The Journal of Systems and Software 83 (2010) 1995–2013

Contents lists available at ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

Modular analysis and modelling of risk scenarios with dependencies

Gyrd Brændeland[a,b,*], Atle Refsdal[a], Ketil Stølen[a,b]

[a] SINTEF ICT, Oslo, Norway
[b] Department of Informatics, University of Oslo, Oslo, Norway

ARTICLE INFO

Article history:
Received 17 October 2008
Received in revised form 3 April 2010
Accepted 28 May 2010
Available online 11 June 2010

Keywords:
Modular risk analysis
Risk scenario
Dependency
Critical infrastructure
Threat modelling

ABSTRACT

The risk analysis of critical infrastructures such as the electric power supply or telecommunications is complicated by the fact that such infrastructures are mutually dependent. We propose a modular approach to the modelling and analysis of risk scenarios with dependencies. Our approach may be used to deduce the risk level of an overall system from previous risk analyses of its constituent systems. A custom made assumption-guarantee style is put forward as a means to describe risk scenarios with external dependencies. We also define a set of deduction rules facilitating various kinds of reasoning, including the analysis of mutual dependencies between risk scenarios expressed in the assumption-guarantee style.

1. Introduction

Mutual dependencies in the power supply have been apparent in blackouts in Europe and North America during the early two thousands, such as the blackout in Italy in September 2003 that affected most of the Italian population (UCTE, 2004) and in North America the same year that affected several other infrastructures such as water supply, transportation and communication (NYISO, 2003). These and similar incidents have lead to increased focus on the protection of critical infrastructures. The Integrated Risk Reduction of Information-based Infrastructure Systems project (Flentge, 2006), identified lack of appropriate risk analysis models as one of the key challenges in protecting critical infrastructures. There is a clear need for improved understanding of the impact of mutual dependencies on the overall risk level of critical infrastructures. When systems are mutually dependent, a threat towards one of them may realise threats towards the others (Rinaldi et al., 2001; Restrepo et al., 2006). One example, from the Nordic power sector, is the situation with reduced hydro power capacity in southern Norway and full hydro power capacity in Sweden (Doorman et al., 2004). In this situation the export to Norway from Sweden is high, which is a potential threat towards the Swedish power production causing instability in the network. If the network is already unstable, minor faults in the Swedish north/south corridor can lead to cascading outages collapsing the network in both southern Sweden and southern Norway. Hence, the threat originating in southern Norway contributes to an incident in southern Sweden, which again leads to an incident in Norway. Due to the potential for cascading effects of incidents affecting critical infrastructures, Rinaldi et al. (2001) argue that mutually dependent infrastructures must be considered in a holistic manner. Within risk analysis, however, it is often not feasible to analyse all possible systems that affect the target of analysis at once; hence, we need a modular approach.

Assumption-guarantee reasoning has been suggested as a means to facilitate modular system development (Jones, 1981; Misra and Chandy, 1981; Abadi and Lamport, 1995). The idea is that a system is guaranteed to provide a certain functionality, if the environment fulfils certain assumptions. In this paper we show how this idea applies to risk analysis. Structured documentation of risk analysis results, and the assumptions on which they depend, provides the basis for maintenance of analysis results as well as a modular approach to risk analysis.

By *risk* we mean the combination of the consequence and likelihood of an unwanted event. By *risk analysis* we mean the process to understand the nature of risk and determining the level of risk (ISO, 2009). *Risk modelling* refers to techniques used to aid the process of identifying and estimating likelihood and consequence values. A risk model is a structured way of representing an event, its causes and consequences using graphs, trees or block diagrams (Robinson et al., 2001). By *modular risk analysis* we mean a process for analysing separate parts of a system or several systems independently, with means for combining separate analysis results into an overall risk picture for the whole system.

* Corresponding author at: SINTEF ICT, Oslo, Norway. Tel.: +47 99107087; fax: +47 22067350.
E-mail address: gyrd.brendeland@sintef.no (G. Brændeland).

0164-1212/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2010.05.069

1.1. Contribution

We present an assumption-guarantee style for the specification of risk scenarios. We introduce *risk graphs* to structure series of events leading up to one or more incidents. A risk graph is meant to be used during the risk estimation phase of a risk analysis to aid the estimation of likelihood values. In order to document assumptions of a risk analysis we also introduce the notion of *dependent risk graph*. A dependent risk graph is divided into two parts: an assumption that describes the assumptions on which the risk estimates depend, and a target. We also present a calculus for risk graphs. The rules of the calculus characterise conditions under which

- the analysis of complex scenarios can be decomposed into separate analyses that can be carried out independently;
- the dependencies between scenarios can be resolved distinguishing bad dependencies (i.e., circular dependencies) from good dependencies (i.e., non-circular dependencies);
- risk analyses of separate system parts can be put together to provide a risk analysis for system as a whole.

In order to demonstrate the applicability of our approach, we present a case-study involving the power systems in the southern parts of Sweden and Norway. Due to the strong mutual dependency between these systems, the effects of threats to either system can be quite complex. We focus on the analysis of blackout scenarios. The scenarios are inspired by the SINTEF study *Vulnerability of the Nordic Power System* (Doorman et al., 2004). However, the presented results with regard to probability and consequences of events are fictitious.

For the purpose of the example we use CORAS diagrams to model risks (Lund et al., in press). The formal semantics we propose for risk graphs provides the semantics for CORAS diagrams. We believe, however, that the presented approach to capture and analyse dependencies in risk graphs can be applied to most graph-based risk modelling languages.

1.2. Structure of the paper

We structure the remainder of this paper as follows: in Section 2 we explain the notion of a risk graph informally and compare it to other risk modelling techniques. In Section 3 we define a calculus for reasoning about risk graphs with dependencies. In Section 4 we show how the rules defined in Section 3 can be instantiated in the CORAS threat modelling language, that is how the risk graphs can be employed to provide a formal semantics and calculus for CORAS diagrams. In Section 5 we give a practical example on how dependent risk analysis can be applied in a real example. In Section 6 we discuss related work. In Section 7 we summarise our overall contribution. We also discuss the applicability of our approach, limitations to the presented approach and outline ideas for how these can be addressed in future work.

2. Risk graphs

We introduce risk graphs as a tool to aid the structuring of events leading to incidents and to estimate likelihoods of incidents. A risk graph consists of a finite set of vertices and a finite set of relations between them. In order to make explicit the assumptions of a risk analysis we introduce the notion of dependent risk graph, which is a special type of risk graph.

Each vertex in a risk graph is assigned a set of likelihood values. A vertex corresponds to a threat scenario, that is, a sequence of events that may lead to an incident. A relation between threat scenarios t_1 and t_2 means that t_1 may lead to t_2. Both threat scenarios and relations between them are assigned likelihood values. A threat scenario may have several causes and may lead to several new scenarios. It is possible to choose more than one relation leaving from a threat scenario, which implies that the likelihoods on relations leading from a threat scenario may add up to more than 1. Furthermore, the set of relations leading from a threat scenario does not have to be complete, hence the likelihoods on relations leading from a threat scenario may also add up to less than 1.

There exists a number of modelling techniques that are used both to aid the structuring of threats and incidents (qualitative analysis) and to compute probabilities of incidents (quantitative analysis). Robinson et al. (2001) distinguishes between three types of modelling techniques: trees, blocks and integrated presentation diagrams. In Section 2.1 we briefly present some types of trees and integrated presentation diagrams, as these are the two categories most commonly used within risk analysis. In Section 2.2 we discuss how two of the presented techniques relate to risk graphs. In Section 2.3 we discuss the need for documenting assumptions in a risk analysis and explain informally the notion of a dependent risk graph. The concepts of risk graph and dependent risk graph are later formalised in Section 3.

2.1. Risk modelling techniques

Fault Tree Analysis (FTA) (IEC, 1990) is a top-down approach that breaks down an incident into smaller events. The events are structured into a logical binary tree, with and/or gates, that shows possible routes leading to the unwanted incident from various failure points. Fault trees are also used to determine the probability of an incident. If all the basic events in a fault tree are statistically independent, the probability of the root event can be computed by finding the minimal cuts of the fault tree. A minimal cut set is a minimal set of basic events that is sufficient for the root event to occur. If all events are independent the probability of a minimal cut is the product of the probabilities of its basic events.

Event Tree Analysis (ETA) (IEC, 1995) starts with component failures and follows possible further system events through a series of final consequences. Event trees are developed through success/failure gates for each defence mechanism that is activated.

Attack trees (Schneier, 1999) are basically fault trees with a security-oriented terminology. Attack trees aim to provide a formal and methodical way of describing the security of a system based on the attacks it may be exposed to. The notation uses a tree structure similar to fault trees, with the attack goal as the root vertex and different ways of achieving the goal as leaf vertices.

A *cause-consequence diagram* (Robinson et al., 2001; Mannan and Lees, 2005) (also called cause and effect diagram Rausand and Høyland, 2004) combines the features of both fault trees and event trees. When constructing a cause-consequence diagram one starts with an incident and develops the diagram backwards to find its causes (fault tree) and forwards to find its consequences (event tree) (Hogganvik, 2007). A cause-consequence diagram is, however, less structured than a tree and does not have the same binary restrictions. Cause-consequence diagrams are qualitative and cannot be used as a basis for quantitative analysis (Rausand and Høyland, 2004).

A *Bayesian network* (also called Bayesian belief network) (Charniak, 1991) can be used as an alternative to fault trees and cause-consequence diagrams to illustrate the relationships between a system failure or an accident and its causes and contributing factors. A Bayesian network is more general than a fault tree since the causes do not have to be binary events and causes do not have to be connected through a specified logical gate. In this respect they are similar to cause-consequence diagrams. As opposed to cause-consequence diagrams, however, Bayesian networks can be used as a basis for quantitative analysis (Rausand and