The goal of the project is to study formalization of regulations and regulatory compliance. Technical objectives involve addressing two verification problems:

- Consistency of regulation / Compliance can be achieved only if the regulation is internally consistent. This verification problem answers the question whether any organization is capable of complying with the regulation.
- Compliance of organizations / This verification problem answers the question whether the operation of an organization complies with the regulation. Formalization and verification questions were studies in the context of a case study that concerns regulation of blood banks by the U.S. Food and Drug Administration in the Code of Federal Regulations that the administration publishes.

Accomplishments

The two major accomplishments of this project are the run-time verification framework for regulatory trace compliance and the application of conformance testing to regulatory compliance of software.

The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.
EXTRACTING FORMAL MODELS FROM INFORMAL REQUIREMENTS AND USING THEM FOR VALIDATION

Closeout Report

1 Administrative

ARO grant number: W911NF-05-1-0158.
Project title: EXTRACTING FORMAL MODELS FROM INFORMAL REQUIREMENTS AND USING THEM FOR VALIDATION.
Duration of the grant: 4/15/05 – 4/15/08.
Program Manager:
   Dr. David Hislop, Army Research Office
Principal Investigator:
   Prof. Insup Lee, University of Pennsylvania
Institution:
   University of Pennsylvania
   3451 Walnut Street Room P221
   Philadelphia, PA 19104
Project Team:
   University of Pennsylvania   Prof. Insup Lee
   Prof. Aravind Joshi

2 Program Objective

The goal of the project is to study formalization of regulations and regulatory compliance. Technical objectives involve addressing two verification problems:
• Consistency of regulation
  Compliance can be achieved only if the regulation is internally consistent. This verification
  problem answers the question whether any organization is capable of complying with the
  regulation.

• Compliance of organizations
  This verification problem answers the question whether the operation of an organization
  complies with the regulation.

Formalization and verification questions were studies in the context of a case study that con-
cerns regulation of blood banks by the U.S. Food and Drug Administration in the Code of Federal
Regulations that the administration publishes.

3 Technical Approach

Our approach was to translate regulation into a collection of deontic logic formulas. The transla-
tion involved manual annotation of a substantially large fragment of the regulation, followed by
automated parser training. Once the translation was complete, we performed static verification
(model checking, conformance testing) on DBSS, a software system for blood bank management.
Verification aimed to established whether compliance is ensured by the given software.

We also explored a runtime verification approach. Runtime verification is a technique for
monitoring execution traces for compliance. Verification is performed on a log of operations and
determines whether performed operations are compliant with the regulation.

4 Accomplishments

The two major accomplishments of this project are the run-time verification framework for reg-
ulatory trace compliance and the application of conformance testing to regulatory compliance of
software.

4.1 Formalization of regulatory documents

We have developed a translation scheme based on Natural-Language Processing (NLP) techniques.
Regulatory documents are translated one sentence at a time, preserving the structure of the regula-
tion. This techniques has two important advantages:
• Structural mapping enhances traceability. Whenever a violation is discovered, our translation allows the verification process to identify the statement in the original regulatory document that was violated.

• Efficiency of the parser is improved, since NLP techniques work best at sentence level.

An important feature of our formalization approach is the explicit representation of exceptions that are omnipresent in regulatory documents. That is, obligations stipulated in a regulatory statement are predicated on exceptions described elsewhere in the document. Exceptions are handled by means of the reference operator, a new modal operator in our logic, along with the deontic operators of permission and obligation. These new modal operators are embedded into linear-time temporal logic (LTL), a commonly used formalism for capturing behavioral and temporal requirements.

Conformance checking is based on existing runtime verification algorithms for LTL. The complication introduced by our formal representation lies in the handling of references. Our algorithm resolves references on the fly by means of annotations that are obtained by a fixed point operator. We have implemented a prototype checker for our logic and applied it to a fragment of the blood bank regulation.

4.2 Conformance testing of the DBSS system

Defense Blood Standard System (DBSS) is the DoD-developed software system for the management of blood bank operations. In our case study, we explored compliance of the DBSS to FDA CFR 610.40 regulation. The case study identified incompleteness in the regulation, where inconclusive test outcomes could be ignored. We have implemented automatic test generator from formal requirements and an automatic test execution engine that executed the generated tests. We have observed several failed tests during the execution of the test suite. Failed tests corresponded to ambiguous requirements specified in the regulation. Incompleteness in the regulation was resolved differently in the implementation and in test generation.

5 Suggestions for the Future

Overall, the project led to a number of successful developments that have reached, or are close to reaching, the technology transfer stage. At the same time, a number of hard open problems in the area of formalization of regulatory documents and conformance checking remain. While academic research will be able to make further progress towards solving these problems, its full potential will be realized only through team projects that bring together academic researchers with domain experts from industry.
EXTRACTING FORMAL MODELS FROM INFORMAL REQUIREMENTS AND USING THEM FOR VALIDATION

ARO W911NF-05-1-0158
Insup Lee, Aravind Joshi
University of Pennsylvania

Goals of the project

- Formalization of regulations and regulatory compliance
- Two verification problems
  - Consistency of regulation
    - Can compliance be achieved? Only if the regulation is internally consistent!
  - Compliance of organizations
    - Does operation of an organization comply with the regulation
- Case study
  - Regulation of blood banks
Technical approach

- Translate regulation into a deontic logic
  - Manual annotation
  - Automated parser training
- Static verification (model checking, conformance testing)
  - Given the software for blood bank management, is compliance ensured?
- Runtime verification (monitor trace for compliance)
  - Given a log of operations, is it compliant?

Formalizing regulation

- Approach: regulatory documents are translated one sentence at a time
  - Enhance traceability via structural mapping
  - NLP techniques more efficient at sentence level
- Challenge: cross-references between sentences
  - E.g., actions are predicated on exceptions described elsewhere
- Solution: extend temporal logic with operators for obligation, permission and references
Annotation and translation to logic

Except as specified in paragraphs (c) and (d), each donation must be tested for the following diseases:

- Annotation
- Logical Form

Runtime checking of compliance

- **Reference logic RefL**
  - Extends predicate LTL with deontic operators for permission and obligation
  - Introduces operator byL(\(\phi\)), where L is a statement label that captures references

- **Checking based on runtime verification algorithms for LTL**
  - Algorithm resolves references on the fly by means of annotations
  - Prototype checker implemented
Static verification: case study

- Defense Blood Standard System (DBSS)
  - DoD-developed software
  - Compliance to FDA CFR 610.40
- Identified incompleteness in the regulation
  - Inconclusive test outcomes are ignored
- Technical approach: conformance testing
  - Automatic test generation from formal requirements
  - Automatic test execution engine implemented
  - Failed tests correspond to ambiguous requirements
    - Incompleteness resolved differently in implementation and test generation

Personnel

- Faculty
  - Aravind Joshi
  - Insup Lee
- Graduate students
  - Nikhil Dinesh
    - NLP, logic, formalization
  - Michael May
    - Policy formalization, logic
  - David Arney
    - Formalization, conformance testing
Collaborations

• The project is a collaborative effort between the NLP (Joshi) and formal methods (Lee) groups at Penn
  - Nikhil Dinesh, a Ph.D. student, is co-supervised by both PIs

• Extensive collaboration with the FDA on the CFR formalization

• Collaboration with DoD’s Clinical Information Technology Program Office on DBSS

• Initiated collaboration with TATRC on validation w.r.t. informal requirements

Publications

• 5 peer-reviewed conference / workshop papers

• 2 papers submitted to conference