Reliability issues related to the usage of Cloud Computing in Critical Infrastructures

Oscar Diez
Head of Datacentre, European Medicines Agency, London, UK

Andres Silva
GIB Research Group, Facultad de Informatica, Universidad Politécnica de Madrid, Spain

ABSTRACT: The use of cloud computing is extending to all kind of systems, including the ones that are part of Critical Infrastructures, and measuring the reliability is becoming more difficult. Computing is becoming the 5th utility, in part thanks to the use of cloud services. Cloud computing is used now by all types of systems and organizations, including critical infrastructure, creating hidden inter-dependencies on both public and private cloud models. This paper investigates the use of cloud computing by critical infrastructure systems, the reliability and continuity of services risks associated with their use by critical systems. Some examples are presented of their use by different critical industries, and even when the use of cloud computing by such systems is not widely extended, there is a future risk that this paper presents. The concepts of macro and micro dependability and the model we introduce are useful for inter-dependency definition and for analyzing the resilience of systems that depend on other systems, specifically in the cloud model.

1 INTRODUCTION

Virtualization and Cloud computing have changed the way organizations are using ICT services. Cloud services are starting to be used for almost all types of organizations including organizations that are involved in CI (Critical Infrastructure) systems. As with virtualization at the beginning, it is been introduced by stages, and starting with services that are not part of critical systems. There is a long list of reasons for using the cloud model as elasticity, mobility, costs and the possibility for the organization of focusing on the core business and treat the ICT as the 5th Utility. The main risk with the use is not what we see, but what we do not see, the complexity increase, and new variables are introduced, in most cases without the knowledge of the organization. Egan (Egan 2007) use the term "rafted networks" to describe this type of systems that began with simple systems that evolve into very complex systems in an unplanned manner.

The utilization of cloud computing will change the current ICT models for most of the industries and organizations, including public ones, impacting the current systems, the reliability and the risks associated to these new models. It is considered as well that in the next years and due to the number of systems both private and public, cloud computing facilities will be consider a critical infrastructure, and similar protection to other critical infrastructure systems should be implemented. It should be considered the interdependencies for these systems, and assess the impact of possible cascade effects. This paper exposes these risks; the effects on the reliability, and possible solutions for improve the visibility of the risks and try to improve the reliability.

At the beginning of the paper some examples are presented of the use of cloud computing by critical infrastructure systems, as well as some of the risks related to the reliability of these systems. In the next sections, an overview of current proposals is presented. In the final sections, a model to represent the dependencies of these systems is described; the model is based in the concepts of macro and micro dependability that are explained. These concepts and model do not pretend to replace previous ones like the coupling and hidden interactions defined by Perrow (Perrow 1999), but complement them, so both could be applied. As well an example is used to illustrate the use of this model and possible implementation in case of being used by organizations. No distinction is done related to the different type of cloud models and architectures, but most of the times we will use as examples Infrastructure as a Service model, and the Private/Community cloud for micro dependability, and Public/Community for Macro Dependability. The cloud model concepts are not described here as this is not the focus of the paper and there is plenty of information in other publications like “A view of cloud computing” (Ambrust 2010) or the Security Guidance from the CSA (CSA 2009).

2 EXAMPLES OF CLOUD SERVICES IN POTENTIONALY CRITICAL SITUATIONS

Most of the examples of uses of cloud computing in critical systems are using the Software as a Service or Infrastructure as a service model. As has been expressed before in most of the cases these systems are replacing the ‘non-critical’ parts of the system. The main reasons to move to these technologies are costs and improved functionality.

2.1 *Cloud offering for SCADA systems*

Supervisory Control and Data Acquisition (SCADA) system, Distributed Control Systems (DCS), and other control systems are found in industrial sectors and critical infrastructure. These are known under the general term Industrial Control System (ICS). ICS are normally used in industries such as electrical, water, oil and gas. The reliable operation of infrastructure depends on computerized systems and SCADA. In the last years different vendors are providing solutions for integrate these systems with Web Dashboards that live in the cloud. The information of collected by these devices can be viewed and controlled from different types of devices from different locations. An example of an issue with SCADA systems has been the problem with the Stuxnet virus (Schneier 2010). This It is the first discovered worm that spies on and reprograms industrial systems. It was specifically written to attack Supervisory Control And Data Acquisition (SCADA) systems used to control and monitor industrial processes. This particular virus is not related to cloud systems, but what will be the effect of a virus like this in a service similar to the previous example offered by a cloud provider where the services are used by multiple tenants?

2.2 *Department of defense rapid access computing environment (RACE)*

The pentagon cybersecurity Robert Lentz (Lentz 2009) presented the benefits of private cloud computing for DoD. To meet this, the Defense Information Systems Agency (DISA) is trying a DoD-managed cloud computing environment called RACE, which enables DoD users to access virtual services and storage from a Web portal. DISA currently manages the IT infrastructure for 4 million DoD users and operates 14 data centers over the world.

The RACE portal defines this system as: “This quick-turn computing solution uses the revolutionary technology of cloud computing to give you the platform that you need today, quickly, inexpensively and, most importantly, securely.” Currently the system as described by the DoD is not used for Critical functions of the DoD, but more for new test systems (i.e. YouTube for troops and families) (Kubic 2008), but this could change soon due to the success of the system.

2.3 *Critical Government services in Peru*

IBM and FONAFE (Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado) are working on the creation of a private cloud infrastructure for centralizing the IT operations of 10 government companies that provide critical services like transportation, power utility, postal, port shipping in Peru. This will include the consolidation of 10 datacentres, using an outsourced model based on private cloud. The purpose is to reduce costs and improve efficiency.

2.4 *Radio system for emergency services (SaaS)*

The purpose of this system is to allow the fire brigade, police, emergency management and other type of public agencies to connect their private push-to-talk radio systems to others inside their agency and connect as well with other agencies that has been authorized previously. These tasks are not executed in their local servers and instead are moved into shared data centers accessed via the Internet.

There are several benefits described by these companies on the use of these infrastructures, for these agencies, most of them related to the use of Cloud systems. The main benefits are the low entry barriers of cost for using these technologies, as there is no need of big investment on interoperability infrastructure, as this is changed for a pay-per-use model.

2.5 *Nasa Nebula IaaS*

Nebula is an open-source cloud computing project and service created by NASA (Nebula 2010). It was developed to provide an alternative to the costly construction of additional data centers used by NASA scientists or engineers require additional data processing. Nebula as well provides a simplified way for NASA scientists and researchers to share large, complex data sets with external partners and the public. The model is based on the open standard “OpenStack” for open source cloud computer that follows a similar model to Linux, and is based on two key components, OpenStack

Compute that is software to provision and manage large groups of virtual servers, and OpenStack Object Storage, for creating redundant, scalable object storage using clusters of commodity servers to store large quantities of data.

3 RELIABILITY IN CLOUD SERVICES

Reliability is defined as the continuity of service, or the probability that a system or service remains operable for a specific period of time, or the ability of a system to perform its required functions under stated conditions for a specific period of time (Sterbenz 2010). And is normally measured in terms of the MTTF, or mean time to failure, based on data that is accumulated after a long use of the systems based on experience on that system. The formula used for measure the reliability is defined (Dhillon 2003) by:

$$R(t) = 1 - \mid f(t)a$$

Where R(t) is the reliability at time t and f(t) is the failure density function. This is used together with the reliabilities networks (Dhillon 2003), including the series, parallel, series-parallel, parallel-series and standby systems. These concepts, which are used for all kind of systems for calculating reliability, can be used in the model described later in this paper.

For most of the cloud services the contracts and SLAs are defined based on availability, and not always based on previous data, but on estimation based on the provider's criteria. All the main concerns that apply to use of Internet or networks for CIs applies as well to the cloud services, because most of them are provided using interconnected datacentres over networks and most of cases the Internet, as well the access to these systems is done over internet. On this paper we will focus in the reliability, some pros and cons for each cloud model related to reliability are described in table 1, but other aspects should be covered in the use of cloud services for CIs, especially legal, regulatory compliance, response, recovery and security. Cloud services are here to stay, and will become a new utility, so why not to use it in the same way that most of CIs industries use other utilities like water or electricity supplies? There are two main differences, one is complexity associated with the cloud model that his higher that in other models, the second is the time that took to these utilities to become reliable, as we know it now, and basically all of them are now in a very mature stage. Even in these cases, for CIs there are systems to improve reliability and availability when these utilities fail, like electrical generators or water tanks for chemical plants with continuous processing.

Table 1. Cloud models and reliability.

Model	Public	Community	Private
Pros	.elasticity & absorb demand .Geographical distribution .Large pool .Low control	.medium to full control .common requirements	.governance .monitoring .Full control of solution .less prone to attacks
Cons	.monitoring is difficult .prone to attacks .issues related to Tenancy .Lack of governance	.trust on other members of community. .smaller pool than public	.small pool .elasticity & absorb demand .lack of geo-redundancy
Managed by	External provider	Oraganization/ External	Organization

3.1 *Private clouds*

In the case of the private clouds, usually the customer does the design and control of the solution, and can control most of all of the supply chain involved in the service. This provides the possibility as well of implement services that could not be provided on other models like specific fail-safe or cluster mechanisms, as well as a closer management of the solution. It is possible as well to specify the system in detail and define SLAs for the service based on the requirements of the solutions. The solution can be tested thoroughly including all the components and a detailed business continuity plan can be created (except for geo-redundancy requirements). The main disadvantage of this model is that is more expensive than the others, due to the economies of scale of other models. It is true that not always the reliability and availability is better, because usually in public or community models due to the bigger number of resources to serve peaks or DOS attacks. Other issue that can affect the reliability in some cases is the lack of geo-redundancy in business continuity.

In general, even if this model in theory could provide more reliability and availability due to the fact that can be customized, in reality and in long term, could not be similar to the redundancy or the availability offered by a public cloud provider. Private cloud models can be used for services where the public o community ones cannot be used, and as a staged approach to the use of other models. Private model is a good candidate for CI organizations that would like to use cloud services, as the current public services offer solutions for non-critical services or average enterprise services. Some vendors, like VMWare with vcloud offerssolutions for IaaS that permit migrate virtualize environments to internal clouds, and in a later stage move with minimum changes to a hybrid or public cloud.

3.2 *Public clouds*

The main benefits from this model come from the economy of scale factor, and the fact that the pool is very large. The reliability is high due to the high number of hardware resources and the simplification of the infrastructure model. The control of the infrastructure is done by the vendor, as well as the business continuity strategy, that commonly is geo-located in different regions/countries. From the security and the monitoring point of view, the resources dedicated are higher.

But this homogenous and simplified model that improve economies of scale and lower costs, is at the same time the main issue now for CI systems, mainly for the lack of offer of specific services that meet the demanded services. This will change in the future and more services will be offered to meet the requirements of more critical systems. Other possible problem is the lack of control in all the stages of the supply chain of the service and the fact that this could be an attractive target for hackers. The SLAs for these services are normally pre-defined by the provider, and there are not possibilities for negotiation, doing difficult to agree in specific reliability and availability figures needed for CIs. Unlike the private or community models where the datacentres can be implemented inside the premises of the customers, in the public are outside, and the reliability of the Internet or wan network needs to be taken into account.Other possible issue that could affect reliability for public cloud is the reputation fate sharing, where basically the issues with one of the tenants could affect to other tenants, an example is the case (Joshi 2009) where premises of a datacentre where closed and disconnected by the FBI due to investigation of criminal activities of one of the tenants.

3.3 *Community clouds*

This model is a combination of the two previous models, with the benefits and in some cases weaknesses of both, limiting the costs due to a low cost entry barrier due to the fact that is divided between the different consumers, as well give more flexibility. In community clouds similar requirements of similar type of customers are met. This is particularly important for CI organizations, where the public cloud model does not meet the requirements and reliability criteria requested by these systems. Similar organizations or government agencies can use this model for improve reliability and elasticity due to the increase in resources, and at the same time reduce costs due to the economies of scale. The users that can be part of this community cloud are restricted and normally well known, reducing the risks of having multi-tenancy.

Due to the common requirements and objectives the same utilization patterns could appear, reducing elasticity and flexibility in high peaks. Could be a more attractive target for hackers/attackers, especially in community clouds for CI systems. Changes and improvements to the infrastructure and services needs to be agreed by the members, and is not always easy to find a consensus. Other models like industrial cloud (Wlodarczyk 2009) are similar concepts to the community cloud, but with specialized collaboration concepts and are not described in detail in this paper.

3.4 *Cloud service models*

From the three main cloud models (Software as a Service SaaS, Platform as a Service PaaS, Infrastructure as a ServiceIaaS),SaaS is the one that offers less control to the customer, and this is linked usually to lack of control of the reliability of the system. In the other side, IaaS gives more direct control by the customer over the solution including the reliability of the system. In the same way, the private cloud offers more control of the solution to the customer than the community, hybrid or public.

3.5 *Threats to reliability in cloud services*

It is important when talking about reliability and what can affect differentiate between planned downtime and un-planned downtime. One of the advantages of using cloud systems is that if properly designed and due to the heavily use of virtualization the planned downtime is reduced to minimum, in some cases with providers offering 3 nines (99.9% or 8 hours per year). What is more important here is the un-planned downtime. Table 2 shows some of the recent downtimes by main cloud providers (Ambrust 2010). AS it happened with network providers when they started to offer new services, the reliability improves as the services mature. This happens because of the experience acquired by staff and proven processes as part of a better governance of the cloud services.

Part of the reliability is linked to the backup strategy of the provider, and the time to restore in case of an incidence. Security would be as well paramount for reliability. Other aspect is the monitoring of the systems components and the systems as a whole, specially the proactive monitoring and capacity planning. The threats will depend on what assets will be moved to the cloud services, if are going to be specific processes, or data or functions

Table 2. Outages in cloud providers.

Service and Outage	Duration	Date
S3 outage: authentication service overload leading to unavailability	2 hours	15/2/08
S3 outage: Single bit error leading to gossip protocol blow-up	6–8 hours	20/7/08
AppEngine partial outage: programming error	5 hours	17/6/08
Gmail: site unavailable due to outage in contacts system	1.5 hours	14/5/09

that currently are done by internal processes (CSA 2009). It helps to do a risk assessment on the reliability for the assets that will be moved to the cloud, and the impact of the Critical Infrastructure if the reliability is impacted. As described in the previous sections, the threats can be different depending of the type of cloud that will be used.

Cloud computing threats that could affect the reliability of the service are:

- Bad use by other tenants, in some cases being even hackers or attackers to the target systems. It is easy to attack from the inside. As well the reputation fate sharing, where issues of one tenant could affect the rest.
- Use of shared resources/technologies like the use of virtualization, one bug could affect to all systems even if the Operating systems where are running are different.
- Attractive targets for attackers and hackers due to the high number of tenants and importance of these services in the case of CIs.
- Lack of control over all the supply chain of components that are part of the service, where in some cases even the provider does not have control as he is using other services from other providers.

There are some initiatives in order to help to minimize the risks and assure reliability for cloud environment, like the CSA Guidance, the Common Assurance Maturity Model (CAMM) or the Consensus assessment, but are very focused on the security aspects of the cloud services.

4 PROPOSED MODEL

The last threat described in the previous section, the lack of control over all the complete supply chain, has been the base for the proposed model, where the dependencies between different parts of the cloud services are defined. As organizations move more services to the cloud, the impact in their internal complexity and in the reliability of the systems they are offering to the organization itself and their clients will increase. Not always this added complexity and associated risks to their reliability are seen.

4.1 *Macro and micro dependability*

When two or more CI systems are interacting, the risks of one can propagate to the rest, distributing the risks. We have introduced the term micro-dependability to define this concept; micro-dependability is defined in the context of Computer Systems as the relations of the Computer systems inside organizations that could affect on the reliance of the services that these deliver. However, most of these systems could be part of a bigger system, that can be a Critical Infrastructure, in some cases these boundaries and connections are not clear, and only when real problems appear is when the connection of these systems as part of the CIs are seen, but sometimes is too late, as the disaster is there. So moving to cloud systems, as well and in a more subtle way, could impact the complexity and the reliability of these Critical Infrastructure systems, even when initially the change was better for the organization.

The other term that we have introduced is Macro-dependability, and is used to refer to how the reliability of a system (including Critical Systems) could be affected when changes are done in some parts of other Systems. In the case of macro-dependability the relations are not inside but within systems of other organizations or bigger systems, and how these could affect on the reliance of the services that these deliver. The main problem with both concepts, but specially the second, is that this could be happening now for companies managing CIs and they will not know the risks until probably is too late, as Egan described for the rafted networks (Egan 2007).

We have used similar terms to the ones used in economy because the way it works for economy for both micro and macro economy, when you do changes in something that could affect the economy of the organization, usually these changes affect initially to the organization, but when this changes are done by more or in specific (or critical) areas could even affect to bigger systems and even the society or the economy of bigger areas (region, country, world).

4.2 *Entities and interactions*

Ourmodel defines the relations of the entities inside organizations with other providers (like cloud services). The entities can be providers, consumers, or monitoring entities, and an entity can have more than one role. Each role has a few characteristics that will define how this role operates and the reliability/dependability of that entity for that role.

The attributes should be simple to describe and to allocate a measure that could be validated by the monitoring roles of the entities. These monitoring roles can be allocated to an external entity that corroborates the previous allocation by the entity.

An example organization is shown in Figure 1, the organization is a community provider that has been created between different governmental organizations for provide monitoring and authorization services for pharmacovigilance and critical trials. In this fictitious example two services provided by this organization (cloud provider) have been created. In the entity are two main services that produce services that other organizations can use. For example, for the service pharmacovigilance there are two main subservices, AddSafetyReport used for adding new safety reports for an adverse reaction of a drug. In this example, there are a few attributes that are interesting from the reliability and dependability point of view, as well as for the monitoring of that service. Other entities (organizations) or the same one can consume those services. In this example the entity has a consumer service that is used for managing the email with other providers (like a company that provides messaging services).

The use of other services of different providers is very common, and is using these other services where the interdependencies are more difficult to control. The use is more normal in a cloud model, where services are specialized and are becoming more specialized. Email is a good example; currently there are companies like Messagelabs that provide antivirus, antispam scanning or encryption of email. The consumer organization uses the services, and only is interested in a few metrics like availability, responsiveness and effectiveness, but not in parameters like the type of infrastructure that this producer organization is using to support the services, or where the physical service is located.

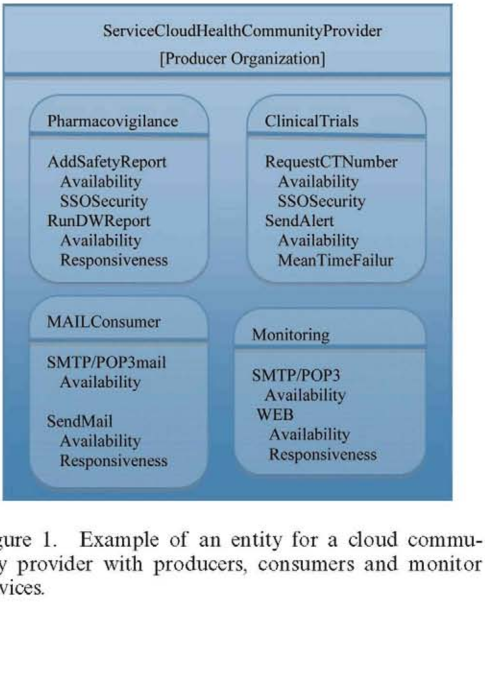

Figure 1. Example of an entity for a cloud community provider with producers, consumers and monitor services.

The third type of service for an entity is the monitoring service; in this case there is a small monitoring service for the web interfaces and for email. In this example these two could be used for internal (web) or external (email) services, and for each monitoring service there are some attributes that are monitored. This permits to have information that can be used and shared with other monitoring services from other organizations in order to get information about the reliability of those services offered by the provider. This is more useful if the monitoring organization is an external independent one.

4.3 *Macro and micro dependability interactions*

Other information that is not shown in figure 1 are the relations between the entities (organizations). The consumers will connect to producers to use the services. This information in shown in the diagrams using links between consumers and producers, and from the point of view of dependability it is the most important. In the previous example only one entity is shown, with no interactions between each entity services. In reality, there are interactions, as well as monitoring, of these services. These interactions and the dependencies between different systems of the organization define micro-dependability for that organization. And once that these interactions are recorded, it will be simple to track dependencies of one service with other, as well as to monitor them.

Continuing with the example of the cloud Community provider for Pharmacovigilance and clinical trials applications, in Figure 2 there is a consumer of the services as well. In this case the consumer can be an external organization that is acting as a consumer of both services of the cloud community provider. In this example, it is a pharmaceutical company that needs to send Safetyreports and request Clinical Trial approvals. There are two types of interaction or connections between the entities, the dotted line that is used for monitoring of services and should be indicated the interval for monitor, and the continuous lines that are used for expressing the real use of services from a consumer to a provider. It can be with more detail and we can explain other step in the link that will be the role of the consumer of the Service cloud community provider of services of an external cloud organization EmailServices, that provides secure email services with antispam, virus free and extra

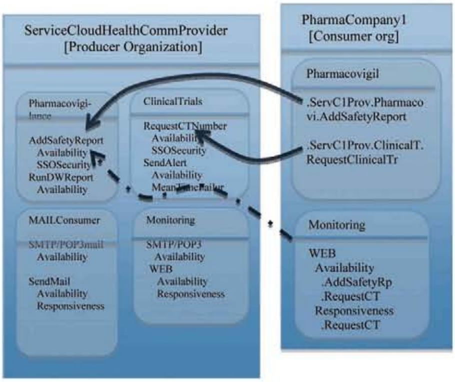

Figure 2. Example of interactions between one cloud producer organization and a cloud consumer.

mail services that the community provider needs to use. These services are consumed from other cloud organization because secure email services are not the core business of the Pharmacovigilance cloud community provider that is specialized on pharmacovigilance services only. Now, in the diagrams we can see the links of the complete supply chain for these services that are provided, the attributes that are interested from the reliability point of view and the values of the monitoring from our point of view but from other providers of each of these attributes. This information can help to improve the risk assessment for the complete supply chain for that service. These connections/interactions between entities are mainly logical, and according to other interdependencies models (Rimaldi, 2004) will be "Logical Interdependencies", but others like geographic or physical could be added to the model. There are other models that can be used, like one of the three types of "dependability" models defined by Boudali (Boudali, 2007), but usually to apply them is a very slow process, because must be done each time a new provider must be used and validated periodically to confirm that are still valid, mainly because this information cannot be reused very easily between different organizations.

4.4 *Qualitative values for reliability*

In order to get quantitative values for the services reliability on the model we can use the reliability networks defined (Dhillon 2003) depending of the type of service that is offered (series, parallel, series-parallel, parallel-series and standby systems). In the example that we are using the services that the consumer Pharmaceutical companies use from the "Service Cloud Health Community Provider" Producer are at the same time using the mail services of other producer providing email with scan services, and only these, if this fails there is not a parallel Producer, in this case we use the series network, where the reliability is expressed as $R = R1R2R3\ldots Rn$. So if the reliability of SendAlert is 0.95 and the SendEmail from the other provider is as well 0.95, the reliability of that function will be 0.8145.

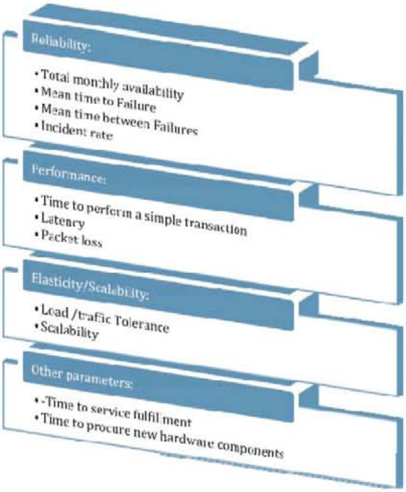
Reliability:
•Total monthly availability
•Mean time to Failure
•Mean time between Failures
•Incident rate
Performance:
•Time to perform a simple transaction
•Latency
•Packet loss
Elasticity/Scalability:
•Load /traffic Tolerance
•Scalability
Other parameters:
•-Time to service fulfil ment
•Time to procure new hardware components

Figure 3. Possible metrics that can be used for the attributes.

Other models that could be applied are:

- Parallel in case of different services used in parallel so the Service will only fail when all the producers fail. R = 1 – (1-R1)(1-R2)(1-R3)…(1-Rn)
- Series-parallel, where the service is using n active sub-services (usually from that organization) in parallel.
- Parallel-series, in this case the service is using n other sub-services in parallel.
- Standby systems, where normally the service is using only one service, but there is a backup that is used if the main one fails.

These should be applied first for the services of the organization (micro) and later once the values are calculated for the micro, use these for include other organizations (macro).

4.5 *Attribute metrics*

It is important to define correctly the metrics that will be used in order to measure the attributes. These could be used as well for create the SLAs that will be agreed with the provider and in order to monitor if these SLAs are met. In this paper the metrics are focused on the reliability, but others that could affect directly or indirectly should be added in a real scenario (legal, security…). Some of the possible metrics that could be used are listed in Figure 3.

5 CONCLUSIONS AND FUTURE WORK

The proposed model and the concepts are used to provide a better understanding of the services that would like to be used in a cloud solution, showing the dependencies and how these affect the reliability of those services. Currently we have presented the model to be used on ICT systems and mainly cloud solutions, but the model can be adapted for other type of ICT systems and even interaction with other non-ICT Systems, and the roles of producers/consumers and supported/supporting Infrastructure with other CIs like the Electric grid (Rinaldi 2001).

Before cloud services are adopted by an organization, interdependencies should be reviewed not only for the organization that offers the service but also for the other organizations that act as providers for the one we will use. Once the risks are clear, the right cloud service and model can be chosen. And whatever solution is chosen, there should be plans in case of cloud service unavailability and a mechanism should be in place to provide service, even if it is a degraded service.

The model can be improved by using the concept of Web Service Level Agreement defined by Keller (Keller 2002) and Patel (Patel 2009), and using this in a combination with the UML tools dependability models defined by Boudali (Boudali 2007). As well can be used for bigger systems (Macro dependability) that include more than one small systems (Micro dependability), with more variables like price and security and more than one view (ICT, electricity).

In the near future we plan to work in developing the model with more detail and test it for a real system that could be implemented in the cloud. As well describe in more detail how the big cloud services are becoming a new critical infrastructure.

ACKNOWLEDGEMENTS

Dr. Silva participation is partially funded by the DICODE project (FP7-ICT-20095257184).

REFERENCES

Alexander Keller, Heiko Ludwig; *The WSLA Framework: Specifying and Monitoring Service Level Agreements for Web Services*. JOURNAL OF NETWORK AND SYSTEMS MANAGEMENT. Volume 11, Number 1, 57–81.

Alice Lipowicz. April 2009. *Cloud computing moves into public safety*. Federal computer week.http://fcw.com/articles/2009/04/16/cloud-computing-moving-into-public-safety-realm.aspx.

Armbrust M, Stoica I, Zaharia M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A. A view of cloud computing. April 2010. *UC Berkeley Reliable Adaptive Distributed systems Laboratory.*

Charles Perrow, *Normal Accidents*. Princeton University Press. 1999.

Cloud Security Alliance. *Security Guidance for Critical Areas of Focus in Cloud computing V2.1*. December 2009. http://www.cloudsecurityalliance.org/csaguide.pdf.

Dhillon B.S. *Engineering Safety*. Series on Industrial & Systems Engineering—Vol 1.Wold Scientific. 2003.

ENISA, Jan 2011. *Security & Resilience in Governmental Clouds.*Cloud Security Alliance, 2009. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.

Gewndal Le Grand, Michel Riguidel. *A global framework to enhance critical infrastructure protection*. Securing Critical Infrastructures. Grenoble, October 2004.

Hichem Boudali, Boudewijn R. Haverkort, Matthias Kuntz, Marielle Stoelinga; *Best of Three Worlds: Towards Sound Architectural Dependability Models*, 8th International Workshop on Performability Modeling of Computer and Communication Systems (PMCCS), September 20–21, 2007, Edinburgh, UK.

James P.G. Sterbenz, David Hutchison, Egemen K. Cetinkaya, Abdul Jabbar, Justin P. Rohrer, Marcus Sholler, Paul Smith. *Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines*. Computer Network 54. 2010.

Joshi, K.R.; Bunker, G.; Jahanian, F.; van Moorsel, A.; Weinman, J. *Dependability in the Cloud: Challenges and Opportunities.* IEEE/IFIP International Conference on Dependable Systems & Networks. July 2009.

Matthew Jude Egan, 2007. *Anticipating Future Vulnerability: Defining Characteristics of Incresingly Critical Infrastructrue-like Systems*. Journal of Contingencies and Crisis Management, Vol. 15, No. 1, 4–17.

NASA Nebula project http://nebula.nasa.gov.

Rimaldi, S.M. Modeling and Simulating Critical Infrastructures and Their Interdependencies. Hawaii International Conference on Systems Sciences. 2004.

Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K.; *Identifying, understanding, and analyzing critical infrastructure interdependencies*. Air Force Quadrennial Defense Review, Washington, DC. Dec 2001.

Robert F. Lentz. May 2009. U.S. House of Representatives Armed Services committee of terrorism, unconventional threats & capabilities. http://armed-services.house.gov/pdfs/TUTC050509/Lentz_Testimony050509.pdf.

Ted G. Lewis. *Critical Infrastructure Protection in Homeland Security. Defending a networked nation*. John Wiley & Sons. 2006.

Tomasz Wiktor Wlodarczyk, Chunning Rong, Kari Anne Haa-land Thorsen. Industrial Cloud: *Toward Inter-enterprise Inte-gration*. CloudCom 2009. Beijing, China. Springer 2009.

Vincenzo Fioriti, Gregorio D'Agostino, Sandro Bologna. *On Modeling and Measuring Inter-dependencies among Critical Infrastructures.* Complexity in Engineering. IEEE Computer Society. 2010.