Janos Sztipanovits

Title: Towards Model-Based Software Synthesis for Resilient Control Systems

Abstract: The focus of the paper is the extension of model-based software design methods developed for the synthesis of high-confidence real-time control software with security as a new design concern. The proposed approach expresses the resilient control system design task as a synthesis problem that addresses functional, security and resource requirements the following way:

1. Functional requirements - expressed as control and observer dynamics models - are mapped into software component code, software component architecture, and timing models.

2. The integrity and confidentiality aspects of security requirements are expressed as restrictions on information flows defined by software/system architecture models.

3. The models of implementation platforms for computing and communication are complemented by performance and security characterization.

The synthesis problem is defined as finding a deployment model where the information flows satisfy all functional ad security requirements and the allocated computation and communication resources satisfy all timing requirements. The paper discusses initial ideas for the modeling language suite, the underlying semantics expressed in the constraint logic programming framework FORMULA and presents initial experiments and results.