A New Method to Assess Telecom Service Availability Risks

Eelco Vriezekolk
Radiocommunications Agency Netherlands
& University of Twente
eelco.vriezekolk@agentschaptelecom.nl

Roel Wieringa
University of Twente
roelw@ewi.utwente.nl

Sandro Etalle
Eindhoven University of Technology & University of Twente
s.etalle@tue.nl

ABSTRACT

Protection of society against natural and man-made disasters is high on the societal and political agenda. Effective crisis management is more important than ever. Nowadays, crisis organisations depend crucially on reliable telecom services, and unexpected failure of telecommunication may have serious consequences. In order not to be caught unprepared, crisis organisations should therefore perform a risk assessment on telecom availability. Unfortunately, assessment of availability risks of modern, multi-operator telecom services is difficult; information sources are unreliable, and the relevant information is uncertain and difficult to obtain. This paper describes some of these difficulties, as well as the requirements of availability risk assessment methods for crisis telecommunication services. The paper outlines a new method that can be applied without requiring full knowledge of the physical layout of the telecom infrastructure. This new method relies on telecom service diagrams as a tool for risk analysis and to facilitate dialogue among the analysts.

Keywords

Risk assessment, availability, crisis management, telecommunication services.

INTRODUCTION

Society nowadays demands effective crisis management. Modern crisis organisations depend on telecommunication services, such as telephony, data and video links (Van de Ven, Van Rijk, Essens, Frinking, 2008). When these services become unavailable during a crisis, damage will increase and people may die. Crisis organisations must therefore know their telecom service availability risks. This means that crisis organisations need to perform a risk assessment (RA). RA is challenging in this domain because of three complicating factors. First, telecom services are composed of networks and services of many independent, competing companies which makes it very hard to obtain reliable information about the network. Secondly, even if complete information were available, a risk model showing all physical components is difficult to construct because it is excessively complex. Thirdly, risk assessment cannot be based on technological factors only; the priorities and preferences of society are relevant as well. To assess telecom service availability risks for crisis organisations, a RA methodology is needed that handles these complications efficiently and effectively. We are not aware of any RA method matching these requirements. In fact, crisis organisations often do not perform any RA at all, and instead rely on service level agreements (SLAs) with their telecom service providers. SLAs are unsuitable, as they typically exclude disasters and other exceptional circumstances. This situation is undesirable, given the importance of effective crisis response. To remedy this situation, we are developing a RA method that is tailored for this domain and its challenges.

BACKGROUND

Reviewing Statement: This short paper has been fully double-blind peer reviewed for clarity, relevance and significance.

Risk assessment (RA) is the overall process of risk identification, risk analysis and risk evaluation (IEC/ISO, 2009). The purpose of RA is to provide stakeholders (including decision makers) with the knowledge that is necessary to make risk treatment decisions. This knowledge encompasses the causes, mechanisms, and expected effects of threats. In this paper we focus on natural, physical threats that cause availability risks.

Modern telecom services are composed of networks and services operated by many independent and often competing companies. For instance, a phone call may originate at a virtual mobile network operator, using the GSM network of a wholesale operator, that has outsourced its physical network. The information that analysts require as input to their RA has to be obtained from each of these parties. Three complications then arise. First, a detailed physical model cannot be constructed, for it is impossible in practice to discover the arrangement of all cables, wireless links, routers, switches and other components participating in delivering a service. Secondly, the companies are not necessarily aware that they participate in delivery of a compound service. For example, a cable may carry data for some essential service without the company that manages the cable knowing it. Even if companies are aware of the services, they have little incentive to co-ordinate its availability with competitors. It is possible that they understate the availability risks for competitive advantage. The accuracy and reliability of the information that analysts obtain from companies will therefore be uncertain or suspect. Lastly, since crisis organisations render a public service to society as a whole, risk assessment cannot be based on technological factors only; the preferences, fears and concerns of a multitude of stakeholders are relevant as well. Several additional risk factors have been identified, such as irreversibility of threatening events, dread of fearsome threats, and social inequality in risks (Klinke and Renn, 2002; Slovic, Flynn and Layman, 1991). We call these factors *social risk factors.*

A RA method is needed that can be applied despite the complications listed above. Current risk assessment methods do not suffice. We are therefore developing a new RA methodology, intended for the availability risks of telecom services faced by crisis organisations. This research is still in progress, and we can only show preliminary results here.

REQUIREMENTS OF RISK ASSESSMENT METHODOLOGY

In order to develop a new risk assessment method, we need to define its requirements. We identified three groups of requirements: to handle the challenges (R1-R3), to ensure ease of execution (R4-R6), and to guarantee the usefulness of the results of the method (R7-R9).

R1 No full model: the method must not require the entire telecom system to be modelled in detail.

R2 Uncertainty: the method must take into account uncertainty about the correctness of input information.

R3 Social risk factors: the method must be able to take into account a diverse range of social risk factors.

R4 Usability: Experts from different fields (telecommunications, crisis management, engineering) must be able to understand and apply the method. Telecoms experts are able to understand the failure mode of technical components and mitigating factors, but only crisis management experts can indicate the impact that this failure will have. Other experts bring their legal knowledge or knowledge of organisational structures to the table. A team of experts from mixed backgrounds must be able to perform the RA.

R5 Effort: it must be possible to execute the method in an acceptable amount of time. Experts have little time, and a method that is time consuming is therefore unlikely to be used in practice.

R6 Exceptional circumstances: the method must be able to take account of large-scale disruption and other exceptional circumstances that likely arise during crisis situations. It is not sufficient to base the risk assessment on quiet situations between crises. Among other things, this implies that service level agreements are likely not a sufficient basis by themselves, as service level agreements typically exclude disasters and other exceptional circumstances.

R7 Identify all risks: the new method must identify all causes of unavailability that are within the scope of the RA.

R8 Over-aggregation of information: although RA may be based in part on subjective evaluations, it should always be possible to retrace the reasoning that led to a particular assessment of risk. The new method must therefore not summarise or hide key information, and the effects of any uncertainties in the input information must be reflected in the risk assessment.

R9 Priorities and treatment options: the new method must support the determination of risk priorities and the selection of preferred risk treatments.

OUR APPROACH: THE RASTER METHOD

We propose a method, called Raster, that is based on *stepwise refinement* of a model of the telecommunication

services. Stepwise refinement means that the method starts with a simple model of the services, and that detail is added during application of the method.

Raster models telecommunication services as a graph of typed components. Five node types are used: actors, wired links, wireless links, equipment, and unknown links. Actors represent users of the telecommunication service. Actors can be a single individual or a group of individuals with a common role, such as members a crisis organisation, public figures, the press or the general public. Wired links represent physical cables, such as fibre optic cables, analogue telephone copper pairs, and marine cables. Wireless links represent radio-frequency connections, such as public broadcasting networks, point-to-point links, or shared channels used by handheld two-way radios. Equipment nodes represent active components such as switches, exchanges, computing equipment and handsets. Finally, unresolved links represent subsystems of the telecommunication service of which we may have little or no knowledge. Unlike wired and wireless links, which represent single physical channels, unresolved links represent a collection of wired and wireless links and equipment. The inclusion of unresolved links in telecommunication service models is a novel idea in this work. Using unresolved links a model can be built for any telecommunication service. This model will be complete in scope, but may not yet have enough detail for RA.

We say that a telecom service model is well formed if it conforms to certain rules. The model must form a simple, connected graph (no edges from a node back to itself, no multiple edges between two nodes, and no disconnected partitions). Actor nodes must not connect directly to wired or wireless links. Wired and wireless link nodes must connect to exactly two equipment items or unresolved links. Lastly, equipment nodes must not be connected to each other. Nodes correspond to physical entities, and the rules correspond to their physical restrictions. The model must have at least two actors for communication to occur. The graph can thus meaningfully represent a physical reality.

Any telecommunication service model that contains an unresolved link can be refined. By refinement extra detail is added to the model; the lack of knowledge that is represented by the unresolved link is reduced. When a model is refined, an unresolved node *u* is replaced by a set of new nodes and edges between those nodes that jointly have the same interface as *u* (see Figure 1). Both the old model and its refinement describe the same physical reality. However, the new model – having more nodes and edges – can capture this physical reality in more detail.

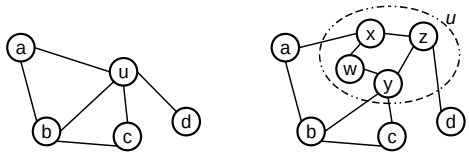

Figure 1. Model refinement. Unresolved node *u* is replaced by a set of new nodes and edges.

Models of telecommunication services are graphs, and can therefore be expressed graphically. The example in Figure 2 models satellite telephony as used by a small crisis team. The shape of a node indicates its type. To make the diagrams more meaningful to non-technical participants, nodes can be decorated with icons representing the physical component.

Risk assessment in the Raster method consists of four consecutive stages: preparation, refinement, common cause failures, and evaluation.

In the *preparation stage*, the crisis organisation and its context are described to facilitate the modelling and analysis. This description establishes the goal and boundaries of the risk assessment. It includes a list of disaster scenarios and checklists with frequently appearing vulnerabilities. The list of disaster scenarios limits the effort involved in applying the method. For example, if the disaster scenarios exclude dike breaches in a particular area, the risk of flooding of equipment cabinets in that area can be ignored for the purpose of this risk assessment. The checklists are used to aid risk identification.

During the *refinement stage*, a telecommunication service model is created for each telecommunication service used by the crisis organisation. For each telecommunication service, the initial model is drawn according to existing knowledge of the service. It will likely include one or more unresolved links. The remainder of this stage is then iterative. In each step one unexamined non–actor node is analysed; risks associated with actors are not taken into account.

For nodes that represent equipment, wired links or wireless links, the analysis describes likelihood, consequences and social risk factors. This description also includes a classification on a coarse grained, qualitative scale as well as an indication of uncertainty. The checklists should be consulted to ensure that all relevant threats have been considered.

For unresolved links no checklists are used. Instead, all types of vulnerabilities – those that apply to equipment,

wired links, and wireless links – are analysed as the subsystem may contain such components. If no reliable

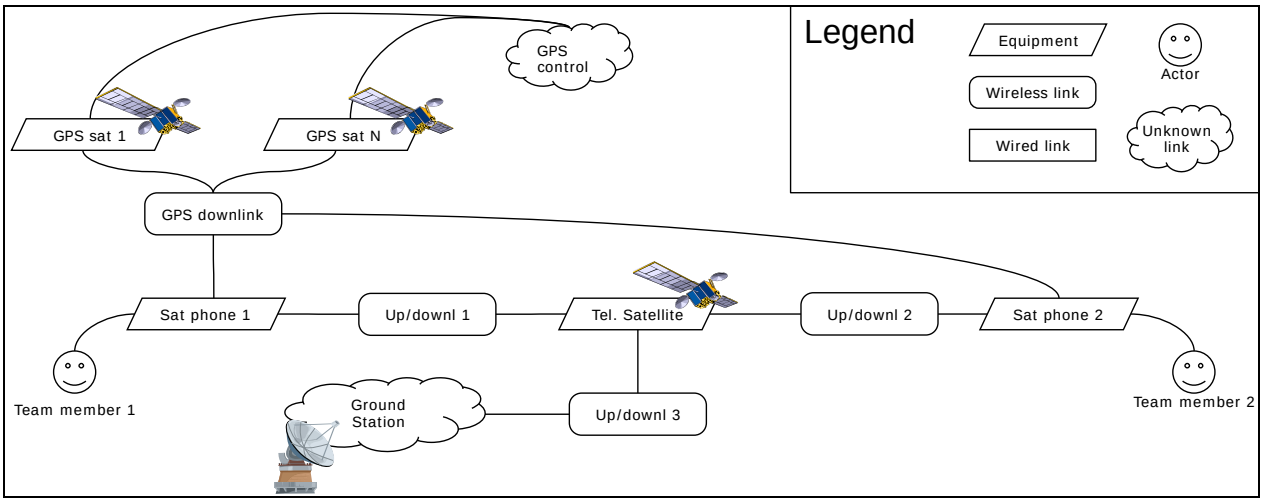

Figure 2. Example of a telecom service diagram: satellite telephony as used by a small crisis team.

analysis can be made due to lack of knowledge, the unresolved link must be expanded, and hence described in more detail.

Common cause failures (CCFs) are multiple failures that share a single underlying cause. Identification and analysis of sources of CCFs is the object of the third stage. We distinguish identity and proximity CCFs. Identity CCFs arise when the same node is present in two different models. Failure of that node could be a common cause for the failure of those telecommunication services. The first step in this stage is therefore to identify all nodes that exist in multiple models. Proximity CCFs arise when two nodes are physically sufficiently close together for them to be affected by the same threat. For example, two equipment items within the same room could be destroyed together in a fire; two cables within the same duct could be damaged by a single trenching incident; two wireless links could be affected by the same jammer. The second step in this stage is therefore to identify all combinations where such vulnerabilities may arise. As in the previous stage, further refinement of unknown links may be required. Common cause failures are described and classified in the same way as single vulnerabilities, as described above.

In the *evaluation stage*, all results from the previous stages are collated. The analysts determine the overall magnitude of each identified risk and rank them. For risks with a magnitude above some threshold, treatment options and their associated cost are described as well.

DISCUSSION

In this section we briefly compare Raster to the nine requirements listed in the introduction.

R1 No full model: The use of unrefined links and their refinement allows for the creation a model that is complete, but does not contain more information than necessary for the risk assessment. This treatment of unresolved links is central to the Raster method.

R2 Uncertainty: Raster explicitly takes account of reliability in information and disagreement among experts (ambiguity). However, uncertainty must first be recognised as such. Our experience from limited pilot studies indicates that analysts' group size and group composition are important for this. When the group is too small and too homogeneous, it appears less likely that uncertainty will be recognised, but further study is necessary to confirm this, and to determine optimal group size and composition. Limited amounts of uncertainty on the likelihood and impact are accounted for by the use of value classes, instead of numeric value estimates. This is a natural result of using a coarse grained qualitative scale.

R3 Social risk factors: Social risk factors are explicitly accounted for in Raster in the analysis of vulnerabilities. All social risk factors can be included; the current method does not cover a specific list and mechanism. We expect to give further guidance on this activity in later versions of the method, based on results from the current pilot projects.

R6 Exceptional circumstances: One of the input documents to Raster is a list of disaster scenarios. These scenarios are explicitly taken into account during the analysis stages.

R7 Identify all risks: Analysts use the checklist and their experience to enumerate failure causes for each component. They follow a structured methodology, but discovery of all possible failure causes is not

guaranteed by the method. A possible extension would be to employ Hazop analysis to generate the list of relevant events, rather than depend on checklists (IEC, 2001). In particular, we are investigating an adaptation of Hazop for use with programmable electronic systems (Redmill, Chudleigh and Catmur, 1997).

R9 Priorities and treatment options: A risk ranking is created in the evaluation phase. We believe that risk treatment options for these classes are in most cases obvious, as they will often be limited to simply accepting the risk or stop using the service. Risks with high uncertainty in their risk factors require discussion between all stakeholders. Possible treatment options include (temporarily) halting the use of that telecom service, or further studies.

Because of our limited experience with the Raster method, we cannot yet comment on requirements R4 (usability), R5 (effort required), and R8 (information over-aggregation). We are currently engaged in a pilot project, with the aim of learning more about the applicability and usefulness of Raster, and further case studies are being prepared.

RELATED AND FUTURE WORK

Failure Mode and Effect Analysis (FMEA) can be used to analyse telecom service models (IEC 2006). FMEA by itself does not meet our requirements, as it assumes the model already exists and does not guide its creation, does little to assist risk discovery and, most importantly, does not support discovery and analysis of common cause failures (CCFs). Fault Tree Analysis (FTA) also assumes a pre-existing model, but has extensions for analysis of CCFs (Mosleh 1991). Baiardi et al. describe a method that allows for model refinement during the analysis (Baiardi, Telmon and Sgandurra 2009). This method addresses information security risks only. None of the methods above take social risk factors into account. Klinke and Renn describe a scheme that does include social risk factors, but this is a general approach to risk decision-making, not a RA method (Klinke and Renn 2002).

Future research is needed to refine Raster, to investigate whether it meets all requirements. Especially, we intend to investigate whether improvements can be made to risk identification by using an adaptation of the Hazop methodology. Further work is also needed to improve risk evaluation in Raster, and to give more guidance on performing the risk analysis and use of social risk factors. We are planning an empirical evaluation of Raster in cooperation with local crisis organisations. We are interested whether this work can be extended to other organisations than crisis organisations, and possibly to critical infrastructures other than telecommunication. We also intend to investigate the relation between this work and risk in extended enterprises in general.

REFERENCES

1. Baiardi, F., Telmon, C. and Sgandurra, D. (2009) Hierarchical, model-based risk management of critical infrastructures, *Reliability Engineering and System Safety,* 94, 9, 1403–1415.
2. IEC (2001) Hazard and operability studies (HAZOP studies) – Application guide, International Standard 61882.
3. IEC (2006) Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA), International Standard 60812.
4. ISO/IEC (2009) Risk management – Principles and guidelines, International Standard 31000.
5. Klinke, A., and Renn, O. (2002) A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies, *Risk Analysis*, 22, 6, 1071–1094.
6. Mosleh, A. (1991) Common cause failures: an analysis methodology and examples, *Reliability Engineering & System Safety,* 34, 3, 249–292.
7. Redmill, F., Chudleigh, M. F., and Catmur, J. R. (1997) Principles underlying a guideline for applying HAZOP to programmable electronic systems, *Reliability Engineering and System Safety,* 55, 3, 283–293.
8. Slovic, P., Flynn, J. H. and Layman, M. (1991) Perceived Risk, Trust, and the Politics of Nuclear Waste, *Science*, 254, 5038, 1603–1607.
9. Van de Ven, J., van Rijk, R., Essens, P. and Frinking, E. (2008) Network Centric Operations in Crisis Management, *Proceedings of the 5th International ISCRAM Conference,* 764–773, Washington, DC, USA.