# 仕　様　書

1. 件名:ユニバーサルセンサのFPGA実装作業

2.研究の概要

国立研究開発法人産業技術総合研究所（以下、「産総研」という。）サイバーフィジカルセキュリティ研究部門では、新エネルギー・産業技術総合開発機構（NEDO）委託事業「経済安全保障重要技術育成プログラム／先進的サイバー防御機能・分析能力強化／サイバー空間の状況把握・防御技術の向上及び共通基盤の整備」における研究課題「耐タンパー性向上技術」に取り組んでいる。このうちの具体的研究項目［5］-①-1「ユニバーサルデジタルセンサーの研究開発」における取り組みとして、FPGA 上に構築可能なユニバーサルデジタルセンサの研究開発を行っている。これまでの取り組みでFPGAで利用可能なセンサの選定を行っており、これらのセンサの攻撃検知性能およびオーバヘッドを評価することが今後の目標である。これにあたり、本作業においては 7 種類の異なる方式のセンサを2種類のFPGAに実装する。

3.作業の概要

産総研は遅延変化からICの環境を観測する7種類のフォールトセンサの選定をしており、本作業ではこれらのセンサの単体性能を評価するために 2 種類のFPGA(SRAM型/Flash型)に7種類のセンサを個別に単体で実装する。実装するセンサは回路合成時に 1 種類選択し、他の異なる種類のセンサは同時に実装しない。

図 3.1 にFPGAに実装する回路の基本構成を示す。実装する回路はUART制御部、暗号コア部、センサ部の3要素から成っており、PC上からPythonスクリプトを使ってUART経由で暗号コアおよびセンサを制御する構成となっている。

センサはICのPVT環境を計測し、デジタル値として出力する。計測値が設定した閾値を超えた際にアラーム信号を有効にする。センサの計測値およびアラームは外部ピンに出力される。

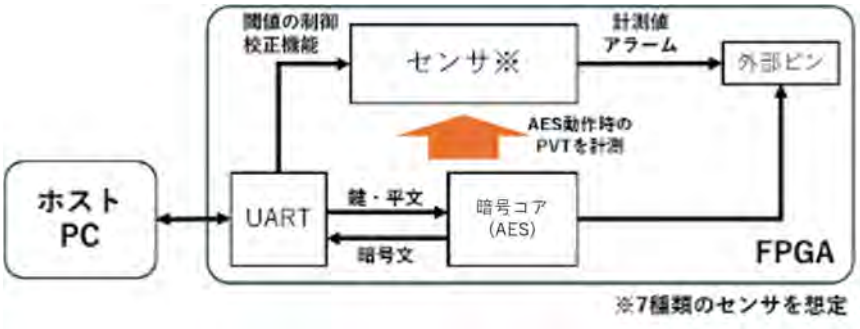


図 3.1 実装する回路の基本構成

4. 作業の構成

4-1:センサ実装作業

4-2:マニュアル作成作業

5. 構成別仕様

5-1: センサ実装作業

5-1-1:実装先のデバイスは産総研が貸与する SRAM 型 FPGA および Flash 型 FPGA（以下、「対象ボード 1」および「対象ボード 2」とする。）とすること。受注者が同一製品を用意できる場合にはそれらを使用してもよい。

5-1-2:対象ボード 1 および対象ボード 2 には産総研が用意する 7 種類のセンサを実装すること。2 種類はデバイス固有のオンチップアナログセンサであり、残りの 5 種類は LUT・FF・キャリーロジックを利用した遅延ベースのセンサである。センサの詳細は別紙 1 を参照のこと。

5-1-3:回路合成時に実装するセンサを選択できるようにすること。

5-1-4:UART を介してセンサの校正および閾値の制御が行えるように実装すること。

5-1-5:実装作業にあたり、産総研が貸与するソースコードにセンサ回路を追加し、対象ボード 1 および対象ボード 2 上へ実装すること。

5-1-6:制御用の Python スクリプトを利用し、暗号コアおよびセンサの動作確認を行うこと。

5-1-7:センサ実装の際には、対象ボード 1 および対象ボード 2 においてそれぞれで利用可能なキャリー専用ロジックを効率的に利用した実装を含めること。

5-1-8:センサはすべて単体で実装し、複数種類のセンサを 2 つ以上配置しないこと。

5-1-9:上記で実装したソースコードを納入すること。

5-2:マニュアル作成作業

5-2-1:5-1 で実装したソースコードの利用方法についてのマニュアルを作成し、納入すること。

6.貸与品

6-1:対象ボード 1（TROCHE 社製、型番：SAKURA-X）1 個

6-2:対象ボード 2（Aries Embedded 社製、型番：M100PF-1AC）1 個

6-3:ソースコード（暗号コア部および UART 制御部のソースコード）　一式

6-4:制御用 Python スクリプト　一式

※6-1、6-2 は郵送にて貸与、6-3、6-4 はメール等の電子的手段で貸与する。

7.出荷前検査

受注者は、納入に先立って、自己の標準的な検査項目に準じて出荷前検査を実施し、仕様書を満たしていることを確認した上で、その結果を動作検証報告書として提出すること。

8.納入物品

8-1:センサを実装した対象ボード 1 および対象ボード 2　各 1 個

8-2:ソースコード（電子媒体）　一式
（プロジェクトファイル・コンパイル済みビットストリーム等含む）

8-3:マニュアル（電子媒体）　1 部

8-4:動作検証報告書（電子媒体）　1 部

※電子媒体は原則としてメール・ファイル転送サービスなどの電子的手段で納入すること。

9.納入場所

東京都江東区青海 2-3-26
国立研究開発法人産業技術総合研究所
サイバーフィジカルセキュリティ研究部門
臨海副都心センター本館 1 階 1110 室

10.納入の完了

本件は「8.納入物品」に記載された納入物品が過不足なく納入され、仕様書を満たしていることを確認して、納入の完了とする。

11.納入期限

2026 年 1 月 30 日（金）

12.付帯事項

12-1:本仕様書の技術的内容及び知り得た情報については、守秘義務を負うものとする。

12-2:本仕様書の技術的内容に関する質問等については、調達請求者と協議すること。また、本仕様書に定めのない事項及び疑義が生じた場合は、調達担当者と協議のうえ決定する。

12-3:本業務に起因する不具合等に関しては、原因究明に関し、納入の完了後1年間は無償で対応を行うこと。

12-4:サプライチェーン・リスクに対応するため、別紙2に記載する事項に従って契約を履行しなければならない。

13.セキュリティ要件

13-1:情報セキュリティポリシーに関する要件

①本業務の遂行に当たっては、産総研の情報セキュリティポリシー(別途定める読み替え条項に従うものとする。以下同じ。)を遵守するとともに、情報セキュリティポリシーにおいて産総研に求められる水準の情報セキュリティ対策を講じること。産総研の情報セキュリティ規程については、下記URLを参照のこと。その他の情報セキュリティポリシーの詳細については受注者決定後に提示する。

【国立研究開発法人産業技術総合研究所情報セキュリティ規程】
https://www.aist.go.jp/Portals/0/resource_images/aist_j/outline/comp-legal/pdf/securitykitei.pdf

②産総研の情報セキュリティポリシーの見直しが行われた場合は、見直しの内容に応じた情報セキュリティ対策を講じること。なお、対応内容については調達請求者に事前に報告し承認を得ること。

13-2:その他セキュリティに関する事項

①受注者は、本業務の履行に際して、秘密である旨を示されて貸与を受けた秘密情報を秘密として適切に保持することとし、第三者に開示又は漏洩してはならない。

②受注者は、本業務の履行によって知った一切の情報を本業務の履行以外の目的に利用してはならない。契約終了後も同様とする。

③貸与品は調達請求者の了解なしに所外に持ち出しまたは複製してはならない。

# センサ仕様書

## 1. はじめに

本資料は「ユニバーサルセンサの FPGA 実装作業」に関する補足資料であり、実装する 7 種類のセンサの仕様についてまとめたものである。

## 2. 実装する回路の基本構成

図 2.1 に FPGA に実装する回路の基本構成を示す。回路は暗号回路 x1，UART 回路 x1，センサ回路 x1 で構成される。回路は UART を介してホスト PC と接続され、ホスト PC から受信した平文を鍵で暗号化し、暗号文をホスト PC に送信する。なお、AES 回路・UART 回路については AIST からソースコードを提供する。センサは暗号回路に 1 つのインスタンスを実装する。

センサは IC の PVT 環境を計測し、デジタル値として出力する．センサは計測した値が閾値を超えた際にアラーム信号を有効にする。センサの計測値とアラーム信号は FPGA の外部ピンから出力する。また,センサの閾値は UART を介してホスト PC 側から閾値の設定や校正を行える機能を実装すること。暗号回路は FPGA ダイの中央部に実装し，センサはその周辺に配置する。

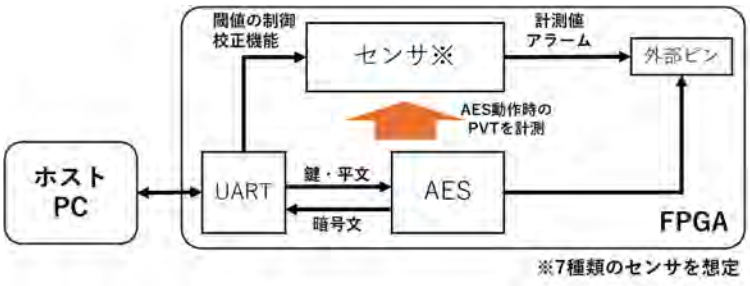


**図 2.1 実装する回路の基本構成**

以下は今回実装を依頼する 7 種類のセンサである．各センサの仕様については 3 章を参照のこと。

・Time-to-Digital Converter(TDC)[1]
・カウンタ方式 RO センサ(CRO)[2]
・Fault-to-Time Converter(FTC)[3]
・1LUT Sensor (1LUT)[4]
・Tunable Replica Circuit(TRC)[5]
・デバイス固有の電源センサ(XADC/VTS)[6][7]

# 3. センサ仕様

本章では 7 種類のセンサの仕様について説明する。

## 3.1. TDC(Time-to-Digital Converter)[1]

図 3.1.1 に TDC センサのアーキテクチャを示す。TDC は$n_0$個のバッファで構成される Initial Delay Line(IDL)と$n_1$個のバッファで構成される Tapped Delay Line(TDL)からなる。TDL は加算器用のキャリーロジック（Kintex-7 では CARRY4、Polarfire ではキャリーチェーン）と Flip-Flop(FF)を使用して実装する。IDL はクロック周期の N/2 周期分の遅延を挿入し、TDL の$\frac{n_1}{2}$番目の FF においてクロックのエッジがサンプリングされるように調整する。

電源電圧が変動すると IDL のバッファにおける遅延量も合わせて変動し、TDL にてサンプリングされるエッジの位置が変化する。電源電圧が低下すると遅延量が増加しサンプリング時にエッジが$\frac{n_1}{2}$番目以前の FF でエッジがサンプリングされる。逆に電源電圧が上昇すると遅延量が減少しサンプリング時に$\frac{n_1}{2}$番目以降の FF でエッジがサンプリングされる。

TDC の出力は過去 8 サイクル分の出力の平均値と比較され、その差分が事前に設定した閾値以上の場合にアラームを'1'にする。

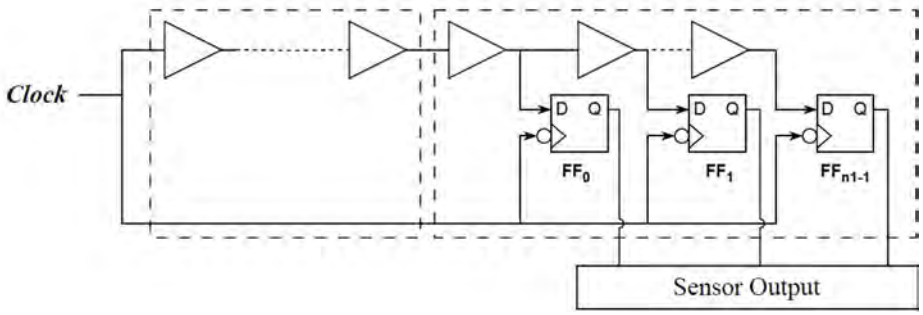


**図 3.1.1 TDC センサのアーキテクチャ**

・実装するセンサの仕様

・TDL：専用キャリーチェーンで構成

・IDL：直列に接続した LUT(BUF)で構成、クロック 1 周期分の遅延を挿入

・UART を介してセンサの閾値を制御できる機能を実装すること

## 3.2. カウンタ式 RO センサ(CRO) [2]

図 3.2.1 に CRO センサのアーキテクチャを示す。センサは 1 つのリングオシレータとカウンタで構成される。リングオシレータは NANDx1 をループ状に構成した回路である。カウンタ式 RO センサはクロック 1 周期分の期間における RO の発振回数をカウントすることで周波数を計測する．RO の発振周波数は電源電圧に比例して変動するため，RO の周波数をカウントすることで間接的に電源電圧を監視する。カウンタには加算回路ではなくリングカウンタもしくはジョンソンカウンタを使用する。カウンタの値はクロックでサンプリングした後に 10 進数の値にエンコードし、1 サイクル前の値と差分を取ることで発振周波数を得る。サンプリングされた周波数は予め設定された最大/最小閾値と比較され、閾値を超えた場合にアラームをトリガする。

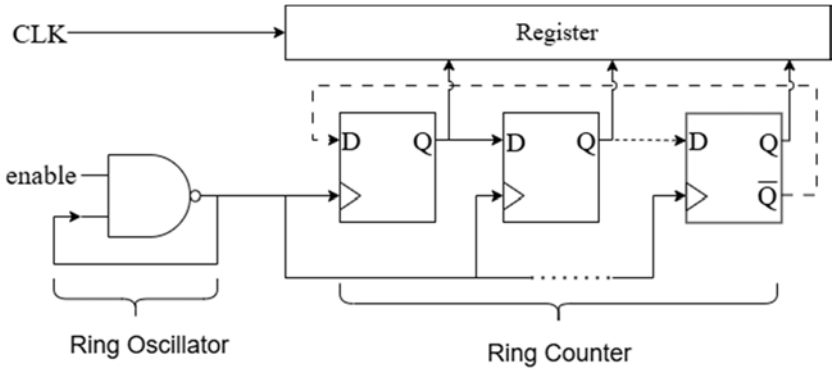


**図 3.2.1 CRO センサのアーキテクチャ**

・備考

・リングオシレータ：NANDx1 で構成

・カウンタにはジョンソンカウンタもしくはリングカウンタを使用すること

・UART 経由でホスト PC から閾値(上限/下限)を設定可能にする

・カウンタの値と閾値を毎サイクル比較し異常時にアラームを出力する

・クロックでサンプリングしたカウンタの値とアラームをピンに出力する

## 3.3. FTC(Fault-to-Time Converter) [3]

FTC は閾値電圧の異なる 2 種類のセル(HVT/LVT)を使用した 2 本の遅延線・ラッチ・FF・Bubble Proof Encoder で構成されるセンサである(図 3.3.1)。遅延線は初期遅延を挿入する IDL(Initial Delay Line)と、出力をタップした ODL(Observable Delay Line)で構成される。電源電圧が低下した場合は LVT 側よりも HVT 側の信号遅延が増加し、電源電圧が上昇した場合は HVT 側よりも LVT 側の信号遅延が減少する。この 2 本の遅延線の ODL の XOR から電源電圧変動を検知する。Bubble Proof Encoder は 2 本の遅延線の XOR において'1'となった最初と最後のビット位置を 10 進数の値に変換して出力する。FPGA は閾値電圧の異なるセルを利用できないため、HVT と LVT の遅延線を構成する LUT 数を変えることでこれを再現する。

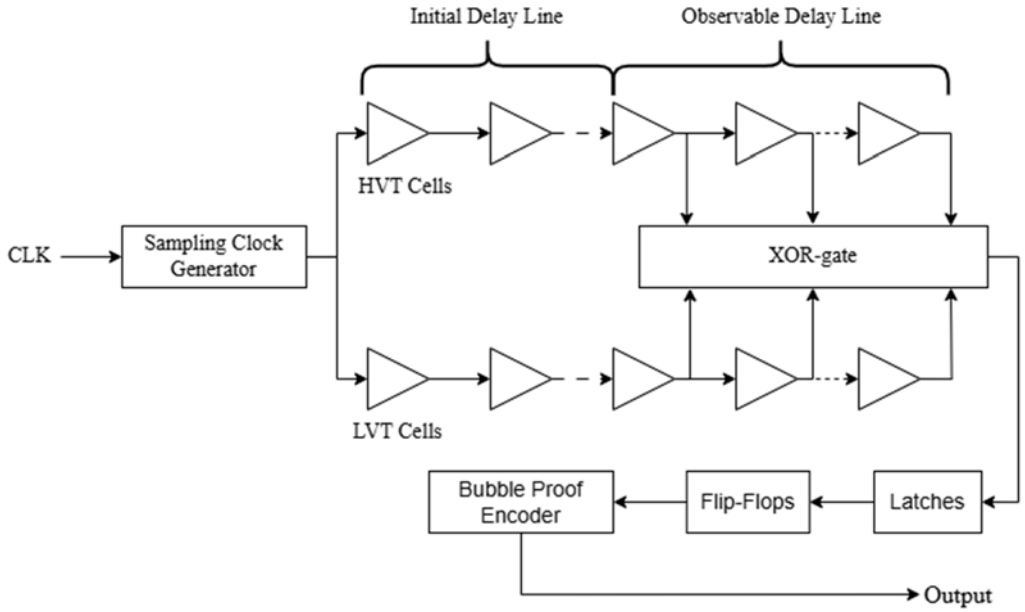


**図 3.3.1 FTC のアーキテクチャとセンサの出力**

・備考

・ODL：キャリーロジックで構成すること

・IDL：直列接続した LUT(BUF)で構成。LVT と HVT の LUT 数の比を 1:2 とすること

・IDL は HVT/LVT 共に遅延量がクロック半周期分となるよう LUT 数・配置を調整すること

## 3.4. 1LUT センサ[4]

1LUT センサは FPGA の単一の LUT を利用して電圧変動を計測する小型のオンチップ電圧センサであり、LUT の MUX を遅延線とした 1bit の TDC である。図 3.4.1 に 1LUT センサのアーキテクチャを示す。$\delta_{LUT}$は LUT の信号遅延量であり、供給される電源電圧に応じて変動する。Sensor Signal からはクロックが入力され、FF でサンプリングされる。$\delta_{CLK}$は遅延モジュールで挿入される遅延量であり、センサ校正時に適切な遅延量を設定する。

電圧が一定値以下まで低下すると、遅延量$\delta_{LUT}$の増加によりセットアップタイム違反が発生し、FF で 0 がサンプリングされる。1LUT センサはこのセットアップタイム違反が連続して発生した回数から消費電力波形を復元する。

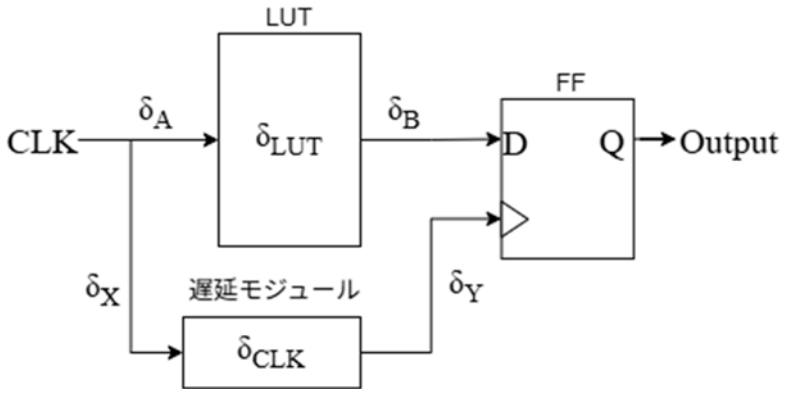


**図 3.4.1 1LUT センサのアーキテクチャ**

・備考

・論文の Appendix 記載の Xilinx 7series 用のソースコードが利用可能

・使用リソース： LUTx1, FF x1, 遅延モジュール※

※Kintex-7：IODELAY, Polarfire：DDC(Dynamic Delay Control)

・Sensor Signal にクロック信号を入力(600MHz を想定)

- システムクロック or 外部クロックを逓倍して使用

・UART 経由でホスト PC から遅延モジュールの遅延量$\delta_{CLK}$を制御する機能を実装する

・$\delta_A + \delta_{LUT} + \delta_B$と$\delta_X + \delta_{CLK} + \delta_Y$を以下の条件を満たすように調整

- 暗号コア非動作時には FF が'1'を記録する
- 暗号コア動作時に電圧が一定値まで低下した場合は FF が'0'を記録する
- FF が 0 を記録する電圧の閾値は遅延量$\delta_{CLK}$により変更できるようにする

## 3.5. Tunable Replica Circuit[5]

TRC(Tunable Replica Circuit)はクロックグリッチと電源グリッチを検知することを目的としたセンサである。図 3.5.1 は TRC のアーキテクチャである。このセンサは 2 つの FF と長さが制御できる遅延線(Tunable Delay Chain)、XOR ゲートで構成される。Tunable Delay Chain の長さは外部から制御可能であり、保護対象の回路のクリティカルパスの長さと同じ長さに設定される。

通常時の FF のサンプリングエッジでは tc_data_ref と tc_data_actual が同じ値となり、TRC Capture では 0 が記録される。外部からの攪乱により保護対象のクリティカルパスでセットアップタイム違反が発生するほど電源電圧が低下すると trc_data_actual の遅延量増加により TRC Capture FF でもセットアップタイム違反が発生して 1 が記録される。逆に外部からの攪乱によりオーバークロックが生じた場合も、TRC Capture FF でセットアップタイム違反が発生し 1 が記録される。

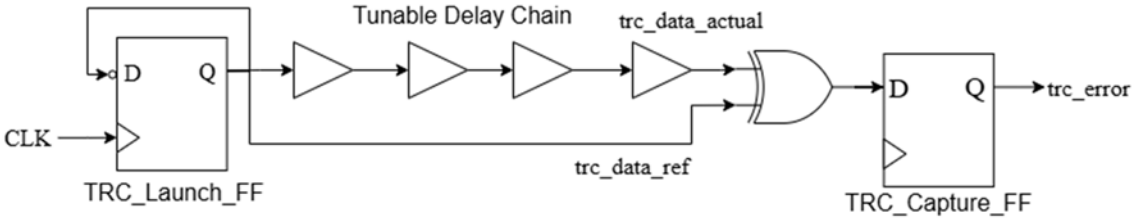


**図 3.5.1 センサのアーキテクチャ[5]**

備考：

・UART を介してホスト PC から Tunable Delay Chain を制御できるようにすること

・Tunable Delay Chain の長さは暗号コアのクリティカルパス以上の長さとすること

## 3.6. XADC[6]

XADC は Xilinx 製 FPGA で利用できる ADC であり、外部アナログ入力される信号の A/D 変換器と電源センサ・温度センサを持つ。今回は XADC を電圧センサとして使用する。電源センサは $V_{CCINT}$、$V_{CCAUX}$、$V_{CCBRAM}$ をモニタし、12bit の値で内部の 16bit ステータスレジスタ（アドレス:01h, 02h, 06h)に MSB 詰めで格納される。これらには DRP を介してアクセスできる。これらの値は予め XADC 内部の制御レジスタに格納された上限/下限の閾値と比較され、異常時にアラーム ALM がトリガされる。この制御レジスタは同様に DRP を介してアクセス可能であり、外部から閾値を設定することが可能である。各制御レジスタのアドレスと対応するアラームについては図 3.6.2 を参照のこと。その他詳細は参考文献[6]を参照のこと。

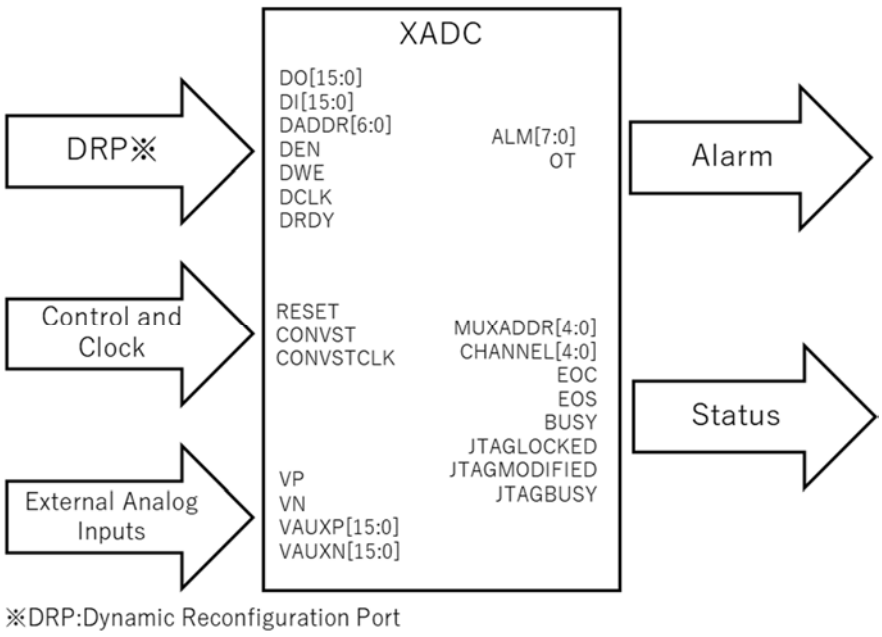


**図 3.6.1 XADC の入出力[6]**

| 閾値レジスタアドレス | 説明 | 対応するアラーム |
|---|---|---|
| 50h | 温度上限 | ALM[0] |
| 51h | $V_{CCINT}$上限 | ALM[1] |
| 52h | $V_{CCAUX}$上限 | ALM[2] |
| 53h | OT アラームリミット | OT |
| 54h | 温度下限 | ALM[0] |
| 55h | $V_{CCINT}$下限 | ALM[1] |
| 56h | $V_{CCAUX}$下限 | ALM[2] |
| 57h | OT アラームリセット | OT |
| 58h | $V_{CCBRAM}$上限 | ALM[3] |
| 5Ch | $V_{CCBRAM}$下限 | ALM[3] |

**図 3.6.2 アラームおよび閾値レジスタ[6]**

備考

・対象ボードが SAKURA-X(SASEBO-GIII)[8]の場合に実装

・クロック信号：システムクロック(100MHz) or 外部クロックを想定

・DRP を介して $V_{CCINT}$ の取得と $V_{CCINT}$ の閾値の上限/下限を制御する機能を実装すること

・$V_{CCINT}$ の閾値の上限/下限は UART を介してホスト PC から制御できるようにすること

・UART 経由でホストＰＣからアラームの閾値を制御する機能を実装すること

## 3.7. Voltage Temperature Sensor(VTS)[7]

図 3.7.1 は Polarfire FPGA の耐タンパー用マクロ PF_TAMPER である。PF_TAMPER は内部に電圧・温度センサ（VTS：Voltage Temperature Sensor)を有し、電源電圧が事前に設定した閾値を超えた場合に自動的にアラームが VOLTAGE_DETECT_XXX_HIGH/LOW から出力される。今回は FPGA のコア電圧 1V を本センサで監視する。

図 3.7.2 は Polarfire に搭載されている温度・電圧センサの VTS である。VTS はダイの温度、VDD（1.0V/1.8V/2.5V）の電源レールの電圧のいずれかを選択して 16bit の値で出力する。16bit の内、最上位ビットは signed bit, [14:3]は整数値, [2:0]は小数値を示す。

その他、PF__TAMPER および VTS のより詳細な仕様は参考文献[7]を参照のこと。

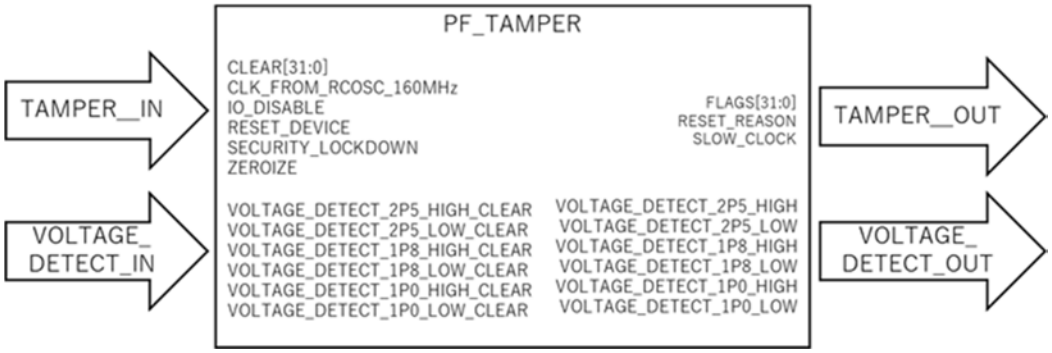


**図 3.7.1 PF_TAMPER マクロ**

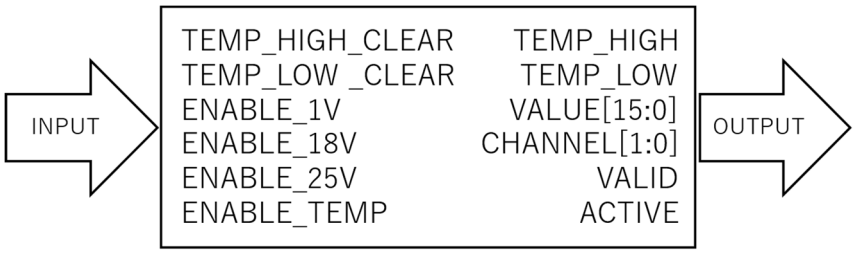


**図 3.7.2 TVS コア[7]**

備考：

・対象ボードが M100PF[9]の場合に実装

・PFSOC_TAMPER を使用してセンサの計測値（16bit）と VOLT_DETECT_1V のアラームを外部ピンに出力すること

・アラームの閾値をホスト PC 側から制御できるようにすること

・クロックグにはシステムクロック or 外部クロックを使用(100MHz を想定)

# 4. 参考文献

[1] Ebrahimabadi, Mohammad, et al. "DELFINES: Detecting laser fault injection attacks via digital sensors." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 43.3 (2023): 774-787.

[2] Zhao, Mark, and G. Edward Suh. "FPGA-based remote power side-channel attacks." *2018 IEEE symposium on security and privacy (SP)*. IEEE, 2018.

[3] Muttaki, Md Rafid, et al. "Ftc: A universal sensor for fault injection attack detection." *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2022.

[4] Jayasinghe, Darshana, Brian Udugama, and Sri Parameswaran. "1lutsensor: Detecting FPGA voltage fluctuations using lookup tables." *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2024.1 (2024): 51-86.

[5] Nemiroff, Daniel, and Carlos Tokunaga. "Fault-Injection Countermeasures, Deployed at Scale." *2024 IEEE Physical Assurance and Inspection of Electronics (PAINE)*. IEEE, 2024.

[6] 7 Series FPGAs and Zynq-7000 SoC XADC Dual 12-Bit 1 MSPS Analog-to-Digital Converter User Guide (UG480), Accessed: June 9, 2025. [Online]. Available: https://www.amd.com/content/dam/xilinx/support/documents/user_guides/ug480_7Series_XADC.pdf.

[7] PolarFire Family FPGA Security User Guide, Accessed June 9, 2025, [Online]. Available: https://www.microchip.com/content/dam/mchp/documents/FPGA/ProductDocuments/UserGuides/Microchip_PolarFire_FPGA_and_PolarFire_SoC_FPGA_Security_User_Guide_VA%20(2).pdf

[8] SAKURA(SASEBO-GIII), Accessed June 9, 2025, [Online]. Available: https://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-X.html

[9]M100PF – SoM Featuring Microchip Polarfire FPGA, Accessed June 9, 2025, [Online]. Available: https://www.aries-embedded.com/polarfire-microchip-fpga-m100pf-som-mpf100t-pcie-serdes

## サプライチェーン・リスク対応に係る特記事項

1. サプライチェーン・リスクへの対応

受注者は、機器等の意図的な不正改造及び情報システム又はソフトウェアに不正なプログラムを埋め込むなど、国立研究開発法人産業技術総合研究所（以下、「産総研」という。）の意図しない変更が加えられたときに生じ得る情報の漏えい若しくは破壊又は機能の不正な停止、暴走その他の障害等の情報セキュリティ上のリスク（以下「サプライチェーン・リスク」という。）に対応するため、受注者は「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」（平成 30 年 12 月 10 日関係省庁申合せ）に基づく対応を図らねばならない。

2. 意図しない変更に対する対策

①受注者は、本業務の履行に際して、サプライチェーン・リスクが潜在すると知り、又は知り得るべきソースコード、プログラム等（以下「ソースコード等」という。）の埋込み又は組込みその他産総研担当者の意図しない変更を行ってはならない。

②受注者は、本業務の履行に際して、サプライチェーン・リスクが潜在すると知り、又は知り得るべきソースコード等の埋込み又は組込みその他産総研担当者の意図しない変更が行われないように相応の注意をもって管理しなければならない。

③受注者は、本業務の履行に際して、情報の窃取等により研究所の業務を妨害しようとする第三者から不当な影響を受けるおそれのある者が開発、設計又は製作したソースコード等（受注者がその存在を認知し、かつ、サプライチェーン・リスクが潜在すると知り、又は知り得るべきものに限り、主要国において広く普遍的に受け入れられているものを除く。）を直接又は間接に導入し、又は組み込む場合には、これによってサプライチェーン・リスクを有意に増大しないことを調査、試験その他の任意の方法により確認又は判定するものとする。

3. サプライチェーン・リスクにかかる調査の受入れ体制

①受注者は、本業務に産総研担当者の意図しない変更が行われるなど不正が見つかったときは、追跡調査や立入検査等、産総研と連携して原因を調査し、サプライチェーン・リスクを排除するための手順及び体制を整備し、当該手順及び体制を示した書面を産総研担当者に提出しなければならない。

4. サプライチェーン・リスクを低減するための対策

①受注者は、サプライチェーン・リスクを低減する対策として、本業務の設計、構築、運用・保守の各工程における不正行為の有無について定期的または必要に応じて監査を行う体制を整備するとともに、本業務により産総研に納入する納入物品に対して意図しない変更が行われるリスクを回避するための試験を行わなければならない。当該試験の項目は、情報セキュリティ技術の趨勢、対象の情報システムの特性等を踏まえ、受注者において適切に設定するものとする。

②機器の納入であり、かつ、設計、構築、運用・保守の各工程が存在しない場合は、4. ①の対応は不要。

5. 受注者の業務責任者等

①受注者は、本業務の履行に従事する業務責任者及び業務従事者（契約社員、派遣社員等の雇用形態を問わず、本業務の履行に従事する全ての従業員をいう。以下同じ。）を必要最低限の範囲に限るものとする。

②機器納入であり、かつ、設計、構築、運用・保守の各工程が存在しない場合は、5. ①の対応は不要。

6. 再委託

6.1 本業務の第三者への委託の制限

受注者は、産総研の許可なく、本業務の一部又は全部を第三者（再委託先）に請け負わせてはならない。ただし、6.2 に定める事項を遵守する場合はこの限りではない。

6.2 第三者への委託に係る要件

①受注者は、本業務の一部又は全部を第三者に再委託するときは、再委託先の事業者名、住所、再委託対象とする業務の範囲、再委託する必要性について記載した承認申請書を、委託元である産総研に提出し、書面による事前承認を受けなければならない。

②受注者は、本業務の一部又は全部を第三者に再委託するときは、再委託した業務に伴う再委託者の行為について、全ての責任を負わなければならない。

③受注者は、知的財産権、情報セキュリティ（機密保持を含む。）及びガバナンス等に関して、本仕様書が定める受注者の責務を再委託先も負うよう、必要な処置を実施し、その内容について委託元である産総研の承認を得なければならない。

④受注者は、受注者がこの仕様書の定めを遵守するために必要な事項について本仕様書を準用して、再委託者と約定しなければならない。

⑤受注者は、前号に掲げる情報の提供に加えて、再委託先において本委託事業に関わる要員の所属、専門性（情報セキュリティに係る資格・研修実績等）、実績及び国籍についての情報を委託元である産総研へ提出すること。

⑥受注者は、再委託先において、産総研の意図しない変更が加えられないための管理体制について委託元である産総研に報告し、許可又は確認（立入調査）を得ること。

7. その他

①提出された資料等により産総研担当者に報告された内容について、サプライチェーン・リスクが懸念され、これを低減するための措置を講じる必要があると認められる場合に、調達担当者は受注者に是正を求めることがあり、受注者は相当の理由があると認められるときを除きこれに応じなければならない。

②産総研は、受注者の責めに帰すべき事由により、本情報システムに産総研担当者の意図しない変更が行われるなど不正が見つかった場合は、契約条項に定める契約の解除及び違約金の規定を適用し、本業務契約の全部又は一部を解除することができる。