Xilinx FPGA Certification Challenge

This white paper discusses how Global ETS is able to identify counterfeit Xilinx FPGAs for our customers. After a brief introduction of how Xilinx tried to prevent counterfeit FPGAs from entering the supply chain, we will discuss the Global ETS solution to this problem. The overall details of our approach are as follows:

- We support all package types via a custom IC test fixture
- Comprehensive testing data is taken to adequately determine part authenticity
- Fast turn time – complete testing for our customers can be completed in 7 days
- We have the ability to accurately determine the speed ranges at specified chip temperature
- This is accomplished with a proprietary program using an AI algorithm and machine learning
- This includes the ability to determine if devices are Engineering Samples or Production devices

Starting in 2016 to early 2017 Xilinx introduced a 2D board code marking on all 28nm, 20nm and 16nm FPGAs and MPSoCs. The 2D bar code was an industry trend to improve device level tracking and improve product traceability to maintain tighter device manufacturer control. Unique to each device 2D bar code was manufacturing genealogy information including device lot, date code, speed, temperature grade and SCD information. This was added to 7 Series, UltrScale, UltraScale+, Zynq-7000 and Zynq UltraScale+ parts.

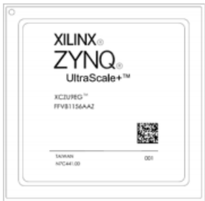
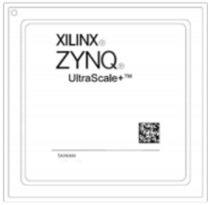
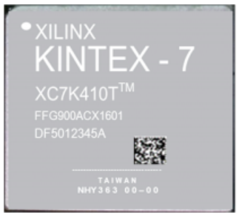
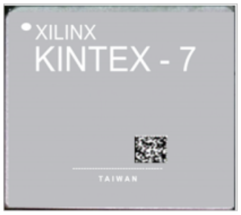
Product Family	Current	After Transition (Refer to XTP544)
(Existing Production) UltraScale+		
(Existing Production) 7-Series Zynq UltraScale		

Figure 1: Product marking examples for current production devices.

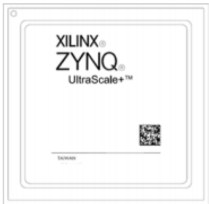
Product Family	After July 1, 2019
(New Products) 7-Series Zynq Ultrascale UltraScale+	

Figure 2: Product marking example for new products, or family expansion.

With the new 2D bar code marking, all critical device information was no longer marked on the device. More importantly approval from Xilinx was required to use their 2D bar code scanning app or login to upload a 2D image. Recently Xilinx took the ability to scan the 2D bar code away from independent suppliers and/or third-party test laboratories. As a result, the device lot, date code, speed and temperature grade cannot be independently confirmed. This is a huge problem since suppliers and end users do not know what part they have/purchased, especially when manufacturer traceability is not available.

How can Global ETS Help?

At Global ETS we have been fighting the battle against fake parts for years and have deep-experience with identifying counterfeit parts for our customers. One of the biggest challenges the global supply chain is facing is counterfeit FPGAs, such as the popular Xilinx family of chips. Not only are bogus parts being sold as OEM, but OEM parts are being intentionally marked as high-speed using various means. This overview document has been put together so that the global supply chain will understand how to combat this problem so that bogus parts don't enter critical systems such as aerospace and military platforms [1]

"The challenge of microelectronics counterfeit prevention is to detect fake OEM parts, but what if the part is an actual OEM's part and yet still counterfeit? Not only is it possible, it's common. The most counterfeited product in the global microelectronics market is not always a fake. Very often it is a true OEM original but has been altered and is not suitable for the full requirements of system performance and use in a critical military system[2]."

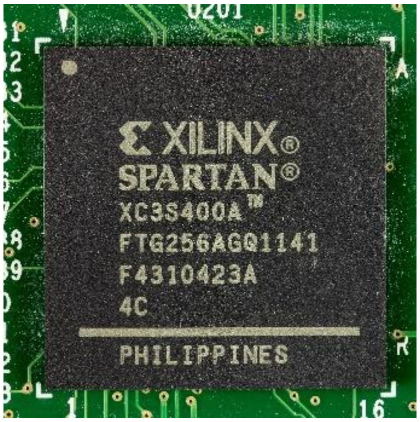


Figure 3: The huge volume of e-waste provides an inexpensive means for counterfeiters to re-purpose obsolete/used high-end electronics for resale. https://en.wikipedia.org/wiki/File:RetiredCPUs.jpg.
Xilinx FPGA's are the top high-end ICs being counterfeited world-wide. Not only are non-OEM parts in the supply chain, but OEM parts with fake speed grade markings continue to wreak havoc at all levels of the global supply chain, especially for high-end military and avionics systems [3].

At Global ETS we have the expertise to not only identify counterfeit parts by comparing them to OEM parts, but we can discriminate between speed grades to ensure that our customers are using parts with the performance they pay for. One example is FPGA speed grades where counterfeiters alter the designation from slow to medium or fast speed.

"For example, take an FPGA [field-programmable gate array] that has four speed grades. Speed grade #1 is priced at $350.00; speed grade #2 at $3,500.00; speed grade #3 at $35,000 and so on. In this example, the core/parent part numbers are consistently the same, with the last -XX being the unique identifier for binning (ex: SE123456789-01). The counterfeiters take the speed grade #1, change the last -01 to an -03 marking, and ostensibly make it a speed grade #3."

In order to effectively identify counterfeit parts, it helps to understand how they are created in the first place. E-waste is often the source of such parts and the following flow chart shows the methods often used to prepare bogus parts for sale:

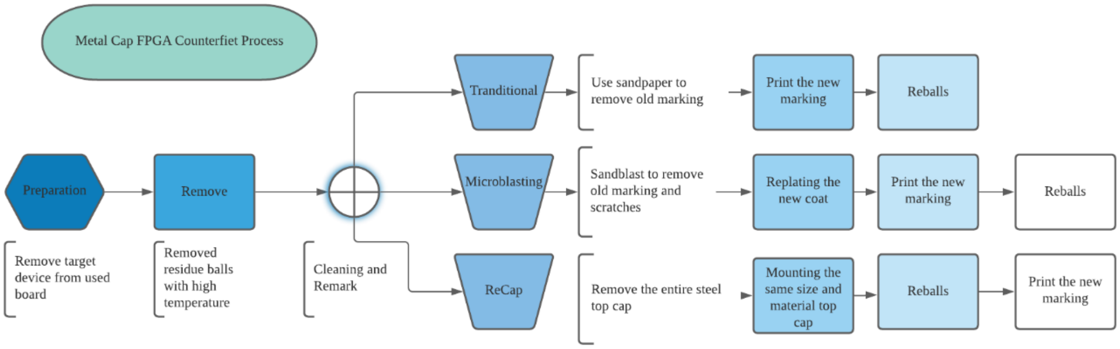
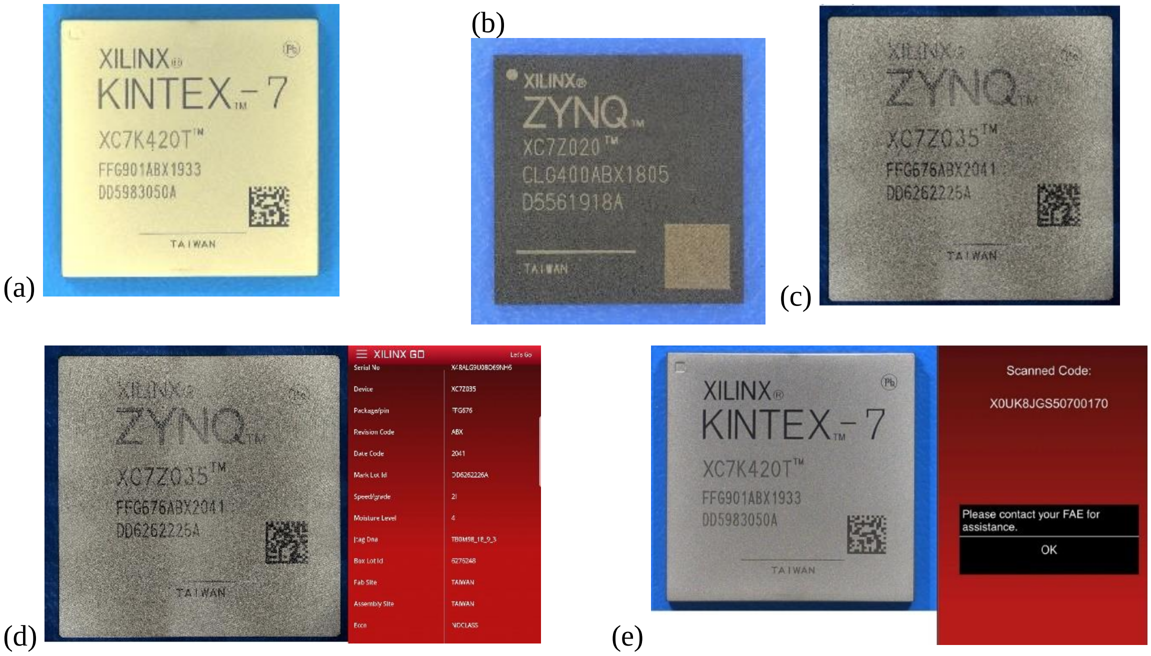

Metal Cap FPGA Counterfeit Process
Preparation
Remove
Remove target device from used board
Removed residue balls with high temperature
Cleaning and Remark
Trandiitional
Use sandpaper to remove old marking
Print the new marking
Reballs
Microblasting
Sandblast to remove old marking and scratches
Replating the new coat
Print the new marking
Reballs
ReCap
Remove the entire steel top cap
Mounting the same size and material top cap
Reballs
Print the new marking

Figure 4: Typical process(es) used to prepare counterfeit parts for sale/resale at a higher speed grade. Starting with used parts on a PCB, the target is detached from the board, the solder dots cleaned and the parts are then ready for 3 tracks: remark the chip lid using sandpaper (top), microblasting to remove the marking (middle) and complete removal of the cap (bottom). At Global we are familiar with how to test for each case and details of this are presented here.


(a)
XILINX KINTEX-7 XC7K420T FFG901ABX1933 DD5983050A TAIWAN
(b)
XILINX ZYNQ XC7Z020 CLG400ABX1805 D5561918A TAIWAN
(c)
XILINX ZYNQ XC7Z035 FFG676ABX2041 DD6262225A TAIWAN
(d)
XILINX ZYNQ XC7Z035 FFG676ABX2041 DD6262225A TAIWAN
XILINX GO
Let's Go
(e)
XILINX KINTEX-7 XC7K420T FFG901ABX1933 DD5983050A TAIWAN
OK

Serial No	X-RALG9U08O69NH6
Device	XC7Z035
Package/pin	FG676
Revision Code	ABX
Date Code	2041
Mark Lot Id	DD6262226A
Speed/grade	2I
Moisture Level	4
Jtag Dna	TB0M98_18_9_3
Box Lot Id	6275248
Fab Site	TAIWAN
Assembly Site	TAIWAN
Eccn	NOCLASS

Scanned Code:

X0UK8JGS50700170

Please contact your FAE for assistance.

Figure 5: Photographs of commonly seen fake FPGAs to aid the manufacturer in rooting out counterfeit parts from the supply chain. (a) Bogus bar code, (b) erased barcode and (c) certified OEM part. Using the Xilinx app a bar code scan (d) confirms part authenticity whereas (e) is identified as a fake device.

There are many ways that fake parts enter the supply chain. On the manufacturing side these parts often look legitimate, but often, on closer visual inspection, it is obvious that something is no correct. Everything from re-stamping a part number or speed designation (for example -11 to -13) to placing a completely new lid on the chip. Below is a figure that shows examples of some of the practice commonly used to prepare fake chips for sale:

One of the most pressing issues, as quoted above, is to determine if the OEM chip speed grade is correct or the package altered to sell a slower, less expensive, chip as a faster, much more expensive, chip. A simple strategy has been developed at Global to address this issue:

Using our speed grade identification method, we can quickly determine the speed of a suspect part and compare it with our extensive parts database to determine if the part is OEM and the speed grade properly designated. The speed-grade testing system is shown below:

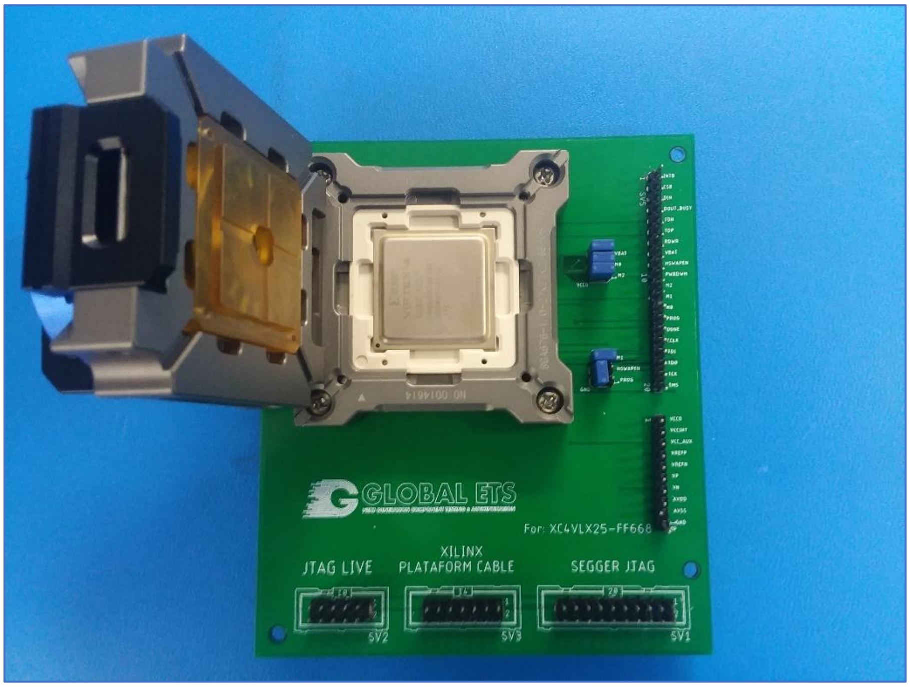


Figure 6: Speed grade system to determine the speed performance of an FPGA chip. The measured speed is first compared to a simulation, followed by comparison with our extensive FPGA speed grade parts database.

One example of system performance is shown below whereby the simulated and measured speed differential between -10, -11 and -012 is listed for both simulated and measured performance:

Table 1

Simulated Average Speed-Up/Slow-Down: 5000 gates

Speed Grade	Average Speed-Up		Speed Grade	Average Slow-Down
-10 -> -11	0.143337241		-12 -> -11	0.129144689
-11 -> -12	0.114368933		-11 -> -10	0.167719484

Measured Average Speed-Up/Slow-Down: 5000 gates

Speed Grade	Average Speed-Up		Speed Grade	Average Slow-Down
-11 -> -12	0.073314442		-12 -> -11	0.079135074

Comparing the data a clear distinguishing trend is apparent and allows for counterfeit ID:

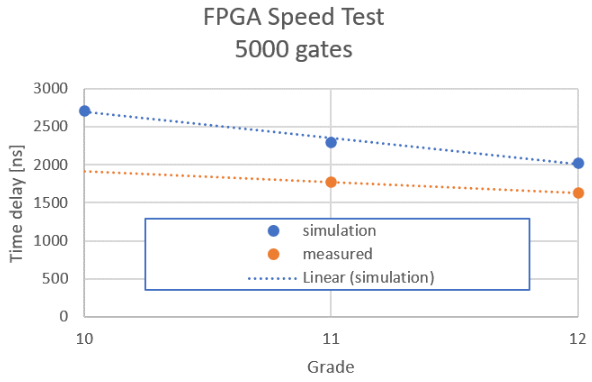


Figure 7: FPGA speed assessment using both a linear simulations and measurement using our FPGA speed grade testing system. Note slowest chip (Grade -10) has a longer delay than the higher speed -11 and -12 chips. Measured data allows for accurate speed grade testing using the Global ETS system.

How to verify a XILINX FPGA

At Global we have developed a comprehensive approach to detecting counterfeit FPGAs. Each method has been tested and verified as effective in identifying counterfeit parts, usually by comparing to a known good ‘gold standard’ part. Some of these methods utilize AI/machine learning as a means to discriminate between suspect and known good parts in cases where the observed discrepancies are large.

Due to recent production and supply chain disruptions the world-wide chip shortage is providing an opportunity for counterfeit parts to more easily get into the supply chain. One of the prime examples of this is the Xilinx Artix-7 FPGA family of ICs. In this technical note we will introduce proven methods to determine the authenticity of these parts which involves several complimentary methods of analysis.

There are basically three (3) steps needed to ascertain if a Xilinx Artix-7 is an authentic part. First visual scanning of the package (lid and solder bumps). Second C-SAM observation of the die attach layer to the lid. Third high-speed functional testing using the JTAG interface. First let us begin with an overview of changes that the manufacturer has made to combat counterfeit parts.

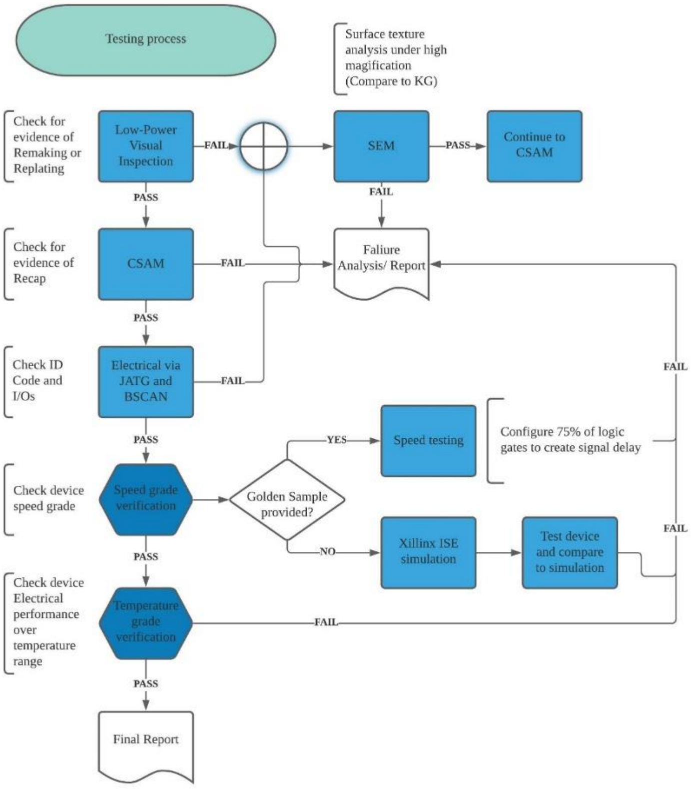

Testing process
Surface texture analysis under high magification (Compare to KG)
Check for evidence of Remaking or Replating
Low-Power Visual Inspection
FAIL
SEM
PASS
Continue to CSAM
FAIL
PASS
Check for evidence of Recap
CSAM
FAIL
Faliure Analysis/ Report
PASS
Check ID Code and I/Os
Electrical via JATG and BSCAN
FAIL
FAIL
PASS
YES
Speed testing
Configure 75% of logic gates to create signal delay
Check device speed grade
Speed grade verification
Golden Sample provided?
NO
Xillinx ISE simulation
Test device and compare to simulation
FAIL
PASS
Check device Electrical performance over temperature range
Temperature grade verification
FAIL
PASS
Final Report

Figure 8: Global ETS FPGA measurement methods used to identify bogus parts in the global supply chain. This uses physical, chemical and visual analysis along with electrical performance to determine part authenticity. Of particular note is our new system to assess part speed which is needed to flag remarked parts where the speed grade was altered.

Originally the lid contained information on the chip family, speed, temperature specifications, and a bar-code to allow for inventory control. Due to the global shortage, clearing houses have removed the bar code making it difficult to know if the chip in question is a legitimate Xilinx part. Fig. 1 shows examples of the former packaged part lid and the newer version with the bar code removed:

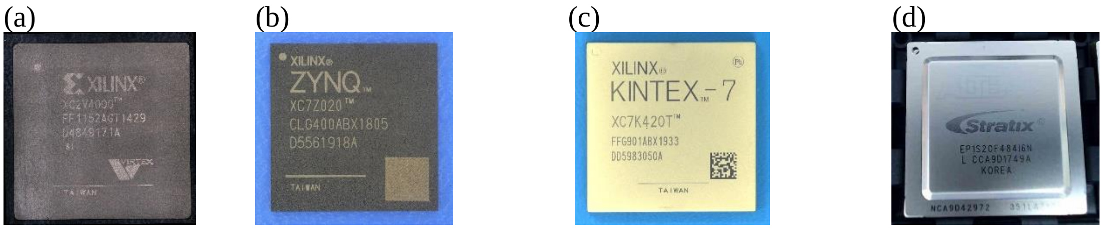


Figure 9: Photographs of FPGA parts. (a) re-marked (51) lid, (b) 2D bar code has been abrasively removed, (c) KINETX-7 package with 2D bar code (fake parts) and Stratix that passed visual inspection and all electrical tests but failed C-SAM).

For parts that fail visual inspection the package lids may be evaluated in an SEM (scanning electron microscope). This can be non-destructive whereby the lid and solder balls are evaluated for their texture and chemical composition. A case study involving the Xilinx Virtex-4 FPGA is included here to demonstrate how this method can identify counterfeit parts. First the parts are photographed and the markings, etc. studied to verify they are authentic. The two parts are shown below:

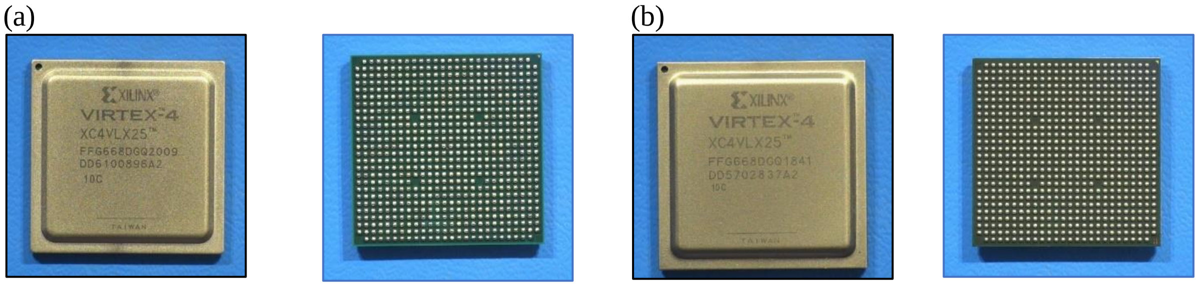


Figure 10: Xilinx Vertex-4 parts studied using the SEM via package lid (left) and solder ball (right) characterization. (a) Known-good and (b) suspect part.

The packages were then placed under vacuum on the SEM and the lid and solder ball topology and chemistry evaluated. Based on the morphology alone it was possible to identify the fake part as revealed by texture analysis – EDS (soft x-ray chemical identification) did not discriminate between the parts as they were made using the same chemical composition:

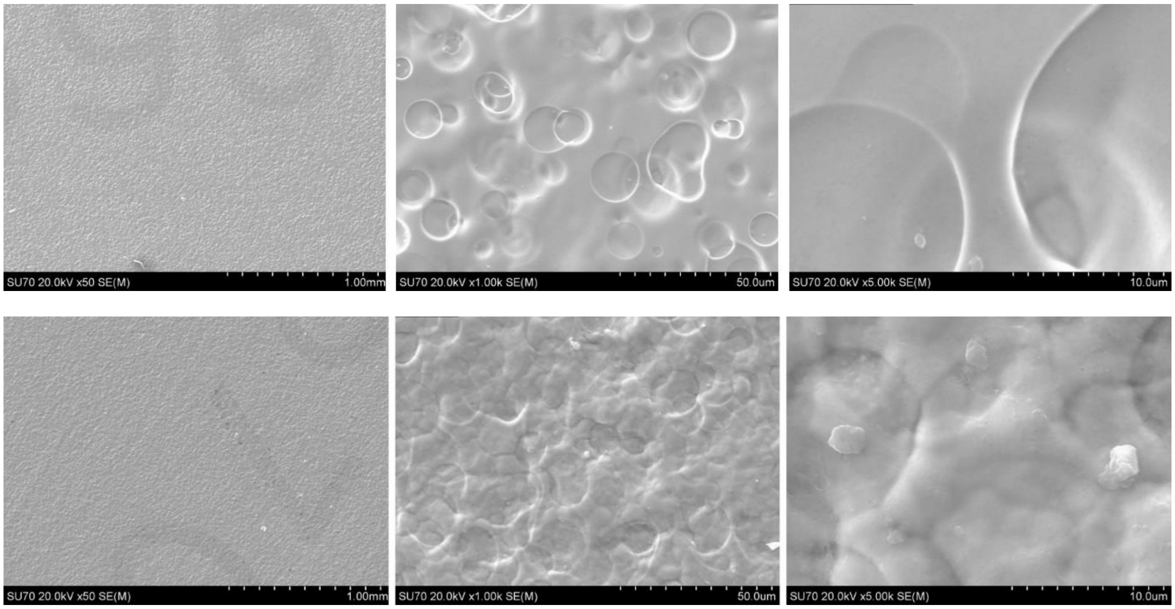

SU70 20.0kV x50 SE(M) 1.00mm
SU70 20.0kV x1.00k SE(M) 50.0um
SU70 20.0kV x5.00k SE(M) 10.0um
SU70 20.0kV x50 SE(M) 1.00mm
SU70 20.0kV x1.00k SE(M) 50.0um
SU70 20.0kV x5.00k SE(M) 10.0um

Figure 11: SEM micrographs of Xilinx Vertex-4 lid surface. The known good part (top) contains a smooth to touch morphology while the fake part (bottom) is rougher as confirmed by SEM analysis.

It is also possible to compare solder ball texture and chemistry using this method:

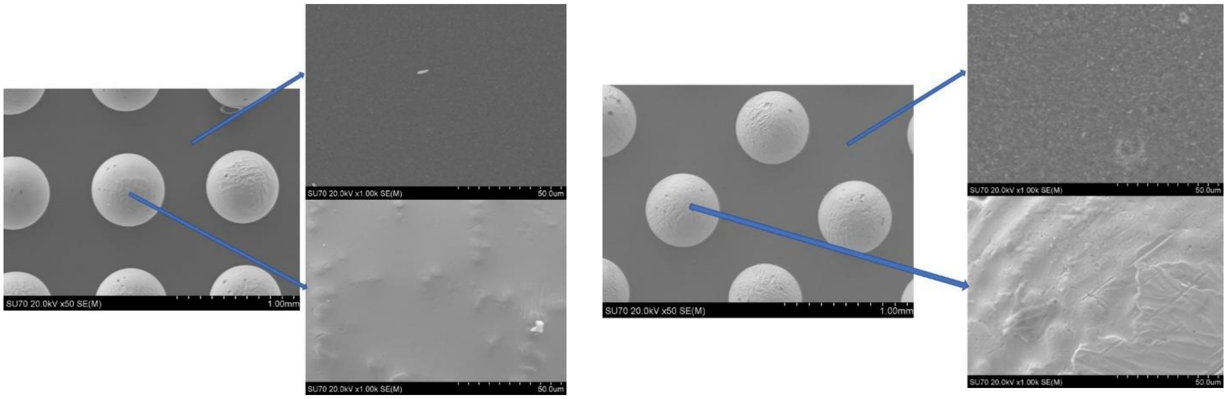


Figure 12: SEM micrographs of Xilinx Vertex-4 solder ball surface. The known good part (left) contains a smooth morphology while the fake part (right) is significantly rougher as confirmed by SEM analysis. Based on this result the suspect part was classified as counterfeit.

Following visual inspection, the parts were loaded into a Scanning Acoustic Microscope (C-SAM) for evaluation of the die-attach under the lid. Figure 2 below shows examples of this for the same parts listed above in Fig. 1

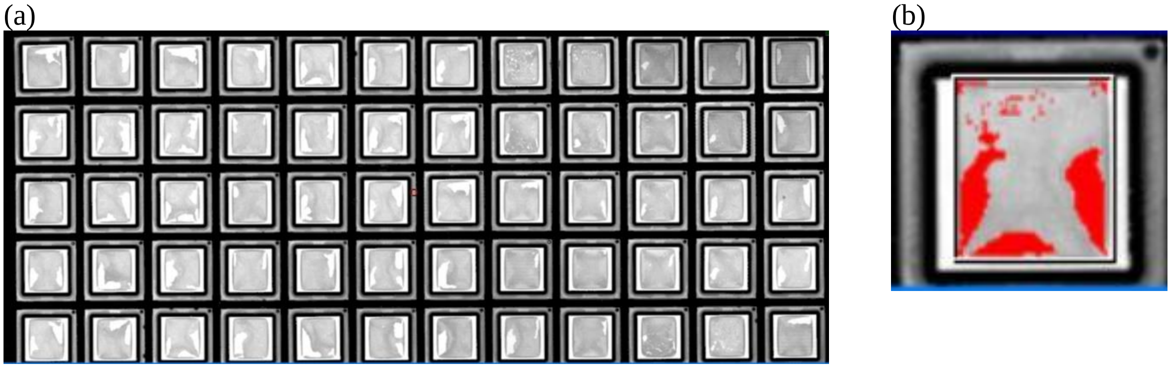


Figure 11: C-SAM data from Stratix part . (a) 5x12 chip tray showing the presence of voids for all devices tested. (b) higher magnification with enhanced color void delineation (red). Note that, in all cases, the package lid was removed and re-attached without proper thermal paste applied.

For component level testing, we use the boundary-scan register to access to each pin for the purpose of driving stimuli, capturing responses or both in the case of bi-directional pins. Also, if the optional IDCODE instruction and associated identification register is implemented, the IC manufacturers code, the part number and its revision will be checked. It is required that this infrastructure be operational before any other test will yield useful results.

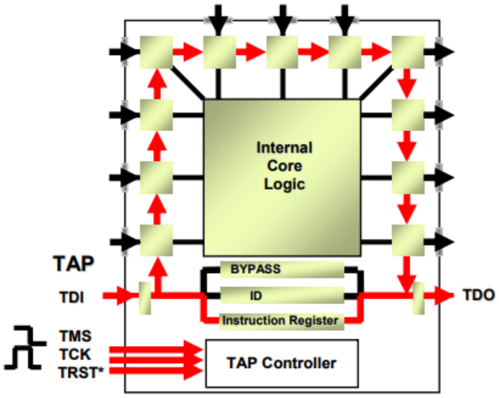
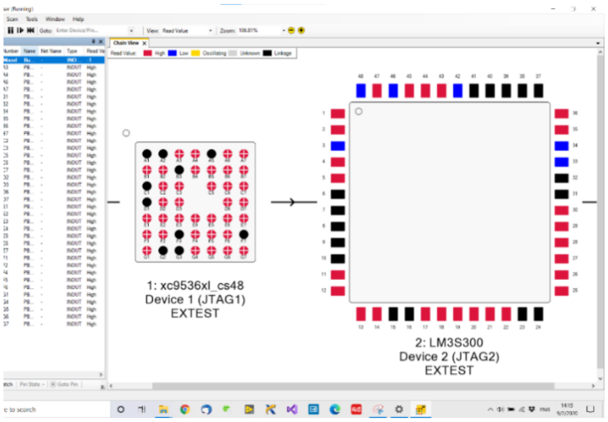
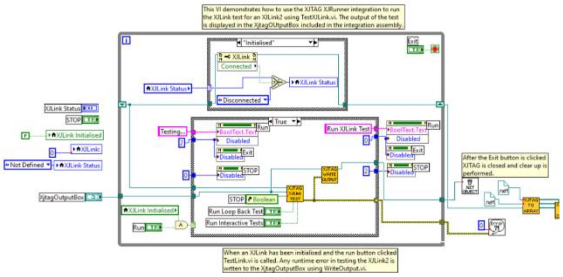


Figure 12: Component level boundary-scan to drive device each pin and verify device manufacturers ID code.





This VI demonstrates how to use the XJTAG XJRunner integration to run the XJLink test for an XJLink2 using TestXJLink.vi. The output of the test is displayed in the XjtagOUtputBox included in the integration assembly.

When an XJLink has been initialised and the run button clicked TestLink.vi is called. Any runtime error in testing the XJLink2 is wrtten to the XjtagOutputBox using WriteOutput.vi.

After the Exit button is clicked XJTAG is closed and clear up is performed.

Figure 13: Configured Device I/Os to verify Pins status. ***Figure 14:*** Lab-view based ATE system

The complex FPGA/MCU have thousands of pins in one chip, the traditional testing method is expensive, and time consuming for one single chip. Boundary-scan has proven itself as an invaluable tool in testing today's complex digital device. Boundary-scan enables a fast and inexpensive method to perform testing during environment stress screening with pin-level diagnosis upon failure. The firmware updates without disassembly required.

FPGA Delay Simulation and Speed Testing

To verify the speed of a particular FPGA chip, a design whose purpose is to act as a buffer is written up in an HDL, simulated in a development environment, like Xilinx ISE or Vivado, and the real-world implementation is compared with the simulation results. The buffer can be any number of logic gates that will create a significant amount of delay.

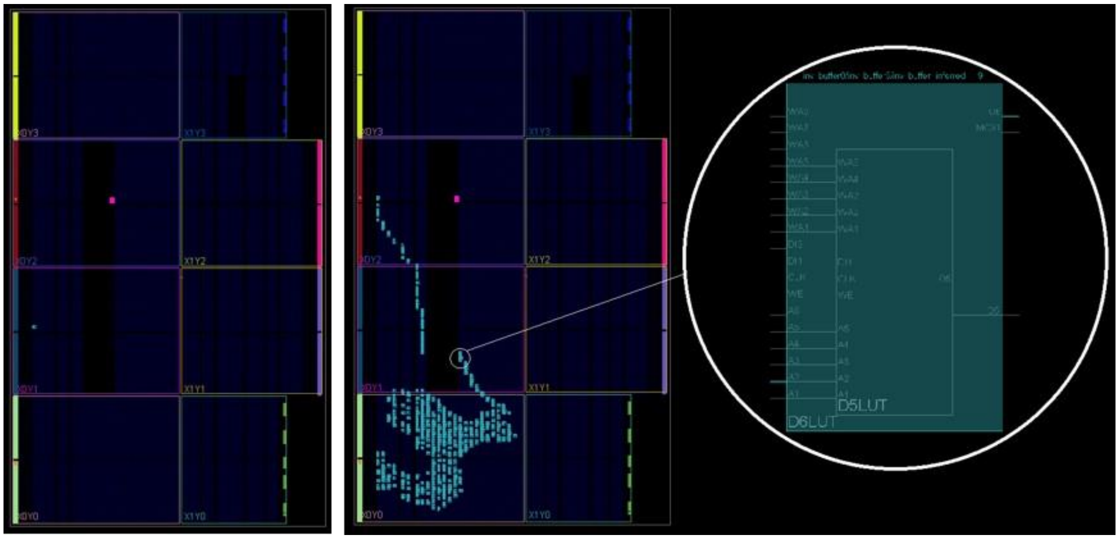


Figure 15: Artix-7 device usage without (left) vs. with (right) dont_touch attribute applied.

This testing method was experimented with on Virtex-4 devices (XC4VLX25-{, 11, 12}FFG668C), and the buffers used consisted of 50, 500, 1000, and 5000 inverters. The designs have an internal register/signal called “input” which is the input at the beginning of the inverter chain. An external clock signal is driven into one of the Virtex-4’s GC pins which connects to one of the device’s global clock buffers. After 20 clock cycles, the input register is inverted, and the output will change accordingly after the delay that results from the chain.

After running synthesis and implementation for 5000 inverters on a -12 Virtex-4, the synthesis report states around 0.535 ns delay for each LUT performing an inversion, so around 2675 ns / 2.675 μs delay from change in input to output. After place and route, the timing report states a 2060 ns / 2.06 μs delay but doesn’t list out the distributed delay between the LUTs.

The designs’ bitstreams were generated, the devices were programmed using the JTAG interface. The yielded results showed that the simulated and real delay are more similar at a lower number of logic gates.

Table 2

Simulated Delay (ns)				**Real Delay (ns)**			
# of Inverters	**-10**	**-11**	**-12**	**# of Inverters**	**-10**	**-11**	**-12**
50	43.703	37.517	33.32	**50**	42.2	43.76	43.56
500	299.623	254.052	223.076	**500**	217.36	217.36	205.64
1000	564.831	483.26	428.706	**1000**	410.36	415.64	396.36
5000	2692	2319	2060	**5000**	2049.56	2076.84	1967.2

Overall, all speed grades' real delay did not exceed their simulated delay at 500 inverters and up. Place-and-route in ISE may give the worst-case delay for simulation which results in the discrepancy at larger numbers of logic gates.

REFERENCES

[1] https://spectrum.ieee.org/semiconductors/processors/the-hidden-dangers-of-chopshop-electronics

[2] https://militaryembedded.com/comms/power-electronics/counterfeit-components-risky-business

[3] https://en.wikipedia.org/wiki/Field-programmable_gate_array

[4] Xilinx. *XST User Guide for Virtex-6, Spartan-6, and 7 Series Devices*, UG687 (v 14.5) (2013). Accessed: May 12, 2021. [Online]. Available: https://www.Xilinx.com/support/documentation/sw_manuals/Xilinx14_7/xst_v6s6.pdf, p.351

[5] Xilinx. *Vivado Design Suite User Guide: Synthesis*, UG901 (v 2012.2) (2012). Accessed: May 12, 2021. [Online]. Available: https://www.Xilinx.com/support/documentation/sw_manuals/Xilinx2012_2/ug901-vivado-synthesis.pdf, p.33

[6] "IEEE Draft Standard Test Access Port and Boundary Scan Architecture," in IEEE P1149.1/D2012.e27, September 2012, vol., no., pp.1-434, 24 Oct. 2012.

[7] Be Van Ngo, P. Law and A. Sparks, "Use of JTAG boundary-scan for testing electronic circuit boards and systems," 2008 IEEE ~~AUTOTESTCON, Salt Lake City, UT, 2008, pp. 17-22, doi: 10.11~~09/AUTEST.2008.4662576.