特集

バウンダリスキャン設計の現状と展望

The Current Status and Prospect in Boundary Scan Design

バウンダリスキャン研究会

1. はじめに

半導体チップの高集積化によりパッケージは多ピン化し，現在はBGAパッケージなど実装時に外部からの観測が困難なデバイスが普及している。直接観測やプロービングが困難な実装基板の素子間の接続を電気的にテストする手法としてバウンダリスキャンが活用されている。

さらにチップの集積度が限界に近づく中で，実装面積を小さくする手段として，複数チップを1つのパッケージに収める技術が用いられている。近年ではTSV（シリコン貫通ビア）を用いる3D IC, 2.5D ICといった積層技術が開発され，それにより歩留まりなどの問題から1チップに収めていた機能をチップレットと呼ばれる小さな複数ダイに分割して1パッケージに収める構成が採用されるようになってきた。これらのパッケージ内チップの接続テストにおいてもバウンダリスキャンおよびその拡張機能が規格化され利用されている。

バウンダリスキャン研究会では，昨年より本誌において「バウンダリスキャン技術講座」を連載してきた。第7回（2020年9月号）ではバウンダリスキャンに関する研究事例をいくつか紹介したが，本稿では，近年の課題として挙げられる偽造ICやセキュリティとバウンダリスキャンとの関連についてより詳しく紹介する。

2. バウンダリスキャンによる実装部品の検査の動向

バウンダリスキャンはIEEE1149.1規格として標準化されている検査容易化設計である[1)]。バウンダリスキャン対応のICでは図1のように入出力端子にバウンダリスキャンレジスタ(BSR)が設けられており，TDI端子からBSRに任意の値を設定し，TDO端子から観測することができる。TDI, TDO端子に加えて動作制御のためのTMS, TCKおよびTRST（オプション）端子の4ないし5端子を設け基板上で接続することでIC内部のコア回路に依存せずIC間接続のテストが行える利点がある。

基板上のICのバウンダリスキャン回路においては，TDO端子とTDI端子をチェーン状に接続し，TMS, TCK, TRSTが共通に接続される。したがって，多数のICが搭載されていても検査に必要な端子は5つに抑えられる。また，IC間接続テストでは検査対象ICのBSRの制御・観測を行い，対象外のICはバイパスレジスタ経由でTDIからの制御値・観測値がTDOへ伝搬される。

TDI, TDOの接続を用いるIC間接続テストのイメージを図2に示す。IC2とIC3間のテストを行うために，IC2のBSRにIC1のバイパスレジスタ経由で制御値を設定し，IC3

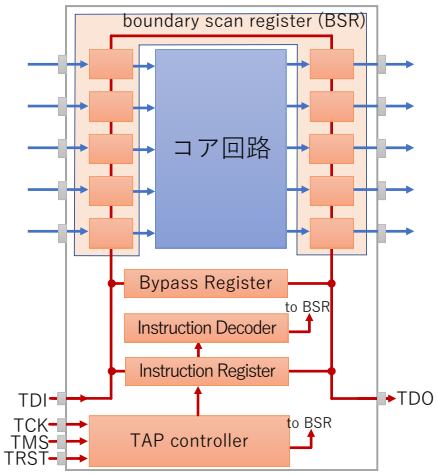

図1. バウンダリスキャン回路

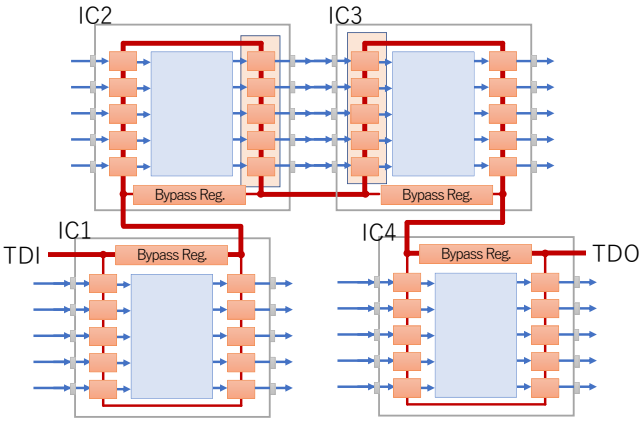

図2. バウンダリスキャンを用いる接続テスト

のBSRで取り込んだ値をIC4のバイパスレジスタ経由で観測する。

また，バウンダリスキャンにより個別ICへの信号供給が可能であることから，各ICを独立してテストしたりデバッグなどの用途にも利用される。個別ICのテストの際の信号伝搬は図3に示すように行われ，対象のIC2の入出力をBSRにより制御・観測し，対象外のICはバイパスレジスタ経由で信号供給・観測を行う。

近年では，実装部品の正当性を確認するためにもバウンダリスキャンが適用されている。バウンダリスキャンのIDCODE命令では，ICに書き込まれた製造元や部品番号などの情報を読み出し正しい部品が実装されているかをテスト実行前に確認できる。さらに，偽造ICや再利用ICを検知するためにIC固有の情報を各ICから読みだす機能もIEEE1149.1-2013規格において追加されている[2)]。ICを個別識別するためにPUF (Physically unclonable function) と呼ばれる情報を用いる。PUFは半導体のばらつきにより応答が異なる回路の特徴を利用して，製造元で個別ICを識別する特徴量を収集しておくことで真贋判定が可能な技術である。特徴量としては，電源投入時のメモリやフリップフロップの初期値，図4のアービター回路で選択した2経路の信号到達時間の差異などが用いられる。

出荷時テストにおいてはインサーキットテストやX線による観測などの手法が適用可能であるが，出荷後のオンラインテストでは適用できないため，電気的なテスト手法が必須となる。バウンダリスキャンは出荷前・出荷後いずれにも適用可能であり，従来よりも重要度が増している。

ただし，出荷後にもバウンダリスキャンを利用可能とする場合には，内部回路へのアクセスが容易となるため悪用の危険性についても考慮が必要となる。

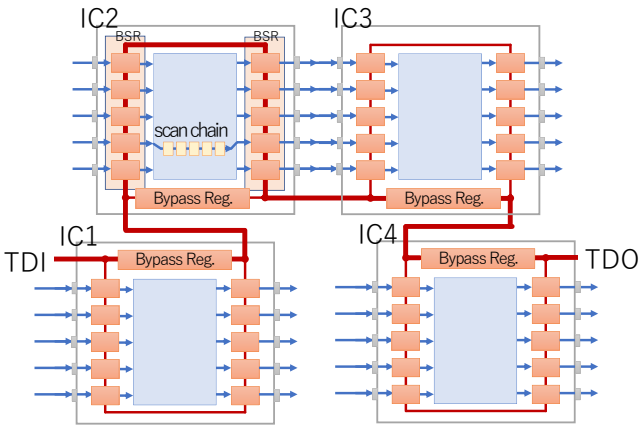

図3. バウンダリスキャンを用いる個別ICのテスト

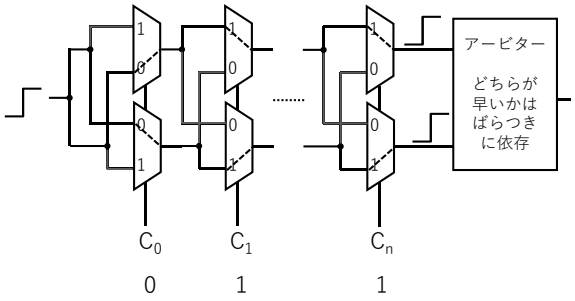

図4. アービターPUFの例

3. セキュリティを考慮するバウンダリスキャンの利用

テスト容易化設計では付加回路により可観測性・可制御性を向上することで，テストカバレッジ向上やテスト時間の削減を行うが，他方で内部回路への不正なアクセスを抑制するためのセキュリティに関する対策も進められている。

バウンダリスキャンの悪用の可能性として，図5に示す構成の下での脆弱性が考えられる[3),4)]。個別ICのテストがIC2に適用される際に，テスト対象以外のIC1, IC3がバイパスモードに設定され，IC2のテストパターンを供給・観測されると仮定する。このとき，IC1やIC3などの検査対象以外のデバイスにおいて，データをバイパスしながらデバイス内部に蓄積することで，秘密情報の解読などに悪用することが考えられる。このような不正回路は，本来の機能には影響しないハードウェアトロイとして挿入することが可能であり，通常のテストの適用ではこれら不正回路の検出は困難である。また，これらがデバイスの入力側・出力側の双方に存在する場合には，入出力を読み出すことで

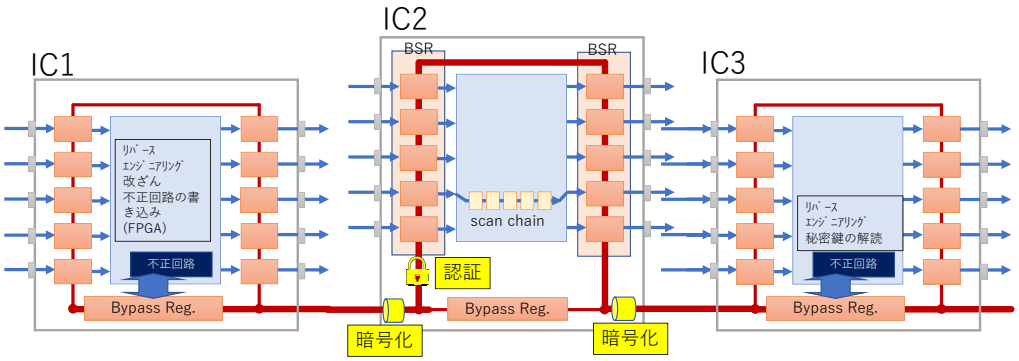

図5. 信頼できないデバイスの影響可能性とその対策

内部動作の推測を行うリバースエンジニアリング攻撃が可能となる。バウンダリスキャンがファームウェアの書き換え，マイコンのデバッグ，FPGA の回路書き込みなどに利用できる場合には，脆弱性のあるファームウェアの書き込みや不正回路の書き込みなどの恐れも想定される。

暗号化チップなどにおいては，暗号化・解読の繰り返し処理が行われるが，内部状態の制御・観測を行うスキャン設計†経由で繰り返し途中の内部状態を読み出すことで秘密鍵との相関から，デバイスの持つ秘密鍵が推定される可能性がある。

これらの攻撃可能性についてさまざまな対策法が提案されている。

TAP コントローラにロック／アンロック機能を持つ IC の利用で不必要なアクセスを制限することが可能である。図 5 の IC2 がロック／アンロック機能を持つ IC と想定すると，バウンダリスキャンセルへのアクセスは規定のパターンを与えることで始めて許可されるように設計されている。許可の認証に用いるパターンは固定のパスコード，LFSR (Linear Feedback Shift Register) による擬似乱数を用いるもの，PUF を用いるものなどが考案されている。擬似乱数発生器である LFSR を用いる認証法は，乱数のシード値と生成される乱数の正しいペアを与えることで認証される。LFSR の構造を知らないと正しいシードと乱数のペアを与えることができない。PUF による認証は 2 章で述べたように製造時に得られる IC 個別の固有値を与えることで行われる。

入出力パターンの保護に関しては，チップに供給するパターンに圧縮展開や暗号化を施すことで内部回路の推定を困難としたり，バウンダリスキャンチェーンのデバイスの接続順序を考慮したり，複数に分割し，特定動作時に他のデバイスを経由しないチェーン構成を設計するなどの対処法が挙げられる。また，チェーン内の BSR の段数が固定であると入出力の対応が推測されてしまうため，チップ内部のバウンダリスキャン回路に IEEE1687 規格の IJTAG (Internal JTAG) の RSN (Reconfigurable Scan Network) を用いることでレジスタ長を可変とする手法がある。図 6 に示すようにチップ内の 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，テスト時のバウンダリスキャン構成を変更可能としている。これらの対策がなされた IC を適切に接続することでバウンダリスキャンをより安全に用いることが可能である。

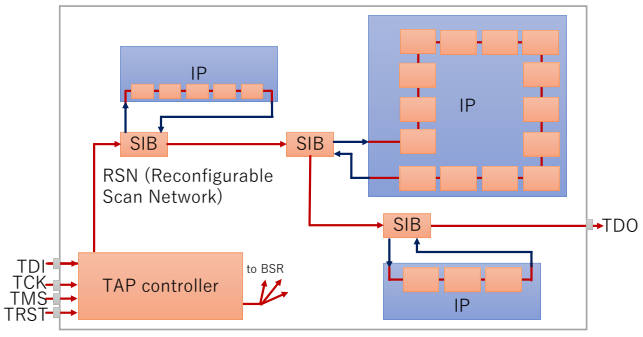

図 6.　IJTAG による可変長のバウンダリスキャン構成

4.　まとめ

IC 間の接続テストに用いられるバウンダリスキャン設計は，近年課題となっている実装部品の偽造防止にも適用可能である。本稿では，偽造 IC などによる攻撃に関する対策についても述べた。回路の機密情報の保持や安全性を担保した上で，出荷後テストにも活用できるテスト容易化設計としてバウンダリスキャンの普及がこれからも進んでゆくことが期待される。

文責・四柳浩之／徳島大学

（2020.10.15- 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) 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
3) K. Rosenfeld and R. Karri: “Attacks and Defenses for JTAG,” IEEE Design & Test of Computers, Vol. **27**, No. 1, pp. 36–47, Jan. 2010
4) 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

† 用語解説

スキャン設計：回路内部のフリップフロップをテスト時にチェーン状に接続しシフトレジスタを構成できるようにしたスキャンフリップフロップに置き換えることで，内部状態の制御・観測を容易とするテスト容易化設計手法

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。