Incorporating Security into DSMLs
Advantages of Design Time Security Modeling

Domain Specific Modeling Language (DSML) examples
- SysML
- AADL
- UML

Security Extension examples
- Partitioning
- Role Based Access Control (RBAC)
- Secure Links
- Fair Exchange (guaranteed transactions)

Vulnerabilities
- Access Violation
- Operation of Authentication
- Violation of Confidentiality
- Violation of Integrity

Comparison of AADL and the Security Extended AADL

AADL Execution Environment

Gain with the Security Extended AADL
Introducing security at design level
- Consistent and automatic configuration of security services offered by the operating system and middleware
- Investigating design tradeoffs between performance and security properties
- Verifying required security properties using explicit security models

Platform Security / Security Service Modeling
Abstracts out security properties of the platform that are essential for the design flow

Security Service Providers
- OS (ex: Linux, LynxOS, WinCE)
- HW (ex: Space Partitioning, Memory protection)
- Services of different applications
- (ex: Web Browser Based Authentication)

Security Extension Metamodel

A DSML Example with the Security Extension
AADL with RBAC and Partitioning

Automatic Code Generation
Code generators traverse the model and produce secure code that enforces the RBAC policies. The code generator makes use of the partitioning capabilities of the underlying platform.