AN5484 – マイクロ コントローラでの 等級B機能安全診断ライブラリ実装

AVR® EAを使うアンモニア ガス検出器

序説

著者: Robert Perkel and Erik Tollefson, Microchip Technology Inc.

機能安全は障害と故障が正しく検出されて処理されなければならない多くの応用の重要な側面です。けれども、最終市場と応用の形式に応じて異なる水準の機能安全があります。例えば、車のﾍｯﾄﾞﾗｲﾄはおそらくｴｱﾊﾞｯｸﾞの展開を担当する回路と違う基準の機能安全要件を持つでしょう。Microchipはこれらの形式の応用開発で使うためにお客様用の機能安全ﾗｲﾌﾞﾗﾘを提供します。

この例はAVR® EA系ﾏｲｸﾛ ｺﾝﾄﾛｰﾗでのｱﾝﾓﾆｱ漏れ検出器でIEC 60730等級Bｿﾌﾄｳｪｱ診断ﾗｲﾌﾞﾗﾘを使う方法を示します。この検出器は応用が正しく動作しているのと走行時のﾏｲｸﾛ ｺﾝﾄﾛｰﾗの状態を監視するのために無料で使える等級Bﾗｲﾌﾞﾗﾘを使います。

目次

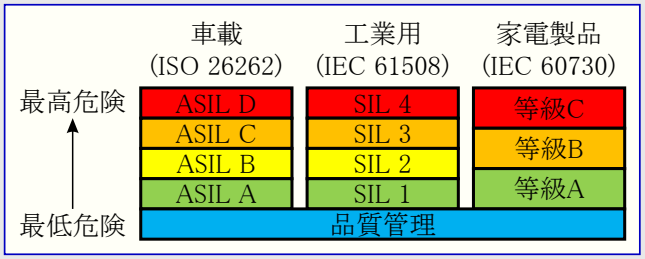
1. 機能安全規格と基準

機能安全は障害と故障を検出してそれらを安全に処理するシステムの能力を言います。検出されることなく発生した場合、損傷、人的損失、物的損害のような重大な結果が起きるかもしれません。機能安全は車載、工業用、家庭用/家電製品、医療、原子力と製造業を含む様々な産業で極めて重要です。これは機械、設備、工程の運用に関連する危険の特定と軽減を含みます。

Microchipは3つの主な機能安全規格、ISO 26262(車載)、IEC 61508(工業用)、IEC 60730(家電製品)を支援します。これらの各々の規格は安全基準を定義し、系内の安全機能信頼性の数値化を助けます。系設計時、各部品や補助系は系の最高安全性を考慮して設計されるべきです。

車載、工業用、家電製品部門に対して、これらの安全基準は各々、自動車用安全度水準(Automotive Safety Integrity Level) (ASIL A,B,C,D)、安全整合水準(Safety Integrity Level) (SIL 1,2,3,4)、等級(Class) (A,B,C)として定義されます。車載応用でASIL Aが最低車載危険度を表す一方でASIL Dは最高を表します。工業用と家庭用の応用でSIL 1が最低の危険度を表す一方でSIL 4は最高を表し、等級Aが最低を表す一方で等級Cが最高を表します。使用者または環境の安全に関連する系がASIL A、SIL 1、または等級Aを下回る時にそれは度々「品質管理」として分類され、それは未だOEM業者が安全を保証するために最高品質になるようにこの系を設計すべきことを意味します。

図1-1. 様々な規格の安全基準と等級



機能安全規格は代表的に次に於いて開発者に助言します。安全な製品寿命、安全整合水準、危険評価、安全要件、検証と妥当性確認、文書化と法令遵守、組織的要件、管理の改革、等々。全体として、機能安全は安全性が重要な系と処理が確実に動作することを保証し、災難、事故、及び人、財産、環境への危害の危険を軽減するのを助けます。

2. 機能安全のツールと資料

Microchipは3つの主な安全規格、ISO 26262、IEC 61508、IEC 60730に対する機能安全支援を提供します。「機能安全準備可」指定を含むマイクロ コントローラは統合したハードウェア機能安全、故障種別の影響と診断分析(FMEDA)報告、安全手引書と、いくつかの場合で応用の認証を助ける診断ソフトウェア ライブラリを提供します。TÜV SÜD®認定のCコンパイラと完全且つ全体的に認定された開発環境も利用可能です。ここは以下の資源とツールが設計の支援をどう助けるかです。

2.1. 安全手引書

安全手引書は様々な診断機構の詳細な説明を提供し、最も安全な動作のためにデバイスをどう使うかの推奨を提供します。

2.2. FMEDA報告

FMEDA報告は補償計画の作成を助けるためにデバイスの故障種別、時間内故障(Failure In Time:FIT)率配給、対応する検出方法を数値化します。より多くの詳細についてFMEDA白書(DS00003638A)を読むことができます。

2.3. ハードウェア機能

ハードウェア安全機能は動作の安全性と信頼性を改善するための電源ONリセット(POR)、低電圧リセット(BOR)、窓化ウォッチドッグ計時器(WWDT)、巡回冗長検査(CRC)を含む組み込み機能です。

2.4. 開発エコシステム

当社の開発エコシステムはTÜV SÜD®認定のMPLAB® XC8コンパイラとMPLABコードド構成部(MCC)を含み、無料のコード生成ツールがマイクロコントローラを構成設定し、APIを生成し、そしてミドルウェア ライブラリを読み込みます。素早い設計試作はCuriosity Nano開発基板によって許され、殆どのマイクロ コントローラ系統に対して利用可能で、8ビットと16ビットから32ビットまでの幅広いマイクロ コントローラが機能安全を支援しますが、この文書は特定の8ビット マイクロ コントローラを目的とします。

3. 応用

アンモニアはHVAC(暖房、換気、空調)系を含む様々な応用で使われる危険物です。アンモニア事故は潜在的に近くの人々を傷つける放出を引き起こすかもしれません。大量に使われる時に、大気中のアンモニア量を監視してそれが臨界値を超えるかどうかが重要な安全対策です。

危険 この応用は現在のアンモニア ガス水準だけを監視し、これは完全に認定されたアンモニア ガス検出器での生命または健康の即時危険(IDLH)検知システムの一部です。

この応用は周辺のアンモニア水準を監視する簡単なアンモニア ガス検出器を実装します。これはAmmonia Clink、Buzz 2 Click、2x2 Clickと共にAVR EA Curiosity Nano評価キット(EV66E56A)を使います。アンモニア濃度変化時、Ammonia Clickのアナログ出力が変化し、これはアナログ比較器CIP(コアから独立した周辺機能)で監視されて閾値に対して比較されます。信号が閾値を超えた場合、AVR EAはBuzz Clickを駆動するためのPWM信号を生成する一方で2x2 Clickは追加の使用者入力釦を加えます。この応用は4.章で説明されます。

この応用はMicrochipによって提供される等級B診断ライブラリから以下のソフトウェア検査、CPUレジスタ検査、SRAM検査、ウォッチドッグ計時器(WDT)、フラッシュ メモリとEEPROMの検査を使います。

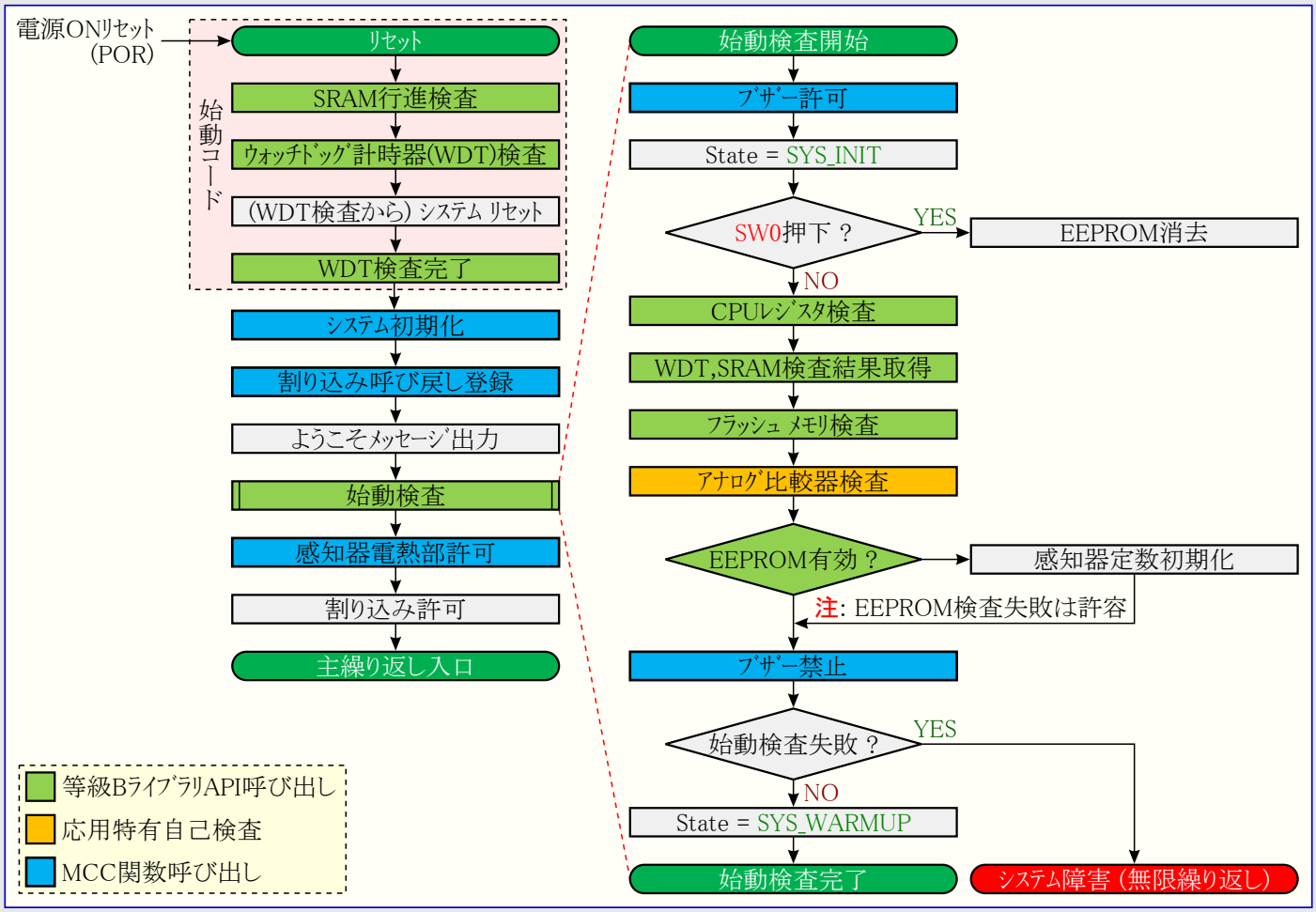
けれども、これは等級Bデバイスとして使うことが認証または意図されません。この意図はMicrochipによって提供された等級Bライブラリをどう実装するかを実演することです。等級B適合を達成するには更なる障害と危険の分析が必要とされます。

危険 この例は等級Bライブラリをどう使うかを示すために開発されました。これは最終応用に対して認証されません。制御された環境と危険な化学物質へのアクセスなしで感知器が正しく動作していたことを検証することは不可能でした。この応用は障害検出時間間隔(FDTI)を考慮しません。

3.1. 始動

始動の動きは下の図3-1.で示されます。図での始動コードは主関数到達前に実行するコードを指します。通常、これは主関数到達前に変数を初期化するためにコンパイラによって使われます。等級Bライブラリに対してMPLABコード構成部(MCC)インターフェースで適切な任意選択がチェックされた場合、関連する検査をこのメモリ領域へ自動的に実装します。等級B検査実装でのより多くの情報については「機能安全検査実装」章を御覧ください。

図3-1. システム始動流れ図

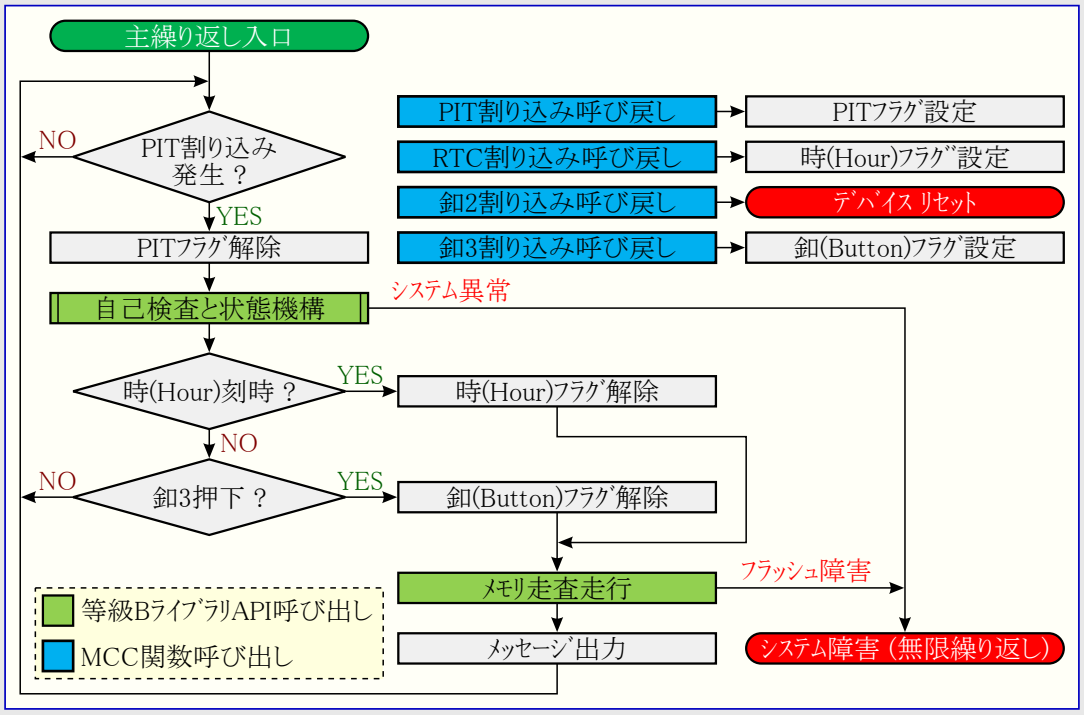


3.2. 主繰り返し

初期化後、システムは周期的割り込み計時器(PIT)がフラグを設定する時の0.5秒毎に周期的に自己検査と状態機構関数を呼び出します。この関数が呼ばれない場合、WDTが決して解消されず、マイクロ コントローラはリセットします。WDTが窓動作で動き、WDTの早すぎる解消の場合にもマイクロ コントローラ リセットを起動します。

状態機構走行後、時(Hour)フラグと釦3メモリ検査フラグが検査されます。これらが有効の場合、適切なフラグが解消され、メモリ走査が実行されます。メモリ走査は稀に呼ばれ、完了が非常に遅いため、自己検査よりもむしろ繰り返し内に置かれます。図3-2.はこの動きを示します。

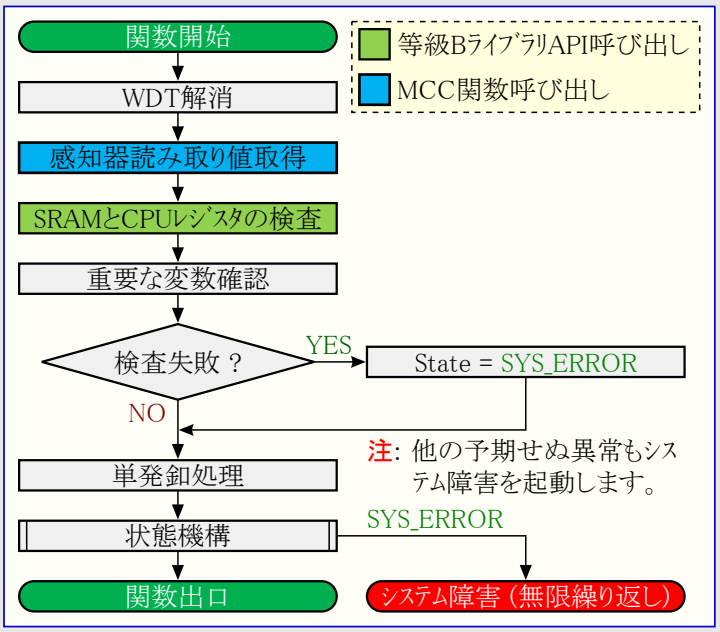
図3-2. 始動後の主繰り返し流れ図



3.3. 自己検査と状態機構

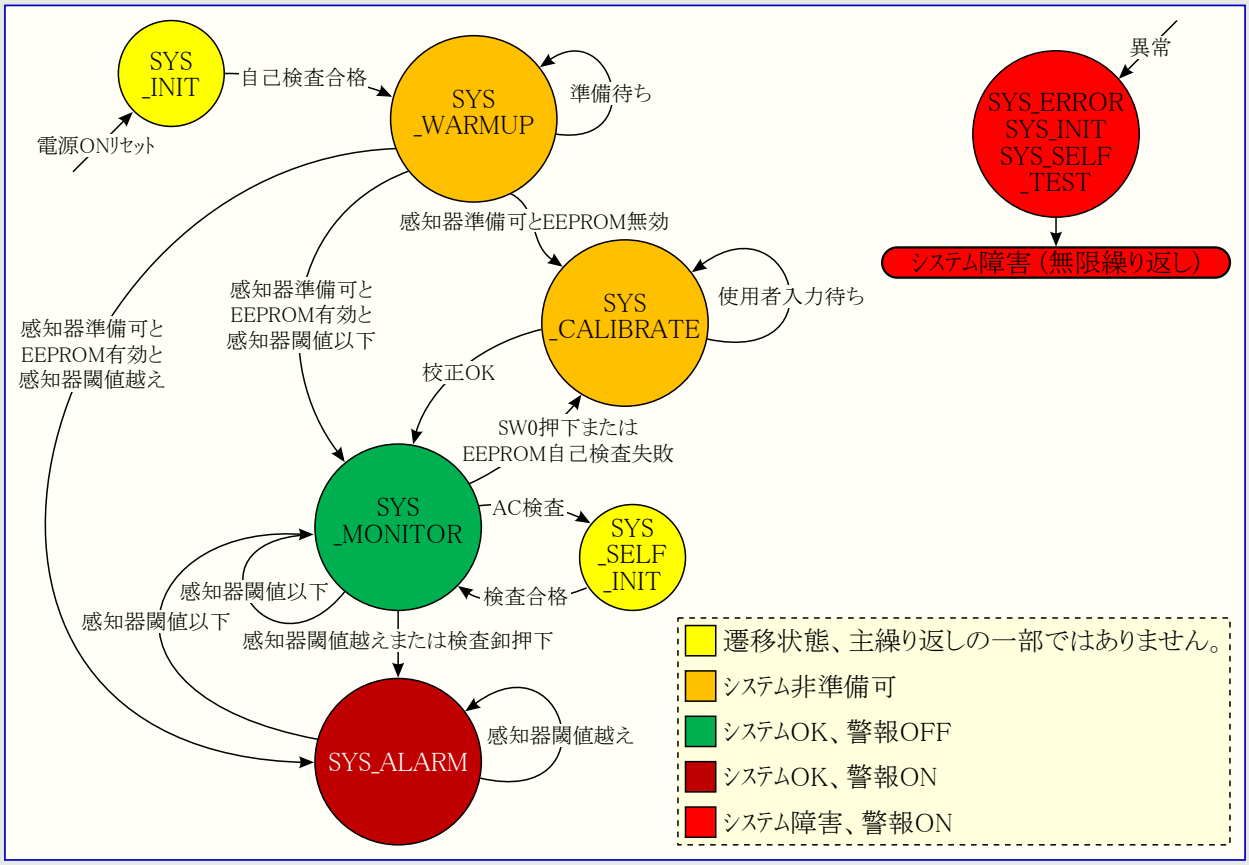
自己検査と状態機構呼び出しはWDT解消、自己検査実行、応用の状態機構管理の責任があります。WDTはいくつかの検査が実行に長くかかるため、自己検査を走行する直前に解消され、これはマイクロ コントローラをリセットするよりもむしろ障害状態繰り返しに入るために重要で、障害警告を隠蔽し得ます。メモリ走査検査(主繰り返し部分を参照)を除き、図3-3.で示されるように、周期的な自己検査がこの関数呼び出しで実行されます。

図3-3. 周期的な自己検査と状態機構関数の流れ図



簡単化した状態機構の状態図が下の図3-4.で示されます。大きな円はこの関数呼び出しで状態機構によって処理される活動用、一方で小さな円は処理の中間で起きますが、状態機構によって決して出会ってはならない遷移状態です。例えば、ｱﾅﾛｸﾞ比較器(AC)自己検査の中間でのｿﾌﾄｳｪｱ機能不全がその検査を予想外に終了させた場合、状態は主処理部が走行している時に未だSYS_SELF_TESTになるでしょう。主処理部がこの状態を見ると、それはｼｽﾃﾑ障害と見做されます。図を簡単化するため、異常を引き起こす条件は示されませんが、全ての状態がその状態に移行し得ます。

図3-4. 状態図



3.4. 安全状態

故障や機能不全の発生で、ﾌﾟﾛｸﾞﾗﾑはﾃﾞﾊﾞｲｽが故障または機能不全にされたことを示す障害状態に移行します。障害状態では割り込みが禁止され、感知器電熱部がOFFに切り替えられ、ﾏｲｸﾛ ｺﾝﾄﾛｰﾗは10秒毎にUARTに出力するよう、周期的に”SYSTEM FAULT”を出力すると同時にﾌﾞｻﾞｰから音型を出力してLEDを点滅します。

4. 応用構築

⚠警告 この例は等級Bライブラリの使い方を実演し – それは最終応用のために認証されません。感知器が正しく動作しているかを確認するために制御された環境と危険科学物質へのアクセスが必要です。

4.1. ハードウェア設定

この例は以下の開発基板を使います。

- AVR EA Curiosity Nano (EV66E56A)
- Curiosity Nanoアダプタ基板 (AC164162)
- MikroElektronikaによるAmmonia Click™ (MIKROE-4151)
- MikroElektronikaによるBuzz 2 Click (MIKROE-2720)
- MikroElektronikaによる2x2 Click (MIKROE-2152)

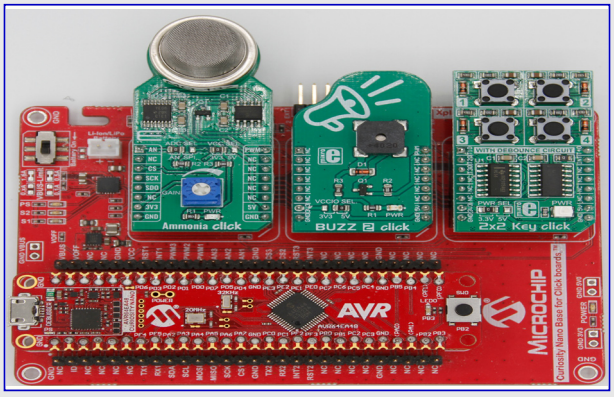
助言: Buzz 2 Clickは任意選択で開発中に音響警報を取り去るために省略することができます。

電源OFFで、次のようにClickを挿入してください。

- スロット1 : Ammonia Click
- スロット2 : Buzz 2 Click
- スロット3 : 2x2 Click

そして、下図で示されるように、Curiosity NanoアダプタにUSBポートを外側に向けてAVR EA Curiosity Nanoを挿入してください。

図4-1. 完全に組み立てたシステム



使う前に、感知器出力が極端な条件で絶対最大入力電圧を超えるかもしれないため、Ammonia Clinkの感度を可能な限り低く落とすことが重要です。しかしもっと現実的に、Click出力はA/D変換器(ADC)の入力範囲を超えるかもしれず、システムを不正な動作にさせます。

4.2. ソフトウェア設定

殆どのコード例は無料(Free)と有料(Pro)の2つのソフトウェア構成を含んで配給します。ソフトウェア使用許可を必要とするPro構成はMPLAB XC8コンパイラの高位最適化を使って設定する一方で、Free構成は基本的な最適化だけでコンパイルされます。表4-1.で示されるように、両構成は高位最適化でのコード量と速度の改善を除いて同じです。

注: この例はもっと入手し易くするために標準XC8コンパイラを使いました。製品では機能安全認証コンパイラを使ってください。

表4-1. MPLAB XC8 v2.46とAVR-Ex_DFP v1.13.715でのコード量比較

ソフトウェア構成	最適化基準	データ メモリ(SRAM)使用量 (バイト)	プログラム フラッシュ メモリ使用量 (バイト)
無料 (Free)	1	373	25,240
有料 (Pro)	S	373	23,560

けれども、この例に対して2つの追加構成が作成されました。Ammonia Clickのガス検知器は安定動作に達する前に24時間の準備時間を必要とします。マイクロ コントローラだけでは短時間の電源不具合と長い停電を区別できず、故に24時間検出器準備は始動で実施されます。けれども、これは開発中に受け入れられず、故に始動を加速するためにdevelopとdevelop_no_cksmの2つの交替構成が作成されました。これらの構成はシステムに自己検査失敗を伴う開始をも許し、これは開発中に重要なことです。

develop_no_cksmでは出力ファイルにそれを追加するのにHexmateユーティリティを使うよりもむしろファームウェアに偽装チェックサム値($87654321)が挿入され、これは挿入したチェックサムがデバッグ用コンパイル時に問題を発生するために必要とされます。次表はソフトウェア構成間の違いの一覧を示します。

表4-2. ソフトェア構成表

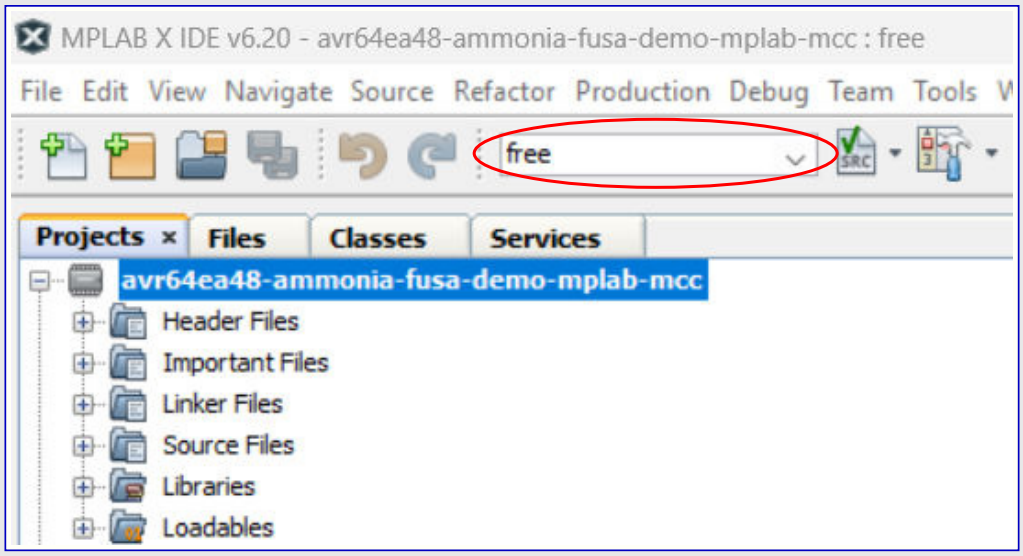
ソフトウェア構成	最適化基準	ハードウェア デバッグ	24時間準備	始動自己検査失敗許容	フラッシュ チェックサム有効
無料 (Free)	1	×	○	×	○
有料 (Pro)	S	×	○	×	○
develop	1	×	×	○	○
develop_no_cksm	1	○	×	○	×

助言: MPLAB X v6.20以降は非書き込み任意選択ために上部メニュー バーで「デバッグ用構築(Build for Debug)」が既定です。書き込み釦(マイクロ コントローラへの矢印)はデバッグ用に構築しません。標準的な構築(Build)(と解消(Clean))はIDEで構築アイコン傍らの小さな矢印をクリックすることによって利用可能です。

4.3. 構成設定変更

MPLAB® X IDEで構成を変更するにはプロジェクト(fusa-ammonia.X)を開いてください。下図で示されるように、構成を選ぶために上部ツールバーで白い引き落とし枠をクリックしてください。

図4-2. 構成選択



4.4. チェックサムの構成と設定

develop_no_cksmを除く直ぐに使える全てのプロジェクト構成はhexファイルにチェックサムを挿入するためにXC8コンパイラと共に含まれるHexmateユーティリティを使って設定されます。Hexmate命令は構築後段階(プロジェクト構成設定(Project Configuration)クリック後に構築(Building)をクリック)に追加され、下で示されます。

```
"hexmate" ${ImagePath} -o${ImagePath} -FILL=0xFFFF@0x0000:0xFFFB
-CK=0x0000-0xFFFB@0xFFFC+0xFFFFFFFFw-4g-5p0x04C11DB7o0xFFFFFFFF
```

この命令を分解してみましょう。最初の要素はHexmateへの入力を指定し、一方で2つ目は出力ファイルを指定します。そして"-FILL"命令はどの未使用メモリも既知の値で満たすのに使われます。未使用メモリの充填は正しいチェックサムの計算に必要とされます。

注: Hexmateは語基準のアドレス指定ではなく、バイト基準のアドレス指定を使います。

命令のチェックサム部分は以下のように翻訳されます。

- 0x0000-0xFFFB@0xFFFCはチェックサムが計算されるメモリ範囲($0000～$FFFB)とそれが格納される場所($FFFC)を定義します。
- +0xFFFFFFFFはチェックサムの初期値を設定します。
- w-4はリトルエンディアン(下位アドレスが下位値)順で4バイトの長さでの出力を定義します。
- g-5はHexmate使用者の手引きによってこれはCRC動作を指定します。
- p0x04C11DB7はCRCの多項式です。
- o0xFFFFFFFFはこの数値によって最終結果を排他的論理和(XOR)します。

助言: Hexmateについてのより多くの情報に関してはHexmate使用者の手引き(DS-50003033C)を見直してください。

4.5. デバイス書き込み

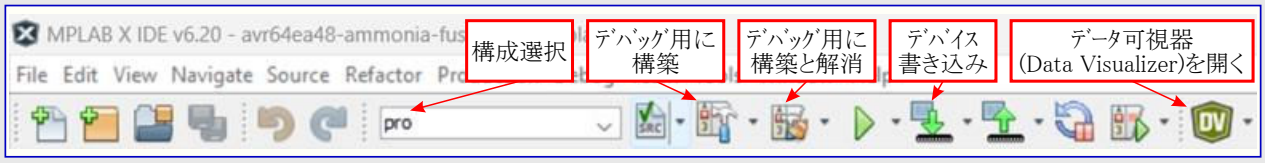
最初に、ソースコードの複製をダウンロードしてください。C:/またはドキュメントのような短いファイル パスを持つ場所にそのファイルを解凍してください。

⚠注意 いくつかの生成されたコードは許容されるファイル限度に迫る長いファイル パスを持ちます。完全なファイル パスが許可されたパス長を超える場合にプロジェクトは正しく構築しないかもしれません。

Curiosity Nanoを繋げてください。MPLAB X IDEを開いてその後にファイル(File)に行ってプロジェクトを開く(Open Project...)をクリックして.X(fusa-ammonia.X)で終わるフォルダを選んでください。構成を選び(より多くの情報については「構成設定変更」を御覧ください)、その後に下図で上部ツールバーの書き込み釦を押下してください。

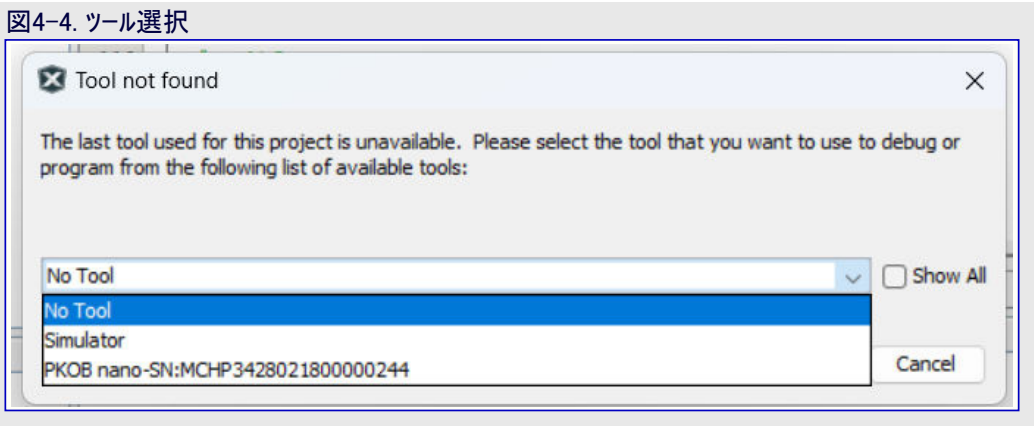
助言: 書き込み釦押下はプログラムを自動的に再構築します。

図4-3. プログラミング ツールバー



思い出した時にツール ウィンドウでCuriosity Nanoを選んでください(下図を御覧ください)。一旦ツールが選ばれると、プロジェクトは構築してCuriosity Nanoを書きます。

図4-4. ツール選択

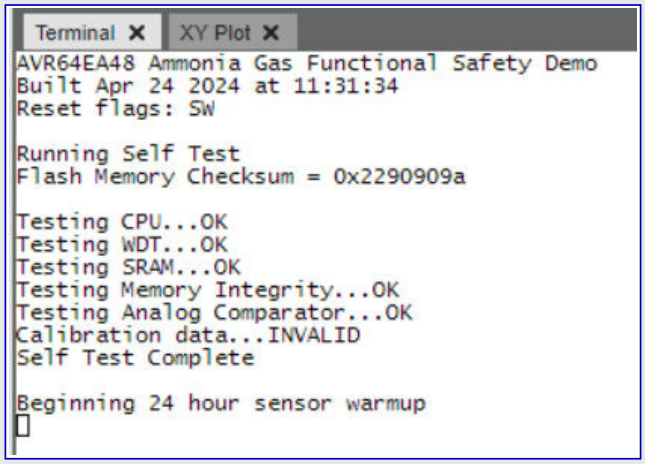


助言: develop_no_cksmだけがデバッグ用に構築することができます。他のどの構成のデバッグ用構築もコンパイルの最後で誤りになります。

その後、上部ツールバーのデータ可視器(Data Visualizer:DV)アイコンを押下してください。画面の左側で、Curiosity Nanoと関連したCOMポートを選び、歯車アイコンを押下してください。ボーレートを115200に変え、その後にメニューを閉じてください。活動(Play)釦を押し、その後に端末へ送ってください。下図で示されるように、Nanoからの出力は今やシリアル端末に向け直されます。

助言: 釦2はマイクロ コントローラをリセットし、下で示されるように、それを再走行させて始動結果を表示させます。

図4-5. シリアル端末出力



5. 検出器の動作原理

Ammonia Click上のｱﾝﾓﾆｱ検出器は加熱された抵抗性感知器です。非線形で大気が増す時に感知器の抵抗が減ります。この感知器は非線形で湿度と温度のような環境的な条件に強く依存します。安定になるまで感知器に対して準備期間も必要です。

助言: 使うｶﾞｽ検出器に対して多くの時間の準備時間が必要とされます。この応用では24時間が既定ですが、製造業者はこれらの特性ﾃﾞｰﾀに対して48時間を使います。開発中の観察から、安定のために必要とされるのは数時間だけと思われます。

検出器出力をｶﾞｽ濃度に変換するため、Microsoft Excelで最適関数が計算されました。この関数は感知器の参照基準抵抗がClick基板の最小感度の100Ωに等しいと想定しています。検出器に5Vを出力させ得る一方でCuriosity Nanoが3.3Vで動くため、感度調整は最高水準に設定されません。可変抵抗器は回路からそれを取り外すことなく安定的に既知の抵抗値に設定することができないため、中間利得値は使い物になりません。

6. 機能安全検査実装

このﾌﾟﾛｸﾞﾗﾑは始動でと走行時に周期的に機能安全検査を実行します。いくつかの検査は継続的に動くにはそれに集中しすぎる(訳補:時間がかかりすぎる)一方で他は問題なく周期的に動くことができます。等級Bﾗｲﾌﾞﾗﾘによって提供されるAPIについてのより多くの情報に関しては各単位部用のｿﾌﾄｳｪｱ手引書を調べてください。

6.1. CPUﾚｼﾞｽﾀ

API参照：https://onlinedocs.microchip.com/oxy/GUID-641A8CC3-34E7-4FE7-9923-7F86A2135AF5-en-US-1/GUID-AE36DB17-1231-40E7-BFEB-6062C510A02A.html

- 検査が走行する時：始動と周期的

CPUﾚｼﾞｽﾀ検査は市松模様と後続する反転市松模様を書くことによってCPUﾚｼﾞｽﾀ内の動かないﾋﾞｯﾄを調べます。

6.2. ﾌﾗｯｼｭ ﾒﾓﾘ

API参照：https://onlinedocs.microchip.com/oxy/GUID-1AB1E325-9BB2-4783-B223-5BE21C8A4C83-en-US-1/GUID-6142E093-8557-4AEC-AC4B-B56D7FF8C4D5.html

- 検査が走行する時：始動と周期的
- 構成：CRC-32参照表(LUT)

ﾌﾗｯｼｭ ﾒﾓﾘ検査はｼｽﾃﾑ ﾒﾓﾘでCRC-32ﾁｪｯｸｻﾑを実行することによってﾌﾟﾛｸﾞﾗﾑ ﾌﾗｯｼｭ ﾒﾓﾘ(PFM)の完全性を検証します。

6.2.1. ﾊｰﾄﾞｳｪｱCRC支援

執筆時点で、等級Bﾗｲﾌﾞﾗﾘはﾏｲｸﾛ ｺﾝﾄﾛｰﾗ内のCRCﾊｰﾄﾞｳｪｱの使用を支援しません。ﾊｰﾄﾞｳｪｱを使う場合、ﾊｰﾄﾞｳｪｱ周辺機能はｿﾌﾄｳｪｱ走査よりももっと速くﾒﾓﾘを走査してﾁｪｯｸｻﾑを計算します。これを実演するためにこの応用でCRCﾊｰﾄﾞｳｪｱを利用する関数が開発されました。application.hでFUSA_ENABLE_FLASH_HW_SCANﾏｸﾛが定義される場合、等級Bﾗｲﾌﾞﾗﾘの代わりにこれを使うことができます。

6.2.2. 等級Bﾗｲﾌﾞﾗﾘに対する変更

ﾌﾗｯｼｭ ﾒﾓﾘ等級Bﾗｲﾌﾞﾗﾘは同じ応用でﾊｰﾄﾞｳｪｱCRCと等級Bﾗｲﾌﾞﾗﾘを支援するために僅かに微調整されました。この変更はﾊｰﾄﾞｳｪｱ単位部がﾘﾄﾙｴﾝﾃﾞｨｱﾝ形式のﾁｪｯｸｻﾑを必要とするため、ﾒﾓﾘのCRCﾁｪｸｻﾑ符号化をﾋﾞｯｸﾞｴﾝﾃﾞｨｱﾝからﾘﾄﾙｴﾝﾃﾞｨｱﾝに変えました。この変更はﾊｰﾄﾞｳｪｱCRCを使わない限り必要ありません。

6.3. EEPROM

API参照：https://onlinedocs.microchip.com/oxy/GUID-BEF91AF0-2788-4CB6-B0BD-6B5A3CC43361-en-US-1/GUID-1BA1682A-124D-47B7-8058-ABA651C9DD8B.html

- 検査が走行する時：始動、周期的、EEPROM書き込み
- 構成：CRC-16-CCITT LUT

EEPROM検査はﾒﾓﾘでCRC-16ﾁｪｯｸｻﾑを実行することによってEEPROMﾒﾓﾘが有効であることを検証します。

6.3.1. ﾁｪｯｸｻﾑ動作形態

開発の間、等級Bﾗｲﾌﾞﾗﾘが利用可能になる前にﾌﾟﾛｸﾞﾗﾑで簡単な16ﾋﾞｯﾄ ﾁｪｯｸｻﾑが実装され、これはおそらく等級Bﾗｲﾌﾞﾗﾘによって実行されるCRC-16よりも堅牢性が低いですが、より速い計算時間を持つことが期待されます。このﾁｪｯｸｻﾑを許可するには、application.hでFUSA_ENABLE_EEPROM_SIMPLE_CHECKSUMﾏｸﾛを設定してください。

6.4. SRAM

API参照：https://onlinedocs.microchip.com/oxy/GUID-1BC922B5-0BDE-4D42-AC92-68359BB22BEC-en-US-1/GUID-E58EEFF6-B49E-48AC-B5F9-3A380DE1CDFB.html

- 検査が走行する時：始動と周期的

始動で、SRAM検査は故障を見つけるためにﾏｲｸﾛ ｺﾝﾄﾛｰﾗのSRAMﾒﾓﾘ全体を破壊的に検査します。けれども、この検査が破壊的なため、応用を再始動することなく再実行することができません。代わりに、故障に関して周期的にﾒﾓﾘの小さな部分が走査されます。

7. ｳｫｯﾁﾄﾞｯｸﾞ

API参照：https://onlinedocs.microchip.com/oxy/GUID-D4D71DC7-56E8-4A68-95EB-E061FA699CCD-en-US-1/GUID-2C4747CE-F408-4CCA-B8B8-2F7988C11DED.html

・検査が走行する時：始動

ｳｫｯﾁﾄﾞｯｸﾞ検査はWDTがﾊｰﾄﾞｳｪｱ水準で機能することを検証します。これはﾏｲｸﾛ ｺﾝﾄﾛｰﾗをﾘｾｯﾄするため、WDTが許可されて走行時に動作することを検証することができません。

8. 応用特有自己検査

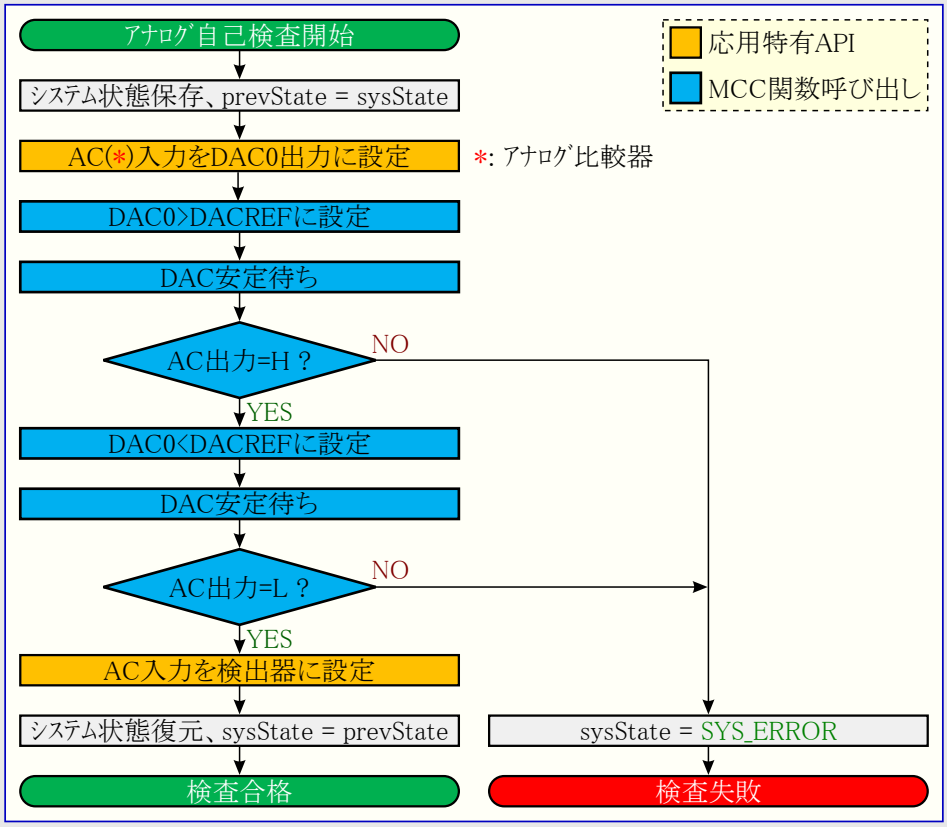
等級Bﾗｲﾌﾞﾗﾘが起こり得る可能性の故障の多くを網羅するとは言え、いくつかの故障は応用特有です。これらの検査が応用に対して実装されました。

8.1. ｱﾅﾛｸﾞ自己検査

走行で、ｼｽﾃﾑは検出した現在のｱﾝﾓﾆｱ濃度をｼﾘｱﾙ端末へ出力します。けれども、この計算された値は実際の警報の部分として使われません。警報はｱﾅﾛｸﾞ比較器(AC)とそれに関連するDACREFを使って実装されます。

これの利点はﾊｰﾄﾞｳｪｱ単位部が継続的に動き、校正後に実行するのにADCとCPUに依存しないことです。更に、表示される検出器は非直線性の動きを示し、機能に即した関数から逸脱するかもしれません。代わりに、設定点が既知の条件なら、例え検出器の反応が期待される動きと一致しなくても、ｼｽﾃﾑは未だ正しく機能します。けれども、その時にｼｽﾃﾑはACとDACREFが機能することを検証しなければなりません。これを行うために(下図で示される)DAC0を使う複数段階処理が開発されました。

図8-1. DAC校正流れ図



8.2. 重要な変数

変数のいくつかは応用が正しく動くために重要です。これらが破壊されていないままであるのを保証するために冗長な変数の複製があります。誤動作がこの変数の1つを不一致にさせる場合、ｼｽﾃﾑはこれをｼｽﾃﾑ障害として扱います。

これを適用する、fusa.cのsysState(ｼｽﾃﾑ状態変数)、alarmLowVal (SENSOR.c)、alarmHighVal (SENSOR.c)の3つの変数があります。alarmLowValとalarmHighValは同時に変わる値で、これら2つの値の排他的論理和(XOR)だけが格納されます。この値の1つだけが変わる場合、計算されたXORは不一致になり、ｼｽﾃﾑ障害警報を起動します。

9. 自己検査の制限

この例は既製品の開発基板を使うように開発され、与えられたﾊｰﾄﾞｳｪｱ故障に対する網羅を制限します。

9.1. ｱﾝﾓﾆｱ検出器

検出器が正しく動くのを止めた場合、現在の実装はをそれを検出できないかもしれません。検出器が短く故障する場合、ｼｽﾃﾑはその障害を非常に高い水準のｱﾝﾓﾆｱとして検出するでしょうが、検出器が高ｲﾝﾋﾟｰﾀﾞﾝｽ(Hi-Z)として故障するなら、ｼｽﾃﾑはこの故障を正しく検出しないでしょう。これは走行時に異常に高い検出器抵抗の割合を探すことによって、または出力で測定した電圧が非常に低い場合にHi-Z故障を検出することが可能かもしれません。短絡回路故障の場合では、故障は非常に高いｱﾝﾓﾆｱ水準として検出され、これは警報を起動するでしょう。

発生し得る別の障害は加熱系の故障です。検出器が加熱されない場合、ｶﾞｽ反応は未知です。検出器が加熱されているのを確認するのに、加熱部を通る電流の流れや外囲器の温度を監視してください。

最後に、検出器周りの環境的な条件が監視されるべきです。製造業者からのﾃﾞｰﾀは湿度や温度に依存して反応がかなり変わることを示します。これらの変化は応用で監視されて修正されるべきです。

9.2. ﾌﾞｻﾞｰ

ﾌﾞｻﾞｰは安全ｼｽﾃﾑに不可欠な部分で、危険を使用者に警告します。ﾏｲｸや電流監視器のように、ﾌﾞｻﾞｰが有効なことを保証する有効な監視はありません。

10. 結び

機能安全は高い信頼性の組み込みシステムの開発で重要な考慮すべきことです。これらの安全規格に合うのを助けるため、MCC内の等級Bライブラリは応用の開発に対して良い開始点を提供します。FMEDAのような機能安全認証に関して必要とされる文献は殆どのデバイス系統に関してMicrochipからも入手可能です。8ビット マイクロ コントローラでの機能安全についてより多くの情報に関しては8ビット機能安全ホーム頁を訪ねてください。

11. 改訂履歴

文書改訂	日付	注釈
A	2024年6月	初版文書公開

Microchip情報

Microchipウェブ サイト

Microchipはwww.microchip.com/で当社のウェブ サイト経由でのオンライン支援を提供します。このウェブ サイトはお客様がファイルや情報を容易に利用可能にするのに使われます。利用可能な情報のいくつかは以下を含みます。

- **製品支援** – データシートと障害情報、応用記述と試供プログラム、設計資源、使用者の手引きとハードウェア支援資料、最新ソフトウェア配布と保管されたソフトウェア
- **全般的な技術支援** – 良くある質問(FAQ)、技術支援要求、オンライン検討グループ、Microchip設計協力課程会員一覧
- **Microchipの事業** – 製品選択器と注文の手引き、最新Microchip報道発表、セミナーとイベントの一覧、Microchip営業所の一覧、代理店と代表する工場

製品変更通知サービス

Microchipの製品変更通知サービスはMicrochip製品を最新に保つのに役立ちます。加入者は指定した製品系統や興味のある開発ツールに関連する変更、更新、改訂、障害情報がある場合に必ず電子メール通知を受け取ります。

登録するにはwww.microchip.com/pcnへ行って登録指示に従ってください。

お客様支援

Microchip製品の使用者は以下のいくつかのチャネルを通して支援を受け取ることができます。

- 代理店または販売会社
- 最寄りの営業所
- 組み込み解決技術者(ESE:Embedded Solutions Engineer)
- 技術支援

お客様は支援に関してこれらの代理店、販売会社、またはESEに連絡を取るべきです。最寄りの営業所もお客様の手助けに利用できます。営業所と位置の一覧はこの資料の後ろに含まれます。

技術支援はwww.microchip.com/supportでのウェブ サイトを通して利用できます。

Microchipデバイス コード保護機能

Microchip製品での以下のコード保護機能の詳細に注意してください。

- Microchip製品はそれら特定のMicrochipデータシートに含まれる仕様に合致します。
- Microchipは動作仕様内で意図した方法と通常条件下で使われる時に、その製品系統が安全であると考えます。
- Microchipはその知的所有権を尊重し、積極的に保護します。Microchip製品のコード保護機能を侵害する試みは固く禁じられ、デジタル ミレニアム著作権法に違反するかもしれません。
- Microchipや他のどの半導体製造業者もそれのコードの安全を保証することはできません。コード保護は製品が"破ることができない"ことを当社が保証すると言うことを意味しません。コード保護は常に進化しています。Microchipは当社製品のコード保護機能を継続的に改善することを約束します。

法的通知

この刊行物と契約での情報は設計、試験、応用とのMicrochip製品の統合を含め、Microchip製品でだけ使えます。他の何れの方法でのこの情報の使用はこれらの条件に違反します。デバイス応用などに関する情報は皆さまの便宜のためにだけ提供され、更新によって取り換えられるかもしれません。皆さまの応用が皆さまの仕様に合致するのを保証するのは皆さまの責任です。追加支援については最寄りのMicrochip営業所にお問い合わせ頂くか、www.microchip.com/en-us/support/design-help/client-support-servicesで追加支援を得てください。

この情報はMicrochipによって「現状そのまま」で提供されます。Microchipは非侵害、商品性、特定目的に対する適合性の何れの黙示的保証やその条件、品質、性能に関する保証を含め、明示的にも黙示的にもその情報に関連して書面または表記された書面または黙示の如何なる表明や保証もしません。

如何なる場合においても、Microchipは情報またはその使用に関連するあらゆる種類の間接的、特別的、懲罰的、偶発的または結果的な損失、損害、費用または経費に対して責任を負わないものとします。法律で認められている最大限の範囲で、情報またはその使用に関連する全ての請求に対するMicrochipの全責任は、もしあれば、情報のためにMicrochipへ直接支払った料金を超えないものとします。生命維持や安全応用でのMicrochipデバイスの使用は完全に購入者の危険性で、購入者はそのような使用に起因する全ての損害、請求、訴訟、費用からMicrochipを擁護し、補償し、免責にすることに同意します。他に言及されない限り、Microchipのどの知的財産権下でも暗黙的または違う方法で許認可は譲渡されません。

商標

品質管理ｼｽﾃﾑ

Microchipの品質管理ｼｽﾃﾑに関する情報については www.microchip.com/quality を訪ねてください。

日本語© *HERO* 2024.

本応用記述はMicrochipのAN5484応用記述(DS00005484A-2024年6月)の翻訳日本語版です。日本語では不自然となる重複する形容表現は省略されている場合があります。日本語では難解となる表現は大幅に意訳されている部分もあります。必要に応じて一部加筆されています。頁割の変更により、原本より頁数が少なくなっています。

必要と思われる部分には( )内に英語表記や略称などを残す形で表記しています。

青字の部分はﾘﾝｸとなっています。一般的に赤字の0,1は論理0,1を表します。その他の赤字は重要な部分を表します。

世界的な販売とサービス

米国	亜細亜/太平洋	亜細亜/太平洋	欧州
本社 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 技術支援: www.microchip.com/support ｳｪﾌﾞｱﾄﾞﾚｽ: www.microchip.com	**ｵｰｽﾄﾗﾘｱ - ｼﾄﾞﾆｰ** Tel: 61-2-9868-6733	**ｲﾝﾄﾞ - ﾊﾝｶﾞﾛｰﾙ** Tel: 91-80-3090-4444	**ｵｰｽﾄﾘｱ - ｳﾞｪﾙｽ** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393
ｱﾄﾗﾝﾀ Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455	**中国 - 北京** Tel: 86-10-8569-7000	**ｲﾝﾄﾞ - ﾆｭｰﾃﾞﾘｰ** Tel: 91-11-4160-8631	**ﾃﾞﾝﾏｰｸ - ｺﾍﾟﾝﾊｰｹﾞﾝ** Tel: 45-4485-5910 Fax: 45-4485-2829
ｵｰｽﾁﾝ TX Tel: 512-257-3370	**中国 - 成都** Tel: 86-28-8665-5511	**ｲﾝﾄﾞ - ﾌﾟﾈｰ** Tel: 91-20-4121-0141	**ﾌｨﾝﾗﾝﾄﾞ - ｴｽﾎﾟｰ** Tel: 358-9-4520-820
ﾎﾞｽﾄﾝ Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088	**中国 - 重慶** Tel: 86-23-8980-9588	**日本 - 大阪** Tel: 81-6-6152-7160	**ﾌﾗﾝｽ - ﾊﾟﾘ** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79
ｼｶｺﾞ Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075	**中国 - 東莞** Tel: 86-769-8702-9880	**日本 - 東京** Tel: 81-3-6880-3770	**ﾄﾞｲﾂ - ｶﾞﾙﾋﾝｸﾞ** Tel: 49-8931-9700
ﾀﾞﾗｽ Addison, TX Tel: 972-818-7423 Fax: 972-818-2924	**中国 - 広州** Tel: 86-20-8755-8029	**韓国 - 大邱** Tel: 82-53-744-4301	**ﾄﾞｲﾂ - ﾊｰﾝ** Tel: 49-2129-3766400
ﾃﾞﾄﾛｲﾄ Novi, MI Tel: 248-848-4000	**中国 - 杭州** Tel: 86-571-8792-8115	**韓国 - ソウル** Tel: 82-2-554-7200	**ﾄﾞｲﾂ - ﾊｲﾙﾌﾞﾛﾝ** Tel: 49-7131-72400
ﾋｭｰｽﾄﾝ TX Tel: 281-894-5983	**中国 - 香港特別行政区** Tel: 852-2943-5100	**ﾏﾚｰｼｱ - ｸｱﾗﾙﾝﾌﾟｰﾙ** Tel: 60-3-7651-7906	**ﾄﾞｲﾂ - ｶｰﾙｽﾙｰｴ** Tel: 49-721-625370
ｲﾝﾃﾞｱﾅﾎﾟﾘｽ Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380	**中国 - 南京** Tel: 86-25-8473-2460	**ﾏﾚｰｼｱ - ﾍﾟﾅﾝ** Tel: 60-4-227-8870	**ﾄﾞｲﾂ - ﾐｭﾝﾍﾝ** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44
ﾛｻﾝｾﾞﾙｽ Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800	**中国 - 青島** Tel: 86-532-8502-7355	**ﾌｨﾘﾋﾟﾝ - ﾏﾆﾗ** Tel: 63-2-634-9065	**ﾄﾞｲﾂ - ﾛｰｾﾞﾝﾊｲﾑ** Tel: 49-8031-354-560
ﾛｰﾘｰ NC Tel: 919-844-7510	**中国 - 上海** Tel: 86-21-3326-8000	**ｼﾝｶﾞﾎﾟｰﾙ** Tel: 65-6334-8870	**ｲｽﾗｴﾙ - ﾎﾄﾞﾊｼｬﾛﾝ** Tel: 972-9-775-5100
ﾆｭｰﾖｰｸ NY Tel: 631-435-6000	**中国 - 瀋陽** Tel: 86-24-2334-2829	**台湾 - 新竹** Tel: 886-3-577-8366	**ｲﾀﾘｱ - ﾐﾗﾉ** Tel: 39-0331-742611 Fax: 39-0331-466781
ｻﾝﾎｾ CA Tel: 408-735-9110 Tel: 408-436-4270	**中国 - 深圳** Tel: 86-755-8864-2200	**台湾 - 高雄** Tel: 886-7-213-7830	**ｲﾀﾘｱ - ﾊﾟﾄﾞﾊﾞ** Tel: 39-049-7625286
ｶﾅﾀﾞ - ﾄﾛﾝﾄ Tel: 905-695-1980 Fax: 905-695-2078	**中国 - 蘇州** Tel: 86-186-6233-1526	**台湾 - 台北** Tel: 886-2-2508-8600	**ｵﾗﾝﾀﾞ - ﾃﾞﾙｰﾈﾝ** Tel: 31-416-690399 Fax: 31-416-690340
	中国 - 武漢 Tel: 86-27-5980-5300	**ﾀｲ - ﾊﾞﾝｺｸ** Tel: 66-2-694-1351	**ﾉﾙｳｪｰ - ﾄﾛﾝﾊｲﾑ** Tel: 47-72884388
	中国 - 西安 Tel: 86-29-8833-7252	**ﾍﾞﾄﾅﾑ - ﾎｰﾁﾐﾝ** Tel: 84-28-5448-2100	**ﾎﾟｰﾗﾝﾄﾞ - ﾜﾙｼｬﾜ** Tel: 48-22-3325737
	中国 - 厦門 Tel: 86-592-2388138		**ﾙｰﾏﾆｱ - ﾌﾞｶﾚｽﾄ** Tel: 40-21-407-87-50
	中国 - 珠海 Tel: 86-756-3210040		**ｽﾍﾟｲﾝ - ﾏﾄﾞﾘｰﾄﾞ** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91
			ｽｳｪｰﾃﾞﾝ - ｲｪｰﾃﾎﾞﾘ Tel: 46-31-704-60-40
			ｽｳｪｰﾃﾞﾝ - ｽﾄｯｸﾎﾙﾑ Tel: 46-8-5090-4654
			ｲｷﾞﾘｽ - ｳｫｰｷﾝｶﾞﾑ Tel: 44-118-921-5800 Fax: 44-118-921-5820