



# Built-in-Test plays a key role in system integrity

By Duncan Young



Often perceived as just a tick in the box during the selection process, Built-in-Test (BIT) is an invaluable component of modular, embedded systems that are used for critical applications such as avionics mission systems, sensors, and weapons. BIT provides a level of confidence in the correct operation of each module at both power-up and during normal operation. As more of these critical embedded systems are assembled from off-the-shelf hardware and software components, it is increasingly important to evaluate BIT's performance and its potential for interaction with software such as RTOS.

These types of systems are typically configured from VMEbus, VXS, VPX, or CompactPCI from vendors such as GE Fanuc, Curtiss-Wright, Mercury, and Thales using OSs from Green Hills Software, LynxOS, and Wind River. The way embedded computing systems are architected is changing rapidly: more highly integrated at the platform level plus extensive communications and network connectivity for cooperative engagement in the field. BIT supplied by hardware vendors is changing to reflect these new requirements by moving away from the traditional three-layer approach toward greater BIT functionality running concurrently with the application.

### Three-layer approach

The traditional approach to BIT is representative of a much less complex era, when federated subsystems could be tested individually without impacting other subsystems. It has three layers:

- Power-up BIT (PBIT) – Comprehensive tests of hardware functionality extending as close to the edge of a module as possible.
- Initiated BIT (IBIT) – Usually invoked following a failure, IBIT initiates tests to isolate a fault within a system or subsystem. In general, IBIT will halt the current application, run its tests, and either resume or restart the application.
- Continuous BIT (CBIT) – These are any tests performed while the application is active. They may be part of the application itself or might be supplied by the hardware module vendors to run periodically.

### IBIT becoming impractical

PBIT is still a necessary requirement to provide confidence in the hardware integrity. It is usually the SBC vendor that provides the basic PBIT package enhanced with PBIT modules for each of the additional hardware components. The concept of IBIT makes good sense where there are many discrete subsystems that do not interact with each other, for example, a Naval radar receiver or Electronic Counter-Measures (ECM) system. However, on other weapons platforms such as Unmanned Aerial Vehicles (UAVs), single seat combat aircraft, helicopters, or ground vehicles, the operators will not have the time nor the skills to employ intrusive test methods to diagnose and repair faulty equipment during a

mission. Modern avionics systems are becoming more integrated as their mission computers perform many different functions using the same hardware, making it more difficult for an individual function to be diagnosed and rectified using IBIT.

### Online BIT holds key for the future

As the value of IBIT diminishes with more system integration, the burden of hardware confidence must pass to either the application software, the operating system, or the hardware vendor's CBIT. Deployable systems make use of all of these; nevertheless, as the OS and CBIT are off-the-shelf products, their vendors have a responsibility to ensure tight integration without degrading the OS's key performance parameters or determinism. To be nonintrusive, CBIT must have very low latency and always return control to the application with the hardware environment unchanged. This can be achieved by running CBIT in a secure partition and ensuring that tests run with the minimum impact on the operational hardware environment (for example, by running memory tests in dedicated segments per bank). These techniques are used by GE Fanuc Intelligent Platform's Deployed Test Solutions product, which offers extensive CBIT testing in the form of Background Condition Screening (BCS).

It has always been a goal of the military to operate their platforms with some subsystems inoperative or with reduced functionality in the event of insufficient maintenance, spare parts, or battle damage. In the era of federated systems, this was easily achieved by disconnecting or ignoring nonserviceable subsystems. However, this approach is not always possible with an integrated system or with functions of a system that rely on extended connectivity through a network for their correct operation. CBIT has an important role to play by monitoring and logging the state of the hardware environment which, together with data gathered by the application, will allow a user to make an informed decision on which operations can be trusted and which should not.

Taking a glimpse into the future, one of the higher integration costs of embedded COTS subsystems is integrating BIT across dissimilar vendors' hardware. This might be perceived as one of the few remaining areas for market differentiation between vendors but could, usefully, be targeted for standardization. Additionally, in the future it is likely that as transistor count of processor cores continues to multiply, there will be a surplus of processing capacity that could be used exclusively for BIT, decreasing its latency and increasing its coverage. BIT is not a static piece of firmware in flash EPROM. It is continuing to evolve from a diagnostic maintenance aid to meeting the user's needs for high system availability by providing practical feedback on the ability of the hardware to meet its critical-mission requirements.

*To learn more, e-mail Duncan Young at [young.duncan1@btinternet.com](mailto:young.duncan1@btinternet.com).*