ANALYZING RISKS OF NETWORKED TECHNICAL SYSTEMS CONSIDERING AS EXAMPLE INTERNET VIRUS ATTACKS

Martin Diergardt

Laboratory for Safety Analysis, ETH Zurich, Weinbergstrasse 11, CH-8092 Zurich

Introduction: The increasing number of networked technical systems exhibit special risks which are difficult to analyze with established techniques due to the prevailing complexity, dynamics, and uncertainty. As a consequence, more advanced risk analysis approaches need to be developed which are able to overcome these limitations. By considering as example the risks through internet virus attacks the proposed contribution introduces a novel approach how risk analysis of complex networked technical systems can be performed.

Background: In the early hours of January 25, 2003 the SQL Slammer worm hit the internet and infected more than 90 percent of vulnerable computers within 10 minutes causing significant disruption to financial, transportation, and government institutions. Techniques to efficiently analyze the frequency and consequence of such undesired events in advance which would support the service providers in identifying suitable security measures are currently hardly available.

Research objectives: In order to extend the application area of risk analysis techniques the traditional branched event sequence modeling techniques, e.g., fault tree, event tree, need to be expanded to incorporate cascading event sequences. Additionally, the approach should also facilitate an efficient and intuitive presentation of complex sequences of undesired events and represent a sound basis for subsequent simulations to generate risk curves.

Approach: By taking advantage of the enhanced structured knowledge representation of complex information systems by business process modeling techniques and especially of Event Driven Process Chains (EPCs) it is possible to model cascading event sequences. Furthermore the derived model technique can be used for subsequent simulations, by using transformation rules to map the compiled semiformal models into Petri nets and system dynamics models. In order to examine the practicability of this novel approach, undesired events similar to the SQL Slammer incident were analyzed in more detail.

Expected results: Although the detailed analysis of undesired events similar to the SQL Slammer incident has not yet been completely finished, it is expected that the described approach is able to provide valuable insights for service providers confronted with internet virus attacks. Additionally, this novel approach can also be applied for risk related questions for other networked technical systems, e.g. energy supply systems.