Belgian Francqui Chair
2006-2007

Engineering Requirements for Mission-Critical Software Systems

Prof. Dr. Axel van Lamsweerde
http://ssel.vub.ac.be/francqui/

Inaugural Lecture
Modelling Software Systems and Engineering their Requirements: Why Should we care?
Thursday April 26, 16:00-18:00
Vrije Universiteit Brussel, campus Etterbeek
Room D.0.08
Requirements engineering (RE) embodies a wide range of concerns. The objectives to be achieved by the system-to-be have to be elicited and analyzed within some organizational or physical context; such objectives are to be operationalized into specifications of services, constraints, and assumptions; and the responsibilities for such specifications need to be assigned among the humans, devices, or software components forming the system. Requirements emerge from this process as prescriptive assertions on the software-to-be, formulated in the vocabulary of the environment. Getting high-quality requirements is difficult and critical. The system stakeholders in general have diverse, partial, and often conflicting concerns. Poor requirements have been recurrently recognized to be the major cause of project cost overruns, delivery delays, failure to meet expectations, or severe degradations in the environment controlled by the software.

The course overviews a systematic, goal-oriented approach to requirements engineering for high-assurance systems. The target of this approach is a complete, consistent, adequate, and structured set of software requirements and environment assumptions. The approach is model-based and partly relies on the use of formal specifications, when and where needed, for specific kinds of analyses.

The course first introduces basic principles of goal-oriented requirements engineering. Key notions such as “goal”, “requirement”, “domain property”, and “environmental assumption” are defined and related to each other. A multi-view modeling framework is then introduced in the specific context of engineering requirements for complex, large-scale systems. Different kinds of models are used to integrate different kinds of facets of the system-to-be: goals and their refinements; hazards and threats to safety and security goals, respectively; conceptual objects referenced by goals together with their inter-relationships; operations that ensure the goals; agents, their responsibilities, behaviors, and interaction scenarios. The emphasis here is on a method for constructing such multi-view models in a systematic way.

Critical model items need to be formalized to enable their formal analysis for higher assurance. We briefly review some rudiments of real-time linear temporal logic for specifying goals, domain properties, hazards, and threats; goal-structured pre-/postconditions for specifying operations; fluents for linking goals to operations; and specification patterns for lightweight specification.

The course then presents a variety of formal techniques supporting the following RE-specific tasks:

• refining goals, operationalizing fine-grained goals, and checking the correctness of refinements;
• animating goal-oriented models for checking their adequacy;
• analyzing safety hazards by generating obstacles to goal satisfaction and resolving them;
• analyzing security threats by generating malicious plans to break security goals, and counter-measures to address these;
• analyzing conflicts among stakeholder goals, and resolving them;
• generating agent behavior models inductively from interaction scenarios and goal specifications;
• assessing alternative goal refinements and responsibility assignments based on quality goals refined in the model.

The presentation will be illustrated through representative examples and tool demonstrations.
Axel van Lamsweerde is Full Professor at the Department of Computing Science of the Université catholique de Louvain, Belgium. He was formerly research associate at Philips Research Labs and professor at the universities of Namur and Bruxelles. He was also research fellow at the University of Oregon and the Computer Science Lab of Stanford Research Institute (Menlo Park, CA). He was co-founder of two software technology transfer centers supported by the European Union.

His research interests are in precise techniques for requirements engineering, system modeling, high assurance systems, lightweight formal methods, process modeling and analysis, medical safety, and knowledge-based software development environments. Since 1990 he has been instrumental in the development of the KAOS goal-oriented modeling language, method, and toolset. The method and toolset have been used worldwide in more than 25 industrial projects. He is author of the forthcoming book “Requirements engineering: From System Goals to UML Models to Software Specifications” (Wiley).

Axel van Lamsweerde was Editor-in-Chief of the ACM Transactions in Software Engineering and Methodology (ACM, New York), Program Chair of major international software engineering conferences including ESEC’91 and ICSE’94, founding member of the IFIP WG2.9 Working Group on Requirements Engineering, and is currently Associate Editor of the IEEE Transactions on Software Engineering. He has been keynote speaker at major conferences in the field including the International Conference on Software Engineering (ICSE’2000) and the International Joint Conference on Requirements Engineering (RE’04). He is an ACM Fellow and is recipient of the ACM SIGSOFT Distinguished Service Award.