Macrofy and Refactor: Transforming FRETish Requirements for Safety-Critical Systems

Formalised Requirements: Blueprints for Safety

To ensure the safe operation of critical systems like space rockets and aircraft, engineers use tools such as NASA's Formal Requirements Elicitation Tool (FRET) to create detailed, structured blueprints for safety in the form of system and software requirements. These blueprints, formalised using FRET's structured natural-language (FRETish), are then analysed along with models of the system by advanced software tools to verify that the system is in compliance with the requirements and identify any potential design flaws. Focused on essential properties like safety and correctness, these requirements serve as the foundation for reliable, safe and secure system design.

In previous work, we conducted an extensive case study with an aerospace company demonstrating how FRET can effectively formalise complex requirements, providing crucial support to systems engineers in their design tasks [1]. The study also revealed a significant issue: the requirements often contain considerable repetition which complicates maintenance and extension [2]. To address this, we propose "macrofication," which involves introducing suitable abbreviations for repeated terms to simplify maintenance and updates as the requirements set and system development evolve.

Macrofication: From Ontologies to FRET Requirements

Previous work at Manchester developed a versatile framework for identifying regularities and repetitions in formal languages, which was successfully applied to ontologies [3, 4]. This framework has been implemented in a software tool that generates optimal macro candidates to rewrite ontologies into more readable and maintainable versions. Building on this, our project adapts the framework and software for FRET requirements. We enhanced the tool to identify macros that can be used to refactor FRET requirements into a more maintainable format while preserving their original meaning. To achieve this, we developed a FRET parser to provide suitable input for the macro-generator. Our goal was to apply this tool to existing FRET requirements and determine whether the identified repetitions could be useful for refactoring the requirements.

Macrofication in FRET: NASA, Industry, and Academic Projects

We analysed a range of FRET requirements from diverse sources, including NASA, industry projects (such as Collins Aerospace's aircraft engine software controller), and academic projects (like explainability requirements for autonomous robots in nuclear environments and a mechanical lung ventilator). This analysis led to the identification of numerous macros, with some proving particularly valuable for refactoring. We also applied a metric known as "shrinking power" to assess which macros most effectively reduce formula complexity. Our findings and prototype were presented to the FRET team lead from NASA Ames Research Center, as well as to the research teams at Maynooth University and the University of Nottingham, who are developing a FRET refactoring extension called MU-FRET. The feedback was highly positive, with strong interest in integrating these techniques into both FRET and MU-FRET.

From Prototype to Integration

We aim to advance our prototype so it can seamlessly integrate into the existing FRET tool suite as part of a larger follow-up project. This progress will also facilitate the integration of advanced semantic technologies into FRET requirements, including methods for explanation, modularisation, and dependency analysis.

This seed-corn project supported a new collaboration between investigators at the University of Manchester and Stanford University, while contributing to our active collaboration with NASA Ames Research Center, Maynooth University and University of Nottingham. Since completion, the Stanford and Manchester investigators have held meetings with the FRET team at NASA and hope to apply for further funding to continue this promising research direction.

[1] Marie Farrell, Matt Luckcuck, Oisin Sheridan, Rosemary Monahan. "FRETting About Requirements: Formalised Requirements For An Aircraft Engine Controller". In: International Working Conference on Requirements Engineering: Foundation for Software Quality 2022: 96-111.

[2] Marie Farrell, Matt Luckcuck, Oisin Sheridan, Rosemary Monahan. "Towards Refactoring FRETish Requirements". In: NASA Formal Methods Symposium 2022: 272–279.

[3] Christian Kindermann, Anne-Marie George, Bijan Parsia, Uli Sattler. "Minimal Macro-Based Rewritings of Formal Languages: Theory and Applications in Ontology Engineering (and beyond)". In: AAAI 2024: 10581-10588.

[4] Christian Kindermann, Martin Georg Skjæveland. "Concrete Names for Complex Expressions in Ontologies: A Survey of Biomedical Ontologies". ICBO 2023: 82-93.