Verification & validation of safety-critical systems - Fault Injection

Category: Computer Hardware & Software
Reference: TDO0004

Broker Company Name: Instituto Pedro Nunes (IPN)
Broker Name: Carlos Cerqueira / Inês Plácido
Telephone: +351 239 700 952 / +351 239 700 922
Email: cerqueira@ipn.pt / iplacido@ipn.pt

Abstract:

The solution is provided by an international company offering dependable solutions, services, and software technologies for safety-critical and business-critical information systems, namely embedded control systems in the Aeronautics, Space, Defence, Railway and Automotive segments. The fault injection technology is particularly appropriate for contexts of high availability, reliability, and safety requirements, where failures may lead to the loss of human life, or otherwise result in serious damage to property or cause significant financial losses to businesses. The company is looking for technical / strategic engineering partnerships for further technological developments, testing and roll-out of new applications, and adaptation of the technologies to novel business needs.

Description:

Aerospace, automotive, industry, defense, telecommunications are some of the areas posing new challenges to the software industry in term of high availability, reliability and safety requirements. New applications and systems must be intensively tested before deployment to guarantee that the system and built-in fault-tolerance mechanisms are working as expected. Ensuring the system responds appropriately to unusual or exceptional events is a problem that requires something more than traditional testing.

Used by space agencies around the world, the company's fault injection technology provides the ability to test systems in exceptional situations, and evaluate their behaviour beyond normal limits of operation, to significantly mitigate risks of failure in the field. The technology is complimentary to verification & validation activities used in these fields, and to RAMS (Reliability, Availability, Maintainability, Safety) activities, and strongly influence mitigating FDIR (Fault Detection, Isolation and Recovery) mechanisms that are put in place at time of development.

It can force worst failure scenarios on the systems under test, and spot weak-points, providing feedback for correction or redesign. In addition, the solution has a full family product line that includes several components, making this tool a reference in the market. These include: 1) the main tool, a Software Implemented Fault Injection (SWIFI) technology; 2) a powerful add-on tool enhancement to the main product front-end application and an analysis tool; 3) an extended tool, with the fault injection extensions based on Scan Chain and pinlevel forcing technology.
Innovations and advantages of the offer:

This technology uses advanced debugging and performance monitoring hardware features, available in common processors, to inject faults and monitor the activation of errors and their impact on the target system. The technology can test systems in exceptional situations and force worst-case failure scenarios, while being completely un-intrusive at the software level. In short, it is a unique tool that allows tests in the target embedded system that otherwise would require much more effort and would not be at all possible using common techniques. During Fault Injection campaigns it is possible to spots weak points and which than can be fed back onto the development process and avoid serious or undesirable behaviour in the end product. Systems can in this way be evaluated under realistic conditions, with minimal to no intrusiveness, and reliable validation of fault tolerance mechanisms can be achieved.

Further Information:

Key features of the Fault Injection Technology:

- Automated fault-injection tool
- Supports product certification (dependability and RAMS)
- Professional environment for performing fault-injection based tests
- Performs fault-injection regression with no effort
- Increases confidence in the product and assures compliance to requirements
- Product Performance, Stability, Reliability, Availability and fault tolerance
- Software Implemented fault injection (SWIFI) with limited intrusion
- Scan Chain Implemented fault injection (SCIFI) with minimum intrusion
- Fault injection in source code (C and Ada)
- Fault Injection in binary code
- Fault Injection in Sparc, PPC, ARM and x86 architectures
- Adaptable to other architectures in reasonable times
- Complement to verification and validation activities
- Complement to RAMS activities
- Capability of performing tests according to ISO 26262 automotive standard
Application:

Aerospace, automotive, railway, medical devices, defense, telecommunications, banking and insurance are some of the areas posing new challenges to the software industry in terms of high availability, reliability and safety requirements. Examples of critical embedded-driven systems whose failure threatens human lives can be found in the aerospace sector (e.g., satellite navigation systems), railway control (e.g., track side signalling control equipment and interlocking systems), medical life-support (e.g., pacemakers), industrial plant control, nuclear power plants, the automotive industry (e.g., engine control units), and in the defence sector (e.g., weapons control systems), among others.

Space Heritage:

ESA missions/projects:
- Herschel/Planck application software and operating system validation;
- Sentinel-1 operating system and run time environment validation;
- Free/open-source real-time, executive for on-board space applications;
- Remote Exploration Experiment for validating the cluster of computers on-board the spacecraft.

Other non-ESA customers: NASA, CASC and JAXA and Chinese Telecom and Avionics institutions.

Broker comments:

The technology has huge potential of application in non-space sectors (where Critical has a sound position) and Critical has been very active in the search for TT opportunities. Namely, they have been funded by the PTTI and are developing a TT project for the automotive market.

This technology description was downloaded from www.esa-tec.eu