Objectives: Tool chain to analyze security properties of large cyber-infrastructure installations

Requirements:
Develop formal models which incorporate various aspects of security
Should allow people with minimal knowledge of formal methods to describe the system

Some Best Practices in Security
• Least-Privilege
  Every entity should be given the least privilege required for its tasks
• Complete Mediation
  Every operation must be verified to see if should be allowed.
• Least common mechanism
  If some mechanism is common amongst users with different privileges there is potential for misuse.
• Separation of Privilege
  Privileges to perform various phases of critical operations must be spread into multiple users
• Work Factor
  The amount of work required for accessing a resource should be commensurate with the value of that resource

Solution
Authentication: Use Hierarchical Role-Based Access Control as underlying model, abstract RBAC as equational-logic
Workflows: Annotate YAWL with RBAC security.
Extract workflow transitions as FSM in term-rewriting systems.
Architecture: Annotate CIM with RBAC. Represent as sorts.
Express policies, best practices, common criteria profiles as LTL constraints.
Use Model Checking (in Maude) to verify formulae are satisfied or find a counter-example.

Example
Distributing avionics software and loading it into planes

Security property: The process of updating the avionics software and verifying the update cannot be done by the same technician for a given plane