DOCTORAL CANDIDATE:	Rajwinder Kaur Panesar-Walawege
DEGREE:	Philosophiae Doctor
FACULTY:	Faculty of Mathematics and Natural Sciences
DEPARTMENT:	Department of Informatics
AREA OF EXPERTISE:	Software Engineering
SUPERVISORS:	Lionel Briand and Mehrdad Sabetzadeh
DATE OF DISPUTATION:	3rd of August 2012

DISSERTATION TITLE: *Using Model-Driven Engineering to Support the Certification of Safety-Critical Systems*

Critical systems such as those found in the avionics, automotive, maritime, and energy domains are often subject to a formal process known as certification. The goal of certification is to ensure that such systems will operate safely in the presence of known hazards, and without posing undue risks to the users, the public, or the environment. A key prerequisite for effective collection of evidence is that the system suppliers be aware of the requirements stipulated in the relevant standard and the evidence they require.

This often proves to be a very challenging task because of the sheer size of the standards and the fact that the textual standards are amenable to subjective interpretation. Notably, suppliers find it hard to interpret the evidence requirements imposed by the safety standards within the domain of application; little support exists for recording, querying, and reporting evidence in a structured manner; and there is a general absence of guidelines on how the collected evidence supports the safety objectives.

The main contribution of this thesis is a model-driven process that enables the automated verification of compliance to standards based on evidence. The Unified Modeling Language (UML) is used to create a UML profile based on a conceptual model of a given standard, which provides a succinct and explicit interpretation of the underlying standard. The profile is augmented with constraints that help system suppliers with establishing a relationship between the concepts in the safety standard of interest and the concepts in the application domain. This in turn enables suppliers to demonstrate how their system development artifacts achieve compliance to the standard.

Additionally, UML profiles are further used to systematically capture how the evidence requirements of a generic standard are specialized in a particular domain. This provides a means of explicitly showing the relationship between a generic and a sector-specific standard. This tackles the certification issues that arise from poorly-stated or implicit relationships between generic standards and their sector-specific interpretations.

Finally, the tool infrastructure needs for supporting the collection and management of safety evidence data is tackled by proposing tools for upfront planning of evidence collection activities and the storage of evidence information outside of modelling environments.