Maximum Safety

Nord-Micro: TargetLink in many different aircraft types since 2000

In aircraft with pressurized cabins, special valves and control algorithms have to regulate the air pressure with maximum reliability. At high altitudes, the safety of the passengers and crew has top priority. Since 2000, Nord-Micro has been using TargetLink, the production code generator, to develop cabin pressure controls for a wide range of aircraft types. In Nord-Micro's development processes, the autocoded software effortlessly fulfills the strict requirements of aircraft manufacturers such as Boeing and Airbus, and also those of the FAA and EASA aviation authorities.

Cabin Pressure: Safety First

Automatic cabin pressure control in aircraft is one of the functionalities that passengers and crew hardly notice, except during descent and landing. Yet reliable cabin pressure control is of vital importance to the occupants of any plane. Above a certain altitude, they simply would not survive conditions outside the aircraft. So cabin pressure control is not only important for comfort, it is first and foremost a safety-critical functionality that must function without errors at all times. Errors in the control system or a system failure would make it necessary to immediately begin an emergency descent while the plane's occupants reached for their oxygen masks.

Some of the most vital mechanical components in a cabin pressure control system are the electronically controlled air outlet valves, which regulate circulation according to the fresh air intake and also control the cabin pressure via the waste air. These complex valves are precisely adapted to each specific aircraft type.

The software required for valve control is implemented on several electronic controllers. Each controller is connected via a special interface for signal conditioning (a remote data concentrator) to the aircraft data bus, which connects them all to the flight management system (FMS) (figure 1). Sensors in the cabin pick up the air pressure data and pass it to the responsible controllers, and the FMS provides the environment data.

The cabin pressure control system not only ensures that the air pressure stays within predefined limits, it also performs other tasks. These include regulating the pressure change rate, which affects the comfort of the passengers, and protecting the aircraft's outer skin against the damage that might be caused if the difference between external and internal pressure were too great.

Nord-Micro: Successfully Using TargetLink Since 2000

Nord-Micro has many years of experience in developing powerful, reliable cabin pressure control systems, especially for passenger planes seating more than 80. The company has been using TargetLink, dSPACE's production code generator, to develop and autocode controller software since the year 2000. Thus, numerous aircraft, from regional jets to the Airbus A380, have cabin pressure control systems on board that contain controller software developed and autocoded with TargetLink. The safety-critical software developed in this way meets the rigorous requirements defined by aircraft manufacturers and aviation authorities for software used in aircraft, including certification up to safety level A (figure 2). The main standard is DO-178B, which defines the requirements for software development in aviation. In more recent projects, Nord-Micro employed TargetLink as a design and coding tool, and also used TargetLink's extensive test support functionality to facilitate code reviews, module tests on the target, and tool integration with IBM® Rational® Test RealTime (RTR) for analyzing the required code coverage.

Tough Requirements from Aviation Authorities and Aircraft Manufacturers

Because the software developed by Nord-Micro is intended for use in a safety-critical system, TargetLink has to meet numerous requirements regarding the quality of the models and the generated code:

- *Support for Coding Guidelines*
  Nord-Micro and aircraft manufacturers all have coding guidelines aimed at fulfilling DO-178B. Practical experience has shown that TargetLink generates code that meets the specifications. For example, the tool meets the MISRA guidelines which were incorporated into Nord-Micro's in-house coding standard. Special requirements such as enforcing an explicit return statement in every function can also be fulfilled by compliance with a specific modeling style.

- *Code Readability*
  The code generated by TargetLink is clearly structured, and includes easy-to-understand comments and intuitive symbol names. Its good readability makes it considerably easier for Nord-Micro to carry out code reviews.

- *Requirements for Model-Based Design*
  Model-based design is not yet covered by the DO-178B standard. The European and American aviation authorities have therefore started to publish specifications for translating DO-178B requirements into requirements for model-based design. These specifications relate to issues such as meaningful names for signals in models and the modeling style that is used. Using TargetLink, these rigorous specifications are easy to implement.

- *Deterministic Code Generation*
  The efficiency of Nord-Micro's test efficiency benefits from deterministic code generation. This ensures that any changes made to a subfunction have only a local effect, and functionalities that were already tested are not affected by changes to other model segments. One way of doing this is by using an intelligent mechanism for numbering subsystems that restricts code changes to their own location.

- *High Code Efficiency*
  Even at optimization level 0, which is usually used for safety-critical aviation applications, the code generated by TargetLink is efficient enough for the controller to execute it in the required time.

> "TargetLink effortlessly fulfills the rigorous requirements for model-based development issued by European and American aviation authorities."
>
> *Andreas Alaoui, Nord-Micro*

Efficient Development Steps in TargetLink

In the development process at Nord-Micro, TargetLink is not only used for autocoding, but also in the following features and process steps (figure 3):

- ***Definition of Software Requirements***
  Nord-Micro handles the requirements in Telelogic® DOORS®, a requirements management tool, and links them to TargetLink models by means of the requirements management interface from The MathWorks. This ensures that all the work products created during the development process can be traced back to the software requirements.

- ***Model Design***
  For graphical modeling, Nord-Micro uses MATLAB/Simulink/Stateflow/TargetLink, and also a UML tool.

- ***Automatic Scaling***
  By using TargetLink's worst-case scaling analysis for fixed-point arithmetic, Nord-Micro has been able to eliminate numerous errors at an early stage, saving time and money compared with manual coding. TargetLink's worst-case autoscaling functionality has also assisted in the formal verification of Nord-Micro's system software.

- ***Documentation Generation***
  The documentation that TargetLink automatically produces is also a software design document, so Nord-Micro does not have to create one manually. Consistency with the generated code is always automatic. This saves Nord-Micro a considerable amount of work in carrying out the necessary design reviews.

- ***Code Reviews***
  The code reviews carried out at Nord-Micro are greatly simplified by the clear structure, naming,

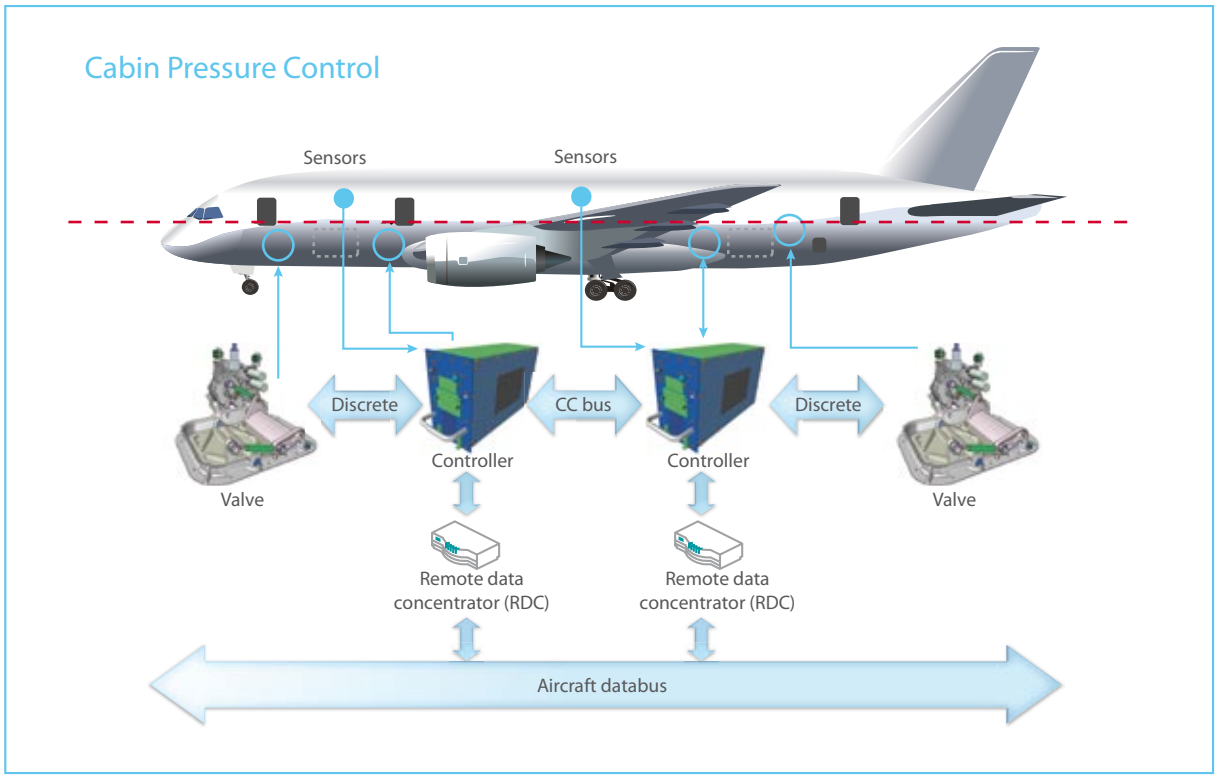


Figure 1: The controllers that control the valves are connected to the flight management system (FMS) via the aircraft's central databus.

and commenting of the generated code, and also by direct traceability between code and model.

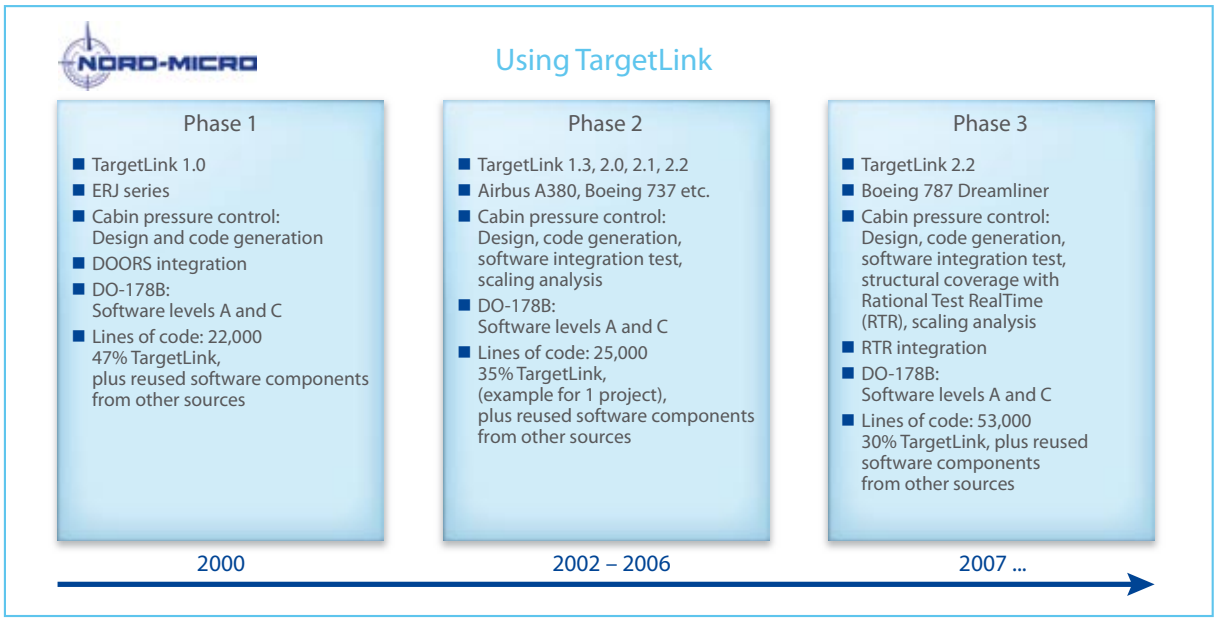
- *Software Integration Tests*
  Nord-Micro uses TargetLink for performing software integration tests (figure 2). The first step is to derive suitable test stimuli from the requirements. Then in TargetLink, the results of a model-in-the-loop simulation are compared with those from a processor-in-the-loop simulation for the test stimuli, using C167 and MPC5554 processors. The integration tests include an analysis of the structural code coverage performed thanks to tool integration between TargetLink and Rational Test RealTime. Nord-Micro can reduce the cost of module testing to the minimum by this means.

> "Using TargetLink, we have successfully carried out several software developments according to DO-178B that were certified for safety level A."
>
> *Andreas Alaoui, Nord-Micro*

Software Integration Tests with TargetLink and Rational Test RealTime

For one of the most recent projects, dSPACE and IBM Rational developed a tool integration between TargetLink and Rational Test RealTime (RTR) to streamline Nord-Micro's test process. First TargetLink code is suitably instrumented with RTR (preparing code for the test), and then RTR is used again to perform code coverage analyses. The integration between the two tools enables Nord-Micro to run the software integration tests on the target processor using TargetLink's simulation features and achieve the structural coverage required by DO-178B as early as the software integration level. This approach radically reduced the workload for module tests to 20% of its original value. As of Version 2.0, TargetLink also had functionalities for measuring structural coverage, but Nord-Micro required a formal tool qualification for structural coverage, which is already available with RTR

Figure 2: Production code generator TargetLink has been used successfully for many years to develop safety-critical software at Nord-Micro.



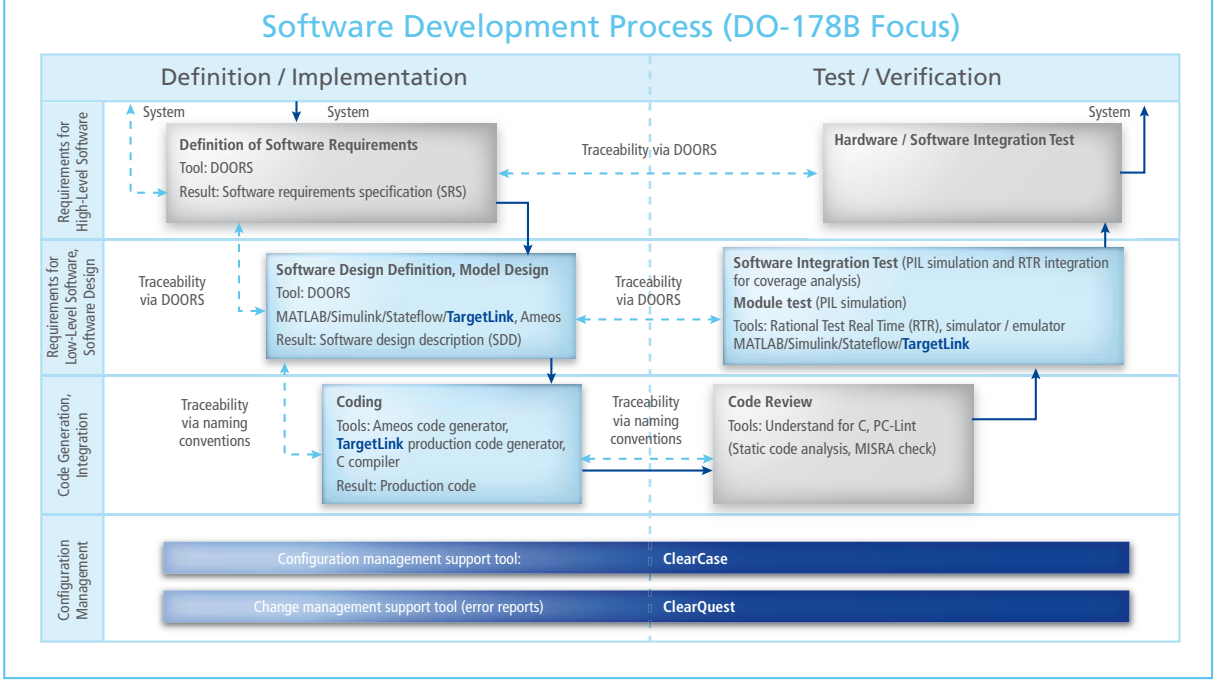


Figure 3: TargetLink in the development process at Nord-Micro.

in the form of a tool qualification kit. Nord-Micro is also using RTR for measuring structural coverage in the hardware/software integration test. For the software integration tests, Nord-Micro creates test data based on the requirements. Then model-in-the-loop simulation is used to test whether the model behaves in compliance with the requirements. If the result is positive, production code is generated and executed on the target, and the results of this are checked against the results of model-in-the-loop simulation. The next step is to generate instrumented production code so that the simulation results can be tested for consistency between instrumented and uninstrumented code. If the results of this are also identical, the required coverage can be verified by measuring the structural coverage on the basis of the instrumented TargetLink code and RTR to verify the required coverage. ■

Andreas Alaoui,
Manager Software Engineering,
Nord-Micro AG & Co OHG
Germany

Summary

The projects carried out between 2000 and today have shown us that TargetLink is an ideal development tool and production code generator for safety-critical aviation applications. Complete compliance with the rigorous requirements of aircraft manufacturers and aviation authorities was achieved by means of TargetLink, so code generated by TargetLink is now in use in numerous aircraft types. Amongst the qualities that we really appreciate are the good readability of the TargetLink code, traceability between the code and the model, and the determinism of code generation, which considerably reduces our test workload.

Moreover, the flexible configurability of the source code enables us to integrate several TargetLink models into our real-time software without much difficulty. The source code is so efficient that our real-time requirement is always fulfilled. Integration with other development tools such as DOORS and Rational Test RealTime ran smoothly. Based on experience gathered so far, Nord-Micro will continue to use TargetLink for developing cabin pressure control systems in new aircraft in the future.