White paper di Rochester Electronics

Combattere il rischio di contraffazione dei semiconduttori

Perché acquistare da fonti pienamente autorizzate

Rochester Electronics LLC • Sede centrale globale

16 Malcolm Hoyt Drive • Newburyport, MA 01950 USA

+1.978.462.9332 / www.rocelec.it

Sintesi

I semiconduttori contraffatti rappresentano una minaccia sempre in agguato per la sicurezza e l'affidabilità delle apparecchiature elettroniche, soprattutto nei periodi di distribuzione o per i pezzi fuori produzione.
L'approvvigionamento di componenti tramite canali indipendenti e non autorizzati per avere forniture o prezzi più vantaggiosi introduce il rischio di contraffazioni e di potenziali danni alle apparecchiature finali dei clienti, costituisce una minaccia per la sicurezza degli utenti finali e mette a repentaglio la reputazione del cliente. È stato ripetutamente dimostrato che l'uso di dispositivi contraffatti ha portato a pesanti sanzioni per le aziende e i dipendenti responsabili.

I rischi associati alle contraffazioni non si possono eliminare del tutto tramite lo svolgimento di ulteriori test, e i processi di controllo di parti terze non possono garantire la qualità. Le gravi limitazioni dei processi di terze parti si ripercuotono potenzialmente sul cliente in termini di scarti, rilavorazioni, inaffidabilità in servizio e controversie legali.

Tuttavia, i rischi di contraffazione dei semiconduttori possono essere eliminati seguendo i principi fondamentali di approvvigionamento. Esistono partner pienamente autorizzati che supportano le carenze attive e la necessità di semiconduttori obsoleti, in alcuni casi anche 30 anni dopo la loro dismissione originaria. I partner autorizzati sono la prima linea di difesa contro i contraffattori.

Che cos'è un prodotto contraffatto?

Le contraffazioni si presentano in molte forme. La definizione più elementare di prodotto contraffatto è “un dispositivo di imitazione destinato a essere venduto in modo fraudolento o fuorviante come autentico, a scopo di lucro". In tempi di scarsità di forniture o quando l'obsolescenza dei componenti ne limita la disponibilità, la prevalenza di dispositivi contraffatti aumenta con l'opportunità di ottenere maggiori profitti.

Con l’aumentare della consapevolezza del mercato, aumenta anche il livello di sofisticazione dei contraffattori. Siamo andati ben oltre ai loghi inesatti dei produttori e ai package IC senza die all'interno, rilevati dalle ispezioni visive eseguite in conformità alla norma AS6081. Oggigiorno i contraffattori possono imitare tutti gli elementi del processo di produzione e duplicare prove che ne attestano falsamente l'autenticità.

Le contraffazioni includono:

- Prodotti non funzionali o di scarto che vengono rimarchiati come conformi e rimessi in vendita.
- Prodotti funzionali di qualità inferiore acquistati dal contraffattore, che vengono rimarchiati e rimessi in vendita come prodotti di qualità standard a un prezzo maggiorato.
- Componenti riciclati e recuperati che vengono rivenduti come componenti nuovi.
- Documentazione di collaudo e di tracciabilità falsificata che occulta le specifiche o la storia reale di un componente.

Come nascono le contraffazioni?

C'è un netto contrasto tra la produzione di semiconduttori autentici e quella di semiconduttori contraffatti. Le aziende produttrici di semiconduttori spendono miliardi di dollari all'anno per sviluppare, produrre, testare e supportare prodotti che funzionino per anni ai massimi livelli di qualità e affidabilità. Le contraffazioni sono spesso ottenute dal recupero di rifiuti elettronici con processi grossolani e scarsamente controllati che danno origine a semiconduttori con tassi di guasto molto più elevati

rispetto ai prodotti originali. Alcuni semiconduttori contraffatti si guastano immediatamente al momento del test elettrico o del primo utilizzo, mentre altri si guastano dopo giorni, mesi o anni di applicazione sul campo.

Conseguenze per clienti e fornitori

"Gli esperti hanno stimato che il 15% di tutti i semiconduttori di ricambio acquistati dal Pentagono sono contraffatti. Complessivamente, stimiamo che la contraffazione costi alle aziende di semiconduttori statunitensi più di 7,5 miliardi di dollari all'anno, il che si traduce nella perdita di quasi 11 mila posti di lavoro". *Presidente della SIA Brian Toohey, Audizione SASC di novembre 2011 (1)*

Per quanto sconvolgenti possano sembrare queste cifre, le contraffazioni rappresentano una minaccia sempre incombente, anche in tempi di eccesso di offerta sul mercato. Le crisi di approvvigionamento dei semiconduttori, come quella del 2020, interessano tutti i clienti in ogni segmento di mercato, portando a strategie di approvvigionamento rischiose. Vedendo l'opportunità, i contraffattori hanno cercato di colmare le lacune del mercato.

Non è possibile conoscere il numero reale di contraffazioni. Sebbene esistano strumenti di autodenuncia, come il Government-Industry Data Exchange Program (GIDEP), i clienti non sono incentivati ad ammettere le irregolarità negli acquisti. Per tutelare i clienti, è più sicuro presumere che tutti i semiconduttori acquistati al di fuori dei canali autorizzati siano potenziali contraffazioni. Ogni contraffazione comporta dei rischi per l'utente.

- ***Rimarchiatura*:** Nel caso di prodotti rimarchiati, il procedimento di reincisione delle marcature esterne originali con prodotti chimici aggressivi o smerigliatrici meccaniche può provocare danni ai collegamenti interni o al substrato. I residui chimici della procedura di pulizia potrebbero infiltrarsi lentamente nei dispositivi rimarchiati e contaminarli, causando guasti al bond pad o al bond wire. La stampa del nuovo marchio è eccezionalmente ingannevole e potrebbe non essere identificata durante il test visivo AS6081. I test di base sul prodotto previsti dalla norma AS6171 non individueranno le differenze di prestazioni per le parti rimarchiate come prodotti con specifiche più avanzate. Inoltre, non saranno individuati i componenti che non superano di poco i test dei produttori di componenti originali (OCM), ma che vengono recuperati illegalmente.

- ***Processo di recupero*:** Il processo di recupero dei semiconduttori usati dai vecchi PCB può anche provocare danni meccanici e termici catastrofici. Il recupero dei circuiti integrati dai PCB è la fase finale di un lungo processo che coinvolge l'uso pregresso e un ambiente di stoccaggio non regolamentato. L'esposizione a umidità eccessiva, acqua o salsedine è molto comune. Il processo finale di ri-placcatura e riformazione dei

- conduttori introduce ulteriori rischi ESD, termici e meccanici. Questo processo può dare origine a prodotti usati superficialmente autentici e di dubbia affidabilità.

- ***Scorte eccedenti identificabili*:** La tracciabilità non autorizzata non fornisce alcuna garanzia sulla qualità, sull'affidabilità o sulla conformità di un prodotto. Spesso considerate come un'opzione priva di rischi, le condizioni di stoccaggio e manipolazione non autorizzate dei semiconduttori non sono controllate. I danni da ESD e le infiltrazioni di umidità sono altrettanto disastrose per l'affidabilità dei semiconduttori autentici in eccedenza. In tempi di approvvigionamenti spregiudicati, lo spazio non autorizzato offre una copertura perfetta per camuffare l'origine delle forniture dei componenti, aumentando così il rischio di contraffazione.

Le conseguenze per il cliente nel consentire l'ingresso nella catena di fornitura di prodotti non conformi alle norme comprendono:

- Riduzione delle rese di produzione e aumento della rilavorazione.
- Introduzione di malware o di modifiche che consentono l'accesso al software da parte di terzi.
- Aumento dei guasti in servizio e riduzione dell'affidabilità.
- Aumento dei rischi e della passività finanziaria associati a malfunzionamenti catastrofici del sistema.
- Potenziale danno alla reputazione.

I clienti non sono gli unici ad essere a rischio, e anche gli OCM sono vittime della perdita di fatturato e, cosa più grave, del danno alla reputazione.

Come proteggersi da questi rischi

L'approccio per minimizzare il rischio di contraffazione è basato su tre elementi. In questo caso, entrano in gioco le misure di controllo governative, le pratiche in uso dai fornitori e la pianificazione dei clienti.

Misure di controllo governative

Episodi di contraffazione di semiconduttori di alto profilo in applicazioni commerciali e militari hanno spinto alla promulgazione del National Defense Authorization Act (NDAA) nel 2012 *(2)*. I guasti ai componenti hanno dimostrato come i dispositivi contraffatti possano compromettere la sicurezza nazionale e provocare lesioni, infortuni o decessi. Alcuni estratti dell'NDAA indicano l'intenzione del governo statunitense di attribuire ai produttori la responsabilità del controllo dei componenti contraffatti:

a) *Gli appaltatori che forniscono parti elettroniche o prodotti contenenti parti elettroniche hanno la responsabilità di individuare e prevenire l'uso o l'introduzione di parti elettroniche contraffatte o "sospette di contraffazione" nei loro prodotti. Devono inoltre intraprendere azioni correttive o rilavorazioni, se necessario, per far fronte a tale utilizzo o introduzione di tali parti.*

b) *I costi delle parti elettroniche contraffatte e delle parti elettroniche "sospette di contraffazione" non sono costi ammissibili nell'ambito degli appalti pubblici. Non sono inoltre consentite le rilavorazioni o le azioni correttive necessarie per rimediare all'uso o introduzione di tali parti.*

Sebbene questa legislazione faccia luce sulla questione e renda i produttori più responsabili del controllo delle contraffazioni dei loro prodotti, non rende necessariamente più facile per l'utente finale recuperare i costi e rimediare ai danni derivanti dalle merci contraffatte.

Secondo un rapporto di eeNews Europe del 2017, nel 2016 l'Associazione europea dell'industria dei semiconduttori ha riferito che più di un milione di semiconduttori contraffatti sono stati sequestrati da un'operazione doganale congiunta. L'Ufficio europeo per la lotta antifrode e le autorità doganali di 12 Stati membri dell'UE hanno collaborato con le dogane olandesi per coordinare un'operazione che ha intercettato parti spedite per posta dalla Cina e da Hong Kong e dirette in Europa. Tuttavia, tutti gli interessati sono consapevoli che operazioni come queste sfiorano solo la superficie di questo enorme flusso illegale. *(3)*

Attuali misure di controllo del produttore del chip originale

Attualmente il settore si avvale di diverse iniziative e metodi per la lotta alla contraffazione. Educare le aziende e gli utenti in merito ai rischi che si corrono riduce le probabilità di danni. Il settore collabora inoltre strettamente con l'Agenzia delle dogane e dei monopoli (Customs and Border Protection) degli USA e con le altre forze dell'ordine per stroncare le catene di approvvigionamento dei prodotti contraffatti e perseguire i soggetti coinvolti. Infine, il settore sta aumentando le misure di sicurezza e sviluppando standard internazionali di garanzia della catena di approvvigionamento.

Sebbene gli OCM non siano responsabili delle contraffazioni dei loro prodotti, molti OCM continuano a vendere componenti in eccesso tramite canali non controllati, non affidabili e non autorizzati. Ciò contribuisce a creare incertezza sul prodotto, a far sì che la qualità dei componenti sia potenzialmente scarsa a valle e a danneggiare il marchio in generale. Il controllo delle vendite autorizzate di semiconduttori attivi e dismessi in eccedenza è essenziale per distinguere i prodotti di qualità garantita da quelli contraffatti. Negli ultimi anni, i produttori di semiconduttori, come Texas Instruments, hanno portato avanti questa iniziativa, interrompendo le vendite autorizzate di componenti a fonti non autorizzate.

Responsabilità del cliente

I semiconduttori contraffatti sono talmente diffusi in tutta la catena di fornitura che la regolamentazione e l'applicazione delle norme si sono dimostrate inefficaci per arginare la loro distribuzione. Le politiche di acquisto e i controlli dei clienti sono la linea di difesa migliore e più attendibile.

Le politiche volte a evitare prodotti contraffatti e di qualità inferiore includono:

- Acquistare solo prodotti dell'OCM o dei suoi distributori autorizzati e produttori con licenza.

- Acquistare da un fornitore autorizzato che offra una garanzia completa su prestazioni, qualità e affidabilità.
- Assicurarsi che il fornitore sia conforme allo standard industriale AS6496 per la manipolazione e lo stoccaggio, e che sia dotato di certificazioni di qualità appropriate per la vendita del componente finale.
- Impiegare un processo di autovalutazione, che analizzi gli acquisti di qualità sospetta o scarsa, prima di mettere in atto rigide azioni correttive.
- Collaborare con un produttore after-market autorizzato.
- Scegliere un programma di test che utilizzi il programma di test dell'OCM originale.
- Ricercare i distributori di componenti autorizzati visitando: https://www.eciaauthorized.com/it.

Il ruolo dei test nell'identificazione delle contraffazioni.

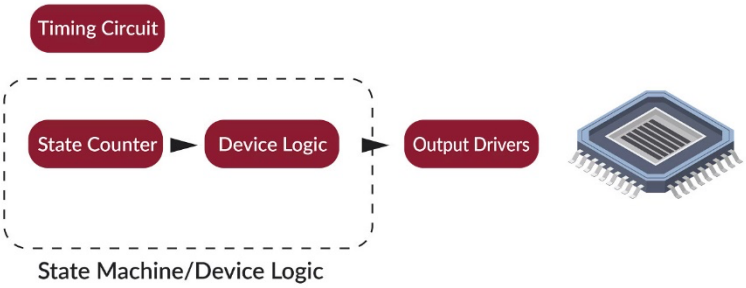
L'ispezione visiva in conformità alla norma AS6081 e le prove elettriche AS6171 sono i due metodi più comuni per l'identificazione di contraffazioni, ma entrambi possono essere inaffidabili per identificare i prodotti contraffatti per via dei seguenti motivi:

- È improbabile che la documentazione e l'ispezione visiva siano in grado di identificare dispositivi contraffatti da professionisti. I documenti e i certificati di tracciabilità sono falsificati regolarmente per facilitare tali truffe.
- Le ispezioni a raggi X potrebbero non essere in grado di rilevare dispositivi fraudolentemente sottoposti a upscreening, dispositivi riutilizzati e recuperati o dispositivi recuperati che non hanno superato i collaudi.
- I test di continuità o funzionali di base non consentono di identificare i dispositivi fraudolentemente sottoposti a upscreening o recuperati e riutilizzati.
- Test funzionali di terze parti (prevalentemente incentrati sugli attributi della scheda tecnica). Le schede tecniche contengono solo un sottoinsieme delle funzionalità testate dall'OCM, e potrebbero non essere testate sull'intero intervallo di temperatura.

Un altro problema dei test di "autenticità" è che non è sempre possibile testare ogni componente di una fornitura per ragioni di tempo e costo. In molti casi, i contraffattori inseriscono strategicamente i componenti funzionali all'inizio e alla fine delle bobine e dei tubi, ovvero in posizioni in cui è più probabile che vengano testati, per superare il test di autenticità.

Il miglior programma di test è quello creato dall'OCM. Ulteriori test condotti da terze parti non saranno altrettanto rigorosi e completi. La loro affidabilità è discutibile. Quando si esegue il test funzionale di un dispositivo, la copertura dei guasti è fondamentale. Senza una copertura del 100% degli errori di test, il dispositivo può presentare guasti residui. Con guasti residui sono intesi dispositivi che contengono difetti ma che superano i test.

Esempio di test funzionale di base: Semplice controllore del traffico:



Functional Truth Table												
State	North			East			South			West		
Count	Red	Yellow	Green	Red	Yellow	Green	Red	Yellow	Green	Red	Yellow	Green
1	On	Off	S-ON	Off	Off	On	On	Off	Off	Off	Off	On
2	On	Off	Off	Off	On	Off	On	Off	Off	Off	On	Off
3	Off	Off	On	On	Off	Off	Off	Off	On	On	Off	Off
4	Off	On	Off	On	Off	Off	Off	On	Off	On	Off	Off

Se la condizione di blocco di cui sopra non viene testata, si ha una copertura dei guasti del 98,96%. È un valore accettabile per la tua applicazione di importanza critica?

Un test efficace richiede un'elevata copertura dei guasti e una modellizzazione accurata degli stessi. Il test dell'MCU più elementare, eseguito dall'OCM, comprende 100 mila ore di sviluppo. L'AS6171 richiede test più approfonditi per i pezzi acquistati da distributori indipendenti, ma questi test coprono solo una minima parte dei parametri del test OCM.

L'unica garanzia al 100% che un dispositivo funzioni secondo le specifiche è quella di testarlo utilizzando le procedure di test dell'OCM.

Un esempio di contraffazione

Nel 2012, un cliente europeo produttore di sistemi di comunicazione militare, con 1.000 sistemi sul campo in tutti i servizi terrestri, marittimi e aerei, ha iniziato a registrare un numero rapidamente crescente di richieste di restituzione sul campo.

Dopo aver analizzato il problema, hanno identificato che la causa principale era un componente comune: un prodotto che era stato classificato come EOL (End Of Life, fine vita) nel 2002, ma che aveva continuato a essere acquistato da fonti non autorizzate fino all'insorgere dei malfunzionamenti. Tutte le scorte non autorizzate acquistate dopo l'EOL sono state sottoposte a test visivi ed elettrici e non avevano evidenziato guasti.

L'ispezione a raggi X dei componenti restituiti ha evidenziato la corrosione dei bond pad e alcuni bond wire completamente guasti.

Ulteriori analisi spettrali hanno identificato un'anomalia del cloro come catalizzatore della corrosione. Si è concluso che il cloro si è infiltrato nel componente durante il processo di recupero e pulizia. La migrazione del cloro all'interno del package di plastica, sui pad del

substrato e sul silicio ha impiegato da 4 a 5 anni. Una volta infiltrato, si sono verificati guasti immediati ai bond wire e alle apparecchiature.

È stato accertato che i dispositivi a semiconduttore erano prodotti recuperati, rimarchiati professionalmente e rivenduti come "nuovi" dopo la data EOL. L'unico modo per affrontare il deterioramento dei record in servizio è stato quello di avviare un costoso programma di sostituzione preventiva dei componenti per l'intera linea di prodotti.

Conclusione

I semiconduttori sono il fulcro dei sistemi elettronici utilizzati nei mercati ad alta affidabilità come quello industriale, dei trasporti, militare, medico, energetico, dell'aviazione civile, automobilistico e delle telecomunicazioni. I prodotti contraffatti e quelli di qualità inferiore agli standard introducono gravi rischi per la salute, la sicurezza e l'incolumità della popolazione a livello globale.

È diffusa l'idea erronea che, una volta che il produttore originale interrompe la produzione di un componente, le fonti non autorizzate o del mercato grigio siano l'unica soluzione. L'acquisto privo di rischi da un fornitore aftermarket autorizzato dovrebbe essere sempre la prima scelta. Gli OCM non offrono garanzie per i prodotti acquistati tramite canali non autorizzati. Molti vietano esplicitamente la vendita di componenti a fonti non autorizzate.

I distributori di semiconduttori completamente autorizzati, come Rochester Electronics, sono conformi allo standard aerospaziale SAE, AS6496. In poche parole, sono autorizzati dall'OCM a fornire prodotti tracciabili e garantiti, senza che siano necessari test di qualità o di affidabilità, perché i componenti provengono esclusivamente dall'OCM.

È possibile che fornitori non pienamente autorizzati si presentino sul mercato come conformi alla norma AS6171/4. Ciò indica che seguono ispezioni e procedure di test standardizzate, ma potrebbero avere requisiti minimi di formazione e certificazione per individuare componenti sospetti o contraffatti. Se viene eseguito il test AS6171, significa che il prodotto non viene testato secondo il programma di test OCM originale. I programmi di test OCM si spingono ben oltre i parametri della scheda tecnica e hanno lo scopo di filtrare i prodotti per evitare guasti anche se le unità vendute sono milioni. I test AS6171 non sono equivalenti ai test OCM.

Lo strumento per eccellenza utilizzato nella lotta ai prodotti contraffatti è l'acquisto di dispositivi a semiconduttore da fonti pienamente autorizzate.

Risorse e letture supplementari:

1. Winning the Battle Against Counterfeit Semiconductor Products, Semiconductor Industry Association, 2013 https://www.semiconductors.org/wp-content/uploads/2018/06/SIA-Anti-Counterfeiting-Whitepaper-1.pdf

2. *Ufficio europeo per la lotta antifrode, Combattere una crescente minaccia globale - Prodotti contraffatti a semiconduttori, dicembre 2022 - https://anti-fraud.ec.europa.eu/media-corner/news/combatting-growing-global-threat-counterfeit-semiconductor-products-2022-12-14_en?prefLang=it&etrans=it*

3. "Operation Wafers": over one million counterfeit semiconductors... (eenewseurope.com) 2017

4. *Commissione per i servizi armati del Senato degli Stati Uniti, Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts, maggio 2012 - https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts*

5. *Biblioteca del Congresso, U.S. Intellectual Property and Counterfeit Goods— Landscape Review of Existing/Emerging Research, A Report Prepared by the Federal Research Division, Library of Congress, Under an Interagency Agreement with the U.S. Patent and Trademark Office, U.S. Department of Commerce, febbraio 2020 https://www.uspto.gov/sites/default/files/documents/USPTO-Counterfeit.pdf*

6. *OECD/EUIPO (2022), Dangerous Fakes: Trade in Counterfeit Goods that Pose Health, Safety and Environmental Risks, Illicit Trade, OECD Publishing, Paris, https://www.oecd-ilibrary.org/governance/dangerous-fakes_117e352b-en.*

7. *https://www.airforcetimes.com/news/your-air-force/2022/09/13/an-f-16-pilot-died-when-his-ejection-seat-failed-was-it-counterfeit/*

8. *Rapporto del Consiglio mondiale dei semiconduttori, giugno 2021 https://www.semiconductorcouncil.org/wp-content/uploads/2021/10/ACTF_WSC-2021-Paper-on-Counterfeit-Semiconductors-and-the-Online.pdf*

9. *Combating Counterfeit Components in the DoD Supply Chain – DSIAC*