バウンダリスキャン研究の最前線

バウンダリスキャン研究会

Current Research Topics on Boundary-Scan Technology

Boundary-Scan Study Group

1. はじめに

バウンダリスキャン技術講座の7回目は，国内外で研究されているバウンダリスキャンの応用技術，バウンダリスキャン関連のセキュリティ技術などの研究動向について紹介する。

バウンダリスキャンは，プリント配線板に実装されたIC間の接続を検査するために用いられる検査容易化設計でIEEE 1149.1規格として標準化されている[1]。JTAGポートと呼ばれる4ないし5本の制御信号（TDI, TDO, TMS, TCK, TRST（オプション））のみにより，IC内部のコア回路から独立してICの入出力を可制御・可観測とすることで，各IC間の接続テストが可能となる。

バウンダリスキャンの構成については，その後，SoCなどのICチップ内部のIPコアなどの各ブロック間を可制御・可観測とし，各IPコアを独立に検査する拡張がIEEE 1500規格として標準化されている。さらに，チップを垂直に積層する3次元積層ICにおけるダイ間接続のテストへのバウンダリスキャンの拡張機能がIEEE 1838として2019年に標準化された。

本稿では，バウンダリスキャンおよびその機能拡張に基づく研究について，検査手法に関する研究とセキュリティ関連の研究についていくつか紹介する。

2. 検査分野におけるバウンダリスキャン研究

2.1 検査対象の拡がり

IEEE 1149.1規格として当初プリント配線板上のIC間を対象として提案されたバウンダリスキャン法は，図1のように入出力に内部コア回路と独立に制御・観測可能なバウンダリスキャンレジスタを配置することで検査を行う手法である。

このコア回路から独立に入出力を制御する特性から，さまざまな拡張がこれまでに行われている。IEEE 1500ではSoCなどのチップ内部のIPコアを独立に検査するテストラッパーが各コアに設けられ，バウンダリスキャンを基としたテスト回路として用いられている（図2）。

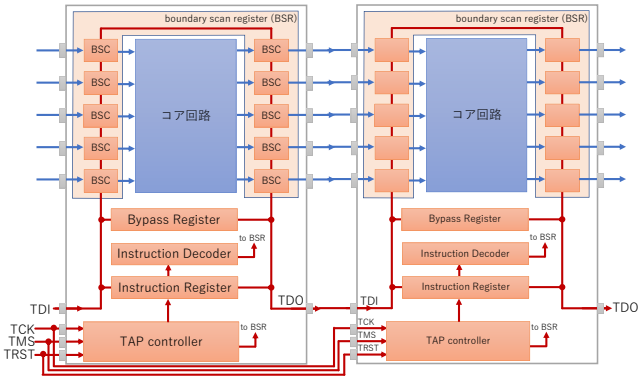

図1. バウンダリスキャンによるテスト回路

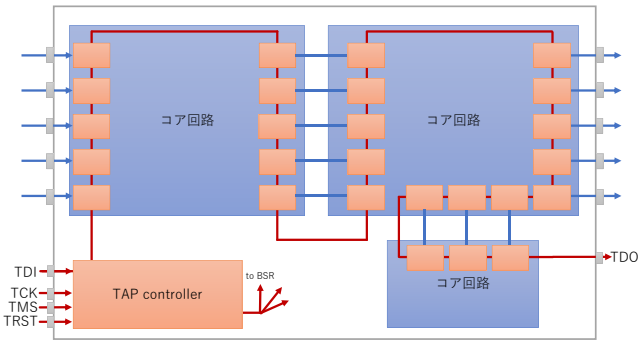

図2. テストラッパーによるテスト回路

また，アナログ回路を対象として内部回路のブロービング機能などが追加されたIEEE 1149.4規格については連載第4回にて紹介されている[2]。

チップ積層技術には，インターポーザ上にチップを平面上に積層する2.5D方式，シリコン貫通ビア(TSV)によりチップを垂直に積層する3D方式，さらにダイの上に複数の垂直積層チップを載せる5.5D方式などが開発されており（図3），これらの積層チップのチップ間配線の検査にもバウンダリスキャン技術を応用したIEEE 1838規格が提案された[3]。3次元実装ICに関しては，TSVによるチップ間接続をする前の検査（プリボンドテスト）に関する研究，チップ間接続後の積層テスト（ポストボンドテスト）に分

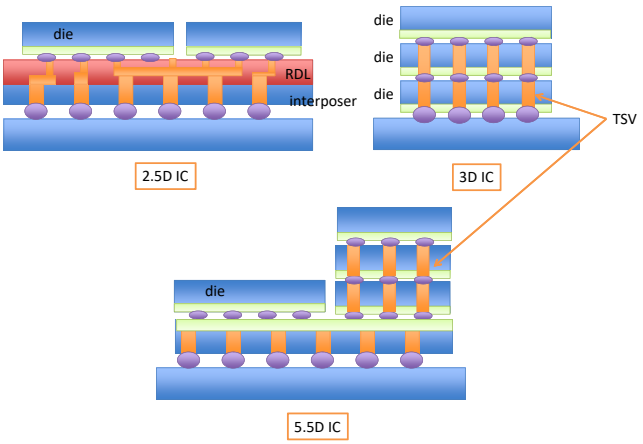

図 3.　チップ積層技術 (2.5D IC, 3D IC, 5.5D IC)

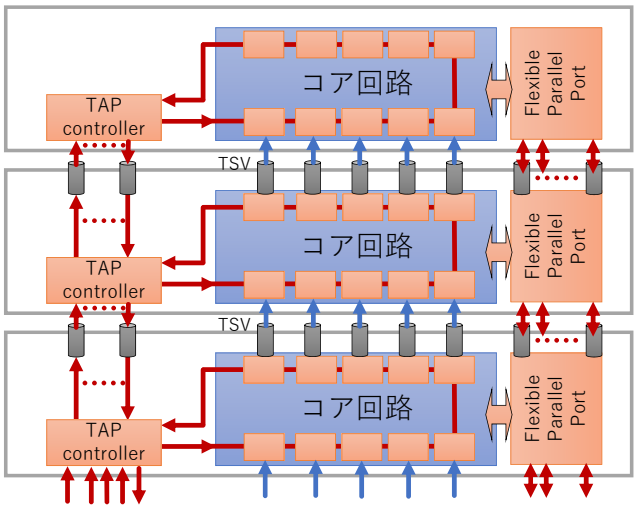

図 4.　テストエレベータによる 3 次元積層 IC のテスト回路

けられる。プリボンドテストは主に TSV が正しく形成されているかを，ポストボンドテストでは TSV とマイクロバンプによるチップ間接続が正しく行われているかを検査する。いずれのテストにおいても信号供給および出力応答を読み出すためにバウンダリスキャンが用いられる。IEEE 1838 による検査容易化設計はテストエレベータと呼ばれ，JTAG バウンダリスキャン，テストラッパーと同様に積層する各ダイの入出力にバウンダリスキャンセルを設け内部回路と独立に制御・観測可能とする技術である。また，オプションとして高速アクセス用のフレキシブルパラレルポートが設けられている（図 4）。

2.2　バウンダリスキャンセルの改良に関する研究

バウンダリスキャンの構成により，各 IC または IC 内の IP コアについて，その入出力を独立に可制御・可観測とすることが可能となる。コア回路の入出力に配置されるバウンダリスキャンセル (BSC) は，通常使用時はセル入力をそのままセル出力へ接続し，テスト時には SI 入力，SO 出力がチェーン状に接続され，セル内部のキャプチャレジスタ，アップデートレジスタを介して BSC の入力観測および出力制御が可能となる。図 5 に基本的なバウンダリスキャンセル BC_1 を示す [1]。

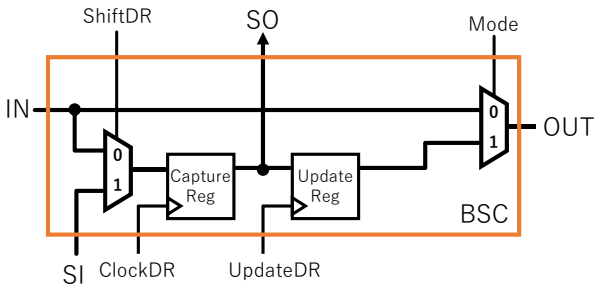

図 5.　標準バウンダリスキャンセル (BC_1)

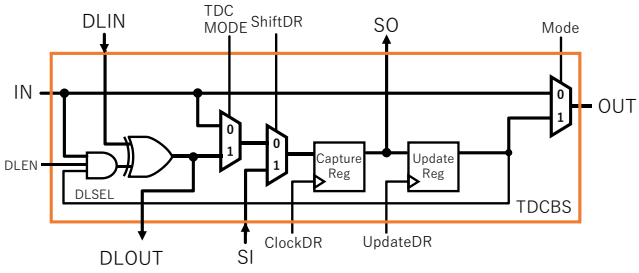

図 6.　TDCBS セル

バウンダリスキャンによる接続テストはあくまで論理値テストによるもので，完全に断線している場合には検出が容易であるものの，BGA 実装のバンプにおけるボイド発生などによる不完全接続（半断線）については見落としが発生する可能性がある。

それらの半断線故障に関しては，標準のバウンダリスキャンセルによる検出は困難であるため，バウンダリスキャンセルの改良により，信号遅延や配線間クロストーク，漏れ電流などの影響を観測し，故障検出を行う手法が複数提案されている。

文献 [4),5)] では，バウンダリスキャンセル内に付加遅延素子を埋め込み，TDC (Time-to-digital converter) 回路を構成できるようにして，チップ間の信号遅延の異常を検出する TDCBS 回路が提案されている。図 6 に TDCBS のバウンダリスキャンセルを示す。TDCMODE = 0 で標準バウンダリスキャンセル互換の動作を行い，TDCMODE = 1 を設定するとセルの DLIN-DLOUT 経路による TDC 回路が構成される。

TDCBS 回路による遅延故障のテストは，図 7 に示すように，接続部の遷移信号を XOR ゲートとキャプチャレジスタで構成される TDC 部に伝搬させ，クロックタイミングまでに遷移信号が到達したセル数 Nslack を計測する。得られた Nslack を正常値と比較することで異常遅延の検出が可能である。

配線遅延やクロストークの影響をバウンダリスキャンを用いて構成したリング発振器により検出する手法が文献 [6)]

で提案されている。図 8 に示すようにバウンダリスキャンセル内のレジスタがリング発振器の接続選択のために用いられ，バウンダリスキャンチェーンの一部をリング発振器構成のために用い，発振回数をコア回路内カウンタによりカウントすることで遅延検出を行うものである。

IC 間接続部の漏れ電流の検査のため，バウンダリスキャンセル内に電流センサを設ける手法が文献[7]で提案されている。図 9 に示すように，バウンダリスキャンセル内に電流比較器を組み込んでいる。参照電流 Iref を選択したセルへ供給し，入力部からの電流量と比較した結果をバウンダリスキャンにより読み出してチップ間の異常電流を検出するものである。

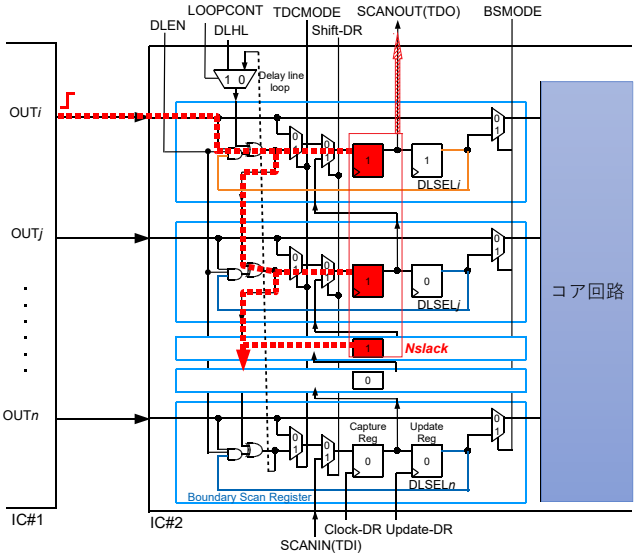

図 7.　TDCBS 回路による遅延故障テスト

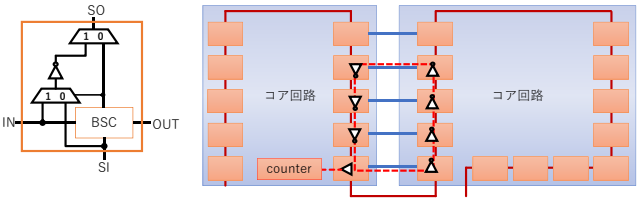

図 8.　リング発振器による接続遅延テスト

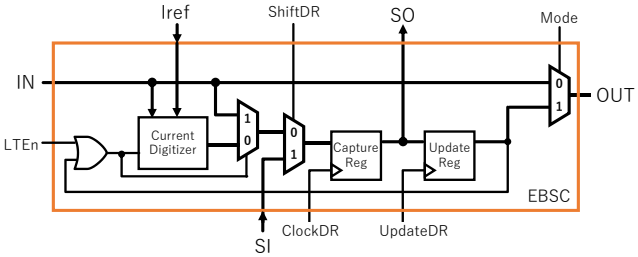

図 9.　電流センサを内蔵する漏れ電流テスト

3.　セキュリティ分野におけるバウンダリスキャン研究

3.1　テスト回路自体のセキュリティ

テスト容易化設計は回路の可制御性・可観測性を向上させることが目的であるが，それ自体が脆弱性をもたらすことがないように機能の改良が加えられている。想定される脆弱性には，バウンダリスキャンやコア回路内部のレジスタの制御・観測を行うスキャン設計によりファームウェアの変更やリバースエンジニアリング，暗号回路の秘密鍵の解読などが挙げられる（図 10）[8)~10)]。

これらに対して，JTAG ポートの利用を出荷時に禁止する，鍵となる信号を最初に印加しなければ JTAG ポートを利用禁止とする，圧縮・解凍回路や暗号化回路により命令コードを複雑化する，などの対策が考えられている[9),10)]。

また，チップ内部のテスト回路を IEEE 1687 規格 (IJTAG) に適応させることでバウンダリスキャンのレジスタ長を容易に推定できなくすることが可能である。IJTAG (Internal JTAG) は，図 11 のようにチップ内の IP コアやセンサ類ごとに SIB (Select Instrument Bit) と呼ばれるレジスタを設け，テスト時のアクセスを制御する。テスト回路を適応的に選択することでテスト時間の最適化が可能である。また，後述のようにテスト用に設けたセンサの測定値の読み出しにも IJTAG が用いられる。

その他にも，与えられる命令シーケンスが正当か否かを検出する回路を TAP コントローラに設ける手法や，機械学習を用いて通常のテストに用いられる命令シーケンスか否

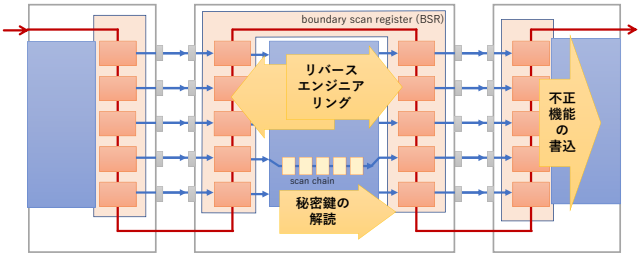

図 10.　想定されるバウンダリスキャンを用いる攻撃例

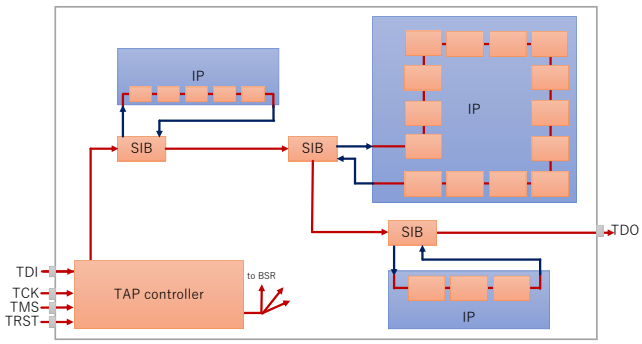

図 11.　IJTAG による IP コアへのテストアクセス

講座

かを判定する手法などがセキュリティ対策として提案されている[11]。

3.2 偽造防止へのバウンダリスキャンの利用

バウンダリスキャン技術をIC間接続や各ICの機能動作の検査のみならず，電子回路の実装部品の偽造防止や偽造ICの検出へ適用することが考えられている。実装部品の偽造については，リサイクルICの利用や，IC内部にハードウェアトロイなどの不正な回路を埋め込まれる偽造ICなどが想定される[11]。

バウンダリスキャンのIDCODE命令（オプション）を用いることで実装部品に書き込まれた製造元，部品番号，バージョンなどを確認できる。また，IEEE 1149.1-2013においてはECID (Electronic Chip Identification) と呼ばれるICチップの個別識別を行う機能が追加されている[12]。

チップごとの個別識別自体にバウンダリスキャンを用いる手法として，チップの真贋判定に用いられるPUF (Physically unclonable function) の一種として，バウンダリスキャン自体をPUFとして用いる手法が提案されている[13]。電源投入時のバウンダリスキャンレジスタの初期値をICおよび基板の固有値として記録しておくことで出荷後のIC偽造などの真贋判定を行う。

文献[14]では，エレクトロマイグレーションの効果を検知するセンサを付加し，センサ出力値をIJTAGなどのバウンダリスキャン機能により読み出すことで劣化度合いを判定，再利用品の検出に用いる手法が提案されている。

これらの手法においては，外部から個別部品へのアクセスが容易なバウンダリスキャンの特長が活かされている。

4. まとめ

本稿では，バウンダリスキャン技術に関する学術面での機能拡張などの研究動向について述べた。新たな実装技術への適用や半断線など非論理故障の検出などへの適応など技術開発が進められている。また，セキュリティや真贋判定においてもバウンダリスキャン技術の適用による効果が期待されている。

（2020.6.26- 受理）

文　献

1) ケンパーカー（著），亀山修一（監訳）：“バウンダリスキャンハンドブック第3版，”青山社，2012.6
2) バウンダリスキャン研究会（亀山修一）：“アナログと高速伝送回路のためのバウンダリスキャン，”エレクトロニクス実装学会誌，Vol. **23**, No. 2, pp. 192–196, 2020年2月
3) E. J. Marinissen, T. McLaurin, and H. Jiao: “IEEE Std P1838: DfT standard-under-development for 2.5D-, 3D-, and 5.5D-SICs,” Proc. 21th IEEE European Test Symposium (ETS), pp. 1–10, 2016
4) H. Yotsuyanagi, H. Makimoto, T. Nimiya, and M. Hashizume: “On Detecting Delay Faults Using Time-to-Digital Converter Embedded in Boundary Scan,” IEICE Trans. Inf. Syst., Vol. **E96. D**, No. 9, pp. 1986–1993, 2013
5) S. Kikuchi, H. Yotsuyanagi, and M. Hashizume: “On Delay Measurement Under Delay Variations in Boundary Scan Circuit with Embedded TDC,” IEEE International Test Conference in Asia (ITC-Asia), pp. 169–174, 2019
6) K. S.-M. Li, C. Su, Y.-W. Chang, C.-L. Lee, and J. E. Chen: “IEEE Standard 1500 Compatible Interconnect Diagnosis for Delay and Crosstalk Faults,” IEEE Trans. CAD., Vol. **25**, No. 11, pp. 2513–2525, Nov. 2006
7) P. M. P. Law, C.-W. Wu, L.-Y. Lin, and H.-C. Hong: “An Enhanced Boundary Scan Architecture for Inter-Die Interconnect Leakage Measurement in 2.5D and 3D Packages,” IEEE 26th Asian Test Symposium (ATS), pp. 5–10, 2017
8) J. Da Rolt, A. Das, G. Di Natale, M. L. Flottes, B. Rouzeyre, and I. Verbauwhede: “Test Versus Security: Past and Present,” IEEE Trans. Emerging Topics in Computing, Vol. **2**, No. 1, pp. 50–62, 2014
9) K. Rosenfeld and R. Karri: “Attacks and Defenses for JTAG,” IEEE Design & Test of Computers, Vol. **27**, No. 1, pp. 36–47, Jan. 2010
10) X. Ren, F. P. Torres, R. D. Blanton, and V. G. Tavares: “IC Protection Against JTAG-Based Attacks,” IEEE Trans. CAD., Vol. **38**, No. 1, pp. 149–162, Jan. 2019
11) E. Valea, M. Da Silva, G. Di Natale, M.-L. Flottes, and B. Rouzeyre: “A Survey on Security Threats and Countermeasures in IEEE Test Standards,” IEEE Design & Test, Vol. **36**, No. 3, pp. 95–116, June, 2019
12) 亀山修一，高橋　寛：“偽造ICチップの脅威と対策―バウンダリスキャンによる真贋判定とトレーサビリティ―，”第32回エレクトロニクス実装学会春季講演大会，pp. 18–20, 2018
13) B. Niewenhuis, R. D. Blanton, M. Bhargava, and K. Mai: “SCAN-PUF: A low overhead Physically Unclonable Function from scan chain power-up states,” IEEE International Test Conference (ITC), pp. 1–8, 2013
14) K. He, X. Huang, and S. X. D. Tan: “EM-Based On-Chip Aging Sensor for Detection of Recycled ICs,” IEEE Design & Test, Vol. **33**, No. 5, pp. 56–64, Oct. 2016

著者紹介

四柳浩之（よつやなぎ　ひろゆき）
平10大阪大学 大学院工学研究科博士後期課程了。同年より徳島大学工学部電気電子工学科助手，現在同大大学院社会産業理工学研究部准教授。順序回路のテスト容易化設計，断線故障の検査などの研究に従事。博士（工学）。エレクトロニクス実装学会，電子情報通信学会，IEEE各会員。