Safe Landing

Esterel solutions help Crane Aerospace & Electronics to design braking systems that are certified for safety.

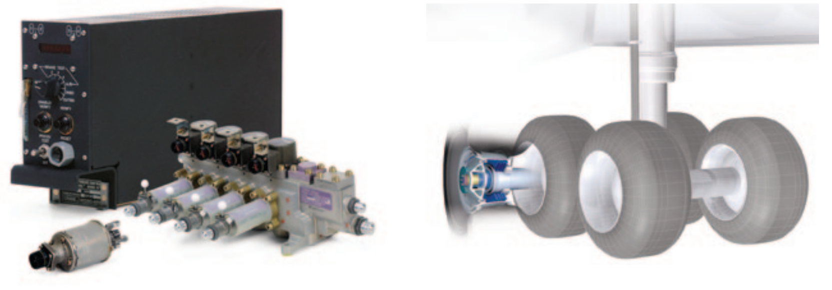
By Gregory Mooney, Systems Software Engineering Lead — Landing Systems
Crane Aerospace & Electronics, Burbank, U.S.A.

Crane Aerospace & Electronics' mission-critical products help to ensure the safety of millions of airplane passengers. The company must meet stringent government safety regulations aimed at ensuring that these products — in this case, braking systems — will perform as expected under a broad range of real-world conditions.

Crane pioneered the antiskid braking industry in 1947 by developing the Hydro-Aire Hytrol Mark I antiskid system for the B-47. Since then, Crane has provided both private- and public-sector aircraft customers with a wide range of brake control systems and other products — including power, cabin, fluid management and sensing systems. The company's guiding principle is to exceed the needs of its customers, a responsibility Crane's engineering team takes very seriously.

Crane is the industry leader in aircraft brake control systems, with 65 percent of the commercial market and 80 percent of the Western military market. The company has more than 25,000 systems in service worldwide today. These braking systems are critical in ensuring passenger safety during routine landings, as well as during challenging rejected takeoffs. (See sidebar.) Brake control systems designed and manufactured by Crane include a number of mechanical and hydraulic parts, such as control, shutoff and parking brake valves as well as wheel speed and pedal position sensors. However, the most complex component in Crane's electronic controllers is an invisible one: the thousands of lines of embedded software code that ensure efficient, reliable brake control when required during landing.

To support reliable software performance, the United States Federal Aviation Administration (FAA) has drafted a set of guidelines under its Federal Aviation Regulations requiring proof that software "performs intended functions under any foreseeable condition." A means to comply with these regulations — that is, a way to show that the system meets its safety objectives — is a standard called RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification. This standard aims to assure



▲ **Braking control systems manufactured by Crane Aerospace include a number of mechanical and hydraulic components — all controlled by thousands of lines of mission-critical software code.**

the safety of software by defining a set of development, verification, requirements management and quality assurance tasks aimed at instilling rigor into the software development process.

Essentially, DO-178B requires developers to test and verify performance of control software under a broad range of operating conditions, a challenging engineering task. Since 2010, Crane Aerospace has relied on SCADE Suite software from Esterel — now a part of ANSYS — to help develop software that satisfies the critical FAA certification process for braking control systems.

BRAKING CONTROLS: NEW COMPLEXITY, NEW CHALLENGES

Since Crane revolutionized the aerospace industry with its first Hydro-Aire antiskid braking system, brake control systems have become increasingly complex. Wheel speed transducers measure high-resolution wheel speeds, enabling modulation and control of brake pressure during operation. Today, brake controls have to dynamically adapt to all runway surfaces, whether wet, dry or icy. For example, most large commercial planes feature brake-by-wire systems, which apply brakes electronically, first introduced by Crane for the U.S. Space Shuttle program in 1973. Continuing this development, Crane introduced the first microprocessor antiskid systems in the early 1980s, which apply sophisticated control algorithms to automate braking and achieve antiskid performance in excess of 90 percent. These systems, like many Crane innovations, have become industry standard.

Today, while the basic mechanics of braking have not changed, brake control systems continue to evolve as an incredibly complex blend of control software, electronically controlled actuators, and high-speed digital communication interfaces with other onboard systems (as well as humans). For instance, in case of an electrical short or other unexpected event, the software not only ensures continuing brake performance, it alerts the flight crew about the issue and sends an automatic alert to maintenance staff to address the problem once the plane lands. Obviously, the underlying code is mission critical, because the consequences for brake failure can be truly catastrophic.

This new complexity has created exceptional challenges for software developers, who must test for each input to the brake control software — as well as for a broad range of operating events. This dictates extremely rigorous, broad-scope testing and verification tasks, even as Crane's customers are working against aggressive development schedules.

Prior to 2010, the company's software engineers managed the requirements of DO-178B via a time- and labor-intensive process, which had some evident drawbacks. Because of the manual nature of the process, the finest details of functionality were hidden in the underlying code. The impacts of customer requirements and system updates were not fully visible — and thus could not be completely verified by Crane's engineering team — until the software was fully developed and implemented.

There were often surprises when software was run in a Crane in-house testing facility or customer lab replicating actual aircraft configuration — which meant that Crane's engineers had to go back to the drawing board and rewrite the code. This was an expensive and time-consuming proposition at such a late stage of software development, especially after hundreds of development hours had been invested.

The resulting high costs, large amount of rework and scheduling issues negatively impacted the company's customer satisfaction levels. In addition, Crane's engineering team had to assemble a wealth of documentation at every stage to satisfy FAA requirements. Crane realized that to accelerate and streamline the software development process — without sacrificing ultimate product integrity or regulatory compliance — it needed to identify an advanced technology solution that would model and predict real-world performance of these smart systems at a much earlier stage.

SCADE PUTS THE BRAKES ON MANUAL WORK

Crane evaluated a number of model-based development environments before choosing SCADE Suite. The company selected SCADE because it is a purpose-built software development tool qualified to meet the standards of DO-178B up to Level A, the highest level of safety for the aerospace industry. In addition, engineers were impressed by the support that they would receive from Esterel while installing and running SCADE solutions.

Software developers must test for each possible input to the brake control software — as well as for a broad range of operating events.

Since implementing SCADE Suite in 2010, Crane Aerospace has realized significant cost, speed and efficiency benefits in its safety-critical software development, verification and validation process. From the earliest stages of code development, the SCADE tool enables software engineers to simulate and confidently predict real-world results, eliminating surprises and rework at later stages. SCADE Suite automates the code-generation process and enables the testing of embedded software code against thousands of inputs, without the need for a target. This significantly reduces the need for manual work involved in code generation as well as related software development, verification and validation tasks.

During software simulations, SCADE Suite allows the engineering team to subject the design to thousands of inputs and events to ensure that the software will function exactly as expected when installed in an actual plane.

SCADE allows customers like Crane to build customized libraries that include general-utility operators, primary and ancillary brake functions, and system interfaces. These reusable libraries make software development even faster. In addition, SCADE Suite generates much of the process documentation automatically, eliminating hours of work that once were invested in meeting stringent government requirements for record keeping.

MOVING BEYOND CODE VERIFICATION

While there are many ways to verify that software performs accurately against customer requirements, Crane engineers leverage SCADE to take logic and control a step further — by validating that software requirements make sense and protect passenger safety. Because simulation makes system behaviors visible, SCADE allows engineers to flag exceptions and identify problems with initial requirements. If not detected and addressed, oversights in initial software requirements can result in late-stage issues that delay projects and add to cost.

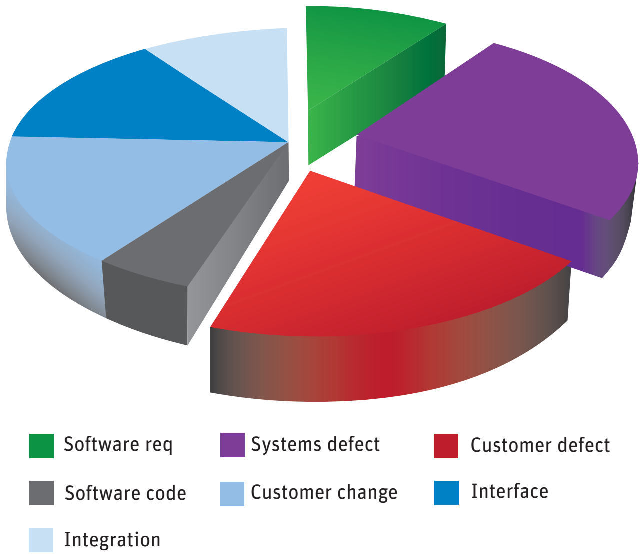
IN-PROGRESS SIMULATION OF FAULT DETECTION SUBSYSTEM

Since Crane Aerospace first implemented SCADE, the solution has identified more than 150 errors in preliminary system requirements and more than 180 flaws in corresponding software requirements. These errors, some major and some minor, were caught and eliminated in early validation exercises — before the systems ever existed in the real world. Prior to the SCADE implementation, these flaws might not have been discovered until very late in the manual software development process — resulting in significant rework for Crane's software engineers.

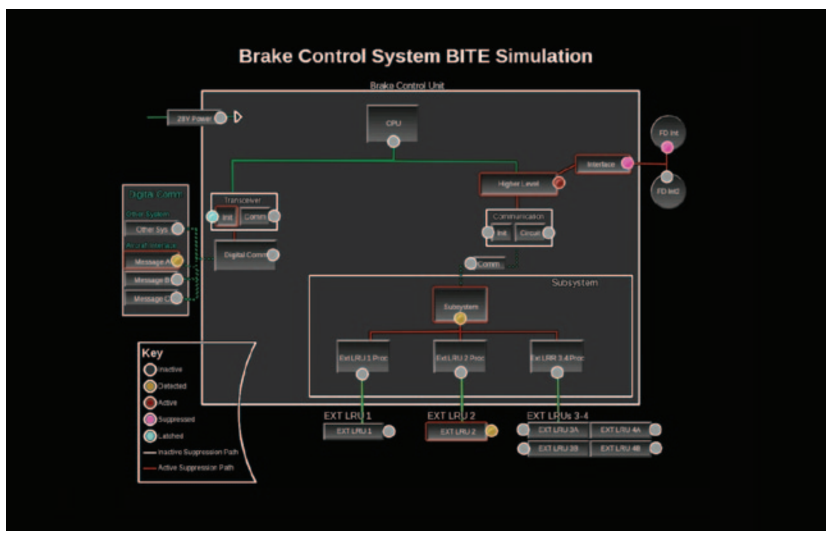
Today when errors are detected, what-if scenarios in SCADE Suite allow software engineers to quickly see the ultimate impact of any design changes on system reliability and braking performance. They can quickly identify the problems in underlying requirements and adapt the software model accordingly.

VISUAL MODELS OFFER OBVIOUS BENEFITS

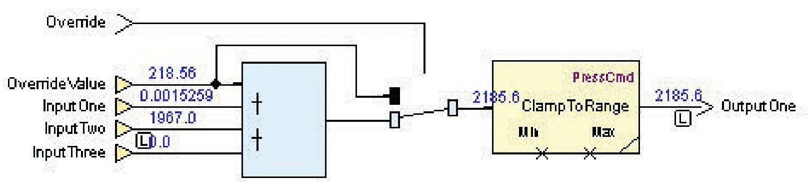
A number of features in SCADE Suite make it easy to communicate defects and other issues to aerospace customers. SCADE



▲ A significant number of late-stage defects in braking control systems arise from first-stage defects in the customer requirement. SCADE Suite allows Crane engineers to identify and address these issues during initial code validation.



▲ In-progress simulation of fault detection subsystem




```
;
BRAKESB:    JBS     STATUS2,1,BRAKESK       ; Check status
            JBS     STATUS2,7,BRAKESK       ;
            LD      LX,PEDALC[WHEEL]        ; Select the greater value
            CMP     LX,PEDALCCP[WHEEL]      ;
            JH      BRAKESC                 ;
            LD      LX,PEDALCCP[WHEEL]      ;
            SJMP    BRAKESC                 ; Continue
;
BRAKESK:    LD      LX,PEDAL[WHEEL]         ; Select the greater value
            AND     LX,#0FFFH               ;
            LD      AX,PEDALCP[WHEEL]       ;
            AND     AX,#0FFFH               ;
            CMP     LX,AX                   ;
            JH      BRAKESC                 ;
            LD      LX,AX                   ;
```

▲ **SCADE Suite improves internal and external communication by transforming dense lines of software code (bottom) into intuitive graphics (top). These reveal the software's underlying logic in a highly visual manner that all stakeholders can quickly understand.**

enables Crane software engineers to generate easy-to-understand graphic models and reports that reveal the inner workings of software code in a way that all process stakeholders — including Crane customers — can quickly comprehend. During simulations, users can view real-time software performance values and easily understand the immediate impacts of model changes.

SCADE Suite translates lines of unintelligible software code into visual, intuitive graphics that make the software logic — and any disconnects — apparent, even to non-SCADE users. This has helped to create a higher level of customer satisfaction, especially when compared with the original time- and labor-intensive process, as Crane's engineering team interacts with customers during software development, verification and validation.

CUSTOMER SATISFACTION TAKES OFF

With the incredible pressures that aircraft manufacturers face today, SCADE Suite supports Crane's efforts to help its customers meet tight budgets and schedules — by providing faster, highly accurate software development. Shortly after implementing SCADE, Crane successfully used the software's intuitive libraries and graphical models to meet a two-week turnaround for a scaled-down customer demo of a new control system.

Today, Crane is able to deliver on customer requirements, as well as meet the stringent demands of the FAA's DO-178B guidelines, via a compressed development schedule. Day-to-day engineering work is much more quick and efficient, and errors are detected at a much earlier stage.

In addition, SCADE software has increased Crane's agility and speed in adapting to new developments in braking control systems, such as improved microprocessors, offering more robust and sophisticated fault-detection software. Using SCADE Suite positions Crane to easily incorporate any new brake control innovations as it simulates how software code functions as part of a larger aircraft system.

In some cases, Crane's customers have actually used SCADE's systems-level models and what-if simulations to consider enhancements to overall braking system prototypes during iron-bird testing, a dimensionally accurate structure specially fabricated to replicate the aircraft. Instead of identifying "surprise" software performance variations while in the iron-bird environment, customers are uncovering new systems-level insights that inform the entire brake control environment. Supported by SCADE software, Crane can offer its customers industry-leading, forward-looking braking system technologies, on-time delivery and the high product quality they rely on every day. ▲

SCADE Suite has enabled Crane Aerospace to help its customers meet tight budgets and schedules.

Aborted Takeoffs:
A Special Engineering Challenge

Rejected (or aborted) takeoffs pose special challenges for brake control systems. During a rejected takeoff (RTO), an airplane has much more energy than during a normal landing due to higher speed and a significantly heavier weight. Moreover, an aircraft has typically used up much of the available runway when the pilot has to make the difficult decision to abort. While most landings may use only 20 to 30 percent of the plane's available braking capability, during an aborted takeoff up to 100 percent can be needed to stop safely, and, thus, the control software must ensure near-ideal performance. Since pilots are usually focused on the conditions that led to the rejected takeoff, Crane brake control systems offer an automatic braking function that applies full brakes during an RTO. Because rejected takeoffs represent such a great challenge, Crane's software engineers focus particular attention on this demanding event during their SCADE simulations.