Case Study

Pilot Ejection Seat

AdaCore

The GNAT Pro Company

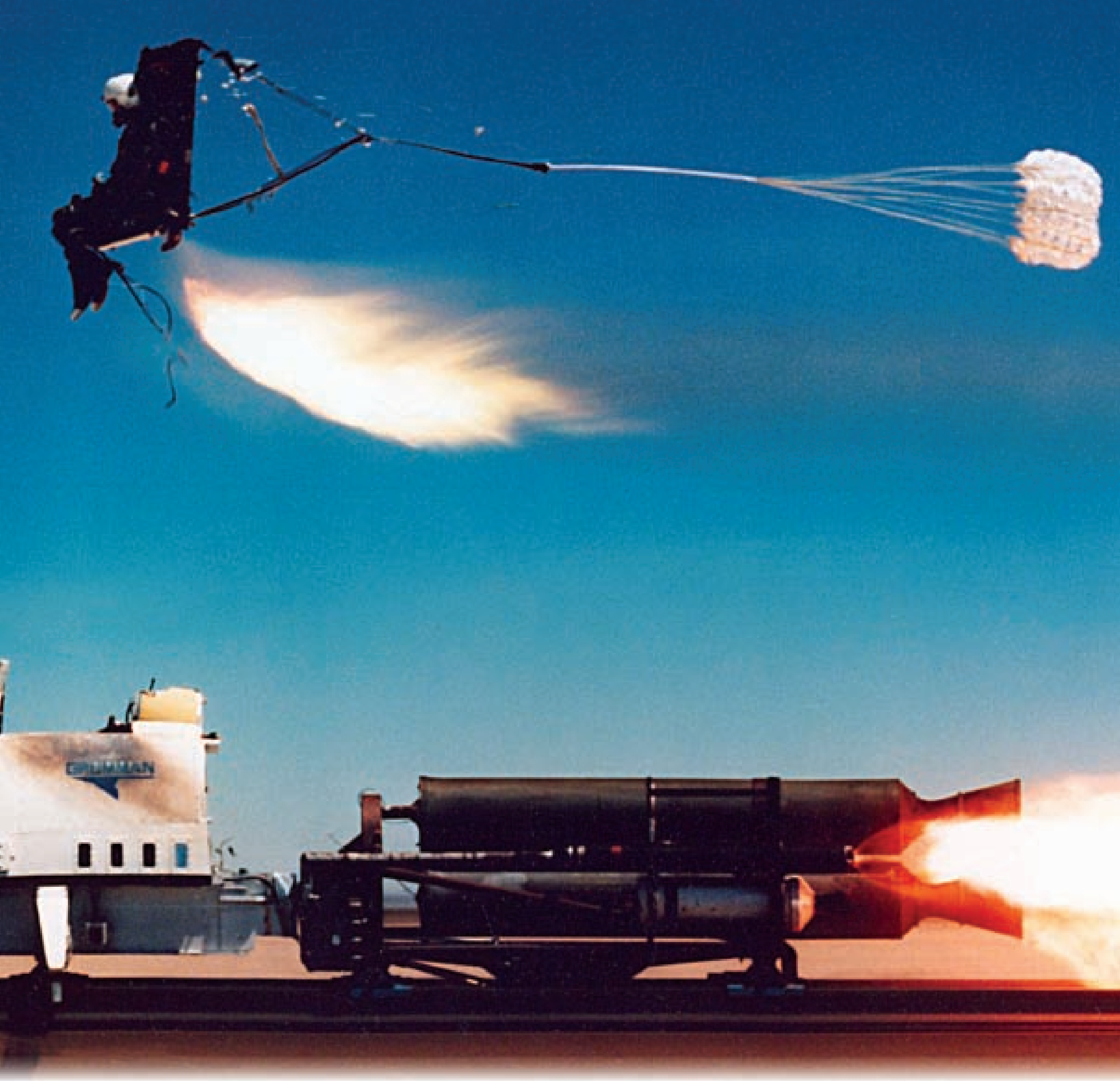
U.S. Navy Fighter Jet Pilots Ride COTS to Safe Landing

SAFETY-CRITICAL ADA ENVIRONMENT HELPS EJECTION SEAT SAVE LIVES/MONEY

BY DR. JASON HENDRICKS, SYSTEMS ENGINEER, MARTIN-BAKER, BRETT PORTER, SENIOR SOFTWARE ENGINEER, ADA CORE, LEE COTTER, NEW BUSINESS & PRODUCT DEVELOPMENT, TELEDYNE

Talk about a safety-critical application! The U.S. Navy is using a new ejection seat sequencer that will catapult a pilot and co-pilot (and the seats) out of a damaged F-18, F-14, or T-45 aircraft within 0.2 seconds from the time the ejection handle is pulled. A complex, triple-redundant digital sequencer senses just the right speed and altitude and then deploys a parachute, contained within the ejection seat, to ensure their safety.The ejection seat is a safety-critical military application designed using all commercial-off-the-shelf (COTS) components and written using the Ada programming language. The project, which was a team effort of Martin Baker, Teledyne Electronic Safety Products, Ada Core Technologies, and the U.S. Navy, is known as FAST (Future Advanced Sequencer Technology). The COTS project resulted in a sequencer that cost half of its predecessor.

The electronic sequencer architecture and the Ada programming environment provided the requisite reliability for this project, and because of its tightly generated object code, helped developers meet size constraints. Because it is easy to



follow/review, using Ada made it easier to make changes to the system for updates and maintenance. In fact, a modified version of the FAST sequencer will be deployed for the ejection seat used in the Joint Strike Fighter (JSF), and using Ada in FAST made the modifications quick and easy to review.

How It Works

The ejection seat is formally the Navy Aircrew Common Ejection Seat (NACES) and is controlled by the electronic FAST sequencer. Actually, the NACES FAST sequencer replaces an original NACES sequencer with a reduced cost, enhanced performance version. The sequencer is energized when the ejection handle is pulled, which then initiates the seat. After the seat has separated from the aircraft during an escape, the sequencer controls all major automatic sequencing functions.

The NACES FAST sequencer is equipped with its own environmental sensors that provide information from which decisions about the correct and optimum sequencing strategy can be made. Sequencing requirements are primarily a function of the initial ejection conditions of airspeed and pressure altitude. Under many situations, the sequencer further modifies the sequence timings in response to the actual progress of the ejection. This not only ensures highly optimized seat performance,

Continued on page 10

but also provides a degree of resiliency to unlikely and unexpected events that could otherwise compromise crew recovery.

Two thermal batteries that are activated at the time of seat initiation power the sequencer. Dual redundant electrical start switches, operated by pyrotechnic gas pressure, form an important safety feature. The sequencer senses switch operation and then executes an ejection sequence, precluding inadvertent initiation of the seat pyrotechnic devices until the seat has physically departed the aircraft.

The first operation is Drogue Deployment. As the seat separates from the aircraft during ejection, the sequencer at a fixed point in time, initiates drogue deployment in all ejections. Just after the drogue deployment Environmental Sensing Time Window operation begins in which the sequencer's onboard sensors record the seat acceleration deceleration (due to aerodynamic drag), the pitot pressure, and the base pressure (pressure behind the seat). These measurements allow the sequencer to determine the ejection speed and pressure altitude conditions.

Four Modes of Operation

At this point, the ejection seat has four modes of operation related to ejection airspeed and altitude conditions. These include:

Zero/Zero mode, under low speed/low pressure altitude ejection conditions (up to 90 KEAS and below 18000 feet) the main parachute is deployed at the earliest practicable (fixed) time after ejection in order to maximize terrain clearance. Inhibiting drogue deployment is not possible because it is initiated before environmental sensing. As such, the drogue bridle is released before drogue lines are taught (as soon as the mode decision is made), effectively disabling the drogue phase.

Low (Altitude) Drogue Mode with Continuous Sensing, in which a seat stabilizing/retarding drogue phase occurs, which is required when the ejection occurs at either a significant airspeed or significant air pressure altitude. The sensed acceleration, pitot pressure, and base pressure values are used to give a prediction of the parachute deployment time when the velocity of the seat has decayed such that peak parachute inflation loads will fall within required limits. The aim is to

NACES/FAST sequencer. The " FAST " is a major upgrade to the original NACES version although the housing remains essentially the same.

optimize seat performance by limiting the parachute inflation load to 17 "g"s at altitude between 0 and 8000 feet, progressively reducing to 10 "g"s at 18000 feet as the risk of terrain proximity diminishes.

Low (Altitude) Drogue Mode No Continuous Sensing, for ejections occurring at altitudes below 18000 feet with velocities that lie between the Zero/Zero Mode and Low Drogue Mode with Continuous Sensing. A seat stabilizing/retarding drogue phase is employed but unlike the Low Drogue with Continuous Sensing Mode, the time at which the main parachute extraction occurs is based on pre-determined timings calculated from the values sensed ejection conditions.

High (Altitude) Drogue Mode, at ejections in excess of 18000 feet, a drogue phase is extended until such time as the sequencer senses the seat has descended below the 18000 feet fall-through boundary, at which time the main parachute is deployed. This ensures that the seat occupant is recovered to more benign atmospheric conditions in the shortest possible time. In this mode, a minimum parachute deployment timing of 4. 62 seconds from the start switch is enforced to cater for ejections occurring close to the mode boundary altitude, eliminating any possibility of parachute deployment at excessive airspeed.

No Single Point of Failure

The sequencer hardware/software has been configured to eliminate single point failures. For the most part, this is achieved by a triple-redundant hardware architecture that uses hardware/software-voting logic. In addition, appropriate failure detection and correction measures have been incorporated to maintain the "no single point failure" philosophy.

The sequencer comprises three microprocessor control channels, each essentially performing the same operations. Each channel has an electrical power supply, microprocessor, memory, inter-channel communications, sensors, signal communication elements (filtering, sampling, and A-D converters), hardware voters, and outputs.

The sequencer senses environmental parameters such as seat absolute base pressure (air pressure behind the seat), seat absolute pitot pressure, and acceleration in three axes. In addition, each channel senses the state of the two start switches. The outputs are four five high-current electrical squib-fire signals for initiation of electro-explosive devices mounted within the seat pyrotechnic cartridges. These include the drogue deployment device, drogue bridle attachments release, parachute deployment device, primary and backup seat harness attachments release, and backup seat harness attachments release.

Once energized, each channel processes its own inputs and makes provisional decisions. The three channels then cross-compare their individual results to harmonize the outputs, and to protect against erroneous decisions made by a malfunctioning channel. Hardware voting provides a further level of protection against incorrect outputs by preventing one channel alone to initiate an electro-explosive device.

The sequencer has a substantial non-volatile memory for keeping a comprehensive record of the ejection history (environmental sensing, decisions, and voting) as it progresses. This data can later be downloaded to facilitate a detailed analysis of the ejection sequence.

The NACES design was tested at extreme speeds and altitudes, as well as more benign conditions, and has been proven extremely reliable. The first production of the original NACES flew in an F-14D in February 1990 and since that time, hundreds of seats have been delivered to the U.S. Navy, most of which are now in service.

AdaCore

The GNAT Pro Company

North American Office
104 Fifth Avenue, 15th floor
New York, NY 10011
USA
Tel. +1 212 620 7300
Fax +1 212 807 0162
Email: sales@adacore.com

European Headquarters
8, rue de Milan
75009 Paris
France
Tel: +33 (0)1 49 70 67 16
Fax: +33 (0) 1 49 70 05 52
Email: sales@adacore.com

www.adacore.com