論　文

セキュアな組込みシステムの構築法

入月　康晴*　　大原　衛*　　坂巻　佳壽美*

An Approach for Improving Security of Embedded Systems

Yasuharu Irizuki*,　Mamoru Ohara*,　Kazumi Sakamaki*

Embedded systems are indispensable existence for home electronics and all industrial equipment appliances. Recently, rapidly growing numbers of embedded systems are connected to the networks. Thus we must to consider the security of such networked embedded systems. We assume the embedded system is constructed with an FPGA (Field Programmable Gate Array), which is a rewritable integrated circuit chip. We propose effective techniques for the improvement of security and safety, based on study results of an embedded system that uses an existing FPGA. Based on existing study results for improved embedded system security, it was thought that two aspects were required: improved information privacy, and prevention of system malfunctioning Techniques were examined for preventing system malfunction and improved information secrecy. We set four problems, and did development produced a demonstration machine for trial purposes.

キーワード：組込みシステム，セキュリティ, FPGA, JTAG, バウンダリスキャンテスト，マルチ CPU システム
Keywords：Embedded systems, Security, FPGA, JTAG, Boundary-Scan Test, Multi-CPU system

1. まえがき

組込みシステムは家電製品をはじめ産業用機器等に欠かせない存在となっており，近年ネットワークに接続される組込み機器が急速に増加している。また，コンピュータソフトウェアメーカ同様，組込み機器メーカもネットワークを介した攻撃による機器のトラブルにより，製造物責任法（PL 法）の観点から責任を問われる可能性も出てきている。そこで組込みシステムの製品開発においては，安心・安全の確保やネットワークを介した外部からの攻撃に対する防護手段などが必要不可欠となっている。

本研究は，書き換え可能な IC チップである FPGA (Field Programmable Gate Array)を用いた組込みシステムを対象とするセキュアな組込みシステムの構築法である。当センターにおけるこれまでの研究成果[(1)-(5)]を踏まえ，「安心・安全性の確保」と「ネットワークを介した外部からの攻撃に対する防護」などに対する効果的な対策手法を提案・開発することで，セキュリティの向上を図った。組込みシステムのセキュリティ向上のためには，システムの誤動作の防止と情報の機密性の向上の２つの観点が必要である。

本研究ではこれらの観点に基づき，４つの具体的課題を提案し，セキュアな組込みシステムの構築を行い，デモ機の試作を行った。

*情報技術グループ

2. システム構築の方針

2.1 セキュリティ向上のための４手法の位置づけ　システムの誤動作は，システム内部への不正アクセス等による要因で引き起こされるものと，プロセッサ外部への出力等の異常による要因で引き起こされるものとが考えられる。そこでシステムの誤動作防止の手法として，プロセッサの内部に施すものと外部に施すものとに分けることを考えた。プロセッサ内部での誤動作防止としては，未使用アドレスへの不正アクセスの監視手法を提案する。また，プロセッサ外部での誤動作防止としては，JTAG (Joint Test Action Group)を用いて組込みシステムの入出力に異常がないかを監視する手法を提案する。

情報の機密性の向上についても同様に，システム内部で用いられている知的財産の機密性（作成プログラム，チューニングパラメータ，内部設定パラメータ）の向上とシステム外部でのネットワークにおける機密性の向上に分けて考える。組込みシステム内部での機密性の向上手法としては，暗号化通信のハードウェア化手法および，システム外部においては，リアルタイム OS の一部をハードウェア化することによる通信の自動暗号化，復号化手法を適用することを提案する。

本研究で取り組んだセキュリティ向上の４手法の位置づけを図１に示す。

図 1 では，セキュリティ向上のための４手法を FPGA 上に実現することを示しており，①「誤動作検知機能を持っ

たマイコン」がプロセッサ内部の誤動作防止機能を，②「JTAG 手法による自己監視制御」がプロセッサ外部の誤動作防止機能を，③「リアルタイム OS によるセキュア化」が，システム内部での機密性向上機能を，④「セキュリティ対策」がインターネット等のシステム外部における機密性向上機能を果たしている。

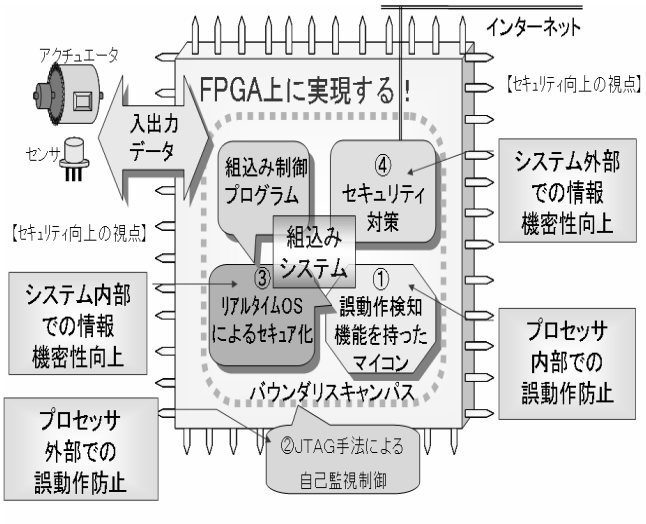

図１． セキュリティ向上の４手法

2.2 JTAG の利用　JTAG (Joint Test Action Group)[6] とは，IC チップの検査方式の一つであるバウンダリスキャンテストの標準方式を定めた団体のことであり，その規格の通称でもある。バウンダリスキャンテストは，JTAG を用いてプローブテストと同様の挙動確認を行なうことのできるテスト法である。図２に示すように，IC チップ内部にバウンダリスキャンセルがあらかじめ配置されている。これらのセルがテストプローブと同様の働きをしており，外部からこれらのセルにテストパターンを入力し，その入力に対して想定される出力に問題が無いかを確認するテスト法である。JTAG 方式のテストシステムは，FPGA のほとんどに内蔵されていて，IC チップ製造時の検査や基板実装後の検査などに利用されている。

スキャンセルは，IC のピンごとに設けられるため，FPGA は非常に多数のスキャンセルを備える。JTAG では，多数のセルを最低限のテスト用ピンで読み書きするために，すべてのスキャンセルは直列に接続され，シフトレジスタとして扱われる。このため，JTAG 方式を用いてすべてのピンの信号値を読み出すためには，セル数分のスキャンクロックをレジスタに入力する必要がある。

JTAG テストには，ノーマルモードとテストモードの二つの動作モードがある。ノーマルモード動作では，バウンダリスキャンセルの存在はデバイスに意識されないため，デバイスは通常動作をする。デバイスのピンを通過するデータを，デバイスの動作に影響を与えないで任意のタイミングで取り込むことができる。また，取り込んだデータは，JTAG コントローラで受け取って JTAG コントローラに接続されているホストコンピュータで解析し，デバイスの動作状況を観測することができる。テストモード動作は，デバイス内部ロジックを外部と切り離すため，デバイス外部との入出力が本質的にできなくなる。したがってテスト信号だけがバウンダリスキャンセルから与えられることになる。IC チップ製造時の検査や基板実装後の検査などにはこのテストモード動作が主として使われている。

本研究では， CPU 稼働時に JTAG テストのノーマルモードを利用して，内部状態の監視を行うことを提案する。つまり, CPU 稼働時にも FPGA から入出力される信号を, JTAG のバウンダリスキャンパスを経由して読み書きができることを利用している。異常な動作を検知した場合には，バウンダリスキャンパスを活用して FPGA の入出力を停止させることで，システムの強制停止を行い，対応することにした。

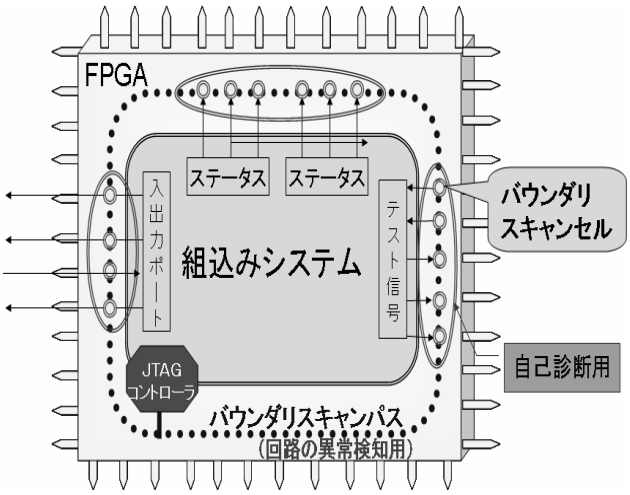

図２． JTAG のバウンダリスキャンパス

3. 開発手法

①誤動作検知機能を持ったマイコン

プロセッサ内部の誤動作を検知するために，図３に示すように CPU とメモリ，入出力装置等を接続する内部バス上にバス監視モジュールを追加して，内部信号の異常監視を行った。FPGA 上には，組込みシステムのアプリケーション用 CPU と監視用 CPU の２つの CPU を載せており，アプリケーション用 CPU 側が問題なく動作しているかを監視用 CPU 側のウォッチドックタイマでチェックしている。異常をバス監視モジュールで検知した場合は，バウンダリスキャンパス経由で監視用 CPU に異常を通知し，アプリケーション用 CPU を停止させる機能を付加した。

未使用アドレスへの不正アクセス検出のチェックとしては，正常動作時はある範囲内のアドレスしかアクセスしないので，未使用アドレスへのアクセスは不正アクセスとなる。未使用アドレスに関するバス監視モジュールを設定し，不正アクセスが検出されたら，バウンダリスキャンパス経由で監視用 CPU に知らせ，アプリケーショ

ン用 CPU を停止させる機能を実現する。

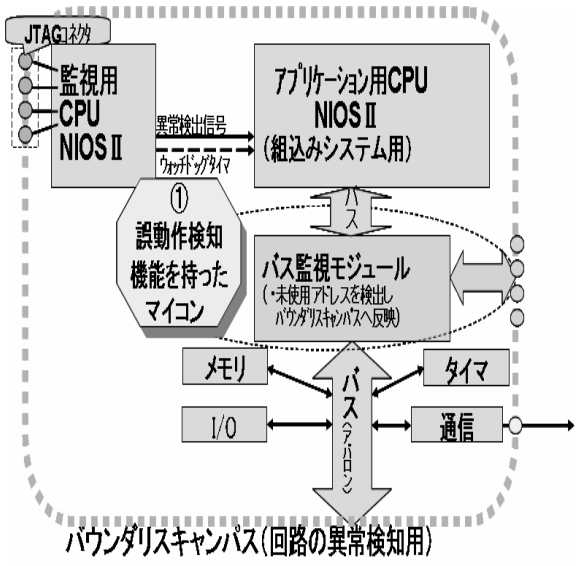

図３． 誤動作検知機能を持ったマイコン

②JTAG 手法による自己監視制御

JTAG 手法による自己監視制御としては，組込みシステムの動作状況の監視にあたり，FPGA 製品検査用の JTAG 手法を用いることを提案する。これは CPU 稼働時に JTAG テストのノーマルモードを利用して，内部状態のリアルタイム監視に用いるものである。CPU 稼働時にも FPGA から入出力される信号を，JTAG のバウンダリスキャンパスを経由して読み書きができることを利用する手法として提案するものである。

プロセッサ内部の誤動作検知機能としては，①のバス監視モジュールを用いて異常を検出し，その後，バウンダリスキャンパス経由で監視用 CPU にて異常を検知し，アプリケーション用 CPU を停止させる。このバウンダリスキャンパス経由で監視用 CPU にて異常を検知する部分に JTAG 手法による自己監視制御を用いている。

③リアルタイム OS のハードウェア化によるセキュア化，および④セキュリティ対策

リアルタイム OS のハードウェア化によるセキュア化としては，システム内部（特に知的財産部分）の機密性向上と，セキュリティ対策としては，インターネット等のシステム外部における機密性向上のための暗号化とハードウェア化について検討した。ネットワーク上の信号を暗号化するにあたっては，アメリカ政府の推奨している暗号化規格 AES （Advanced Encryption Standard）で暗号化するモジュールを作成した。また TCP/IP 通信用のプロトコルのシステムコールのハードウェア化を行った。

命令の流れは，図４で示すように，ユーザープログラムがリアルタイム OS の通信機能のシステムコールを発行し，新規ユーザ定義命令により，実装された暗号化モジュールを操作することで暗号化した信号を送信する。

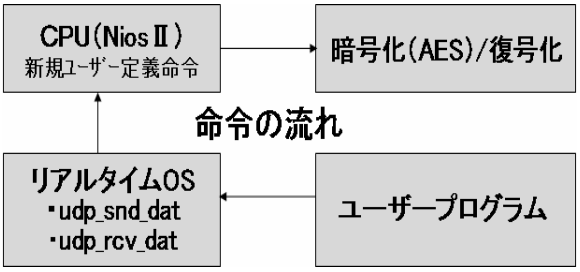

図４． ネットワーク通信命令の流れ

図５は各手法の全体構成を示したもので，バス監視モジュールや入力信号からの異常値を監視用 CPU で検出し，アプリケーション用 CPU をより安全側に停止させることを行っている。

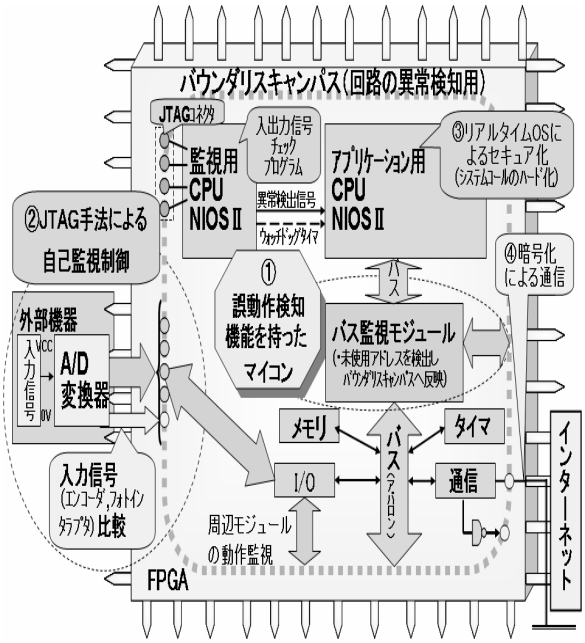

図５． 開発手法の全体構成

4. デモ機の実装

図６にデモ機の概要図を示す。入力装置は RFID カードを用い，本体は FPGA，出力装置はモータで構成し，データ伝送の状況を，ラインモニタで表示し，暗号化／非暗号化信号を同時に表示する。RFID カードから暗証番号を暗号化して送信しラインモニタで表示するようにしている。回転 LED 表示は，常時経過時間を表示するようになっており，RFID 側エラースイッチを押すと入力異常が発生し，異常検出すると回転 LED を点灯した状態でモータが停止するようになっている。回転 LED はダイナミック点灯となっているため，モータが停止した際，LED 点灯を継続すると LED が焼き切れる問題がある。そこで，LED が焼き切れないようにするため，監視用 CPU でモータの停止を監視し，モータが停止した場合は LED を消灯させるようにしている。

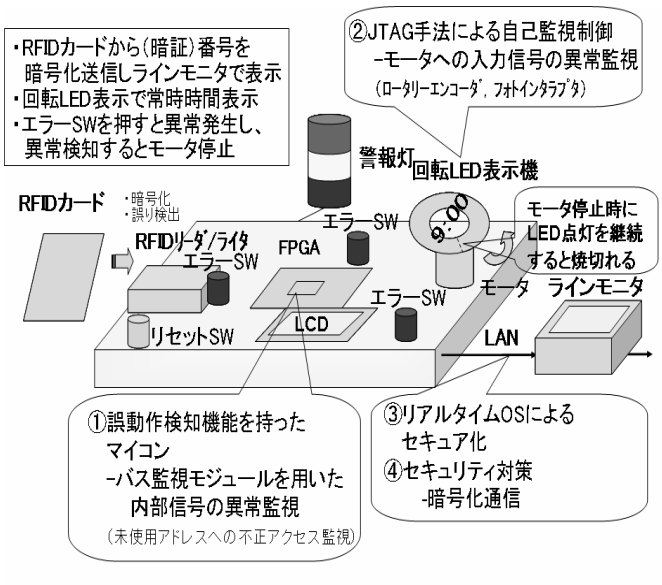

図６． デモ機の概要図

図６の①では，FPGA 側エラースイッチを押すと，未使用アドレスへの不正アクセスが発生する。その異常をバス監視モジュールで検知し異常信号を出力する。監視用 CPU はバウンダリスキャンパス経由で異常信号を検知し，アプリケーション用 CPU を停止し復帰するようになっている。また，検知にかかる時間について実測した。スキャンクロックが 0.1MHz でバウンダリスキャンセルが 1500 程度あるため，おおよそ１回の検知にかかる時間は，17ms であった。②では，モータ側エラースイッチを押すと，モータからの入力信号であるロータリエンコーダ値が検出できなくなり，異常信号をバウンダリスキャンパスへ送信する。監視用 CPU でバウンダリスキャンパス上の異常を検出することにより，アプリケーション用 CPU を停止させるようにしている。また，③，④に関しては，前述のラインモニタで信号を表示し，暗号化／非暗号化信号を同時に表示するデモを行っている。

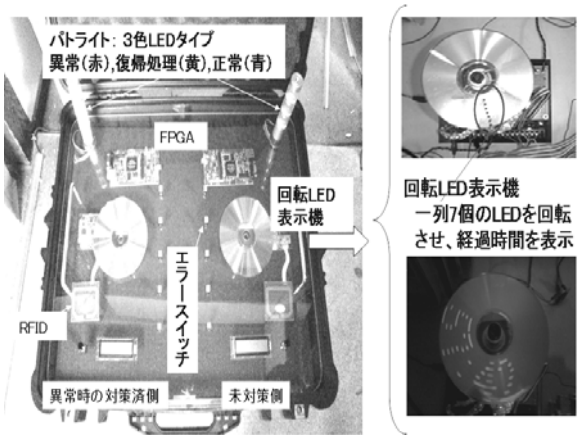

図７． デモ機本体

図７のデモ機本体は，図６の概要図に基づき RFID リーダライタ，FPGA，モータ，パトライト等で構成し，表面はアクリル板で覆っている。同じシステムを２系統つくり，一方に今回開発した各種手法を施してある。両者の動作を比較することにより，それぞれの手法の有効性を容易に比較できるようになっている。パトライトは３色 LED で，異常時は赤，復帰処理中は黄，正常時は青と，それぞれの状態を色で示すことにより，現在どの状態にあるのかを効果的に示すことができる。回転 LED 表示機は，一列７個の LED で構成し，これを回転させることで経過時間を表示するようにしている。

5. まとめ

本研究では，システムのセキュリティ向上の手法として，システムの誤動作の防止と情報の機密性の向上の２つの観点で検討した。その観点に基づき，各手法をデモ機に実装した結果，プロセッサ内部の誤動作検知のための手法とプロセッサ外部の誤動作検知機能としての JTAG テスト手法を基にリアルタイムで自己監視する手法が確立できた。また，システム外部における情報通信の機密性の向上のため，通信を自動的に暗号化する手法と，システム内部での知的財産の機密性の向上のため，暗号化モジュールを操作するためのシステムコールをハードウェア化して通信する手法が確立できた。

組込みシステムの「安心・安全性の確保」の向上に寄与する手法を開発できた。FPGA 製品検査用の JTAG をリアルタイムで自己監視できる手法として確立し，セキュリティの向上に繋がった。FPGA 内で２つの CPU を用い，アプリケーション用 CPU とは別に監視用 CPU を設定することで，監視に対する信頼性の向上に繋がった。また，開発した成果をデモ機として集約し示すことができた。

今後，本手法をベースに「安心・安全性」を確保しながら FPGA を遠隔で再構成できる仕組み作りへの取り組みを行う。

(平成 20 年 7 月 4 日受付，平成 20 年 8 月 27 日再受付)

文　　献

(１)武田有志: 制御プログラムからのリアルタイムプロセッサ生成方式,東京都立産業技術研究所 研究報告 No.8, pp.59-62 (2005)
(２)森久直: リアルタイム OS の FPGA による実現, FPGA コンソーシアム 第 10 回 6 都市 FPGA カンファレンス 2007, pp.79-103 (2007)
(３)坂巻佳壽美: パターンマッチング回路の高速化とフィルタリング装置への応用, 関東経済産業局平成 16･17 年度地域新生コンソーシアム研究開発事業性か報告書（2006）
(４)東京都立工業技術センター: 技術ガイド「マイコン応用システムの高信頼化技術」(1996)
(５)大原衛: 組込み機器のためのソフトウェアによるスタック破壊攻撃検出法に関する一考察, 20 回秋季信頼性シンポジウム, pp. 115-2118 (2007)
(６)坂巻佳壽美, 「JTAG テストの基礎と応用」CQ 出版社, (1998)