To appear in Proceedings of the 15th IEEE International Requirements Engineering Conference (RE 07), October 15-19, Delhi, India, 2007.
Research/Tool Demonstration.

r-AnalytiCA: Requirements Analytics for Certification & Accreditation

Seok-Won Lee, Robin A. Gandhi, Siddharth J. Wagle, Ajeet B. Murty
Dept. of Software and Information Systems, The University of North Carolina at Charlotte
Charlotte, NC 28223-0001, USA. {seoklee, rgandhi, sjwagle, abmurty}@uncc.edu

Abstract

Numerous interdependent quality requirements imposed by regulatory Certification and Accreditation (C&A) processes enable a rich context to gather compliance evidences for promoting software assurance. The goal of the r-AnalytiCA workbench is to make sense out of the large collection of available evidences for a complex software system though multi-dimensional requirements-driven problem domain analysis. The requirements analytics employed in the workbench support C&A activities by leveraging the expressiveness of ontologies used to model C&A requirements and their interdependencies.

1. Introduction

C&A is now perceived as an integrated approach for promoting software assurance. However, given the complexity of current software systems subject to diverse interdependent quality constraints imposed by numerous C&A requirements, the large collection of compliance evidences is often far beyond the capacity of manual approaches to produce meaningful insights.

Natural language C&A requirements specifications lack structural regularity. As a result, little or no guidance exists to understand the applicability of C&A requirements or establish their level of compliance. In addition, for a complex target system, without understanding the risks related to cascading effect of failure among interdependent quality constraints imposed by C&A requirements, the C&A process often merely reduces to a checklist exercise.

Typical commercial C&A tools offer basic support for selection of regulations, project management and documentation. However, establishing software assurance demands for richer understanding of C&A requirements and their compliance evidences. This need is also driving recent C&A toolkits [10] to consider many logical groupings of quality controls.

In our approach, we explicate each C&A requirement based on attributes that capture the goals, scenarios, viewpoints and other domain-specific concepts necessary to establish its common understanding in the problem domain [8]. Driven by the Onto-ActRE framework [6], we use ontological domain modeling to classify and categorize C&A requirements from the following dimensions: 1) a *requirements domain model* of requirement types that hierarchically categorizes C&A requirements; 2) a *viewpoints hierarchy* that models different perspectives from related stakeholders; 3) a C&A process *goal hierarchy with leaf-node scenarios* to express process activities; 4) *domain-specific taxonomies of risk components* of assets, threats, vulnerabilities, and countermeasures; and 5) Interdependencies among these concepts. The resulting Problem Domain Ontology (PDO) reflects the semantics of C&A requirements based on their relationships with each other as well as other relevant domain concepts [9]. The PDO representation is OKBC [1] compliant.

The *r*-AnalytiCA workbench introduced here leverages the expressiveness of the PDO to address the complexities associated with C&A activities. Its purpose is to enable various requirements analytics for providing meaningful insights to a certification analyst into the evidences gathered during the C&A process.

2. The *r*-AnalytiCA Workbench

Figure 1 shows the currently supported application areas of the *r*-AnalytiCA workbench during C&A.

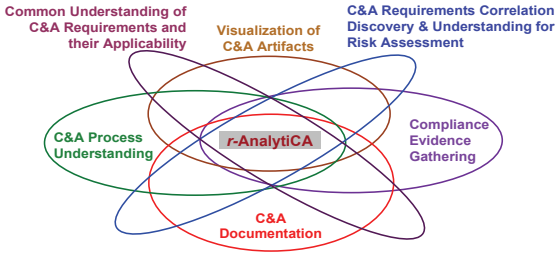

Figure 1: Application Areas of *r*-AnalytiCA Workbench

One of the key strengths of *r*-AnalytiCA is to create synergy among its application areas for producing insightful C&A artifacts. From a methodological aspect, its application areas first facilitate compliance information (evidence) gathering [7] and later support analytical activities [3] upon the collected evidences.

2.1 C&A Information Gathering Activities

– *Common Understanding of C&A Requirements and their applicability.* A primary C&A activity is to understand C&A requirements and determine their applicability to the target system. To this end, rather than selecting regulations (as in other C&A tools), the workbench presents pre-engineered requirements applicability questionnaires [7] through a wizard-based interface. The responses systematically prune the

categories of the *requirements domain model* in the PDO to derive applicable requirements. C&A process stakeholders can then browse the selected applicable requirements, based on categories in the *requirements domain model* as well as related domain concepts in the PDO to establish a common understanding.

– *Compliance Evidence Gathering.* For uniform assessment criteria, a pre-engineered questionnaire for each C&A requirement presents answer options that reflect ordered levels of compliance [9] based on the conjunction of diverse metrics and measures. Dynamic help informs the analyst about related requirements in the PDO and other compliance questions, if any.

2.2 C&A Analytical Activities

– *C&A Requirements-driven Risk Assessment.* Discovering and understanding correlations among quality constraints imposed by C&A requirements is critical to reason about the potential risks due to the cascading effect of non-compliance on overall system behavior. Based on the methodology presented in [3], the workbench supports risk assessment that is triggered by target system operational scenarios. For each scenario the analyst can search for relevant C&A requirements in the PDO based on 1) keywords; 2) focused hierarchical browsing of requirements categories; and 3) browsing multi-dimensional concepts related to requirements. As an exhaustive set of requirements become available, the workbench applies Formal Concept Analysis (FCA) [5] to compute a compact and visual representation (lattice) of all possible correlations among them from the dimensions of risk components as shown in Figure 2. Using a combination of the FCA lattice for a given scenario and the PDO, the workbench supports:

- Explanation of correlations
- Prioritization of C&A requirements
- Non-compliance impact analysis based on C&A requirements compliance scores
- What-if analysis for assessing the impact of potential non-compliance or perceived risks
- Risk upper and lower bound metrics due to non-compliance among a set of C&A requirements
- A comprehensive risk report with textual and visual artifacts resulting from above analyses

– *C&A Process Understanding.* The workbench architecture is easily tailorable to accommodate different C&A processes, quality regulations (e.g. security, safety, privacy, etc.), or organizational needs. A Process-Aspect Ontology [4] dynamically composes the services that expose the domain models in the PDO with user interface components in the workbench. The relevance of workbench tasks to high-level C&A goals is visualized as a goal-operationalization hierarchy.

– *C&A Documentation.* Artifacts resulting from the workbench are aggregated based on the ontological definition of a standard C&A document template and its relation to other concepts in the PDO.

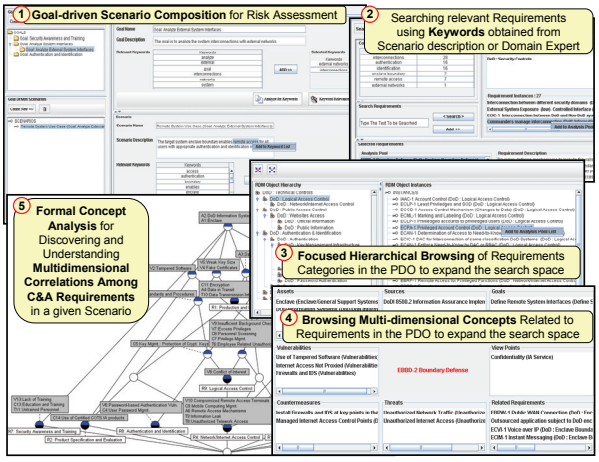

Figure 2: Risk Assessment Interfaces in *r*-AnalytiCA

3. Ongoing and Future work

Currently, *r*-AnalytiCA has been applied in the domain of C&A processes for assessing software system security qualities [2]. The underlying PDO classifies and categorizes a total of 533 security C&A requirements based on 604 ontological concepts. As a future work, the workbench will include capabilities to reason about global system behavior built upon artifacts from individual target system scenarios. We plan to perform a case study to evaluate the workbench with C&A experts from domains related to security, safety and privacy, including the support for a complete PDO development lifecycle.

4. References

[1] Chaudhri, V. K., et al., "OKBC: a programmatic foundation for knowledge base interoperability," In *Proc. 10th Conf. on Artificial intelligence*, AAAI, CA, 1998, pp. 600-607

[2] DoD Instruction 5200.40: DITSCAP, 1997.

[3] Gandhi R.A., Lee, S.W. "Discovering and Understanding Multi-dimensional Correlations among Certification Requirements with application to Risk Assessment" In *Proc. 15th Int'l Requirements Engg. Conf. (RE '07)*, New Delhi, India, 2007.

[4] Gandhi, R. A., Siddharth, W., Lee, S.W., "Process Artifacts Defined as an Aspectual Service to System Models" In *Proc. 2nd Int'l Workshop on Service-Oriented Comp.: Consequences for Engg Requirements (SOCCER'06), 14th Int'l Requirements Engg Conf. (RE'06)*, 2006 Minneapolis/St. Paul, MN, USA.

[5] Ganter, B. Wille, R. *Formal Concept Analysis*. Springer, 1996

[6] Lee, S.W., Gandhi, R.A., "Ontology-based Active Requirements Engineering Framework," In *Proc. 12th Asia-Pacific Soft. Engg. Conf. (APSEC '05)*, IEEE CS Press, 2005, pp: 481-490.

[7] Lee, S.W., Gandhi, R.A., "Requirements as Enablers for Software Assurance," *CrossTalk: The Journal of Defense Software Engg.*, Dec. Issue, Vol. 19 (12), 2006, pp: 20-24

[8] Lee, S.W., Gandhi, R.A., Ahn, G.J., "Certification Process Artifacts Defined as Measurable Units for Software Assurance," *Software Process: Improvement and Practice*, Vol. 12(2), pp.165-189, March/April, 2007, Wiley.

[9] Lee, S.W., Muthurajan, D., Gandhi, R.A., et al., "Building decision support problem domain ontology from natural language requirements for software assurance," *Int'l Journal on Software Engg & Knowledge Engg*, Vol.16(6), pp. 851-884, Dec., 2006.

[10] SEIMENS, UK, CRAMM Toolkit, Version 5.1, 2005