

Survivability Assessment: Modelling Dependencies in Information Systems

Gao, Zhixing; Ong, Chen Hui; Tan, Woon Kiong
DSO National Laboratories
{ gzhixing, ochenhui, twoonkio }@dso.org.sg

1 Introduction

The increased affordability and subsequent flourishing of information technologies over the last decade or so have resulted in the widespread deployment of such technologies. As a wired nation [1], Singapore too deploys information technology widely in her business functions and implementation of essential services. With such pervasive use of information technologies, failures to our information infrastructures can have a significant detrimental impact to our economic and social way of life.

The potential for detrimental impact to our way of life gave rise to the requirement for a well-defined process that can assess the survivability of our information infrastructures. We shall term this assessment process the “survivability assessment process”. Owners of the information infrastructures can employ the survivability assessment process to assess the survivability of their information systems and to prioritise their investments in technology, policy and training.

Assessing the survivability of information infrastructures is a challenging task. Even though there have been discussions on the need for such assessment techniques [2], to date, we have yet to find an open-source, well-developed process or set of tools that can assess the survivability of information infrastructures in a holistic manner.

2 A Preliminary Model

2.1 Model Description

In this paper, we present our first attempt at formulating a model to represent survivable relationships in information infrastructures. Our primary focus is to analyse these relationships to gain insight on how the survivability of components in the information infrastructure impact the survivability of the whole infrastructure.

In our model, we represented information infrastructures as a networked computer-communications system. The components in information infrastructures refer to the underlying computer and communications systems and services (e.g. operating systems, servers, clients, network connectivity) that make up the information infrastructures.

We define survivability of the information infrastructures as the ability of the networked computer-communication system to satisfy and to continue to satisfy its mission even in the face of adverse conditions [3][4]. The mission of the system is a set of critical specifications (e.g., specifications on functionalities, performance, security, reliability, real-time responsiveness, and correctness) that must be met. We call this ability system survivability. In our definition, system survivability is not a binary property of the system but a property that gives a measure of the extent to which the information infrastructures is able to satisfy the critical specifications.

We represent this survivable relationship as shown in Figure 1.

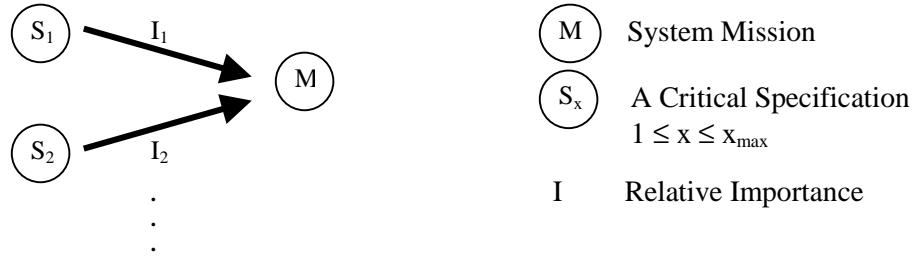


Figure 1 Survivable Relationship between System Mission and Critical Specifications

Figure 1 shows the representation that reflects the relationship between the system mission, M , and its critical specifications, S_1 to $S_{x_{max}}$, as described in the system survivability definition. A mission consists of a set, S , of critical specifications. Each critical specification in S is unique but not necessarily independent. Each critical specification carries a relative importance of I in the fulfilment of the mission. A specification with a higher relative importance will have a greater impact on the overall system survivability than one with a lower relative importance.

Each critical specification is a description of the desired behaviour from the system. There may be many ways to achieve a specification. For instance, a specification S_x can be achieved via a number of alternative methods, C_{x1}, C_{x2}, \dots . This is shown in figure 2. In practice, each alternatives is usually a combination of some services.

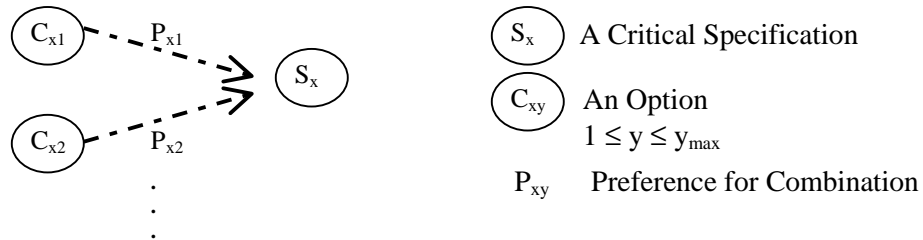


Figure 2 Representing Alternatives

With alternatives in the system design, each specification can be met through the realisation of any one C_{xy} . However, some combinations of services are preferred over others. We denote the preference for the particular alternative, C_{xy} , as P_{xy} .

Each C_{xy} is an option that describes a set of services, SV_{xyz} , provided by the underlying components in the system. Each SV_{xyz} is distinct from but not necessarily independent of others. Included in SV_{xyz} is a description of the survivable qualities that are needed by C_{xy} . Examples of some qualities that may be required of SV_{xyz} are security, ability to recognise its failures, ability to tolerate faults and intrusions and ability to recover.

We define the survivability of a service provided by the underlying components as the ability of the component to provide the required quality of services required for system survivability. We term this components survivability. As shown in Figure 3, $\zeta(SV_{xyz})$ denotes the survivability of each component SV_{xyz} in our model. In this model, ζ is mandatory for all SV_{xyz} .

All the survivable relationships can be summarised in Figure 4 below.

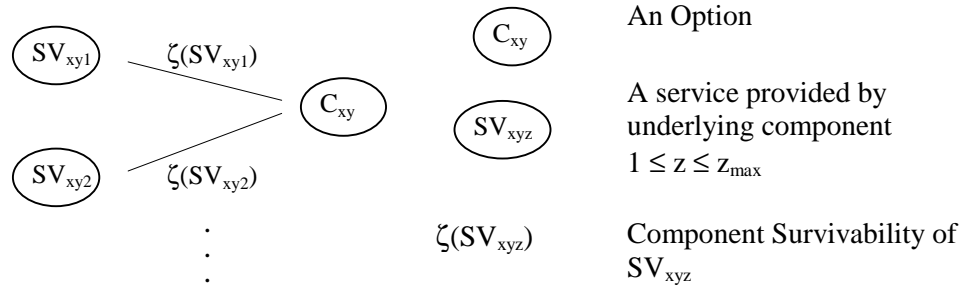


Figure 3 Survivable Relationship between a combination of services and component services

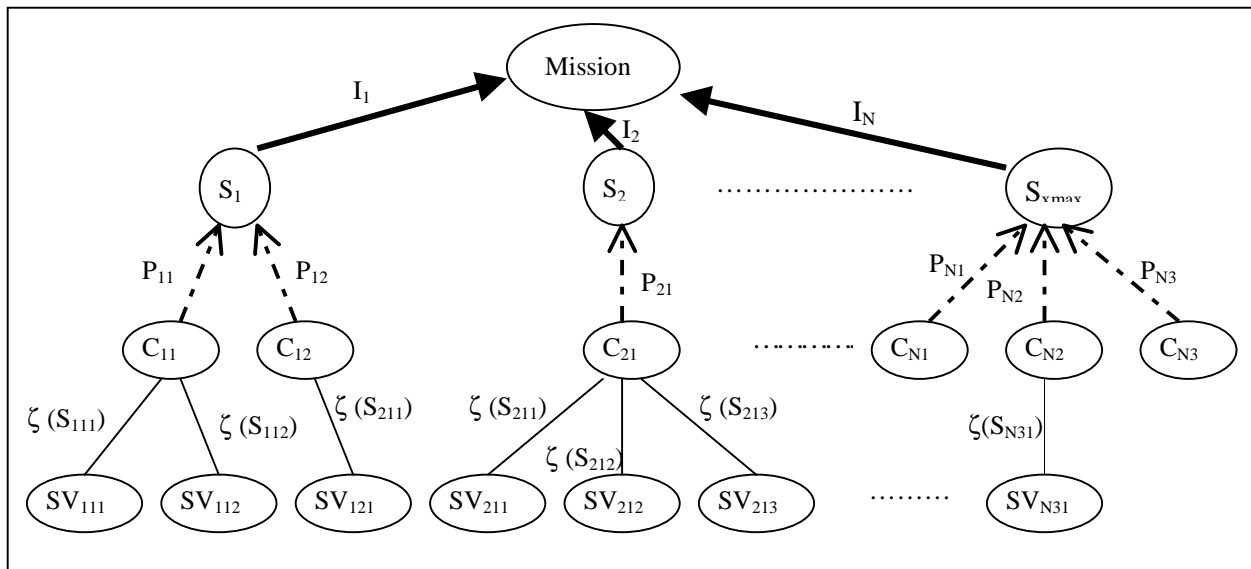


Figure 4 Survivable Relationships in Preliminary Model

2.2 Modelling Objectives

From the preliminary model developed, we hope to gain insights into the following areas:

- A. **Role of Redundancies:** Intuitively, the presence of redundancies in the system will improve system survivability. However, this intuition should not hold if the redundancies share a common failure point. How does redundancies affect system survivability?
- B. **Functional Dependencies:** Should the functionality of a certain component or application be lost, what is the impact on the ability of the system to fulfil its mission? Is it possible to find out the critical points of failure?
- C. **Application Dependencies:** Many information systems depend on similar applications (such as similar OS, similar configurations of its OS) in its implementation. Will increasing the diversity of these applications impact the survivability of the system?
- D. **Remedies:** What remedies will give the greatest yields in enhancing survivability for the organisation?
- E. **Integration of New Technologies:** Many organisations continuously upgrade the components within their information systems to maintain efficiency. How do such upgrade affect the survivability of the networked information systems in these organisations? When new

technologies are invented, how do such technologies impact the networked information systems?

We will test our model on different systems to progressively refine the model. In the testing of our model on real implementation of information infrastructures, information collection tools will be developed to extract the attributes of real implementation of services.

3 Conclusions

In this paper, we presented our preliminary attempts at defining a model to capture some survivability relationships within a networked information system and our plans to use this model to gain insights for the development of a survivability assessment process.

There are several tasks ahead. Foremost of all, we have yet to find an intuitive set of metrics to evaluate components survivability $\zeta(SV)$. This aspect of modelling is further complicated by the overlaps in some of these qualities of survivability [3].

Other problems also arise due to the scale of information infrastructures. Currently, our model is under-constrained. It is difficult to implement an automated generation of our model from real information infrastructures. While it may still be possible to manually formulate the specifications, break them down into combinations and services for small infrastructures, it is no longer practical to perform these tasks manually when studying larger-scale infrastructures. We are looking for natural system phenomena that will constrain our model.

In addition, networked information systems often use a variety of services that interact with each other to achieve a desired behaviour. For a small system, it may be possible to manually collect the configurations of the various components to map out the attributes of the services. Such information collection methods are not practical as the system under study scales in size. We would like to develop a set of tools or methods that could make the collection of attributes feasible.

4 References

- [1] Susan Tsang, Singapore and Taiwan are Asia Pacific's most wired from Singapore.CNET.com, Mar 16 2001
- [2] Dr. John Alger, Deborah Bodeau, Julie Connolly, Survivability and Operational Readiness: Common Needs for Metrics and Assessment, Position Paper to ISW 2000, www.cert.org/research/isw/isw2000/papers/28.pdf, Mitre Corporation
- [3] Peter G. Neumann, Practical Architectures for Survivable Systems and Networks (Phase-Two Final Report), www.csl.sri.com/neumann/survivability.pdf, 30 June 2000
- [4] John C. Knight, Kevin J. Sullivan, Towards a Definition of Survivability, Position Paper to ISW 2000, www.cert.org/research/isw/isw2000/papers/27.pdf, University of Virginia