

Hidden Dangers: Understanding & Preventing the Counterfeiting of Semiconductor Products



Chetan Arvind Patil
Contributing Writer | EPDT

In the complex world of electronics, semiconductors are clearly essential. These components are at the heart of everything from smartphones to medical equipment - ensuring the smooth running of countless facets of our everyday lives. However, within this industry, there exists a significant threat - counterfeit semiconductor products. Counterfeiting costs the semiconductor industry huge amounts of money and represents substantial risks to safety and reliability too. According to the Semiconductor Industry Association (SIA), the financial impact of counterfeit components on US-based semiconductor companies alone is more than \$7.5 billion annually.

crucial when it comes to preventing the spread of counterfeit components.

One standard method is recycling old or discarded chips. Once acquired, these are then cleaned, re-marked and sold as new. This often leads to the presence of components that fail prematurely, thereby jeopardising any systems they are integrated into. Another method involves cloning, where counterfeiters illegally copy the design and functionality of genuine semiconductors. Cloned chips can be nearly indistinguishable from authentic ones, making detection

What is a counterfeit semiconductor product?

These are semiconductors that are fake or unauthorised replicas of genuine component parts. They can have a detrimental effect on the operational integrity of products they find their way into and often fail prematurely. Given the magnitude of such impacts, it is crucial that semiconductor supply chain stakeholders fully comprehend the severity of counterfeiting issues. Only then can the industry develop effective strategies to tackle this threat. These strategies should include enhancing detection technologies, improving supply chain transparency and fostering collaboration between industry leaders and government agencies. By addressing the root causes and strengthening preventive measures, all the companies can protect the integrity of semiconductor products and ensure continued technological advancement.

How counterfeiting occurs

Counterfeiting of semiconductor products occurs through various methods, including exploiting vulnerabilities in supply chains and manufacturing processes. Understanding these methods is

Type of Counterfeit	Description	Risks
Recycled components	Semiconductors are extracted from discarded electronic devices, cleaned, re-marked, then resold as new chips.	This process is unethical and dangerous, as components often fail prematurely.
Cloned chips	Involves illegally copying the design and functionality of genuine semiconductors - with counterfeit chips being almost identical to authentic ones.	Cloned chips often contain hidden vulnerabilities, leading to significant security risks.
Re-marked components	Lower-grade chips get re-marked to indicate higher specifications. For example, a commercial-grade component may be falsely labelled as a high-reliability or military-grade part.	This deception can lead to device failures in critical applications.
Over-produced or left over chips	Excess genuine products are manufactured (due to an order cancellation or other reasons). Left over chips are not disposed of correctly, with genuine parts thus going on the black market.	Unauthorised distribution bypasses quality controls, increasing risk of possible defects.
Forged documentation	Counterfeiters often provide forged documentation to support the authenticity of counterfeit products.	It becomes difficult for buyers to verify the legitimacy of the components, increasing the risk of incorporating counterfeit parts into critical systems.

Table 1: The various forms of semiconductor counterfeiting

extremely challenging. They will often contain concealed vulnerabilities that may compromise system security. These and other forms of counterfeiting are detailed in Table 1.

By being aware of these counterfeiting techniques, industry stakeholders can implement targeted strategies to safeguard their supply chains. These include enhancing traceability measures, adopting advanced authentication technologies, fostering closer collaboration between manufacturers/suppliers/regulatory bodies, etc. Such proactive steps are essential to protect semiconductor product integrity.

Preventing semiconductor counterfeiting

Avoiding counterfeit semiconductors infiltrating the supply chain is paramount for maintaining electronic devices' integrity and reliability. Effective strategies involve a combination of advanced detection technologies, rigorous procurement practices and adherence to industry standards. By implementing these measures, manufacturers can significantly reduce the possibility of counterfeit components appearing on their production lines. Prospective methods that semiconductor companies can apply to avoid counterfeiting of chips are shown in Table 2.

Method	Description	Advantages	Limitations
Visual and electrical testing	These tests are widely used in identifying counterfeit components.	Straightforward and relatively low-cost.	Counterfeiters have become sophisticated, and many can now successfully pass these tests.
Advanced detection techniques	These include embedding cryptographic identities, optical and electrical watermarks, plus applying unique chemical or microscopic markings to chip packages.	Provide a higher level of security and make counterfeiting more difficult.	Implementing these methods can be complex and costly.
3rd party testing	External organisations test/certify components to ensure authenticity.	Provides an additional layer of security and assurance for buyers.	Not foolproof; with effectiveness dependent on the rigour of the testing protocols used.
Cryptographic identities	Embedding unique cryptographic signatures in chips to verify their authenticity.	Offers high level security, making it very difficult for counterfeiters to replicate components.	Requires support and acceptance across the industry for widespread implementation. Raises cost and needs memory.
Optical and electrical watermarks	Using hidden patterns and circuits that can be stimulated under specific conditions to confirm authenticity.	Difficult for counterfeiters to replicate, providing a robust verification method.	Implementation can be complex and may require specialised equipment.
Chemical or microscopic markings	Applying hard-to-replicate chemical dyes or microscopic etchings to chip packages.	Provides a unique and secure way to identify genuine components.	Requires specialised equipment and processes for both application and verification.
Supply chain management	Implementing robust procurement practices, such as purchasing from authorised distributors and maintaining traceability throughout the supply chain.	Reduces risk of counterfeit components entering the supply chain and ensures accountability.	Can be resource-intensive to maintain and requires collaboration across entire supply chain.
Government regulations	Enforcing strict procurement practices and supporting anti-counterfeiting standards.	Helps standardise practices across the industry and provides legal backing for anti-counterfeiting efforts.	Requires cooperation from multiple stakeholders and can be slow to implement.

Table 2: Methods for combatting counterfeiting

In addition to these preventative steps, collaboration between industry stakeholders, governments and law enforcement agencies is essential. Through shared knowledge, resources and continuous improvement of anti-counterfeiting techniques, the semiconductor industry can protect its products in the long term

Industry and government actions

The semiconductor industry has implemented several key initiatives to address the counterfeiting problem. These include awareness campaigns - through educational programs and publications informing manufacturers and consumers about the threat of counterfeit components and the detection methods that can be used to identify them.

The industry also collaborates with customs and police departments to train officials and conduct joint operations - resulting in significant seizures and arrests. Additionally, the development of international standards and best practices (such as JEDEC's JESD243) help guide manufacturers in preventing and detecting counterfeit components. Technological innovations, including advanced anti-counterfeiting technologies and sophisticated testing tools, further enhance the industry's ability to verify semiconductor authenticity.

Governments worldwide also play a crucial role in mitigating the semiconductor counterfeit issue. This can be via enforcing strict procurement practices, supporting anti-counterfeiting standards and strengthening customs/border protection. Regulatory frameworks and compliance programs can ensure that companies adhere to anti-counterfeiting standards, while international cooperation will help with the detection and seizure of counterfeit shipments.

Legislation specifically targeting counterfeit semiconductor production and distribution, along with stringent penalties, will serve as a deterrent to counterfeiters. Public-private partnerships and government-funded research

initiatives will foster collaboration and innovation, driving adoption of cutting-edge solutions to combat counterfeiting.

The future course

Proliferation of counterfeit semiconductors is a growing concern. These items not only cause substantial financial losses, but may also endanger lives by compromising the integrity of critical systems. As evidenced by numerous real-world incidents, the consequences of using counterfeit semiconductors can be catastrophic. Combating counterfeiting requires a concerted effort from all stakeholders involved. The industry must continue to innovate and implement advanced detection/prevention methods, such as cryptographic identities, optical/electrical watermarks and stringent supply chain management practices. Additionally, governments must enforce strict regulations and work closely with industry players to develop and uphold standards preventing counterfeit component proliferation.

Ejection seat failure in US Air Force aircraft	In 2020, failure of the ejection seat sequencer in a military aircraft, which was found to contain several counterfeit components, had a tragic outcome. It resulted in the death of the aircraft's pilot.
AED malfunction	An automated external defibrillator (AED) unit designed to save lives in medical emergencies experienced a critical failure, due to inclusion of a counterfeit semiconductor component. This caused an over-voltage condition, rendering the AED inoperative when it was needed.
Airport landing light system breakdown	The premature failure of counterfeit semiconductor component resulted in a cessation in the power supply operation of an airport landing light system required for safe aircraft landings.
US military helicopter incident	In 2015, a trader was found to have provided falsely marked computer chips to the US military for use in helicopters. Initially produced for commercial applications, these chips were fraudulently relabelled as higher-grade devices. Consequently, the trader was given a prison sentence.
Vacuum cleaner fire	A short-circuit led to a residential vacuum cleaner catching fire, thus placing household residents in danger. This happened because there was a counterfeit semiconductor component in its control circuitry.

Table 3: Examples of high-profile incidents resulting from counterfeit semiconductor products

In conclusion, protecting semiconductor supply chains from counterfeit products is essential for ensuring electronic devices' performance, safety and reliability. By

raising awareness, implementing robust anti-counterfeiting measures and fostering collaboration between industry and government, the risks involved can be lessened.



Build on your proficiency

Quick tips, tools and articles
for purchasing professionals

mou.sr/purchasing-resources