A Systematic Approach For Model Based System Assurance

Ran Wei, Tim P. Kelly, and Richard Hawkins

University of York, United Kingdom
{ran.wei,tim.kelly,richard.hawkins}@york.ac.uk

Abstract. Assurance cases are used to demonstrate confidence in properties of interest for a system, e.g. for safety or security. Typically, the task of constructing assurance cases is a lengthy and informal process. In recent years, there has been work to propose model based approaches to promote automation. The Structured Assurance Case Metamodel (SACM) is an OMG specification designed to represent system assurances in machine-readable models, so that a series of model management operations can be performed to automate the process of system assurance acceptance. However, the adoption of SACM faces difficulties as there is a cognitive gap between the syntax/semantics of SACM elements and the understanding of SACM in the perspective of system assurance practitioners.
In this paper, we provide a definitive guide to SACM with examples so that SACM can be better understood. We also discuss the relationship between SACM and the Goal Structuring Notation (GSN) and the interoperability between them. We also propose a systematic approach for model based system assurance using SACM, so that all corresponding models can be bridged together using the facilities provided in SACM.

1 Introduction

2 Structured Assurance Case Metamodel

3 Structured Assurance Case Metamodel and the Goal Structuring Notation

4 Running example: a systematic approach

5 Tool Support and Related Work

6 Conclusion

Acknowledgements This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 732242.