

Low cost hardware for counterfeit component detection

By Andy Bonner

Electronics marketplace developments have accelerated the incidence of counterfeit components. A risk mitigation strategy that includes affordable component testing is increasingly important to distributors and manufacturers facing this threat.

Washing machines and aerospace control systems have at least one thing in common: they both contain electronics boards. And their manufacturers hope to enjoy many years' stable production to maximise their return on the boards' development costs. However, key component suppliers can fail, withdraw a component or simply impose allocation or impossible lead times to reduce their own stocking overhead in difficult conditions.

Independent, non-franchised component distributors, skilled in locating rare and obsolescent components from many international sources, are often the answer. However the very nature of their operation can increasingly bring risk as well as salvation. How can they and their customers ensure that tempting but relatively new and unproven sources will deliver quality components with no counterfeit content?

Counterfeiting has evolved along with the industry it feeds on. Fifteen years ago, sourcing obsolete components was much simpler. A limited number of excess inventory suppliers offered years of experience in locating stock surplus to requirements for legitimate reasons. They could demonstrate its provenance and therefore its quality.

Of all the factors that have impacted component supply since then, two of the most important are the explosion of the Internet and the emergence of green initiatives such as the European Waste Electrical and Electronic Equipment Directive (WEEE). The Internet has allowed volumes of small suppliers of varying and unknown quality to open a shop window with little difficulty or traceability. And some are selling counterfeits ranging from substandard versions of the expected function to burned out shells whose internal function is completely unrelated to their labels' claim even if they worked.

WEEE and equivalent directives have spawned recycling points that ostensibly render expired electronics safely. However some ship their e-waste to China, where streetworkers harvest components from the PCBs using braziers for sorting and labelling as the 'market' demands. Functional yet potentially substandard components arise from 'Ghost shifting'. Here, illegal out of hours shifts are used to produce undocumented and untested shipments of otherwise legitimate components for unauthorised distribution. Other aberrations appearing on the market include commercial grade components sold as military, floor sweepings, QA failures and dummy parts intended only for sales presentation kits.

Distributors and manufacturers can counter these threats at both commercial and technical levels. Commercially, steps can be taken to minimise the chance of buying counterfeits at all.

Technical measures include visually inspecting and electronically testing incoming batches. However, the cost of test equipment has until now been a barrier in many applications.

A recent counterfeit detection application development has shown how this can be overcome by marrying component test and PC technology. The development has resulted in a PC compatible pod product with a set of ZIF sockets accepting DIL, SOIC, BGA, SSOP and other packages as well as discrete components. It also includes Windows compatible software providing the engineering and operator interfaces.

The system uses a comparative technique to rapidly learn new components and then test them. A known good component is locked into the ZIF socket while a test pattern is applied across all its pins. The component's response to this test pattern, or PinPrint, is automatically measured and stored as a benchmark. Testing between every possible pin combination is included, maximising the chances of capturing internal fault conditions. Henceforth any incoming component claiming to be of the same type can be subjected to the same test, and its PinPrint automatically compared to the benchmark results. Any deviation beyond a preconfigured tolerance is immediately flagged as a failure. This allows a volume of components to be tested rapidly on a simple Go/No Go basis.

As parts become increasingly complex, 100% testing becomes onerous, but 20 – 30% testing on, say 200 pieces is manageable. Experience to date has shown that variations arising from a suspect shipment will reveal themselves well before such a test is complete.

Counterfeit components are an ever present, growing and sometimes subtle threat. This counterfeit detection development has shown how protection can be brought within the budget of most companies through exploitation of PC technology. Apart from using low cost PC display, computing and storage hardware, the Windows based Go/No Go and associated menu software allows use by lower cost non specialist staff with minimal training.

Andy Bonner is Technical Director of Cupio Ltd.

Cupio's website is www.cupio.co.uk