz, B., Lambert, J., Santos, J., Lian, C. and Crowther, K. (2005) 'Inoperability Input-output Model (IIM) for interdependent infrastructure sectors: theory and methodology', *Journal of Infrastructure Systems*, pp.67–79.

Italian Government Working Group on Critical Information Infrastructure Protection (2004) *La Protezione delle Infrastrutture Critiche Informatizzate-La Realtà Italiana* (in Italian).

Panzieri, S. and Setola, R. (2007) 'Failures in critical interdependent infrastructures', *Int. J. Modelling, Identification and Control (IJMIC).*

Rinaldi, S., Peerenboom, J. and Kelly, T. (2001) 'Identifying, understanding and analyzing critical infrastructure interdependencies', *IEEE Control System Magazine*, pp.11–25.

US General Accounting Office (2003) *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233, USA, www.gao.gov.

US Government (2003a) *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*, Washington, USA, www.whitehouse.gov/pcipb/physical.html.

US Government (2003b) *The National Strategy to Secure Cyberspace*, Washington, USA, www.whitehouse.gov/pcipb.