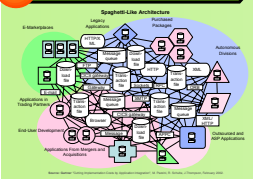
r-AnalytiCA Workbench

Requirements Analytics for Certification & Accreditation (C&A)

Seok-Won Lee, Robin A. Gandhi, Siddharth J. Wagle, Ajeet B. Murty

Knowledge-Intensive Software Engineering (NiSE) Research Group, College of Computing and Informatics, UNC Charlotte, NC, USA

1 The Problem

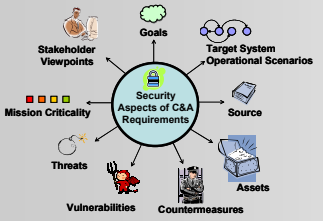


- People
- Organization
- Physical Surroundings
- Laws and Regulations
- Hardware, Software & Firmware
- Policies and Procedures
- Knowledge/Information/Data

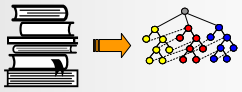
- **The complexity of current software systems**
- **The diversity of socio-technical operational environments**
- **Numerous interdependent quality constraints imposed by regulatory C&A requirements**
- **The resulting LARGE collection of compliance evidences is far beyond the capacity of manual approaches to produce *"meaningful insights"* necessary for software assurance**

2 A Common Understanding of C&A Requirements

- Numerous C&A requirements
  - Ambiguous natural language
  - Different granularity from multiple stakeholders
  - Scattered across regulatory documents
- We explicate C&A requirements from multiple dimensions in a socio-technical environment to promote their **common understanding**



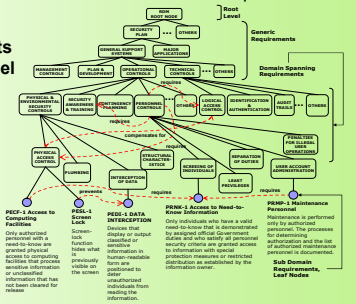
Lee, S.W. Gandhi, R.A., Ahn, G.J.: **Certification Process Artifacts Defined as Measurable Units for Software Assurance**, Int'l Journal of SPIP, April 2007, Wiley



- **The Ontology-based Active Requirements Engineering (Onto-ActRE)** framework guides ontological domain modeling techniques for classifying and categorizing C&A requirements from the dimenions of:
  - **Requirements domain model**
  - **Viewpoints hierarchy** that models different perspectives from related stakeholders
  - **C&A process goal hierarchy** with leaf-node scenarios to express process activities
  - **Domain-specific taxonomies of risk components** of assets, threats, vulnerabilities, and countermeasures
  - **Interdependencies** among these concepts

Problem Domain Ontology (PDO) 3

- The resulting **PDO reflects the semantics of C&A requirements** based on their relationships with each other as well as other relevant domain concepts.
- A Partial **Requirements Domain Model** in the PDO



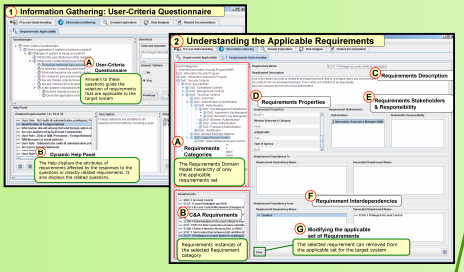
Lee, S.W. Muthurajan, D. Gandhi, R.A. et al.: **Building decision support problem domain ontology from natural language requirements for software assurance**, IJSEKE, 16(6), Dec 06

4 The *r*-AnalytiCA Workbench

The purpose of the *r*-AnalytiCA workbench is to enable rich **requirements analytics** upon the PDO to provide meaningful insights to a certification analyst during the C&A process.

r-AnalytiCA Workbench

Understanding C&A Requirements

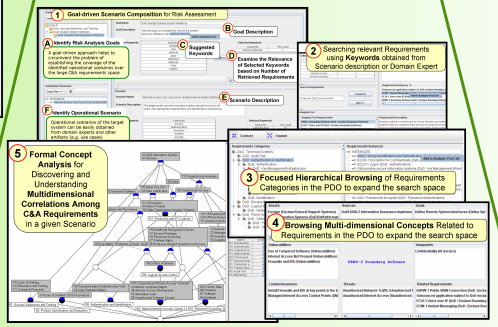


- **Well-defined Requirements Applicability Criteria**
  - Requirements applicability questionnaire
  - Answer options prune the search space consisting of all requirements in the PDO to select only the applicable set of requirements
- **A Common Understanding of Requirements**
  - Understand requirements based on multi-dimensional concepts in the PDO
  - Clear, concise, and structured representation of requirements

Compliance Evidence Gathering

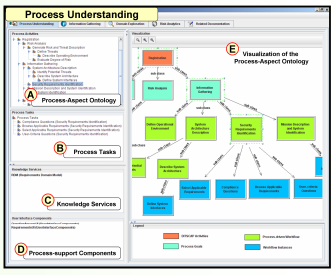
- **Uniform Compliance Assessment Criteria**
  - Requirements compliance questionnaire
  - Answer options defined as a conjunction of diverse metrics and measures to convey ordered level of compliance
- **Understanding & Communicating Compliance**
  - Different categorizations and levels of abstraction available using the PDO

Risk Analytics



- **Understanding Emergent System Behavior**
  - Discover and understand multi-dimensional correlations among C&A requirements
  - **Formal Concept Analysis** as an algebraic model
- **Goal-driven Scenario Composition for Risk Assessment**
  - Target system operational scenario as triggers
  - Multiple-search strategies help to build an analysis pool of diverse requirements relevant in a given scenario
- **Risk Understanding & Communication**
  - Non-compliance impact analysis
  - Risk upper and lower bound metrics
  - Prioritized list of requirements and risk components

C&A Process Analytics



- **Active Process Guidance**
  - Understand the required resources for C&A process goal satisfaction
  - C&A Process visualization and tracking
- **Ontology-driven Architecture Composition**
  - The architecture combines **Service and Aspect-oriented design paradigms**
  - Ability to accommodate different C&A processes or quality regulations

C&A Documentation Analytics

- **Understanding Documentation Artifacts**
  - Ontological model of the C&A document template and their interdependencies
- **Traceability and Progress Tracking**
  - Each section is related to its relevant C&A requirements
  - Support for attaching reports, diagrams and other related C&A artifacts

5 Contributions

- Utilize the synergy among multiple requirements modeling techniques to produce insightful C&A artifacts
- An environment to support multi-dimensional problem domain analysis with well-defined metrics and measures
- Common understanding among C&A stakeholders
- Methodological support for complex C&A process

6 Future Work

- Discovering global (system-wide) correlations among C&A requirements for risk assessment
- Conduct case studies with C&A experts to evaluate the efficiency and effectiveness of the workbench
- Apply the workbench in security, safety and privacy domains
- Support the PDO development lifecycle

7 References

- **Gandhi R.A., Lee, S.W.: Discovering and Understanding Multi-dimensional Correlations among Certification Requirements with application to Risk Assessment, India, RE 07**
- Lee, S.W., Gandhi. R.A.: Ontology-based ACTive Requirements Engineering (Onto-ActRE) Framework, Taiwan, APSEC 05
- Lee, S.W., Gandhi, R.A.: Requirements as Enablers for Software Assurance, CrossTalk, Dec. Issue, Vol. 19 (12), 2006, pp: 20-24