# Compositional Assume-Guarantee Reasoning of Control Law Diagrams using UTP

Kangfeng Ye        Simon Foster

Jim Woodcock

University of York, UK

{kangfeng.ye,simon.foster,jim.woodcock}@york.ac.uk

March 4, 2020

### Abstract

This report is a summary of our work for the VeTSS funded project "Mechanised Assume-Guarantee Reasoning for Control Law Diagrams via Circus". Our Assume-Guarantee (AG) reasoning of control law diagrams is based on Hoare and He's Unifying Theories of Programming and their theory of designs. In this report, we present developed theories and laws to map discrete-time Simulink block diagrams to designs in UTP, calculate assumptions and guarantees, and verify properties for modelled systems. A practical application of our AG reasoning to an aircraft cabin pressure control subsystem is also presented. In addition, all mechanised theories in Isabelle/UTP are attached in Appendices. In the end of this report, we summarise current progress for each work package.

# Contents

**Acknowledgements**.

# References