Modeling Aircraft Mission Computer Task Rates

Jin Song Dong[1], Brendan P. Mahony[2], and Neale Fulton[3]

[1] School of Computing, National University of Singapore
[2] Defence Science and Technology Organisation (DSTO), Australia
[3] Commonwealth Science and Industrial Research Organisation (CSIRO), Australia

Recently the Royal Australian Air Force (RAAF) has been considering an upgrade to the F/A-18 aircraft in Australia. This upgrade may well involve the modification of Mission Computer (MC) systems. Maintaining correct functionality for the upgraded F/A-18 is therefore a major concern for the RAAF. This particular problem received interest from CSIRO and DSTO to support a joint Research Fellowship to investigate specification of hard real-time characteristics by formal method approaches.

Our initial approach [1] used Object-Z to model an aircraft MC Operational Flight Program (OFP) pre-run time scheduler. However, the treatment of timing issues in this approach is cumbersome and it is not well suited for modeling the OFP process concurrent interactions. From this experience, we realised that the state-based Object-Z notation lacks adequate mechanisms for treating real-time and concurrency. Therefore we have developed a notation called Timed Communicating Object Z (TCOZ) [2, 3, 4] which integrates Object-Z with Timed CSP. The MC process definitions, concurrent interactions, and task rate sequences have been effectively formalised in TCOZ. The benefits of the TCOZ model have included consistent use of terminology, a well-defined collection of synchronisation and concurrency primitives, and the ability to apply object abstraction techniques to structure and simplify the description.

During the formalisation process, we also identified a number of ambiguities in the original requirement documentation regarding the synchronisation relationships between the MC processes. Understanding those critical inter-process synchronisations required painstaking reading of different text sections with many clarifications from our local aviation domain expert. Whence we precisely understand those critical inter-process synchronisations differences, in the TCOZ model these differences are clearly captured by using differing communication mechanisms, sensor/actuators or channels as appropriate. We also believe our approach to be complementary to the original requirement documentation, in as much as the tables and diagrams provide a valuable visualisation and comprehension aid to the formal TCOZ model.

References

[1] J.S. Dong, N. Fulton, L. Zucconi, and J. Colton. Formalising Process Scheduling Requirements for an Aircraft Operational Flight Program. ICFEM'97, November 1997. IEEE Press.
[2] J.S. Dong and B. Mahony. Active Objects in TCOZ. ICFEM'98, IEEE Press, December 1998.
[3] B. Mahony and J.S. Dong. Network Topology and a Case Study in TCOZ. ZUM'98, *LNCS*, September 1998. Springer-Verlag.
[4] B. P. Mahony and J.S. Dong. Blending Object-Z and Timed CSP: An introduction to TCOZ. ICSE'98, April 1998. IEEE Press.