JTAG とセキュア

はじめに

PC をはじめとする各種電子機器が普及するとともに、最近では、情報セキュリティについての問題も多く取り上げられるようになってきました。

また、セキュリティに関する危機感と関心を寄せる技術者の方も増えてきているかと思います。

技術的な分野で使われている「セキュア」という意味の定義は、「暗号技術を用いた」 あるいは 「技術的に安全性が保証された」 という意味になることが多いようです。

基板の検査からデバッグまでの幅広い用途に有効な JTAG バウンダリスキャン・テストですが、セキュリティという面に対してはどうなのでしょうか？

ここでは JTAG の「セキュア」という点について、話題に触れてみたいと思います。

JTAG アクセスによる解析

JTAG 機能を使用した Flash メモリや cPLD に対するオンボード・プログラミング・ツールは、バウンダリスキャン・デバイスによって、接続先のデバイスの各端子を制御することで、その機能を実現しています。

これらのオンボード・プログラミングを行うためには、基板上にコネクタやテストパッドなどを設け、TAP 信号を引き出すことによって、バウンダリスキャン・デバイスの制御が可能です。

また、JTAG 方式のデバッガ(インサーキット・エミュレータ)などでも、この TAP 信号用コネクタが基板上に配置されることが多いようです。 (図１．参照)

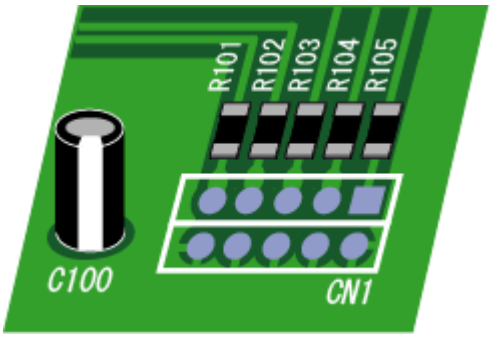

図 1. 基板上の TAP の接続例(コネクタ使用)

JTAG 方式デバッガや cPLD プログラミング・ツールのコネクタ形状やピン・アサインは各社各様ですが、これらも各ツールの情報として一般公開されています。

そのため、これらのコネクタやテストパッドの存在により、TAP 信号の各接続箇所が判明してしまい、誰でも外部からアクセスすることが可能になってしまいます。

基板上の Flash メモリなどの ROM に対してセキュリティをかけていたとしても、このような TAP 信号の不正アクセスによって解析ができてしまう点は問題です。

では、基板上にこのようなテストパッドやコネクタを設けない場合は、いかがでしょうか？

図 2 は極端なケースですが、TAP 信号をアクセスするためにフラットパッケージのピンを切断し、配線にて外部に信号を引き出した例です。

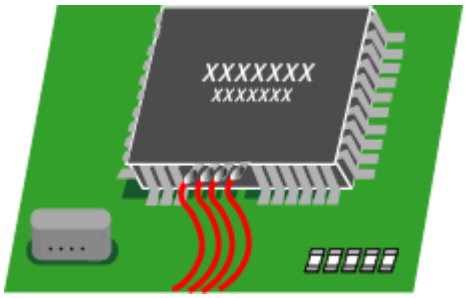

図 2. TAP をアクセスするための改造例

TAP 信号をアクセスさせないために、基板上にコネクタやテストパッドを配置しないとしても、このような不正な配線をすることでアクセスが可能になってしまうようであれば、セキュアという点で問題があります。

JTAG セキュアのための対策

では、セキュアを行うためには、どんな手段があるのでしょうか？

次にいくつかの対策案を挙げてみます。

ーお問い合わせー
アンドールシステムサポート株式会社
システムセールス＆エンジニアリング部
JTAG ソリューションセンター
Tel: 03-3450-7201 E-mail; jtag@andor.jp

(1)デバイスのパッケージでの工夫

前述のようなフラットパッケージやその他のピンが基板外に露出しているパッケージ（SOP、DIP、PGA･･･）では配線による加工が可能です。
そのため、BGA(Ball Grid Array)や CSP(Chip Size Package)などのパッケージ下にピンがあり、基板外から接触できないようなパッケージを選ぶことが有効です。

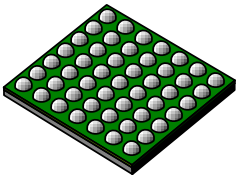

図 3. BGA パッケージのデバイス例

(2)テストピンによる機能制限の利用

バウンダリスキャン・デバイスには、特定のピンに対して特定の固定値を与えないとバウンダリスキャン機能が動作しないというデバイスが多くあります。
このようなピンをテストパッドなどとして基板上に配置し、TAP 信号を使用する際に固定値を与えるようにします。
TAP 信号のコネクタやテストパッドから離れた位置に配置することで、解析され難くすることが可能です。

(3)TAP 回路の分断

TAP 信号の接続箇所を 0Ω抵抗の実装/非実装で接続/分断できるようにしておく方法も有効です。

図 4. 0Ω抵抗の有効利用

デバイスのスキャンチェーン内の TDI と TDO 部分に 0Ω抵抗を実装することで、TAP 信号のアクセスをできるようにしておくと有効です。

基板の量産時には余分な部品はコストにつながるため、非実装としておくかたちになるかと思います。
また、抵抗のパターンなどより接続先を解析されやすいと思いますので、その点の配慮が必要かと思います。

(4)スキャンチェーンの結合

前述の「テストピンによる機能制限の利用」で説明したようなデバイスをスキャンチェーン内に配置する方法も有効です。

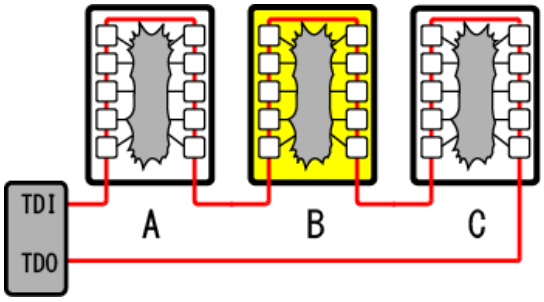

図 5. スキャンチェーンの結合

図 5 では、B の黄色で記したデバイスがバウンダリスキャン機能を動作させるためにピン処理が必要なデバイスを意味しています。
この B デバイスのピン処理がされていないとスキャンチェーン内に配置されている A と C のデバイスのアクセスができなくなります。

(5)cPLD を利用した TAP 切替回路

cPLD の内部回路で TAP 信号の切り替えを実現するという方法も有効です。

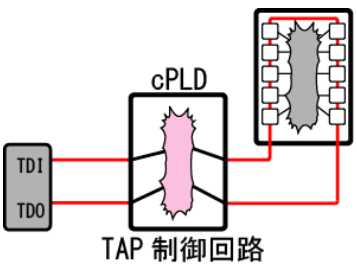

図 6. cPLD0 を利用した TAP 制御回路

ーお問い合わせー
アンドールシステムサポート株式会社
システムセールス&エンジニアリング部
JTAG ソリューションセンター
Tel: 03-3450-7201 E-mail; jtag@andor.jp

バウンダリスキャン対応 cPLD の I/O 端子に TDI 信号と TDO 信号を接続し、cPLD の内部回路で TAP 信号のアクセスを可能にするといった方法です。

量産時には、cPLD にプログラミングする回路を変更することで TAP を無効化する(もしくは、デバッグをしたい際だけ TAP を有効化する)といった制御が可能です。

デバイス・ベンダの取り組み

無権限のプログラム実行や解析などに JTAG を使われないための手段として、Freescale 社では「SJC(Secure JTAG Controller)」としてセキュア JTAG の仕組みを確立しており、i.MX デバイスなどで採用しています。

また、デバイス・ベンダ各社でもこれらのセキュアの点での研究・開発を進めているようです。

まとめ

ゲーム機器や車関連などでは、セキュア(安全性が確保された状態のこと)が重視され、場合によっては量産時にデバイスから JTAG 機能まで外されるというケースもあるようです。

デバイスのピンを簡単にアクセスすることができるバウンダリスキャンですが、これらのセキュリティ面の考慮が必要不可欠ではないかと思います。

<山田 実>

ーお問い合わせー
アンドールシステムサポート株式会社
システムセールス＆エンジニアリング部
JTAG ソリューションセンター
Tel: 03-3450-7201 E-mail; jtag@andor.jp