Modular Formal Requirements-Driven Verification

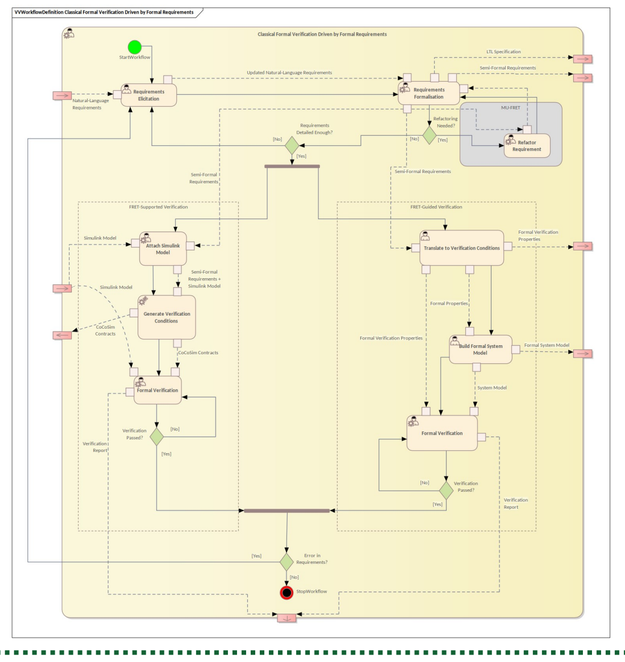
Improved Method

Base Method Description

Requirements are often expressed in natural language, and often at a level of detail that is not suitable for direct formalisation [SFM1]. A semi-formal language may be used as an intermediate between natural- and formal-languages, which avoids slowing down the requirements elicitation process, but still provides enough formalisation to both reduce ambiguities and make the requirements easier to (fully) formalise later on [SFM2].

Improved Method

Our improvement (MU-FRET) extends the existing requirements elicitation tool FRET, adapting software refactoring for FRET requirements and implementing a formal check that the requirement's meaning has not changed. The refactorings are based on existing requirements refactorings [MFRDV1]. This approach will make managing sets of requirements in FRET easier – especially during the elicitation process, where requirements are likely to change.



Layers of the multi-dimensional framework

Evaluation Environment Type	Evaluation Type	Type of Component	Evaluation Stage	Purpose of Component	Type of Requirement	Evaluation Performance Indicator

• **In-the-lab**
• Closed
• Open
	• Experimental – Testing
	• Experimental – Monitoring
	• Experimental – Simulation
	• **Analytical – Formal**
	• Analytical – Semi-Formal
		• **Model**
		• **Software**
		• Hardware
			• Concept
			• **Requirement Analysis**
			• **System Design**
			• **Architecture Design**
			• **Detail Design**
			• Implementation
			• Unit Testing
			• Integration Testing
			• System Testing
			• Acceptance Testing
			• Operation
			• Risk Analysis
			• Other
				• **Sensing**
				• **Thinking**
				• **Acting**
				• **Other**
					• **Non-functional – Safety**
					• Non-functional – Security
					• Non-functional – Privacy
					• Non-functional – Other
					• **Function**
						• V&V Process criteria
						  • Time of test execution
						  • Number of test cases
						  • Joint Management of SCP Requirements
						  • Effort needed for test
						  • Reduced cost and time for work on certification process and functional safety
						• SCP criteria
						  • Error coverage
						  • Number of safety/security requirement violations
						  • Number of malicious attacks and faults detected

Gaps & Limitations Addressed

- **Learning Curve [GAPM-FRV05]: The formalization of requirements is still a manual process and requires that the domain engineer, expert in the domain of the requirements, learns the formal language.**
- **Lack of Automation [GAPM-FRV06]: The formalization of natural language requirements remains largely a manual step.**

Connection to VALU3S Use Cases

- **UC5: Aircraft Engine Controller**

Foreseen Impacts

- **Enables users to rearrange requirements in response to mistakes, new information, or new requirements.**
- **Formally verifying that refactorings have not altered the meaning of the requirements.**
- **Lowers barrier to understanding, by using the terminology/functionality that users may be familiar with from software IDEs.**

Connection to V&V Tools

FRET (https://github.com/NASA-SW-VnV/fret)

MU-FRET (https://github.com/valu3s-mu/mu-fret)

References

- **[SFM1] Rozier, Kristin Yvonne, "Specification: The Biggest Bottleneck in Formal Methods and Autonomy" (2016). Verified Software. Theories, Tools, and Experiments (pp. 8-26). Springer. https://doi.org/10.1007/978-3-319-48869-1_2**
- **[SFM2] Giannakopoulou, D., Pressburger, T., Mavridou, A., & Schumann, J. (2020). Generation of formal requirements from structured natural language. In International Working Conference on Requirements Engineering: Foundation for Software Quality (pp. 19-35). Springer. https://doi.org/10.1007/978-3-030-44429-7_2**
- **[MFRDV1] Ramos, R., Piveta, E. K., Castro, J., Araujo, J., Moreira, A., Guerreiro, P., Pimenta, M. S., Price, R. T. Improving the Quality of Requirements with Refactoring. (2007) Simposio Brasileiro De Qualidade De Software (pp. 141-155). SBC. https://doi.org/10.5753/sbqs.2007.15573**

Involved VALU3S Partners

VALU3S HAS RECEIVED FUNDING FROM THE ECSEL JOINT UNDERTAKING UNDER GRANT AGREEMENT NO 876852. THE JOINT UNDERTAKING RECEIVES SUPPORT FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME AND AUSTRIA, CZECH REPUBLIC, GERMANY, IRELAND, ITALY, PORTUGAL, SPAIN, SWEDEN, TURKEY.