The Tool Qualification Package eased our work with DO-178B a lot.

Thomas Spicker, Software Verification and Test, Liebherr-Aerospace, Lindenberg, Germany.

The Tessy User: Liebherr-Aerospace Lindenberg GmbH

The company was established in 1949. Today it is divided in several units and has more than 30,000 employees.

Liebherr plant in Lindenberg (Source: Liebherr)

In the Aerospace domain, Liebherr supplies aircraft air management, flight control and actuation systems, hydraulic and landing gears systems. These systems are on board of many aircraft programs: Commercial transport aircraft, commuter and regional aircraft, business jets, fighters, military transport, trainer aircraft as well as civil and military helicopters.

Testing Avionics Code

In the project at hand, Liebherr used Tessy to test the low-level requirements of software according to DO-178B, Design Assurance Level A. This software enables the control of an aircraft on its axes (Flap Control Unit) at various aircraft. The software was written in the C programming language and ran amongst others on a microcontroller of type PowerPC MPC565 from company Freescale as target. It was compiled using a Diab compiler from Wind River.

The FCU is a digital computer with an independent Control, Motor Control and Monitor Channel (CC, MCC and MC), and Power Electronics (PE). The Control Channel is designed to perform all flap systems control applications. The Monitor Channel performs surveillance functions designed to prevent critical system states.

This is achieved by two direct hardware connections of the Monitor Channel to the power electronics allowing the Monitor Channel to put the system in a fail-safe state. In the event of an error, the Monitor Channel, independently from the Control Channel, deactivates the motor and brakes power electronics. Dissimilar software and hardware for CC and MC protect the system from single failures being catastrophic. The Motor Control Channel with its power electronic is responsible for controlling the electrical motor.
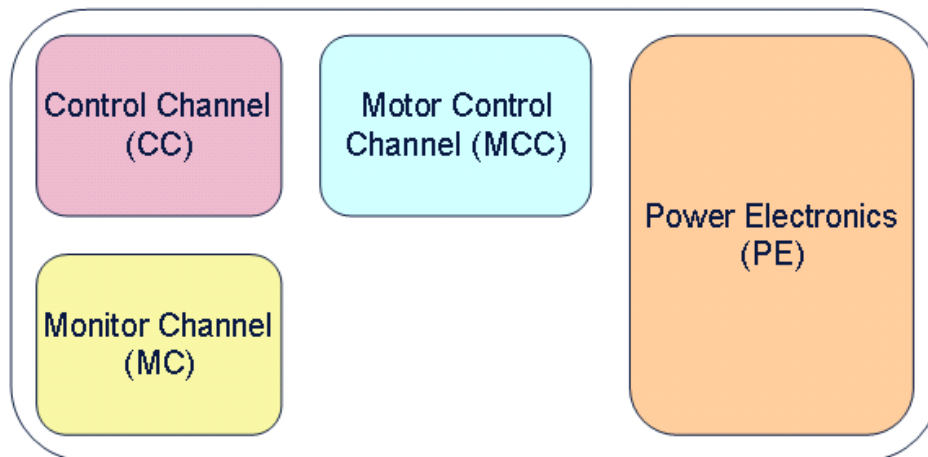
Structure of the Flap Control Unit (Source: Liebherr)

The flap system is normally operated by manual command. For manual control, the computer converts the pilots command received from the Flap Control Lever (FCL) in the cockpit into a corresponding panel movement. If a critical failure occurs, embedded monitors will ensure a safe shutdown of the Motor Control Channel. The system sends status and failure information for cockpit indication and for the Onboard Maintenance System (OMS).

All functions of the system application are software controlled and fully automatic after power up. The communication with other aircraft systems and between flight control system applications are performed by ARINC 429 high-speed buses. The FCU is designed with Built-In Test (BIT) capabilities providing effective system diagnostic. The BIT capability includes power up or event initiated tests and continuous monitoring. The power up or event-initiated test involves a sequence of self-tests to verify correct functioning and integrity of the system hardware and software, whereby these tests are designed to detect latent failures. For easy access to maintenance, rigging and test functions, an independent control unit (RS232 terminal) can be connected to the FCU.

All three channels use 500 functions each with more then 5000 test cases. All functions are tested using Tessy. For development of all test cases the Classification Tree Editor (CTE/ES) was used.

Anomalous behaviour of software on level A would result in catastrophic failure condition for the aircraft. Therefore, testing requirements for this kind of software are

rigorous. For instance, structural coverage analysis needs to measure modified condition / decision coverage (MC/DC), what Tessy can determine without additional effort. Furthermore, software verification tools (like Tessy) involved in the test of software on level A need to be qualified for this purpose, i.e. it should be demonstrated that the tool complies with its Tool Operational Requirements. This qualification process was eased for Liebherr by using a Tool Qualification Package (TQP) provided by Razorcat, the manufacturer of Tessy. This TQP contains documents (e.g. the Tool Operational Requirements) and carefully crafted test cases intended to demonstrate the proper operation of the tool.

In the meantime, the software was certified according to DO-178B without problems and is in production since 2010. Our software from other projects, which is tested by Tessy, is flying for over than 10 years in various aircrafts and helicopters.

Conclusion

Tessy proved to be suitable to test the low-level requirements of software according to DO-178B Design Assurance Level A, Level B and Level C. The Tool Qualification Package provided by the manufacturer eased the qualification of Tessy for its intended purpose a lot.