Risk Analysis for Critical Systems with Reliability Block Diagrams

Weyns, Kim; Höst, Martin

Published in:
Proceedings of the 9th International ISCRAM Conference

2012

Risk Analysis for Critical Systems with Reliability Block Diagrams

Kim Weyns
Lund University
kim.weyns@cs.lth.se

Martin Höst
Lund University
martin.host@cs.lth.se

ABSTRACT

Governmental organisations are becoming more critically dependant on IT systems such as communication systems or patient data systems, both for their everyday tasks and their role in crisis relief activities. Therefore it is important for the organisation to analyse the reliability of these systems as part of the organisation's risk and vulnerability analysis process. This paper presents a practical risk analysis method for critical, large-scale IT systems in an organisation. The method is based on reliability block diagram modelling and was adapted to fit the requirements of governmental organisations and to reduce the effort required to capture complex failure behaviour. The paper first explicitly lists the requirements that such a risk analysis method must fulfil, then presents the proposed risk analysis method and finally outlines the planned evaluation of this method.

Keywords

Risk Analysis, Reliability Block Diagram, Government, Critical System, Availability

INTRODUCTION

In recent years governmental actors have come to depend more on IT systems for all their everyday tasks. For communication, municipalities depend on landline telephone networks, mobile phone networks, webservers, email systems, etc. Other important systems are used for patient administration in health care and social services, school administration or city planning.

Just as for their everyday tasks, governmental organisations now depend on all kinds of IT systems for their responsibilities in crisis situations. These systems include not only specially built systems for emergency situations but also the everyday systems described above (Zimmerman et al., 2006). Therefore, it is important that these systems are an integral part of all major risk and vulnerability analyses conducted. A thorough IT management approach requires an assessment of how critically dependant the organisation is on its most critical IT systems and more specifically what the consequence of a failure of these systems would be for the organisation in different scenarios. To assess the information technology risks for the organisation, this information then needs to be combined with information about the reliability and the availability of these systems (Swedish Emergency Management Agency, 2003).

In this paper we focus on the second part of this risk assessment, namely analysing the reliability of critical IT systems. The analysis of the reliability of large, distributed IT systems is a complex task. Because of the rapid evolution in the field of information technology, where systems are constantly being updated and replaced, there is usually too little statistical data available to assess the reliability of critical IT systems based on measured data from past failures. Instead, a risk analysis technique based on the structure and components of the systems is necessary. A number of risk analysis techniques exist for the assessment of the reliability of technical systems and more specifically IT systems. Many of these techniques, such as Fault Tree Analysis (Ericson, 1999) or Failure Mode and Effect Analysis (Beauregard, 1996), require a detailed analysis of all components of the systems and are therefore more suited for small, embedded systems with a very specific function. To conduct a similar analysis for large, complex systems, such as a patient data system, would require too large an effort to be realistic for most organisations.

Therefore, there is a need for a risk analysis method for large-scale IT systems that requires fewer resources, but that can still capture the complex failure behaviour typical for these systems. In this paper we define a number of requirements that such a risk analysis method needs to fulfil to be useful for a governmental organisation. Further, we propose a specific method based on Reliability Block Diagrams (RBD). Finally, we also briefly describe the planned evaluation of this technique through the use of the risk analysis method in a case study at a Swedish municipality.

RELATED WORK

A number of studies have discussed IT dependability in governmental organisations, particularly with respect to emergency management. For example, Santos et al. (2008), investigated the relation between IT technology and cooperation in emergency response organisations and Zimmerman et al (2006) discussed the interconnections between information technology and other critical infrastructure for emergency response. An earlier study specifically concerning IT dependability problems at Swedish municipalities (Weyns et al, 2009) identified a number of important issues, one of which was the need for practical methods and techniques for risk analysis. In Sweden, the Swedish Civil Contingencies Agency published Basic Level for IT Security (Swedish Emergency Management Agency, 2003), a collection of guidelines concerning IT safety for governmental organisations based on international standards.

Several authors (Office of Government Commerce, 2007, Weyns et al. 2010) propose a process oriented approach to IT dependability management, and in these papers the risk management process is identified as one of the most important aspects in assessing the reliability of IT systems, but no specific, practical methods for this risk analysis are discussed.

Many different techniques for detailed risk analysis of technical systems exist (U.S. Department of Defense, 2007). Fault Tree Analysis (Ericson, 1999) is a top down technique used to analyse all possible conditions that can lead to a certain failure in a technical system. Failure Mode and Effect Analysis (Beauregard, 1996) is a risk analysis technique to assess the probability and effects of possible failures of the system. A third technique, called Reliability Block Diagrams (RBD) (Staley and Sutcliffe, 1974), forms the basis for the method proposed in this paper. All of these techniques require a large effort and assume a very detailed system model. Therefore these techniques are most suited for systems with well-defined components for which the failure behaviour can be predicted. In contrast, in this paper we propose a method better suited for complex, distributed systems, where the other techniques would require too much effort to be of practical use.

Several studies have been published about Reliability Block Diagrams, including a number of practical applications of RBD for specific systems such as uninterruptible power supply systems (Rahmat et al., 2011) and UMTS networks (Dharmaraja et al, 2008).

Vriezevolk et al. (2011) have proposed a risk analysis method for a specific type of distributed systems, namely telecommunication systems. They also explicitly discuss a list of requirements for such a method and their method is also based on step-wise refinement of the system model.

MUNICIPAL RISK ANALYSIS

Swedish municipalities have a central role in the Swedish emergency management system. To prepare for crisis situations, all municipalities are required by law to conduct regular risk analyses concerning their areas of responsibility. Because of their dependence on critical IT systems, this also requires municipalities to analyse the availability of their IT systems and the consequences of a failure in these systems on the organization. This paper focuses on techniques for municipalities to analyse the availability of their most critical systems.

A typical Swedish governmental organisation has a centralized IT service unit that provides IT services to all other organizational units. This IT unit maintains the systems of the organisation and services the systems together with a number of external suppliers.

Based on our experience in cooperating on IT safety with several governmental organisations, we have identified the following requirements for a method to be suitable. These requirements have then been validated with the help of a Swedish governmental organisation currently exploring ways to assess the reliability of their IT systems.

R1: **Result**: The results must be easy to combine with the results of the analysis of the dependence on the system as performed by each of the organizational units in the organisation.

R2: **Understandable**: The results of the method must be easy to understand even for non-technical personnel such as politicians, who ultimately have the authority to decide over risk mitigating actions in governmental organisations.

R3: **Modularity**: The method must be modular, to make it possible to reuse the analysis of subsystems that are part of multiple critical systems.

R4: **Resources**: The risk analysis must only require an acceptable amount of resources, as it must be conducted for all critical systems.

R5: **Uncertainty**: Most risk analysis methods rely partly on expert estimates. The model must make it possible to take into account the sensitivity of the result to the uncertainty of these estimates.

R6: **Model**: The method should not require a detailed technical model of the system, but instead rely on a simple model that is refined as the analysis progresses.

R7: **Cooperative**: A team of experts from different parts of the organization must be able to perform the analysis together, and contribute their expertise on each part of the system.

Requirements 4 to 7 are similar to requirements listed by Vriezekolk et al. (2011) for the risk analysis method they propose for the analysis of telecom services. Requirements 1 to 3 are directly related to the nature of municipalities as large organizations that are critically dependent on a large number of distributed systems (Weyns et al, 2009).

RELIABILITY BLOCK DIAGRAMS

In this paper we propose the use of a variation of Reliability Block Diagrams as a risk analysis method for municipalities to identify and quantify the different risks to the failure of one of their critical IT systems. A Reliability Block Diagram models a system as a collection of blocks representing the system's logical or physical components as shown in Figure 1. The availability of the system is modelled as a path from left to right. The most common configurations are blocks in series (all subsystems must be available) and parallel (at least one subsystem must be available), but more complex relations (such as k-out-of-N) can be modelled. Given the availability functions of the individual blocks (often modelled with the help of exponential or Weibull distributions), the total availability of the system can be calculated directly or through Monte-Carlo simulation. Many commercial software packages are available to assist in the creation and analysis of RBDs.

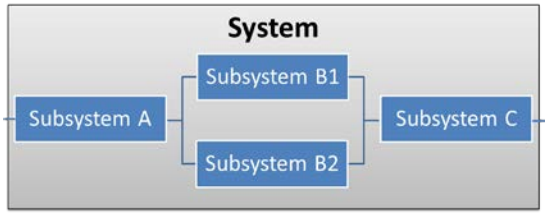

Figure 1. Example of a Reliability Block Diagram. The system is available if and only if Subsystem A, at least one of the Subsystems B1 or B2, and Subsystem C are available.

As illustrated in Figure 2, a RBD of the system can be constructed starting from a very basic model of the system by replacing subsystems by a more detailed RBD representing this subsystem. This process can be repeated until the desired level of detail is reached. The refinement of each subsystem should be done by experts of the respective subsystems. The detailed RBD of the subsystems that are present in multiple systems can later be reused for constructing the RBD of other systems. Analysis of RBDs also makes it possible to calculate the contribution of each individual component to the downtime of the entire system and to quickly analyse the sensitivity of changes to the reliability of one of the components to the reliability of the complete system. This model also makes it easy to calculate the effect of improvements to the structure of the system (for example by adding extra parallel components to those components responsible for most of the failures) on the overall availability of the system. Thereby RBDs automatically fulfil requirements R3, R5, R6 and R7 listed above.

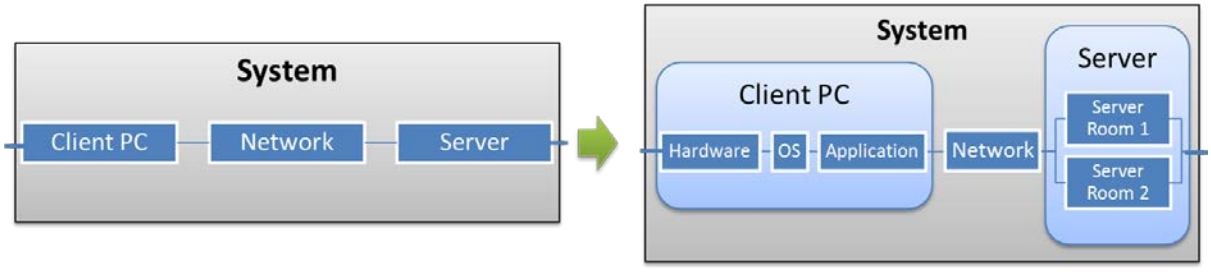

Figure 2. Stepwise refinement of a RBD.

PRACTICAL ADAPTATION OF RELIABILITY BLOCK DIAGRAMS

One of the disadvantages of RBDs is that they require the estimation of the reliability of each of the systems' components, most commonly done by estimating the parameters of the distribution of the mean-time-to-failure (MTTF) and the mean-time-to-repair (MTTR). Also the output of the analysis is formulated as the MTTF and MTTR of the complete system. To make it easier to estimate the reliability of the components and to make the results easier to interpret in the context of a risk analysis for the organisation, this paper proposes to replace the input distributions for MTTF and MTTR of each component by the frequency of the occurrence of a limited number of failure categories, based on the duration of the unavailability of the component (e.g. outages shorter than 1 hour, outages between 1 and 5 hours, outages between 5 hours and 24 hours, and outages lasting longer than 24 hours). These parameters are easier to estimate for professionals involved in the risk analysis. These categories also correspond to the process of IT service at the organisation, where some problems can quickly be fixed by restarting of replacing the failed component by IT personnel of the organisation, while other types of component failures always take longer to repair because they require technical support of outside suppliers. These adaptations to the method are intended to make the method more concrete and understandable for personnel who are unaccustomed to working with complex failure distribution functions, as stated in requirement R2.

The usage of these categories also makes it possible to limit the level of detail required in the reliability block diagram as different types of failures of a component can be attributed to a high level component instead of having to explicitly model all subcomponents that have very different repair characteristics. This makes it possible to still capture complex failure behaviour without having to model low-level components. This is essential for limiting the resources needed for the analysis as required by requirement R4, which is the most important difference compared to the other methods described above in the 'Related Work' section.

However the main reason for this adaption is that the output of the risk analysis will also be described with the help of these outage duration categories, which naturally correspond to the type of outages the organisation needs to prepare for in their emergency management. For many types of systems in a governmental organisation, short outages will cause only nominal disruption, while longer outages will cause considerable problems for the organisation and the services it provides. Therefore, these concrete definitions of different outage categories will make it easier for the results to be included in the overall risk management process than when the reliability is expressed as a complex failure distribution. This is important for Requirement R1 listed above.

Finally, the calculation of the overall reliability of the system can be simplified significantly compared to the general reliability block diagrams. Although Monte-Carlo simulation can still be used for the calculation of more exact results, simple combinatorics can be used to calculate a good approximation of the overall reliability of the system. An example illustrating this calculation, using the fictive system shown in Figure 1, is presented in Table 1.

		< 1 hour		1 < x < 5 hours		5 < x < 24 hours		> 24 hours		Total
Subsystem A		*12*	0,9993	*1*	0,9997	*0*	1	*0*	1	0,999
Subsystem B	Subsystem B1	*0*	1	*0*	1	*0*	1	*6*	0,951	0,951
	Subsystem B2	*0*	1	*0*	1	*0*	1	*10*	0,918	0,918
	Subtotal		1		1		1		0,996	0,996
Subsystem C		*0*	1	*2*	0,9993	*2*	0,997	*0*	1	0,996
System		12	0,9993	2,999	0,9990	2	0,997	0,493	0,996	0,991

Table 1. Example calculation of the availability of a system (shown in Figure 1) based on the availability of its components. The 16 numbers presented in italics are the estimated input parameters, expressing the number of expected failure in each category, expressed as number of failures per year. The numbers in the grey shaded areas are the associated availability, needed to compile the components into one system. In this example, Subsystem A represents a typical component that fails often but can quickly be repaired by locally available personnel. Subsystems B1 and B2 (that act as backup for each other) are components that fail quite often and also take a very long time to be repaired. Subsystem C represents a typical system that only fails a few times a year and for which a maintenance contract with a guaranteed service time shorter than 24 hours is available.

PLANNED EVALUATION

The next step in this research project is to evaluate the practical usage of this method in a real-life setting at a large Swedish municipality. Through the use of action research methodology (Reason and Bradbury-Huang,

2007), the reliability of the most critical IT systems of the organization will be assessed with the adapted version of reliability block diagrams as described above. Afterwards, the methods will be evaluated both concerning usability and the value of the results for the organisation. Further we will evaluate how well this technique fulfils the requirements listed above and how the technique can be further improved.

CONCLUSION

In this paper we first defined a number of requirements that a risk analysis method must fulfil to be of practical use for a large governmental organization such as a municipality to identify and quantify the risks associated with their most critical IT systems.

This work-in-progress paper then proposes a risk analysis method based on reliability block diagrams that could fulfil these requirements. The properties of reliability block diagrams together with the proposed adaptations have the potential to fulfil all the listed requirements.

Finally, this paper also described how this risk analysis method will be evaluated in a practical setting in a case study involving practitioners and experts in the field at a Swedish municipality.

REFERENCES

1. M. R. Beauregard. (1996). The Basics of FMEA. Productivity Press
2. S. Dharmaraja, V. Jindal and U. Varshney. (2008). Reliability and Survivability Analysis for UMTS Networks: An Analytical Approach. In *IEEE Transactions on Network and Service Management*. Volume 5, Issue 3, pp. 132 – 142, 2008.
3. C. A. Ericson. (1999). Fault Tree analysis – A History. In *Proceedings of The 17th International System Safety Conference*.
4. Office of Government Commerce. (2007) Information Technology Infrastructure Library, Version 3.
5. M. K. Rahmat, and S. Jovanovic. (2011). Reliability Estimation of Uninterruptible Power Supply Using Reliability Block Diagram Method. In *International Review Of Electrical Engineering.* Volume 6, Issue 3, pp. 1109 – 1117, May 2011.
6. P. Reason and H. Bradbury-Huang. (2007). The SAGE Handbook of Action Research: Participative Inquiry and Practice, 2nd ed. Sage Publications Ltd
7. R.S. Santos, M.R.S. Borges, J.O. Gomes and J.H. Canós. (2008) Maturity levels of information technologies in emergency response organizations. In *Collaboration Researchers' International Workshop on Groupware (CRIWG). Volume 5411 of LNCS., Springer, Heidelberg*
8. J.E. Staley and P.S. Sutcliffe. (1974). Reliability block diagram analysis. *Microelectronics Reliability.* Volume 13, Issue 1, February 1974, Pages 33–47
9. Swedish Emergency Management Agency, SEMA. (2003) Basic Level for IT Security. *SEMA recommends 2003:2*.
10. U.S. Department of Defense. (2007). Electronic Reliability Design Handbook. *Department of Defense Handbook*. MIL-HDBK-338
11. E. Vriezekolk, R. Wieringa and S. Etalle (2011). A New Method to Assess Telecom Service Availability Risks. In *Proceedings of the 8th International Information Systems for Crisis Response and Management Conference, ISCRAM 2011*
12. Weyns, K., M. Höst, and Y. Li Helgesson. (2010). A Maturity Model for IT Dependability in Emergency Management. In *Proceedings of the 11th International Conference on Product-Focused Software Process Improvement, PROFES 2010*.
13. Weyns K. and M. Höst. (2009). Dependability of IT Systems in Municipal Emergency Management. In *Proceedings of the 6th International Information Systems for Crisis Response and Management Conference, ISCRAM 2009*
14. R. Zimmerman and C. Restrepo. (2006) Information technology (IT) and critical infrastructure interdependencies for emergency response. In *Proceedings of the 3rd International Information Systems for Crisis Response and Management Conference, ISCRAM 2006*