DOCTORAL CANDIDATE:	Sunil Nair
DEGREE:	Philosophiae Doctor
FACULTY:	The Faculty of Mathematics and Natural Sciences
DEPARTMENT:	Department of Informatics
AREA OF EXPERTISE:	Software Engineering
SUPERVISORS:	Prof. Tim Kelly, Dr. Jose Luis dela vara, Prof. Magen Jørgensen
DATE OF DISPUTATION:	27th of March 2015
DISSERTATION TITLE:	*Characterization of Safety Evidence for Assessment and Certification of Critical Systems*

In many domains such as avionics, railway and automotive, software-based systems need to be certified or assured for safety so that the failure of such systems do not cause undue risk to the user, public or the environment. Deeming a system to be safe involves gathering convincing evidence to argue the safe operation of the system, usually according to the requirements of some safety standard.

Nair's thesis is aimed at understanding and characterizing the safety evidence information used for certification and assessment of safety-critical system. The thesis analyses the current state-of-the-art and state-of-the-practice on evidence management focusing specifically on what information contributes as evidence for safety, how is evidence structured and assessed and how is confidence on the evidence documented by human experts. As a result of the analysis, the thesis presents (1) a taxonomical classification of various evidence types, (2) a glossary of development and verification artifacts that contribute to each category, (3) a detailed traceability information model for safety evidence showing the various elements that characterize the evidence, and finally (4) a novel approach and tool support for assessing confidence in safety evidence by explicitly documenting the various reasons for establishing confidence while accounting for uncertainty.

The contribution provided in Nair's thesis have been developed in the scope of OPENCOSS, a large-scale European research project whose goal is to devise a common certification framework for the automotive, avionics, and railway domains.