INTRODUCTION

Software development for safety critical aircraft systems, e.g. flight control systems, is highly demanding. For a model-based software development approach according to RTCA DO-331 [1], an automated process for the translation of Simulink/Stateflow (SL/STF) models to Scade has been developed, see [2] and [3]. This enables the reuse of models from function design in SL/STF for code generation with the qualifiable code generator KCG. The translation is performed with SCADE Suite Gateway for Simulink [4]. This poster shows the used methods, tools and results from the process that verifies the translation of a complex flight control law software (FCL SW) model.

OBJECTIVES

- Develop and implement a highly automated process for the verification of the translation of models from SL/STF to Scade.
- Verify the translation of the example (see Scade model in Fig. 1 and size metrics in TAB. 1).
- Identify different behavior between both models and the root causes.
- Identify missing modelling guidelines for SL/STF that enable correct and complete translation.
- Determine the reachable coverage with closed-loop test cases and generated test cases.
- Check if test case generation with Simulink Design Verifier (SLOV) is suitable to reach the selected model coverage criteria.

EXAMPLE

To demonstrate the approach, the FCL SW of a high aspect ratio utility aircraft, the STEMme S15, (see Fig. 2) is used as a realistic example. The demonstrator aircraft has a wing span of ca. 18m, a MTOM of ca. 1000 kg, and can carry a payload of ca. 150–300 kg.

Flight Control Functions:
- Trim Control and Damping
- Attitude and Flight Path Control
- Altitude, Speed and Track/Heading Control
- Gust Load Alleviation
- Flight Envelope Protections
- Automatic Takeoff (TO), and Landing (LAND)
- Go Around (GA)
- Navigation (3DNAV)
- Automatic Mission (TO$\rightarrow$3DNAV$\rightarrow$LAND)
- Low Level Flight (LLF)

PROCESS AND METHODS (cont.)

- Model coverage is acquired with SCade Suite MTC.
- Test readiness criteria:
  - Model coverage criteria reached
  - Control activation (Mode On/Condition/Decision Coverage (MC/DC))
  - Data Activation.
  - Equivalent behavior (see equivalence criteria in paper).
- Report generation for each module including time series plots of non-equivalent signals (see Fig. 8).
- Automatic summary report generation of the translation and verification for the complete model.

RESULTS

- In TAB. 2 results are shown for:
  - closed-loop test cases (TCS1),
  - generated test cases from SL/STF (TCS2),
  - join of TCS1 and TCS2 (TCS3) and
  - manually reviewed results (TCS*)
- Case of different behavior is shown in Fig. 7.
- More details are presented in the paper.

LESSONS LEARNED

- Models that conforms with guidelines can be translated to Scade correctly and completely.
- The automated process helps to verify the translation in an efficient and repeatable manner.
- The modules bottom-up process is suitable to identify the root cause of different behavior between SL/STF and Scade.
- Closed-Loop test cases are suitable to identify numerical errors (e.g., rounding errors, drift) and lead to good model coverage values.
- Generated test cases from SLOV help to increase model coverage and to verify hard to reach paths in the SW model, but ...
- Reached MC/DC coverage in SCade Suite is lower than the expected MC/DC coverage due to an issue with generated test cases from SLOV.
- The existing modeling guideline catalogue is a good base to enable translatable and equivalent behavior (1 guideline updated, 4 new modelling guidelines identified, see Fig. 9 – Fig. 11 and paper for details)
- The example model shall be improved for equivalent behavior and complete translatableability.

ACKNOWLEDGEMENT

The authors would like to thank the Federal Ministry of Economic Affairs and Energy (BMIW) for the funding of LAPAZ, LAPAZ II, CERTIT-FBW23 and MCAS, results from these projects are presented here. We would also like to thank External Technologies for the admission of our department to the academic program and the technical support.

REFERENCES

1. RTCA DO-331 - Model-Based Development and Verification Supplement to DO-178C and DO-278A, RTCA Inc. Std. 2011
3. Walde, G.; Luckner, E.: Bridging the tool gap for model based design from flight control function design in Simulink to software design in SCade. In: P-1, Sep. 2016