Summary of the PhD Thesis:

Methodology for Documentation and Analysis of

Weaknesses in Communication in Safety Critical Systems

within hierarchical Task Models

By Tomasz Mistrzyk

This thesis describes a methodology for the documentation and analysis of communication weaknesses in safety critical systems. The methodology is based on a new communication model and uses the benefits of a systematic representation of task dependencies by hierarchical task models.

Communication occupies a key position in safety critical systems because it is responsible for the appropriate coordination of tasks in such systems. Weaknesses within the communication between actors in socio-technical safety critical systems are considered to be the main cause for critical events or accidents. These systems include technical components, such as telecommunication devices, machines and computers, as well as human actors performing tasks and using technical devices which support their work.

The target of this thesis is to work out a systematic approach which documents and analyses the communication between actors in safety critical systems. To accomplish this, an appropriate description calculus will be created to model communication. This calculus will help to find improper communication and also identify possible consequences for coordinated tasks. Beyond that, parameters will be proposed to estimate the criticality of the weaknesses in the communication processes.

The methodology allows the discovery of both, weak constellations in the communication process, as well as latent communication failures. Besides this, it allows to point out not only the deficits in the communication but also consequences for the system. The methodology was validated in detail by case studies which stem from the health care domain.