Abstract

The thesis proposes a solution to the problem of recognizing and modeling risk transmission contained in documents describing a system's operation or failure. Relationships are determined in the context of entire documents and go beyond the currently dominant approach of identifying relationships within a single sentence and using classifiers trained on collected dedicated training examples.

The problem being addressed is significant because information about the flow of threats can create complex interactions between system elements described in such a way that they may be scattered throughout the document and even between sources. There is generally a lack of dedicated training sets for classifiers, and existing solutions are limited to selected areas, such as railways, or description formats, such as HAZOP or FMEA.

The proposed solution involves a gradual decomposition of descriptions. The examined text is decomposed into a Semantic Frames Graph (SFG) in the first step. In the second step, the pattern of threat propagation relationships is used to recognize propagation. Recognized propagations are stored in an Intermediate Relationship Graph (IRG). In the final step, propagations are aggregated into the form of an Asset-Vulnerability-Hazard (A-V-H) graph, which allows for a network analysis of the risk contained in the description of the operation of a given system.

The proposed approach allows for modeling risk propagation without needing a dedicated relationship detection mechanism, as this method is based on verbalizing the relationship pattern. Another reason for eliminating dedicated classification is the extension of pattern analysis to analyze the dialog coherence in the path between nodes in the SFG graph. The detection results obtained by combining both methods are verified using current language models (Large Language Models such as chatGPT) and prompt engineering. The threshold above which relationships are accepted is a solution to the multi-criteria optimization task.

Overall, this work presents a new method for detecting relationships and its application in risk analysis. It also explores the potential of semantic pattern methods, dialogic coherence, and prompt engineering in constructing a network risk model, which facilitates modeling complex threat propagation dependencies.