U.S. DEPARTMENT OF ENERGY | Nuclear Energy

Office Of Nuclear Energy
Sensors and Instrumentation
Annual Review Meeting

A Method for Quantifying the Dependability Attributes of Software-Based Safety Critical Instrumentation and Control Systems in Nuclear Power Plants

Dr. Carol Smidts
The Ohio State University

September 16-18, 2014

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Project Overview

Goal, and Objectives

Develop measures and methods to assess dependability attributes early and throughout the life-cycle process of software development

Participants

- University PI: Dr. Carol Smidts, The Ohio State University (Started February 1, 2014)
- Industry PI: Mr. Ted Quinn, Technology Resources (Started February 1, 2014)
- Postdoctoral researcher: Dr. Fuqun Huang, The Ohio State University (Started June 1, 2014)
- PhD Students: Xiang Li, The Ohio State University (Started May 20, 2014)

Project Overview (cont'd)

Schedule

Tasks	Date
Kick-off meeting	April 1 to May 15, 2014
Elicit a causal map describing the dependencies between dependability attributes	May15 to July 15, 2014
For each dependability attributes, elicit the causal map describing occurrence of the event of interest	May 15 to August 31, 2014
Relate measurable concepts to each concept in the event of interest level	August 31 to December 31, 2014

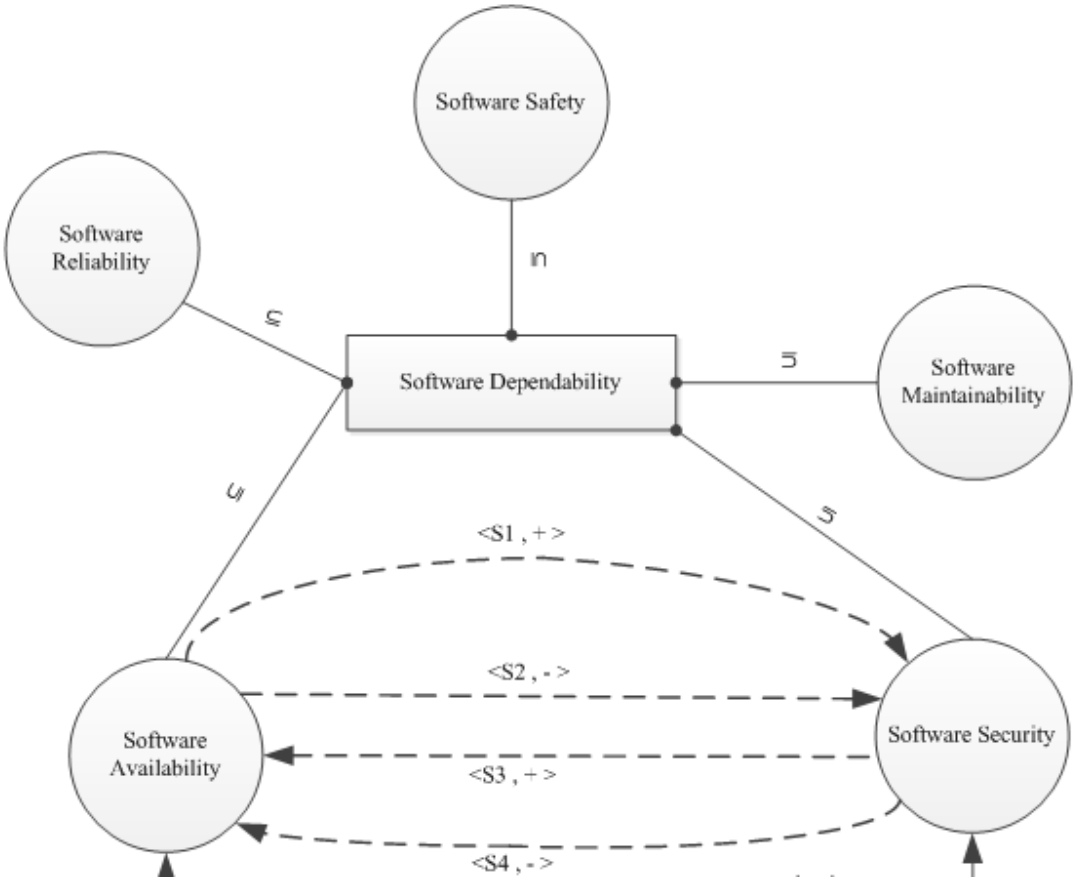
U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Accomplishments

- **Description of milestones, deliverables, outcomes for FY14**
  - M3: Establish a causal mapping structure to capture relationships between software dependability attributes
    - The causal structure was constructed using *expert opinion elicitation*
    - More than 600 experts were identified and 54 were selected based on their relevant publications demonstrating knowledge in at least two dependability attributes
    - The expert selection procedure was inspired from the knapsack problem
    - A semi-structured questionnaire was designed to elicit their knowledge
    - 19 experts were contacted, 14 responses received
    - Categories of concepts and relations were defined to extract causal knowledge
    - Experts' responses were analyzed using qualitative coding and mapped to these

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Accomplishments (cont'd)



Scenario list

S1: Fault tolerant mechanisms are properly designed and do not increase the attack surface
S2: Fault tolerant mechanisms increase the attack surface
S3: Additional complexity resulting from security detection and protection mechanisms does not lead to new design and interaction faults
S4: Security checks may require in some specific scenarios the interruption of service operation to provide protection against an ongoing attack or to update software version or operational procedures
S5: Physical access to the target machines
S6: Software is in a specific state, or at a given time

Causal map between dependability attributes established based on the questionnaire on Dependability & Security

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

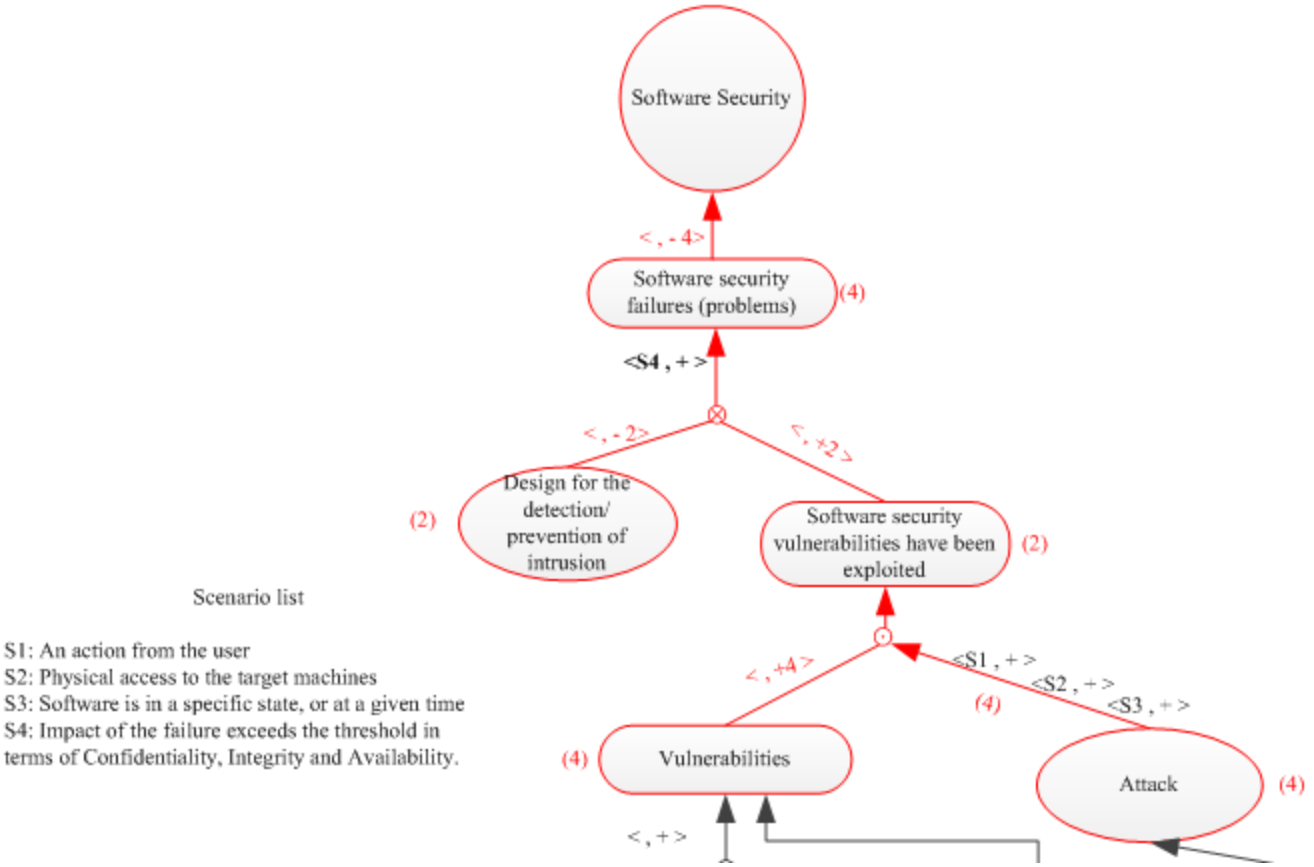
Accomplishments (cont'd)

- The figure in the previous slide shows that reliability, availability, maintainability, safety and security are subsets of dependability
- Security and availability are related to each other, and under different scenarios/conditions, the relation can be either positive or negative.
- Correlations between attributes are formed due to the existence of shared causal factors and mechanisms.

Accomplishments (cont'd)

- **Description of milestones, deliverables, outcomes for FY14**
  - M4: Determine the main causal mechanisms leading to key outcomes of interest associated with each software dependability attribute
    - Experts' responses to the questionnaires also contain detailed information on the causal factors that result in failures of the dependability attributes. For instance, software security failures are caused by the factors shown in the figure in the next slide.
    - The method used to extract the causal failure mechanisms includes:
      1) Merging of the individual causal maps related to a particular dependability attribute;
      2) Slicing of the map which retains only consensus concepts and relations.

Accomplishments (cont'd)



U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Accomplishments (cont'd)

- In the previous slide, the numbers in parentheses indicate the number of experts in agreement.

- The agreed upon causal mechanism for failure is:
  - Existing vulnerabilities may be triggered by attacks through action of a user, physical access to target machines, etc.
  - The intrusion detection/prevention mechanisms are designed to mitigate an exploited vulnerability. When the design mechanisms fail to detect/prevent the event, and if the effect of the exploited vulnerabilities were to exceed a threshold, they will manifest themselves as security failures.

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Accomplishments (cont'd)

- **Description of milestones, deliverables, outcomes for FY14**
  - M4: Identify measureable characteristics and corresponding measures for the outcome of interest associated with each software dependability attribute (will be completed by 12/31/2014)
    - Questionnaires are being designed to elicit experts' opinions on the measurable concepts and corresponding measures for each event of interest. More specifically, a measureable concept for software security is "vulnerability", and the experts are asked to provide the measures for "vulnerability"
    - Experts are now being selected based on their expertise in a single dependability attribute
    - Currently we have designed the questionnaires for security, availability and sent these out to some of our experts. The questionnaires for safety and maintainability are still being developed.

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Technology Impact

- **Method contributions:**
  - Expert knowledge elicitation by semi-structured questionnaire.
  - Causal mechanism extraction, e.g. qualitative coding.
  - Causal mechanism modeling method. The causal maps in this research can represent the logical relations between concepts, and their complex interactions under different circumstances.
  - Causal map merging method. This research provides a set of formal merging rules, which enables us to combine causal maps and produce aggregated maps based on individual causal maps.
  - Causal map analysis methods are being developed, e.g. *consensus* content analysis and major theme analysis.

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Technology Impact (cont'd)

- **Problem domain contributions:**
  - Provide the dependencies between various software dependability attributes.
  - Provide deep insights on the causal mechanisms of these dependencies.
  - Elicit measurements based on a perspective of causal mechanisms rather than just based on correlative shaping factors.

U.S. DEPARTMENT OF ENERGY
Nuclear Energy

Conclusion

- **Our study will provide a systematic science-based method for quantifying the dependability attributes in software-based instrumentation and control systems.**
- **The results of these assessments can be used in two different ways:**
  - To guide development, which will enhance dependability of the final software product thereby reducing the regulatory uncertainty.
  - To build a safety/dependability case.