Dependability analysis of critical infrastructures

Hamed Ghasemieh
Supervisor: Anne Remke, **Promoter**: Boudewijn Haverkort

May 11, 2013

More and more, our society and economy rely on the well-operation of, often hidden, Information and Communication Technology (ICT) infrastructures. These ICT infrastructures play an ever-increasing role in other critical infrastructures, such as the power grid and water and gas distribution networks. The focus of this project lies on the dependability analysis of fluid critical infrastructures, such as water treatment and distribution networks. We will study cyber and physical vulnerabilities of such systems and analyse how quickly such systems recover to acceptable levels of service after the occurrence of failures, natural disasters (e.g., fire earthquakes) or cyber-attacks.

We propose the use of stochastic hybrid models(SHMs) to formally describe fluid critical infrastructures. SHMs combine discrete and continuous quantities with stochastic, hence, allow to model random phenomena in a natural way. The interdependencies between the physical process and the ICT control infrastructure are crucial in critical infrastructures.

To ensure the scalability of our approach, we strive to build compositional models and to conduct compositional analysis. Furthermore, we propose to separate the deterministic and the stochastic evolution of the system, by a conditioning / deconditioning argument. This will speed up the analysis and will allow for a large number of continuous variables in the model, as opposed to existing approaches. We will use a carefully chosen and semantically sound notion of dependability to express the measures of interest and use stochastic model checking techniques to evaluate these measures.

Namely, we introduce hybrid Petri nets with a single general one-shot transition (HPnGs) for modelling fluid critical infrastructures such as water refinery plants. HPnGs allow for a combination of discrete and fluid state variables, and can be used to evaluate, for instance, the probability of fluid reservoirs to become empty before certain events have happened. However, for critical infrastructures, often more complex system properties, most notably also survivability needs to be evaluated. The survivability of a system is defined as the probability that the system recovers within a predefined amount of time to a predefined level of service. We also introduce a new logic and an efficient model checking algorithms for inspecting such questions.