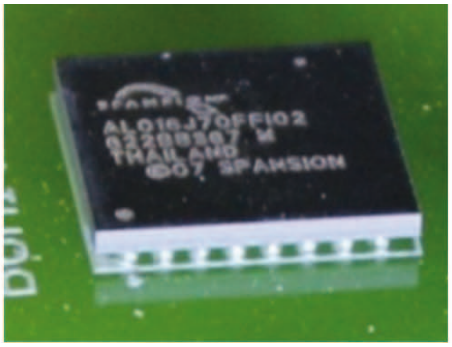
Erkennung von Hardware-Manipulationen durch Lötzinnanalyse

Die IT-Sicherheit einer elektronischen Baugruppe hängt auch maßgeblich von deren Hardware ab. Ist ein Angreifer in der Lage, hier unbemerkte Änderungen vor der Auslieferung durchzuführen, kann er sich dadurch einen dauerhaften Zugriff auf die internen Abläufe der Baugruppe beschaffen. Im Folgenden werden die Ergebnisse einer Studie der HTV GmbH vorgestellt.



Diese Studie wurde für das Bundesamt für Sicherheit in der Informationstechnik durchgeführt [1] und verfolgte das Ziel, zu klären, welche Unterschiede reparierte bzw. manipulierte Baugruppen nach einem sogenannten Rework zeigen, welche Untersuchungsverfahren dafür eingesetzt werden können und welche Verfahren die besten Analyseergebnisse erzielen. Die Analyse erfolgte zum einen an Testleiterplatten und zum anderen an Leiterplatten von realen Mobiltelefonen.

Analyse von Testleiterplatten

Um die Änderungen an den Lötstellen detailliert beobachten und analysieren zu können, wurden in einem ersten Schritt Testleiterplatten mit SOP-, BGA- und QFN-Bauteilen (s. Aufmacher, von links) bestückt und deren Zustand, im Weiteren als Original bezeichnet, erfasst. Die verwendeten Rework-Systeme: Ersa HR 600/2 (Rework A) und Finetech Fineplacer Core (Rework B). Danach erfolgte der Vergleich der Bereiche mit und ohne Rework auf den manipulierten Testleiterplatten mit dem Originalzustand.

- **Übersicht zu den Testleiterplatten**

Die einzelnen Testleiterplatten (LP) stellen einen Nutzen von Sub-Leiterplatten mit Lötflächen für jeweils sechs Bauteile (BT) mit den Gehäusetypen SOP, QFN und BGA dar. Die Sub-LP können bei Bedarf leicht aus der Testleiterplatte herausgetrennt werden (Bild 1).

Da LP mit BGA-Bauteilen standardmäßig ENIG-Lötoberflächen (Electroless Nickel Immersion Gold) aufweisen, erhielten auch die Test-LP ein ENIG-Finish. Die manipulierten Sub-LP sind für die spätere Wiedererkennung mit (m) gekennzeichnet. J-BGA1(m) wäre dann der erste BGA, der manipuliert wird auf der Test-LP mit dem Buchstaben J.

- **Übersicht zu den Arbeitsschritten**

Zur Manipulation wurden die folgenden Änderungen an den Bauteilen auf den Test-LP durchgeführt.

SOP: Pro LP drei BT ablöten, LP reinigen, neues BT in Lotpaste dippen oder LP bedrucken und BT mit Anlage oder mit der Hand einlöten

BGA: Pro LP drei BT ablöten, LP reinigen, neues BT oder altes BT mit

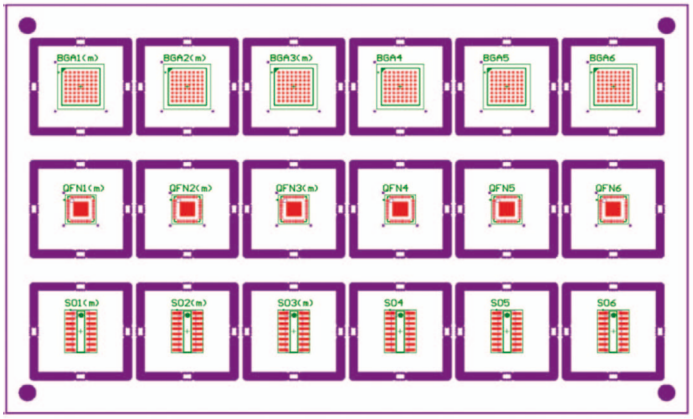


Bild 1: Test-LP mit Sub-Leiterplatten zum leichten Heraustrennen einzelner Regionen

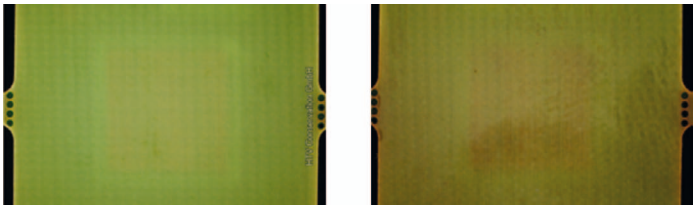


Bild 2: Verfärbte LP-Rückseite, links Original, rechts nach dem Rework

Halbleiter-Test & Vertriebs-GmbH
info@htv-gmbh.de
www.htv-gmbh.de

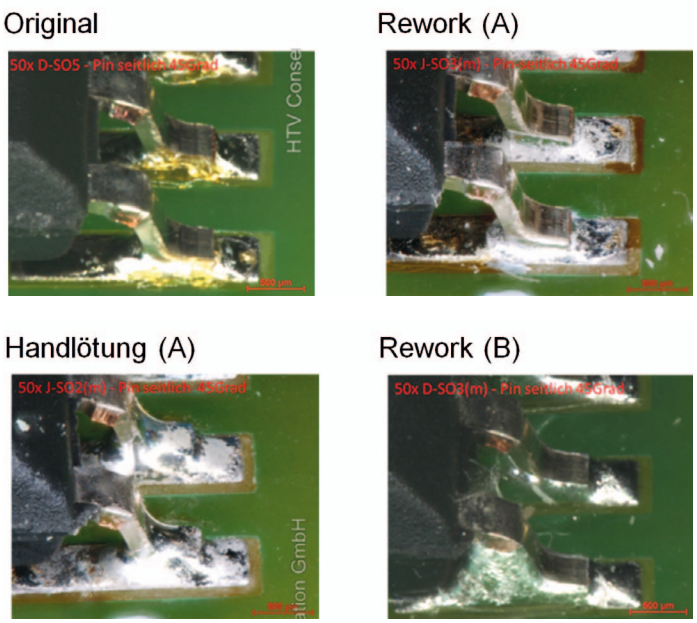


Bild 3: Visuelle Analyse der SOP-Lötstellen

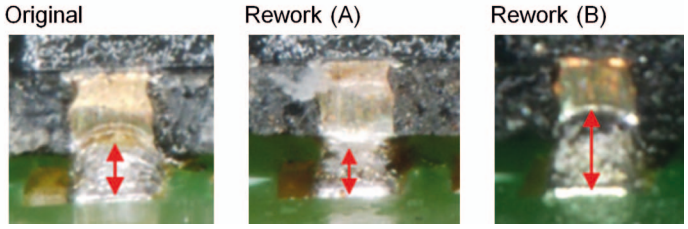


Bild 4: Erkennbare Unterschiede bei der Lotmenge bei den QFN-Bauteilen

Reballing in Flussmittel dippen und BT mit Anlage einlöten

QFN: Pro LP drei BT ablöten, LP reinigen, neues BT mit Lotpaste bedrucken und BT mit Anlage einlöten

- **Untersuchungsergebnisse visuell/mikroskopisch**

Die LP weisen bei beiden Herstellern nach dem Rework dunkle Verfärbung und teilweise auch mechanische Verformungen auf (Bild 2).

Bei den Pins der SOP-BT zeigen sich sowohl bei der Handlötung als auch bei Rework (B) ein auffälliger Unterschied in der Lotmenge. Beim Handlöten gelangte Lötzinn auf die Oberseite der Pins und bei Rework (B) war aufgrund zu großer Öffnungen in der Lotpastenschablone zu viel Lötzinn auf die Leiterplatte vor dem Lötprozess aufgetragen worden (Bild 3). Tabelle 1 informiert zur Lotmenge.

Die BGAs zeigen eine Verfärbung der Balls, falls zusätzliches Flussmittel (z.B. IF8300) vor dem Lötprozess aufgetragen wird. Wenn die BT hingegen nur in eine Schale mit Flussmittel gedippt werden, besteht kein deutlicher visueller Unterschied zwischen den manipulierten BGA-Balls und dem Original.

Bei den QFN-BT zeigt sich ebenfalls ein Unterschied in der Lotmenge nach dem Rework-Prozess sowohl in der Gesamtmenge als auch an der Stirnseite (Bild 4).

Lotmenge Reflow (A)	Lotmenge Handlöten (A)	Lotmenge Reflow (B)
→	↑ (Zinn auch auf Pin)	↑ (viel Zinn unter Pin)
Lotoberfläche: Veränderte Farbe, Flussmittelrückstände		
Legende: → gleich, ↑ mehr, ↓ weniger		

Tabelle 1: Lotmenge bei den SOP-Bauteilen

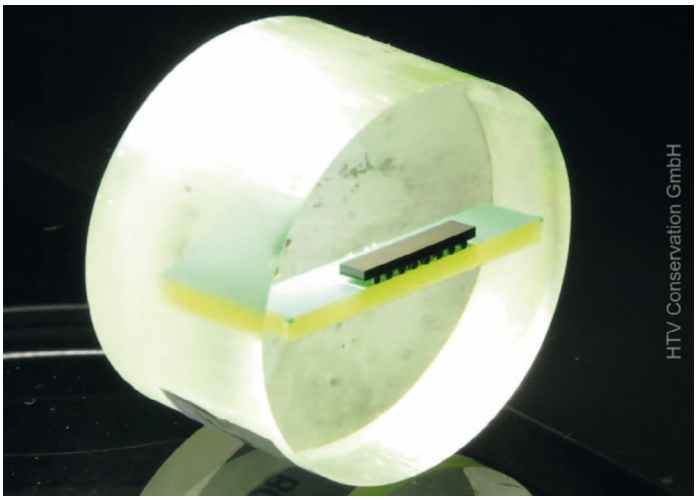


Bild 5: Querschliff durch eine Sub-LP mit BGA

- **Analyse von Schliffbildern**

Mithilfe von Querschliffen durch ein BT oder eine Baugruppe ist es möglich, in den seitlich aufgenommenen Schliffbildern das metallographische Feingefüge der Lötstelle zu analysieren, Materialanalysen durchzuführen und Schichtdicken zu vermessen. Bild 5 zeigt eine vergossene Sub-LP mit BGA nach dem Polierschritt.

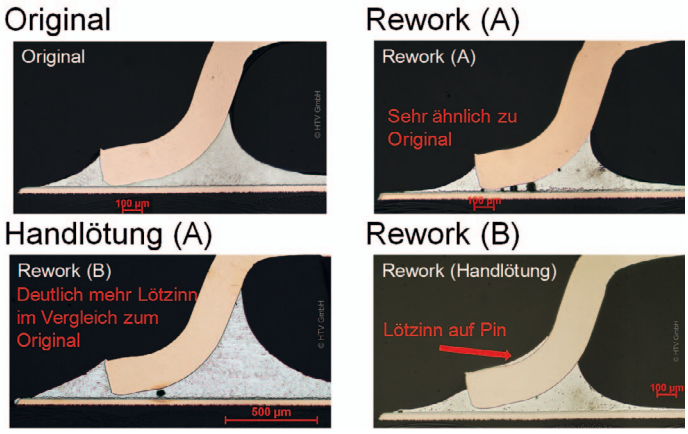


Bild 6: Schliffbilder durch die Lötstellen der SOP-Bauteile

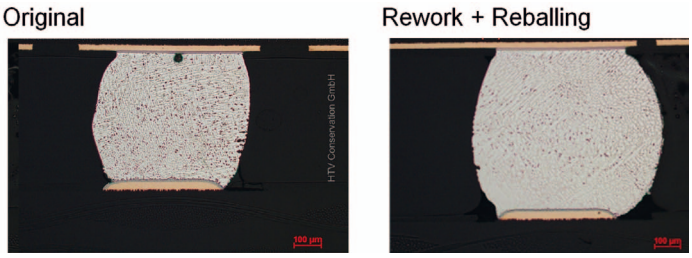


Bild 7: BGA-Balls im Schliffbild, links Original, rechts nach einem Reballing

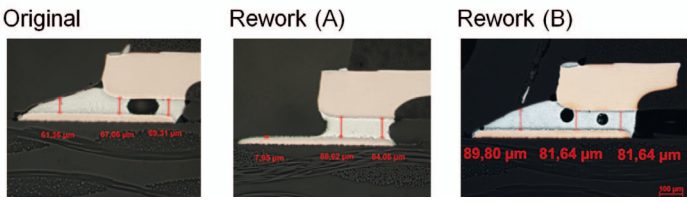


Bild 8: QFN-Kontakte im Schliffbild

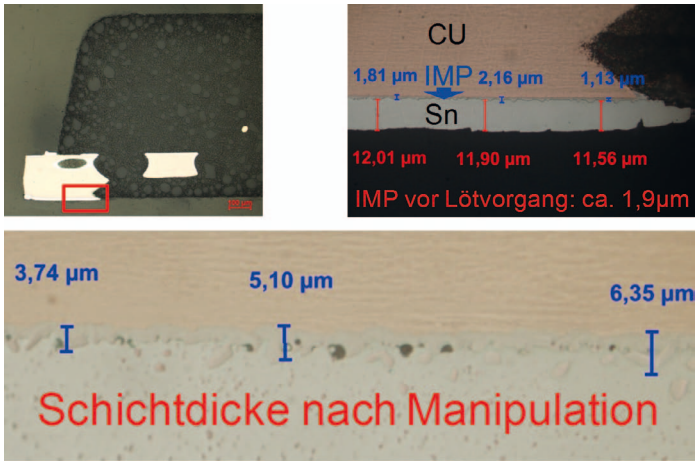


Bild 9: Vermessung der IMP zwischen dem Kupfer des Trägermaterials und der Zinnbeschichtung am Rand eines QFN-Kontakts, links oben Schliffbild durch QFN-Kontakt, rechts oben IMP vor der Manipulation, unten IMP nach der Manipulation

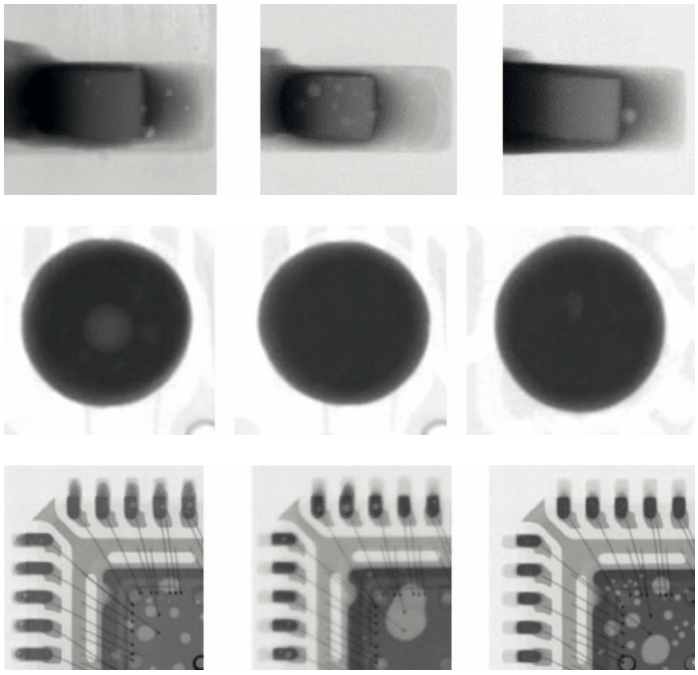


Bild 10: Röntgenuntersuchungen der SOP-Kontakte (oben), der BGA-Balls (Mitte) und der QFN-Bauteile (unten), links Original, Mitte Rework A, rechts Rework B

Wie bei der visuellen Analyse weisen auch die SOP-Pins im Schliffbild einen Unterschied bei der Lotmenge im Vergleich zum Original auf. Während Rework (A) dem Original sehr nahe kommt, zeigt Rework (B) eine deutlich größere Lotmenge bei den SOP-Pins, und bei den von Hand gelöteten Bauteilen sind Lotreste auf der Oberseite der Pins als dünne Schicht erkennbar (Bild 6).

Bei den BGA-Balls sind im Schliffbild im metallographischen Feingefüge keine deutlichen Unterschiede zum Original erkennbar, da es sich in beiden Fällen um eine vergleichbare Zinn-Silber-Kupfer-Legierung handelt. Bei den BT, an denen hingegen ein Reballing erfolgte, zeigt sich ein deutlicher Größenunterschied bei den Balls (Bild 7). Die Schliffbildanalyse der QFN-Kontakte offenbart mehrere Auffälligkeiten (Bild 8). Zum einen ist der Abstand zwischen LP und BT-Anschluss nach dem Rework etwas größer (Tabelle 2), zum anderen hat sich bei Rework (A) das gesamte Lötzinn unter den QFN-Kontakt gezogen.

Abstand zwischen Leiterplatte und QFN-Kontakt		
Original	Rework (A)	Rework (B)
ca. 68 µm	ca. 86 µm	ca. 82 µm

Tabelle 2: Abstand zwischen Leiterplatte und QFN-Kontakt

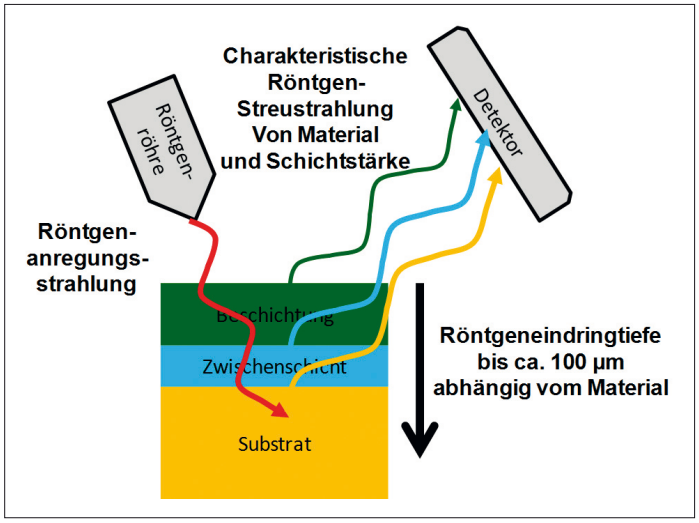


Bild 11: Röntgenfluoreszenzanalyse

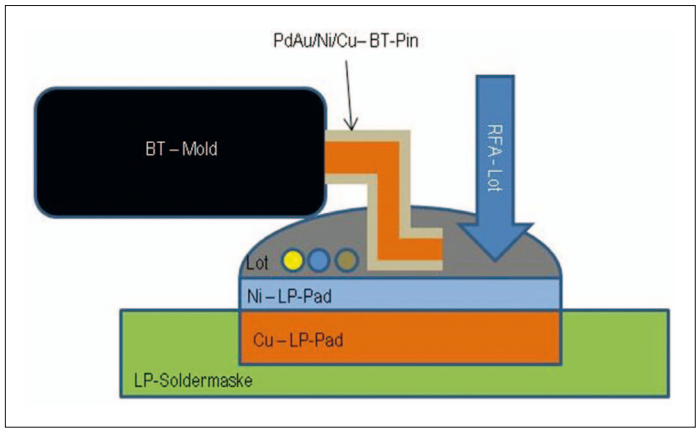


Bild 12: Messgeometrie des Aufbaus. Es wird die Lötstelle vor einem SOP-Pin vermessen

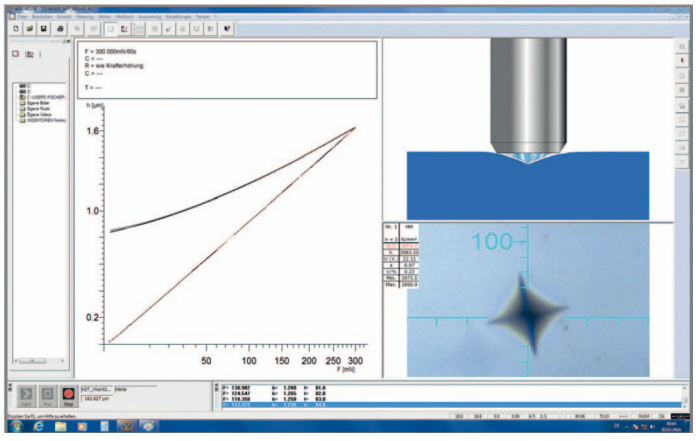


Bild 13: Messkurve mit Eindruckstelle

- **Analyse der intermetallischen Phase**

Oft sind auf dem Kupferträgermaterial unterschiedliche Oberflächenbeschichtungen (z.B. Zinn oder Gold) aufgebracht, die das Grund-

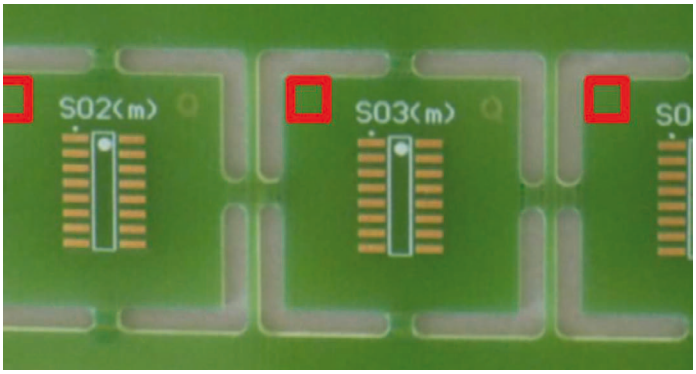


Bild 14: Sub-LP mit markierter Messstelle für Nanoindentation mit 5x5 Messstellen

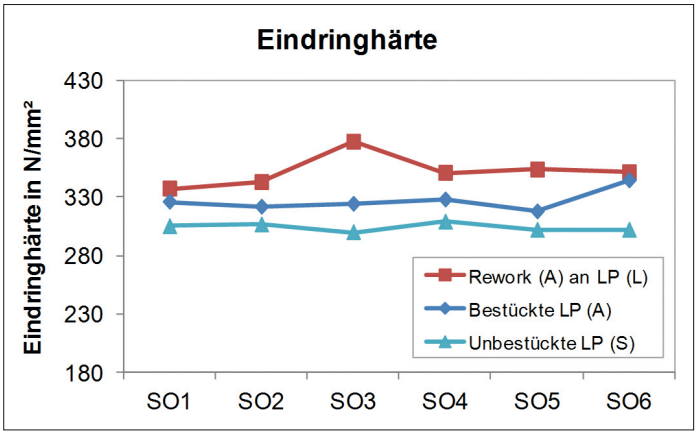


Bild 15: Messung der Eindringhärte

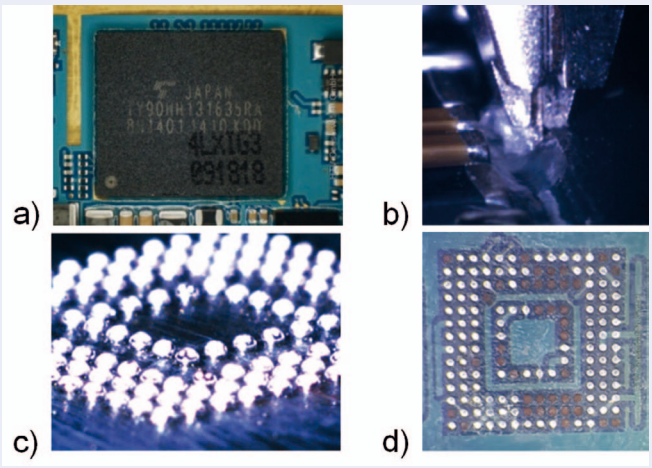
material vor Korrosion schützen und für einen Erhalt der Lötbarkeit sorgen. Durch innere Diffusionsprozesse kann aber das Gold in Kupfer (bei der LP) und das Kupfer in Zinn (beim BT) diffundieren. Für die LP bedeutet das den Verlust der Goldoberfläche nach kurzer Zeit und für den Kontakt des BTs, dass sich nach kurzer Zeit Kupfer in der Zinnbeschichtung befindet und dort eine intermetallische Phase (IMP) bildet. Diese weist einen höheren Schmelzpunkt auf als das Reinzinn und könnte im Lötprozess nicht mehr aufgeschmolzen werden. Um den Diffusionsprozessen entgegenzuwirken, bringen Hersteller oft eine Nickelsperrschicht zwischen Kupfer und der Oberflächenbeschichtung auf.

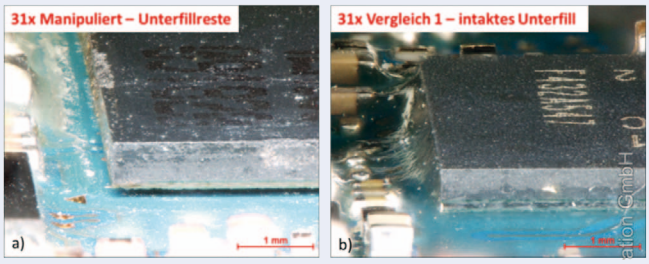
Bei den QFN-BT existiert diese Nickelschicht aber nicht, daher eignen sich diese BT besonders gut für die Analyse der IMP. Wie Bild 9 veranschaulicht, wächst die IMP durch einen Lötprozess. Beim Vergleich zwischen manipulierten und

H-QFN Rework	BT-Pin IMP (SnCu)	
	Mean	Stdabw.
H-QFN1 (m)	5,87	1,76
H-QFN2 (m)	5,24	2,06
H-QFN3(m)	4,88	1,29
H-QFN4	5,69	1,17
H-QFN5	5,25	1,88
H-QFN6	3,88	1,23

Tabelle 3: Vermessung der IMP bei allen QFN-Bauteilen einer manipulierten LP

Analyse von Mobiltelefonen





An der LP des Samsung Galaxy S III i9300 sollte geklärt werden, welche Auffälligkeiten bei einer elektronischen Baugruppe festgestellt werden können, bei der ein BGA, das mit einem Underfill mit der Leiterplatte verklebt ist (a), ent- und nach einem Rework wieder aufgelötet wird.

Zunächst wurde die LP auf 150 °C erwärmt, um das Underfill-Material rund um das BT einschneiden zu können, damit keine benachbarten Bauteile während des Rework-Prozesses abgehoben werden (b). Das BGA wurde dann mit einem speziellen Werkzeug während des Rework-Prozesses bei 240 °C abgehoben. Sowohl BT als auch LP wurden von Underfill- und Lotresten gereinigt. Anschließend wurden in einem Reballing-Schritt neue Lotkugeln auf die Unterseite des BTs aufgebracht (c). Danach wurde das BT in Flussmittel gedippt und wieder auf der LP (d) verlötet. Einige Pads wurden beim Auslötprozess abgerissen.

Die zweite Abbildung zeigt das BGA nach dem Reballing- und Rework-Prozess (a) im Vergleich zu einem Original-BT (b). Bei LP und BT gibt es Rückstände des Underfill-Materials und Kratzer.

Die Funktion ist nach dem Rework-Prozess nicht mehr gegeben! Um das sicher zu vermeiden, darf die LP nicht beschädigt werden. Der Prozess des Austauschens muss also sehr vorsichtig und mit sehr viel Erfahrung durchgeführt werden.

Sn	Ag	Au	Pd	Sb	Pb
Reine **Lotpaste**					
96,53	3,59	0,00	0,00	0,00	0,02
Lotpaste auf Leiterplatte **umgeschmolzen** (ohne Bauteil) (Vergleich mit Lotpaste)					
↓ 95,68	(↓) 3,08	↑ 0,50	0,01	0,25	0,03
Beschichtung der **SOP-Pins**					
0,00	0,00	19,9	80,1	0,00	0,00
Legierung der Lötstelle der **bestückten LP** im **Originalzustand** (Vergleich mit Lotpaste auf LP)					
↓ 93,21	↑ 5,12	↑ 0,87	↑ 0,38	↓ 0,01	0,08
Legierung auf den LP-Pads nach Abnahme der Bauteile und Restlotentfernung (**Vergleich mit Originalzustand**)					
↑ 95,81	↓ 3,07	↓ 0,66	↓ 0,05	↑ 0,26	0,05
Legierung der **Lötstelle mit manipuliertem Bauteil** (**Vergleich mit Originalzustand**)					
↑ 95,34	↓ 3,21	↓ 0,59	↓ 0,18	↑ 0,36	0,03
Tendenz: ↓ abnehmend, (↓) schwach abnehmend, ↑ zunehemend, (↑) schwach zunehmend					

Tabelle 4: RFA-Analyse der elementaren Zusammensetzung einer SOP-Lötstelle

original bestückten BT konnte beim Wachstum der IMP aber kein Unterschied festgestellt werden (Tabelle 3). Dies lässt sich damit begründen, dass die Rework-Systeme die Temperaturen im Lötprozess sehr genau nachbilden und die nicht manipulierten BT nur für kurze Zeit auf etwa 100 °C bringen und in diesem Bereich die Wachstumsrate der IMP nur 21 nm/h beträgt.

- **Röntgenanalyse**

Sie zeigt in nahezu allen Lötstellen einen gewissen Anteil von Hohlräumen bzw. Voids (helle Flecken im Röntgenbild), s. Bild 10. Am auffälligsten sind die Balls der BGAs nach Rework (A); sie weisen keine Hohlräume auf. Bei den anderen Kontakten gibt es zwar leichte Abweichungen zum Original, die aber keine signifikante Auffälligkeit darstellen.

- **Materialanalyse**

Die Zusammensetzung der Legierung in der Lötstelle wurden mittels Röntgenfluoreszenz (RFA) näher analysiert, s. Bild 11. Eine Probe wird mit Röntgenstrahlung beschossen. Diese dringt bis ca. 100 µm ein. Aus dem Spektrum der zurückgestreuten charakteristischen Röntgenstrahlung können dann die im Material enthaltenen Elemente analysiert werden.

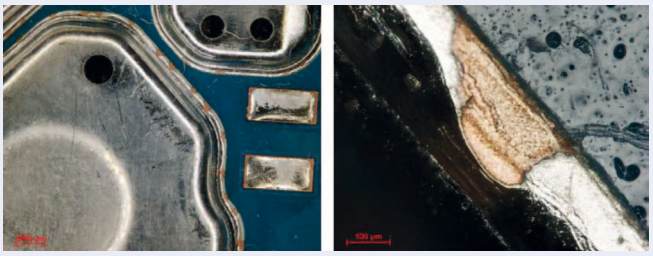
Bild 12 zeigt schematisch die Messgeometrie des Aufbaus. Es wird die Lötstelle vor einem SOP-Pin vermessen. Tabelle 4 enthält die Ergebnisse für sechs wichtige Elemente in unterschiedlichen Phasen des Rework-Prozesses. Der Bleigehalt (Pb) ist allgemein sehr gering. Dies ist typisch, da bleifreie Lotpasten verwendet werden. Die Lotpaste ist eine typische SAC-Legierung (Sn-Ag-Cu) mit einem Silberanteil von 3,5%.

Interessant ist, dass ein reines Aufschmelzen der Lotpaste auf einem Pad der Leiterplatten das Gold der ENIG-Oberflächenbeschichtung löst und dieses anschließend im Lötzinn gemessen werden kann. Die Pins selbst weisen eine Nickel-Palladium-Gold-Beschichtung auf. Durch das Verlöten der Bauteile steigt der Gold- und Palladium-Anteil in der Lötstelle an. Wird jetzt das Bauteil im Rework abgelötet und das Restlot auf dem Pad entfernt, sinkt der Gold- und Palladiumanteil wieder.

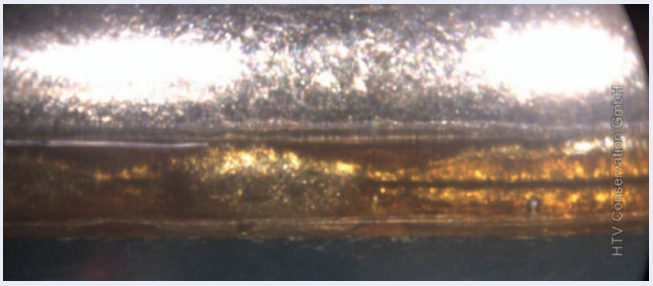
Durch das Aufbringen eines neuen SOP-BTs mit einer SAC-Lotpaste wird nicht in gleichem Maße Gold und Palladium der Lötstelle im Rework-Prozess gelöst. Daher weisen die manipulierten Lötstellen im Vergleich zum Originalzustand einen geringeren Gold- und Palladiumanteil auf.

Wechsel von Schutzblechen

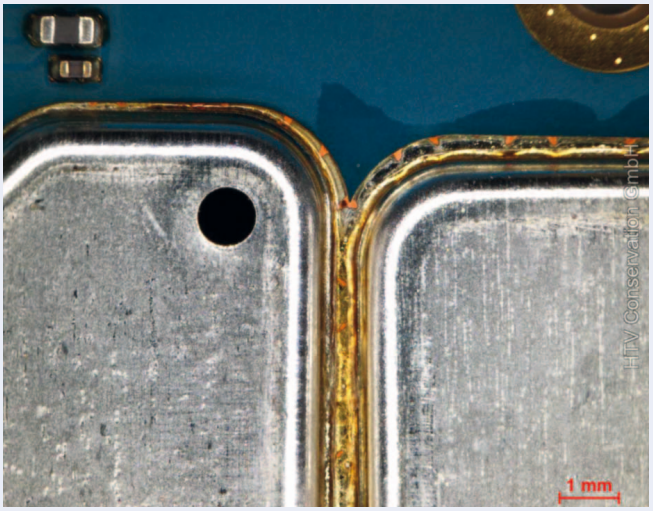
Bei der LP eines BlackBerry-Mobiltelefons Z30 wurde eins der Schutzbleche abgehoben, die Lötstelle auf der LP mit Flussmittel benetzt und das Blech anschließend wieder aufgelötet. Die Untersuchung sollte auch klären, um was für eine Art von Verfärbung es sich beim Blech handelt und ob diese auch noch nach einem Rework-Prozess existiert. Links das Schutzblech, rechts die Verfärbung auf dem Rand des Blechs:



Die folgende Abbildung erlaubt einen seitlichen Blick auf die Lötstelle und zeigt, dass das Lötzinn nicht gleichmäßig den Schlitz zwischen Leiterplatte und Blech ausfüllt und es sogar Bereiche gibt, bei denen das Lötzinn LP und Blech gar nicht verbindet. Die verfärbten Bereiche sind die Zonen, die nur von Flussmittel gefüllt wurden. Diese ungleichmäßige Benetzung beruht wahrscheinlich auf einer mangelhaften Lötbarkeit der Bleche und zum anderen auf einer zu geringen Menge an Lotpaste.



Das folgende Bild zeigt das getauschte Blech nach dem Rework-Prozess. Die auffällige Färbung am Rand bildet sich auch nach dem Rework aus. Ein Unterschied zum Originalblech ist kaum erkennbar. Links das Originalblech ohne Rework, rechts das durch Rework getauschte Blech:



Fazit: Mit einem Rework-Prozess können Schutzbleche leicht getauscht werden, und die Lötstellen am Rand der Bleche kommen im visuellen Erscheinungsbild dem Originalzustand sehr nahe.

Analyse	Mögliche Auffälligkeiten bei elektronischen Baugruppen mit Rework
Visuell / Mikroskopisch	Verfärbungen und Verformungen der LP, Unterschiede bei der Lotmenge und den Flussmittelresten in den Lötstellen, Verschmutzungen, Kratzer und Underfillrste.
Schliffbilder	Applikationsart der Lotpaste erkennbar, Abstand zwischen BT und LP z.T. unterschiedlich (Lotmengenunterschied), Analyse des Feingefüges.
Intermetallische Phase	Keine signifikanten Unterschiede beim IMP-Wachstum.
Röntgen	Unterschiede bei den Fehlstellen in den BGA-Balls und QFN-Bauteilen, Unterschiede bei der Lotmenge z. B. bei den SOP-Bauteilen.
RFA	Bei SO-Bauteilen Nachweis durch Änderungen von Au und Pd-Anteil in der Lötstelle.
Nanoindentation	Änderung der Härte der Leiterplatten durch das Rework.

Tabelle 5: Analysen und Auffälligkeiten

- **Härtemessung mit Nanoindentation**

Um die Härte einer LP zwischen dem Originalzustand und den manipulierten LP zu analysieren, wurde die Nanoindentation verwendet. Ein Verfahren, bei dem eine sehr kleiner Stift mit einer Diamantspitze und spezieller Form in das zu untersuchende Material eingedrückt und dabei die Eindringtiefe und Kraft aufgezeichnet werden (Bild 13). Mit dem Verfahren kann man eine Vielzahl von Kennwerten errechnen (z.B. Eindringmodul, Eindringhärte, Martenshärte und Vickershärte).

Bild 14 zeigt eine Sub-LP mit markierter Messstelle für Nanoindentation mit 5x5 Messstellen. Zur Ermittlung der durchschnittlichen Eindringhärte wurden auf den unterschiedlichen Sub-LP 25 Messwerte auf einem Feld von 5x5 Messpunkten ermittelt. Wie Bild 15 verdeutlich, steigt die Eigenhärte der Leiterplatten durch den Rework-Prozess an. Der Anstieg lässt sich durch das Ausgasen von Weichmachern aus dem Harzmaterial der LP durch die hohen Temperaturen während des Rework-Prozesses erklären.

Fazit

Die vorgestellte Studie verdeutlicht, dass durch einen Rework-Prozess an einer LP u.a. folgende Auffälligkeiten auftreten können:

- Verfärbung des Harzmaterials
- Rückstände von Flussmittel
- Eindringhärte steigt an

Weitere mögliche Auffälligkeiten enthält z. B. [2].

Auffälligkeiten an Kontakten:

- Lotmengenunterschiede
- Hohlräume bzw. Voids in den Lötstellen
- elementare Zusammensetzung der Lötstelle ändert sich merklich (z.B. Gold, Palladium und Antimon)

Verdeutlicht wurden unterschiedliche Aspekte, die beim Rework einer elektronischen Baugruppe berücksichtig werden müssen. Tabelle 5 enthält noch einmal mögliche Analysen und dadurch gefundene Auffälligkeiten. Es zeigt sich: Durch ein Rework können unterschiedliche Abweichungen von der Originalbaugruppe auftreten. Abhängig davon, wie gut das Rework ausgeführt wurde, sind diese leichter oder schwerer zu erkennen.

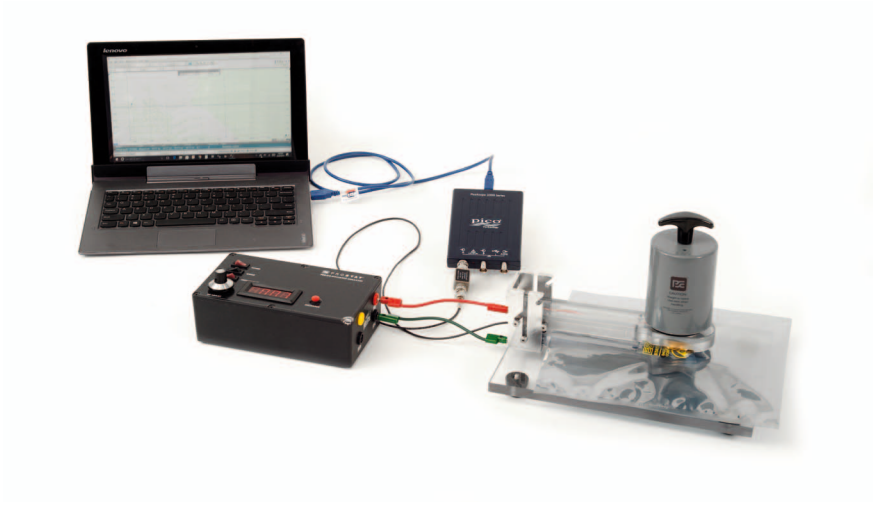
Literatur

[1] Thomas Kuhn, Henry Schäf, Wiebke Valouch: Lötzinn-Analyse, HTV GmbH, Forschungsprojekt für das Bundesamt für Sicherheit in der Informationstechnik, Projekt 249, 15.11.2016

[2] ZVEI: Rework of Electronic Assemblies – Qualifiable Processes for Rework, German Electrical and Electronic Manufacturers' Association, November 2017 ◄

Verpacken/Kennzeichnen/Identifizieren

ESD-Verpackungen testen



Für elektronische Bauelemente, die empfindlich gegenüber elektrostatischen Entladungen und Feldern sind, gelten innerhalb einer EPA folgende Anforderungen:

- Verpackungen, die verwendet werden, müssen bei direktem Kontakt aus ableitfähigem oder leitfähigem Material bestehen.
- Teile, die empfindlicher als <100 V nach dem Human Body Model sind, benötigen eventuell zusätzlichen Schutz in Abhängigkeit von ihrer Anwendung und den Anforderungen eines ESD-Kontrollprogrammplans.

Werden ESDs außerhalb einer EPA transportiert, müssen folgende Anforderungen erfüllt werden:

- Der Transport von empfindlichen Produkten benötigt Verpackungen, die beides sicherstellen:

a) ableitfähiges oder leitfähiges Material bei direktem Kontakt

b) eine Struktur, die eine Abschirmung gegen elektrostatische Entladungen bedeutet

Wenn Materialien für eine Abschirmung gegen ein elektrostatische Feld verwendet werden, um die Abschirmung gegenüber Entladungen sicherzustellen, dann muss ein Material verwendet werden, das eine Barriere gegen einen Stromfluss in Kombination mit einem Material für eine Abschirmung gegen ein elektrostatisches Feld bietet. (Die Anforderungen wurden der DIN EN 61340-5-3 entnommen.)

Für die Messung der Abschirmfähigkeit von ESD-Verpackungen eignet sich ein Messgeräte-Set der B.E.STAT Elektronik Elektrostatik GmbH. Das Set erlaubt die Ermittlung der Abschirmeigenschaften von ESD-Verpackungen bis 50 nJ, aber auch schon nach den erhöhten Anforderungen der ANSI/ESD S541-2018 bis 20 nJ.

ESD-Semina

Geboten wird ein spezielles ESD-Seminar zum Thema „ESD-Verpackungen" am 19.3.2019 in Kesselsdorf. ◄

B.E.STAT Elektronik Elektrostatik GmbH
sales@bestat-esd.com
www.bestat-esd.com
www.bestat-cc.com