AN2747

tinyAVR® 0と1系及びmegaAVR® 0系での頑健性

序説

著者: Per Andreas Gulbrandsen, Øyvind A. Sandberg, Microchip Technology Inc.

「IEEE規格610.12-1990ソフトウェア工学用語の用語集」に於いて頑健性は「無効な入力の存在や負担の多い環境条件でシステムや部品が正しく機能することができる程度」として定義されます。この資料は頑強性応用に使うことができるtinyAVR® 0と1系及びmegaAVR® 0系で利用可能な周辺機能に対する手引きです。

本書は一般の方々の便宜のため有志により作成されたもので、Microchip社とは無関係であることを御承知ください。しおりの[はじめに]での内容にご注意ください。

目次

序説 1

1. 関連デバイス 3
   - 1.1. tinyAVR® 0系統 3
   - 1.2. tinyAVR® 1系統 3
   - 1.3. megaAVR® 0系統 3

2. 電源ONリセット 4

3. 低電圧検出器 4
   - 3.1. 電圧レベル監視部 5

4. ウォッチドッグ タイマ 5

5. CRCSCAN 5

6. 等級B 5

7. 構成設定変更保護 6

8. フラッシュ メモリ領域 6

9. ヒューズ 6

10. 事象と障害処理 7

11. 改訂履歴 7

Microchipウェブ サイト 8

製品変更通知サービス 8

お客様支援 8

Microchipデバイス コード保護機能 8

法的通知 8

商標 9

品質管理システム 9

世界的な販売とサービス 10

1. 関連ﾃﾞﾊﾞｲｽ

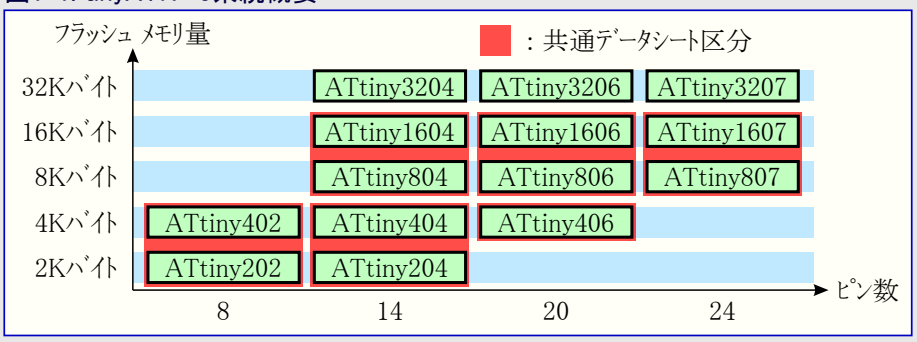
本章はこの資料に関連するﾃﾞﾊﾞｲｽを一覧にします。

1.1. tinyAVR® 0系統

下図はﾋﾟﾝ数の変種とﾒﾓﾘ量を展開してtinyAVR® 0系統ﾃﾞﾊﾞｲｽを示します。

- これらのﾃﾞﾊﾞｲｽがﾋﾟﾝ互換で同じまたはより多くの機能を提供するため、垂直上方向移植はｺｰﾄﾞ変更なしで可能です。
- 左への水平方向移植はﾋﾟﾝ数、従って利用可能な機能を減らします。

図1-1. tinyAVR® 0系統概要



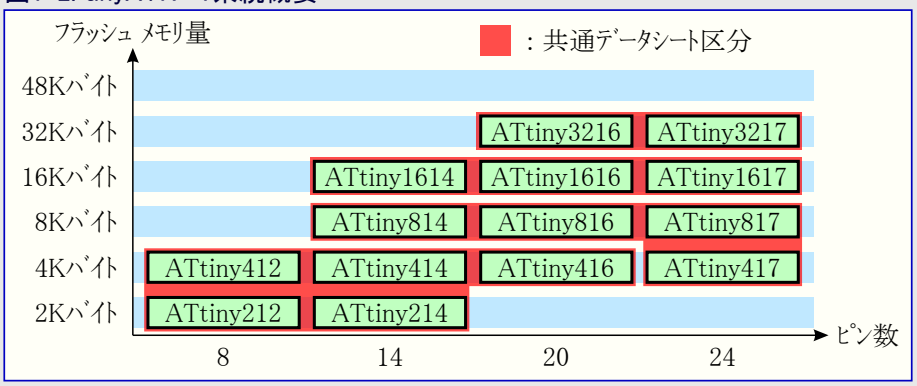
異なるﾌﾗｯｼｭ メモリ量を持つﾃﾞﾊﾞｲｽは一般的に異なるSRAMとEEPROMの量を持ちます。

1.2. tinyAVR® 1系統

下図はﾋﾟﾝ配置変種とﾒﾓﾘ量を展開してtinyAVR 1系統ﾃﾞﾊﾞｲｽを示します。

- これらのﾃﾞﾊﾞｲｽがﾋﾟﾝ互換で同じまたはより多くの機能を提供するため、垂直上方向移植はｺｰﾄﾞ変更なしに可能です。下方向移植はより少ない利用可能ないくつかの周辺機能の実体のためにｺｰﾄﾞ変更が必要かもしれません。
- 左への水平方向移植はﾋﾟﾝ数、従って利用可能な機能を減らします。

図1-2. tinyAVR® 1系統概要



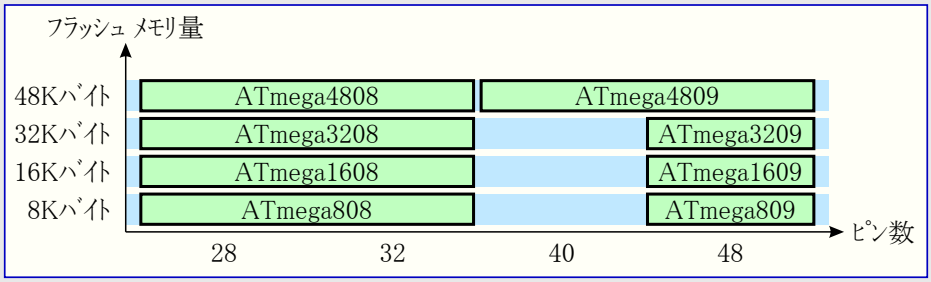
異なるﾌﾗｯｼｭ メモリ量を持つﾃﾞﾊﾞｲｽは一般的に異なるSRAMとEEPROMの量を持ちます。

1.3. megaAVR® 0系統

下図はﾋﾟﾝ配置変種とﾒﾓﾘ量を展開してmegaAVR® 0系統ﾃﾞﾊﾞｲｽを示します。

- これらのﾃﾞﾊﾞｲｽが完全にﾋﾟﾝと機能が互換のため、垂直方向移植はｺｰﾄﾞ変更なしで可能です。
- 左への水平方向移植はﾋﾟﾝ数、従って利用可能な機能を減らします。

図1-3. megaAVR® 0系統概要



異なるﾌﾗｯｼｭ メモリ量を持つﾃﾞﾊﾞｲｽは一般的に異なるSRAMとEEPROMの量を持ちます。

2. 電源ONﾘｾｯﾄ

電源ONﾘｾｯﾄ(POR:Power-On Reset)回路は電源ONﾘｾｯﾄと呼ばれているﾃﾞﾊﾞｲｽが電源ONの時にﾘｾｯﾄされることを保証する構成設定不能な回路です。PORの間に、全ての論理回路がﾘｾｯﾄされ、ﾋｭｰｽﾞから設定されるﾚｼﾞｽﾀを含む全てのﾚｼﾞｽﾀが初期化されます。この手順はMCUが既知の良好な状態で実行を始めることを保証します。

POR回路は常に活性で、上昇と下降のどちらかと固定の閾値ﾚﾍﾞﾙで供給電圧と比較することによって動きます。これらの閾値ﾚﾍﾞﾙはBODﾚﾍﾞﾙと異なり構成設定することができません。「3. 低電圧検出器」章をご覧ください。

POR上昇閾値ﾚﾍﾞﾙとPOR下降閾値ﾚﾍﾞﾙの両方は関連ﾃﾞﾊﾞｲｽのﾃﾞｰﾀｼｰﾄの「電気的特性」章で指定されます。

供給電圧が上昇閾値以下の時にPOR回路は内部ﾘｾｯﾄを真にします。供給電圧が閾値以上に上がると、ﾃﾞﾊﾞｲｽは始動が許されます。

電力低下の場合、POR回路は供給電圧をPOR下降閾値ﾚﾍﾞﾙと比較します。供給電圧低下がこの閾値以下の場合、供給電圧が再びPOR上昇閾値ﾚﾍﾞﾙ以上に上がるまで内部ﾘｾｯﾄが解放されます。

ﾃﾞﾊﾞｲｽがPORによってﾘｾｯﾄされた場合、ﾘｾｯﾄ ﾌﾗｸﾞ ﾚｼﾞｽﾀ(RSTCTRL.RSTFR)の電源ONﾘｾｯﾄ ﾌﾗｸﾞ(PORF)が設定(1)されます。POR後、PORﾌﾗｸﾞ(PORF)だけが設定(1)され、他のﾌﾗｸﾞは解除(0)されます。

3. 低電圧検出器

CPUが命令を成功裏に復号して実行するために、供給した電圧は常に最小電圧水準以上に留まらなければなりません。この水準は選んだ動作周波数によって定義されます。例えば、関連ﾃﾞﾊﾞｲｽで10MHzの動作周波数では最小2.7Vの動作電圧が供給されなければなりません。電圧がこの閾値以下に低下した場合、ﾏｲｸﾛ ｺﾝﾄﾛｰﾗ(MCU)の予期せぬ動きが起こるかもしれません。それは命令の不正な実行、CPUﾚｼﾞｽﾀの化け、ﾌﾗｯｼｭ ﾒﾓﾘ化け、ﾋﾟﾝの予期せぬ切り替えを含み得ます。また、論理回路をﾗｯﾁｱｯﾌﾟにし、ひょっとすると不正な状態に入るかもしれません。

上の問題を避けるために、低電圧検出器(BOD:Brown-Out Detector)を使うことができます。関連ﾃﾞﾊﾞｲｽは電源を監視して設定可能な低電圧閾値ﾚﾍﾞﾙと比較する、構成設定可能なBODをﾁｯﾌﾟ上に含みます。BODは供給電圧が構成設定した閾値ﾚﾍﾞﾙを横切ったことを検出すると、内部ﾘｾｯﾄを真にします。供給電圧が構成設定した閾値ﾚﾍﾞﾙ以下に留まる限り、ﾃﾞﾊﾞｲｽがﾘｾｯﾄを保ちます。供給電圧が閾値ﾚﾍﾞﾙを超えると、標準動作を安全に続けることができ、BODは内部ﾘｾｯﾄを偽にして命令実行をﾃﾞﾊﾞｲｽに許します。

ﾘｾｯﾄ後、BOD設定はﾋｭｰｽﾞから読んで設定されます。BOD機能を制御するのに2つのﾋｭｰｽﾞがあり、これらはﾃﾞﾊﾞｲｽのﾃﾞｰﾀｼｰﾄでﾋｭｰｽﾞ下のBOD構成設定(BODCFG)で見つかります。

1つ目のﾋｭｰｽﾞのACTIVEは活動動作またはｱｲﾄﾞﾙ休止動作中の動作形態を定義します。これらのﾋﾞｯﾄはｿﾌﾄｳｪｱによって変えることはできません。

2つ目のﾋｭｰｽﾞのSLEEPはｽﾀﾝﾊﾞｲまたはﾊﾟﾜｰﾀﾞｳﾝ動作の休止中の動作形態を定義します。これらのﾋﾞｯﾄはｿﾌﾄｳｪｱによって変えることができ、構成設定変更保護(CCP)下です。

ACTIVEとSLEEPのﾋｭｰｽﾞは以下のように構成設定することができます。

- 禁止動作 – BODが不活性にされます。
- 許可動作 – BODが継続的に活性なことを意味します。
- 採取動作 – 供給電圧水準を調べるためにBODが与えられた期間で一時的に活性にされます。頻度は採取周波数(BODCFG.SAMPFREQ)ﾋｭｰｽﾞで125Hzまたは1kHzのどちらかに設定されます。

また、ACTIVEは次の4つ目の任意選択を持ちます。

- BODの準備が整うまで停止された起床で許可 – BODは休止中に不活性です。起き上がりで、BODの準備が整うまでｺｰﾄﾞ実行が停止されます。これはｺｰﾄﾞが実行される時は必ず正しい供給電圧であることを保証します。起き上がり時間が延長されるかもしれません。

採取周波数(SAMPFREQ)とBODﾚﾍﾞﾙ(LVL)もBODCFGで見つかります。これらはBODの動きを制御します。

BODﾚﾍﾞﾙ

BODは閾値ﾚﾍﾞﾙに対して供給電圧を比較します。この閾値は設定可能で使用者は8つの異なるﾚﾍﾞﾙから選ぶことができます。**表3-1.**はATtiny3217のﾃﾞｰﾀｼｰﾄからのBODﾚﾍﾞﾙを示します。正しいBODﾚﾍﾞﾙについては常に関連ﾃﾞﾊﾞｲｽのﾃﾞｰﾀｼｰﾄを調べてください。

表3-1. BOD閾値ﾚﾍﾞﾙ例

名称	BODLEVEL0	BODLEVEL2	BODLEVEL7
説明	1.80V	2.60V	4.30V

BODﾚﾍﾞﾙ設定時、考慮に至るいくつかの事があります。既に言及したように、BODは安全でない操作からｼｽﾃﾑを保護することができます。加えてBODは、例えばADC使用時に電圧ﾚﾍﾞﾙを保証するのに使うことができます。ADCが4.3V内部参照基準を使う採取に設定され、供給電圧がこのﾚﾍﾞﾙ以下に低下する場合、ADCの結果は不正になります。

BODが使われない場合、内部ﾘｾｯﾄとﾁｯﾌﾟ消去の間の安全な動作を保証するために最小ﾚﾍﾞﾙに設定されます。

3.1. 電圧ﾚﾍﾞﾙ監視部

電圧ﾚﾍﾞﾙ監視部(VLM:Voltage Level Monitor)は早期警告として働き、供給電圧が与えられた閾値水準以下へまさに低下しようとしている場合に割り込みを要求します。これは安全な停止を行うことをｼｽﾃﾑに許すことができます。

BOD周辺機能の一部であることで、VLM閾値水準はBODﾚﾍﾞﾙ以上の5%、15%、25%のどれかに構成設定することができます。VLMはBOD機能に従います。BODが採取動作の場合、VLMも採取動作にされます。BODが禁止されるなら、VLMも禁止されます。

VLM割り込みは供給電圧が閾値水準を上から、下から、またはどちらかで横切る時に起動することができます。

4. ｳｫｯﾁﾄﾞｯｸﾞ ﾀｲﾏ

多くの問題、例えば、ｿﾌﾄｳｪｱ ﾊﾞｸﾞや電気的雑音はｼｽﾃﾑを不正や固まり状態にさせ得ます。関連ﾃﾞﾊﾞｲｽで利用可能な1つの安全処置はｳｫｯﾁﾄﾞｯｸﾞ ﾀｲﾏ(WDT:WatchDog Timer)です。これは独立したｸﾛｯｸ元を持ち、ｼｽﾃﾑの残りから独立して動く計時器です。この計時器が溢れると、ﾘｾｯﾄを引き起こします。ｼｽﾃﾑ ﾌｧｰﾑｳｪｱは専用のｳｫｯﾁﾄﾞｯｸﾞ ﾀｲﾏ ﾘｾｯﾄ(WDR:WatchDog timer Reset)命令を用いて周期的にWDTを解消(=0)しなければなりません。ﾌｧｰﾑｳｪｱが例えば、ｼｽﾃﾑ中断や逸脱ｺｰﾄﾞのためにそのように行うことができない場合、ｼｽﾃﾑがﾘｾｯﾄされます。

標準動作

標準動作ではｳｫｯﾁﾄﾞｯｸﾞは0から最大値まで計数し、何時でも解消(=0)することができます。標準動作での周期は8ms～8sの期間で構成設定することができます。

窓動作

頑健性を増すために窓動作が利用可能です。窓動作では閉鎖と開放の両窓が構成設定され、閉鎖窓が周期の始めになります。閉鎖窓の間、WDTの解消は無効操作で、ﾘｾｯﾄに帰着します。一旦閉鎖窓が終わると、開放窓が始まり、今やWDTは解消することができます。窓動作の使用はそれが解放窓でだけｳｫｯﾁﾄﾞｯｸﾞを解消しなければならないため、ﾌｧｰﾑｳｪｱでの更なる必要条件にします。両方の窓は8ms～8sの期間で構成設定することができます。これは16ms～16sの総WDT周期を与えます。

WDT周期と窓制限時間はﾘｾｯﾄ後直ちに活性になるように、ﾋｭｰｽﾞによって構成設定することができます。ﾌｧｰﾑｳｪｱに問題があって正しく開始させない場合、WDTはｼｽﾃﾑをﾘｾｯﾄします。WDTはﾘｾｯﾄ元に関わらず、ﾘｾｯﾄ後に0から計数します。

ｳｫｯﾁﾄﾞｯｸﾞ ﾀｲﾏ実装の目標の1つが暴走ｺｰﾄﾞから回復し得ることであるため、ｿﾌﾄｳｪｱ技術者が考慮する可能性があるいつくかのものがあります。暴走ｺｰﾄﾞは割り込みの実行に影響しません。例えｼｽﾃﾑがいくつかの理由のために不正なｺｰﾄﾞを実行している時でも、どの割り込みﾍﾞｸﾀも正しく読まれます。従って、割り込み処理部からWDTを解消しないでください。また、WDR命令の量を制限することを試みてください。WDT解消がﾌｧｰﾑｳｪｱの多くの部分で行われる場合、暴走ｺｰﾄﾞが実行されつつある時にそれらの1つが実行される可能性がより高くなります。理想的には、1つのWDR命令だけが実装されるかもしれません。これは達成が難しいかもしれませんが、WDR命令の量の制限を試みることは重要です。窓動作の使用は誤って実行されるWDR命令を捕らえるのにも役立ち得ます。

5. CRCSCAN

巡回冗長検査(CRC:Cyclic Redundancy Check)はﾃﾞｰﾀの塊に対してﾁｪｯｸｻﾑを作成し、ﾃﾞｰﾀ塊の誤り検出を許します。関連ﾃﾞﾊﾞｲｽはﾌﾗｯｼｭ ﾒﾓﾘ領域を調べてそれを領域の最後に格納されたﾁｪｯｸｻﾑと比較することができるCRCSCAN周辺機能が特徴です。ﾌﾗｯｼｭ ﾒﾓﾘ領域が図らずも、即ち、化けまたは予期せぬ書き込みのために変更された場合、CRCSCANはこれを検出してﾌﾗｯｼｭ ﾒﾓﾘが不正にされてしまったことをCPUに合図します。

ﾌﾞｰﾄﾛｰﾀﾞ応用では実行を開始する前に応用ｲﾒｰｼﾞを検証するのにCRCSCANを使うことができます。これは壊滅的な結果を持ち得る不正なｿﾌﾄｳｪｱが実行されないことを確実にします。検査が失敗した場合、ﾌﾞｰﾄﾛｰﾀﾞは応用を開始しない、ﾌｧｰﾑｳｪｱ更新を行う可能性、または外部ｼｽﾃﾑに異常を合図する可能性のどれかを選ぶことができます。

CRCSCANは始動で、または応用によって制御される特定間隔で動かすことができます。始動での走行時、ﾌﾗｯｼｭ ﾒﾓﾘはどの命令も実行されるのに先立って異常に対して調べられます。これは実行前に検証されるべき応用の完全性が許します。始動でのCRCSCANはﾋｭｰｽﾞによって構成設定されます。

CRCSCANが応用によって制御される時に、それはﾚｼﾞｽﾀ ｱｸｾｽによって開始されます。開始されると、CRCSCANがﾌﾗｯｼｭ ﾒﾓﾘに対するｱｸｾｽの優先権を持ち、従ってCPUを防ぐため、CPUは検査が行われている間、停止されます。

より多くの情報については「tinyAVR® 0と1系及びmegaAVR® 0系でのCRCSCAN」応用記述を参照してください。

6. 等級B

現代の機器は大部分が電気的に制御されています。電気的制御はより高い効率、付加的な機能、改善された使用者経験を許します。しかし、何かが悪くなると何が起きますか?。IEC 60730は機器に於ける電気的制御の安全性を扱います。この規格は安全性が重要な装置に対する別の規格、例えばIEC 60335によっても参照されます。現在、IEC 60730は欧州で販売される機器に対して必須です。

IEC 60730付属書Hは以下のように機器に対する3つの制御ｿﾌﾄｳｪｱの等級を定義します。

- 等級A – 装置の安全性に頼ることを意図されない制御機能
- 等級B – 機器でｿﾌﾄｳｪｱ障害以外の障害が起きた場合に危険を防ぐことを意図されるｺｰﾄﾞを含むｿﾌﾄｳｪｱ
- 等級C – 他の保護装置の使用なしで危険を防ぐことを意図されるｺｰﾄﾞを含むｿﾌﾄｳｪｱ

等級B要件に準拠する機器に関して制御ｿﾌﾄｳｪｱはｼｽﾃﾑ構成部品に対する障害を検出して処理しなければなりません。等級B要件に従って製品を認証したいお客様に対し、MicrochipはtinyAVR® 1用等級Bﾗｲﾌﾞﾗﾘを提供します。このﾗｲﾌﾞﾗﾘは等級Bに従うのに必要とされる検査を実装し、開発時間と検定費用を減らすことができます。

検査はCPUﾚｼﾞｽﾀ、ﾌﾟﾛｸﾞﾗﾑ ｶｳﾝﾀ、周波数、CRC、割り込み処理と実行、ｸﾛｯｸ、SRAM、ﾌﾗｯｼｭ ﾒﾓﾘ、EEPROM、それとADC、DAC、WDTのような周辺機能で行われます。

より多くの情報については「tinyAVR® 1系でのIEC 60730等級B適合への指針」応用記述を参照してください。

7. 構成設定変更保護

ｼｽﾃﾑで重要なﾚｼﾞｽﾀは偶然の変更から保護され、ﾌﾗｯｼｭ自己ﾌﾟﾛｸﾞﾗﾐﾝｸﾞは偶然の実行から保護されます。これは構成設定変更保護(CPU.CCP)ﾚｼﾞｽﾀによって広範囲に保護されます。これらのどちらかの活動の実行はCCPﾚｼﾞｽﾀに識票が書かれた後でだけ可能です。CCPﾚｼﾞｽﾀに正しい識票が書かれた後、4命令内で臨む活動が実行されなければなりません。これら4周期の間、割り込みは保留を保たれます。

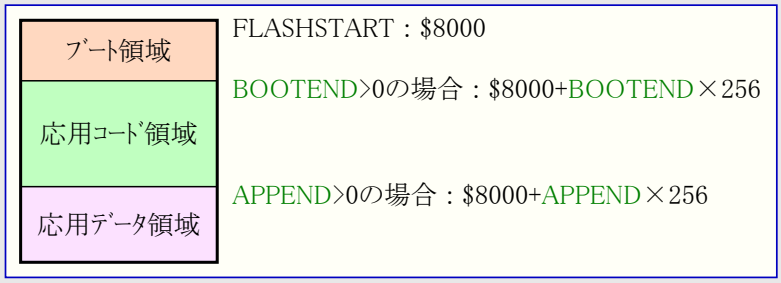
CCPの詳細については関連ﾃﾞﾊﾞｲｽのﾃﾞｰﾀｼｰﾄでCPU章を参照してください。

8. ﾌﾗｯｼｭ ﾒﾓﾘ領域

関連ﾃﾞﾊﾞｲｽのﾌﾗｯｼｭ ﾒﾓﾘはﾌﾞｰﾄﾛｰﾀﾞ(BOOT)、応用ｺｰﾄﾞ(APPCODE)、応用ﾃﾞｰﾀ(APPDATA)の3つの独立した領域に分けることができます。この仕組みはｺｰﾄﾞまたはﾃﾞｰﾀのいくつかの個別区部の保護と安全な記憶を許します。分割の細かさは256ﾊﾞｲﾄです。

3つの領域の大きさはﾌﾞｰﾄ領域の最後(BOOTEND)と応用ｺｰﾄﾞ領域の最後(APPEND)のﾋｭｰｽﾞを用いて設定されます。BOOTENDはBOOT領域の大きさを決めます。APPENDはAPPCODE領域の大きさを決めます。APPCODE領域はBOOT領域の直後に置かれます。残りのﾍﾟｰｼﾞがAPPDATA領域で、APPCODE領域の直後に置かれます。両ﾋｭｰｽﾞが0に設定された場合、全ﾍﾟｰｼﾞがBOOT領域に割り当てられます。これはﾌﾞｰﾄﾛｰﾀﾞなしでﾌﾗｯｼｭ ﾒﾓﾘに応用だけが書かれる場合の標準的な手順です。

図8-1. ﾌﾗｯｼｭ ﾒﾓﾘ領域



FUSE.BOOTENDが$04を書かれ、FUSE.APPEDが$08を書かれた場合、最初の4×256ﾊﾞｲﾄがBOOTで、次の4×256ﾊﾞｲﾄがAPPCODE、そして残りのﾌﾗｯｼｭ ﾒﾓﾘがAPPDATAです。

3つの領域でﾃﾞｰﾀを保護するため、以下の方向性書き込み保護が実装されます。

- BOOT領域のｺｰﾄﾞはAPPCODEとAPPDATAに書くことができます。
- APPCODE領域のｺｰﾄﾞはAPPDATAに書くことができます。
- APPDATA領域のｺｰﾄﾞはﾌﾗｯｼｭ ﾒﾓﾘやEEPROMに書くことができません。

方向性書き込み保護に加えて、制限を増すために2つのﾚｼﾞｽﾀ ﾋﾞｯﾄを使うことができます。

応用ｺｰﾄﾞ領域書き込み保護(APCWP)ﾋﾞｯﾄに1を書くことにより、応用ｺｰﾄﾞ領域は更なる書き込みから保護されます。このﾋﾞｯﾄは不揮発性ﾒﾓﾘ制御器(NVMCTRL)周辺機能の制御B(CTRLB)ﾚｼﾞｽﾀで見つけることができます。このﾋﾞｯﾄはﾘｾｯﾄで解除(0)されます。

BOOT領域がCPUによって決して書かれ得ないため、同じ規則で書き込みからBOOT領域を保護する必要はありません。しかし、NVMCTRL周辺機能のCTRLBﾚｼﾞｽﾀでﾌﾞｰﾄ領域施錠(BOOTLOCK)ﾋﾞｯﾄに1を書くことにより、BOOT領域からの読み込みと実行を防ぐことができます。このﾋﾞｯﾄはﾘｾｯﾄで解除(0)されます。

より多くの詳細ついては関連ﾃﾞﾊﾞｲｽのﾃﾞｰﾀｼｰﾄで不揮発性ﾒﾓﾘ制御器(NVMCTRL)章を参照してください。

9. ﾋｭｰｽﾞ

ﾋｭｰｽﾞは不揮発性ﾒﾓﾘの一部で、ｸﾛｯｸ元、始動時間、ﾌﾗｯｼｭ ﾒﾓﾘ領域などのようなｼｽﾃﾑ設定を構成設定するのに使われます。ﾋｭｰｽﾞはCPUと外部書き込み器の両方によって読むことができますが、外部書き込みによってのみ書かれるまたは消去されることができます。発振器校正のようないくつかのﾚｼﾞｽﾀはﾋｭｰｽﾞに格納された値にﾘｾｯﾄされます。これらの値は始動手順の最後で書かれます。従って、このようなﾋｭｰｽﾞが変更されると、ﾃﾞﾊﾞｲｽは変更が有効になるのに先立ってﾘｾｯﾄされなければなりません。

周辺機能構成用ﾋｭｰｽﾞは以下を含みます。

- ｳｫｯﾁﾄﾞｯｸﾞ ﾀｲﾏ：始動でのWDT窓と制限時間周期を設定するのに使い、故に操作のためにどんなｺｰﾄﾞ実行も不要です。
- 低電圧検出器：BODﾚﾍﾞﾙ、採取周波数、活動とｽﾀﾝﾊﾞｲでの動作形態を設定するのに使い、故に操作のためにどんなｺｰﾄﾞ実行も不要です。
- 16/20MHz発振器：動作周波数を16または20MHzのどちらかにすべきかを構成設定します。校正ﾚｼﾞｽﾀはそれらが工場校正値で設定された後に施錠することも可能です。
- ﾀｲﾏ/ｶｳﾝﾀD：TCD出力ﾋﾟﾝを許可または禁止するのとﾋﾟﾝ既定状態を設定するのにも使います。このﾋｭｰｽﾞはtinyAVR® 1系ﾃﾞﾊﾞｲｽでだけ利用可能です。

- システム構成設定0：始動で動くようにCRCSCANを構成設定し、調べるフラッシュ メモリ領域を選ぶのに使います。
- システム構成設定1：デバイスの追加始動時間を構成設定するのに使います。
- 応用コードの最後：応用コード領域の大きさを構成設定するのに使います。
- BOOTの最後：ブート領域の大きさを構成設定するのに使います。
- 施錠ビット：デバイスを施錠してヒューズ、フラッシュ メモリ、SRAM、EEPROMのアクセスから外部書き込み器を防ぐのに使われます。応用内からの通常のメモリ アクセスは未だ許されます。デバイスを解錠するにはチップ消去が実行されなければなりません

例えば、どんなコードも実行されるのに先立ってWDTを構成設定するのにヒューズを使うことはシステムの頑健性を増します。これは不正なフラッシュ メモリがWDTのソフトウェア駆動の構成設定を失敗させるためです。WDTを許可する命令が不正で正常に実行されないことを想像してください。その結果は不正を行うシステムで、異常な動きを検出するための機構が禁止されます。従って、ヒューズを用いる安全性機能の許可は優位点です。

ヒューズを用いてCRCSCANを許可することはどれかの命令がフラッシュ メモリから取得される前に異常に対して走査されることをフラッシュ メモリに許します。

より多くの情報ついては関連デバイスのデータシートでヒューズ節を参照してください。

10. 事象と障害処理

この章はtinyAVR® 1系のデバイスに対してだけ関係します。タイマ/カウンタD型(TCD)は特にLED駆動、電動機制御、半ブリッジ、電力変換器のような電力応用を制御するように設計されています。TCDの重要な安全機能は組み込み障害処理部です。障害処理部は障害で予め定義されたレベルに固定することをTCDの出力に許します。障害はやって来る事象で、その条件を発見するためにいくつかの他の割り込みや外部周辺機能が存在しなければなりません。

送風機用の電動機を駆動するTCDを想像してください。送風機にアナログ比較器(AC)も接続され、電流消費を監視します。例えば、何かが送風機を動かなくするために電流消費が予め定義された閾値を超えて上がる場合、ACがTCDに事象を送ります。この事象受け取りで、TCDは直ちに全ての出力を予め定義されたレベルに固定し、電動機は停止します。このように、電動機は過熱または妨害を引き起こした物を破壊する前に安全に停止されます。

内部周辺機能の代わりに外部回路を使うと、事象は外部回路に接続されたピンのレベルで端または変化によって生成されます。また、この事象はTCDに送られ直ちに全ての出力を予め定義された状態に固定します。

事象は事象システム(EVSYS)経由で送られます。EVSYSは周辺機能から周辺機能への直接の合図を許します。1つの周辺機能(事象発生部)はCPUを使うことなく、1つまたはいくつかの他の周辺機能(事象使用部)に合図することができます。

記述された例の全ての部分は、例えCPUが行き詰まりにされていてもを意味する、コアから独立(CIP:Core IndePendent)で、この安全機能は意図されたように動くでしょう。

11. 改訂履歴

資料改訂	日付	注釈
A	2018年6月	初版資料公開
B	2018年10月	「**関連デバイス**」章を8/16KバイトmegaAVR 0系デバイスを含めるように更新
C	2019年11月	応用記述がtinyAVR® 0系とmegaAVR® 0系にも関連するのを反映させるように表題変更 **表3-1.**で未支援BODレベルを削除 「**等級B**」、「**ヒューズ**」、「**事象と障害処理**」章でtinyAVR® 1系特有機能を明確化

Microchipｳｪﾌﾞ ｻｲﾄ

Microchipはhttp://www.microchip.com/で当社のｳｪﾌﾞ ｻｲﾄ経由でのｵﾝﾗｲﾝ支援を提供します。このｳｪﾌﾞ 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** – ﾃﾞｰﾀｼｰﾄと障害情報、応用記述と試供ﾌﾟﾛｸﾞﾗﾑ、設計資源、使用者の手引きとﾊｰﾄﾞｳｪｱ支援資料、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、ｵﾝﾗｲﾝ検討ｸﾞﾙｰﾌﾟ、Microchip設計協力課程会員一覧
- **Microshipの事業** – 製品選択器と注文の手引き、最新Microchip報道発表、ｾﾐﾅｰとｲﾍﾞﾝﾄの一覧、Microchip営業所の一覧、代理店と代表する工場

製品変更通知ｻｰﾋﾞｽ

Microchipの製品変更通知ｻｰﾋﾞｽは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http://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http://www.microchip.com/supportでのｳｪﾌﾞ ｻｲﾄを通して利用できます。

Microchipﾃﾞﾊﾞｲｽ ｺｰﾄﾞ保護機能

Microchipﾃﾞﾊﾞｲｽでの以下のｺｰﾄﾞ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ﾃﾞｰﾀｼｰﾄに含まれる仕様に合致します。
- Microchipは意図した方法と通常条件下で使われる時に、その製品系統が今日の市場でその種類の最も安全な系統の1つであると考えます。
- ｺｰﾄﾞ保護機能を破るのに使われる不正でおそらく違法な方法があります。当社の知る限りこれらの方法の全てはMicrochipのﾃﾞｰﾀｼｰﾄに含まれた動作仕様外の方法でMicrochip製品を使うことが必要です。おそらく、それを行う人は知的財産の窃盗に関与しています。
- Microchipはそれらのｺｰﾄﾞの完全性について心配されているお客様と共に働きたいと思います。
- Microchipや他のどの半導体製造業者もそれらのｺｰﾄﾞの安全を保証することはできません。ｺｰﾄﾞ保護は当社が製品を”破ることができない”として保証すると言うことを意味しません。

ｺｰﾄﾞ保護は常に進化しています。Microchipは当社製品のｺｰﾄﾞ保護機能を継続的に改善することを約束します。Microchipのｺｰﾄﾞ保護機能を破る試みはﾃﾞｼﾞﾀﾙ ﾐﾚﾆｱﾑ著作権法に違反するかもしれません。そのような行為があなたのｿﾌﾄｳｪｱや他の著作物に不正なｱｸｾｽを許す場合、その法律下の救済のために訴権を持つかもしれません。

法的通知

ﾃﾞﾊﾞｲｽ応用などに関してこの刊行物に含まれ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。**Microchipはその条件、品質、性能、商品性、目的適合性を含め、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。**Microchipはこの情報とそれの使用から生じる全責任を否認します。生命維持や安全応用でのMicrochipﾃﾞﾊﾞ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

Microchipの名前とﾛｺﾞ、Mcicrochipﾛｺﾞ、Adaptec、AnyRate、AVR、AVRﾛｺﾞ、AVR Freaks、BesTime、BitCloud、chipKIT、chipKITﾛｺﾞ、CryptoMemory、CryptoRF、dsPIC、FlashFlex、flexPWR、HELDO、IGLOO、JukeBlox、KeeLoq、Kleer、LANCheck、LinkMD、maXStylus、maXTouch、MediaLB、megaAVR、Microsemi、Microsemiﾛｺﾞ、MOST、MOSTﾛｺﾞ、MPLAB、OptoLyzer、PackeTime、PIC、picoPower、PICSTART、PIC32ﾛｺﾞ、PolarFire、Prochip Designer、QTouch、SAM-BA、SenGenuity、SpyNIC、SST、SSTﾛｺﾞ、SuperFlash、Symmetricom、SyncServer、Tachyon、TempTracker、TimeSource、tinyAVR、UNI/O、Vectron、XMEGAは米国と他の国に於けるMicrochip Technology Incor poratedの登録商標です。

APT、ClockWorks、The Embedded Control Solutions Company、EtherSynch、FlashTec、Hyper Speed Control、HyperLight Load、IntelliMOS、Libero、motorBench、mTouch、Powermite 3、Precision Edge、ProASIC、ProASIC Plus、ProASIC Plusﾛｺﾞ、Quiet-Wire、SmartFusion、SyncWorld、Temux、TimeCesium、TimeHub、TimePictra、TimeProvider、Vite、WinPath、ZLは米国に於けるMicrochip Technology Incorporatedの登録商標です。

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、BlueSky、BodyCom、CodeGuard、CryptoAuthentication、CryptoCompanion、CryptoController、dsPICDEM、dsPICDEM.net、Dynamic Average Matching、DAM、ECAN、EtherGREEN、In-Circuit Serial Programming、ICSP、INICnet、Inter-Chip Connectivity、JitterBlocker、KleerNet、KleerNetﾛｺﾞ、memBrain、Mindi、MiWi、MPASM、MPF、MPLAB Certifiedﾛｺﾞ、MPLAB、MPLINK、MultiTRAK、NetDetach、Omniscient Code Generation、PICDEM、PICDEM.net、PICkit、PICtail、PowerSmart、PureSilicon、QMatrix、REALICE、Ripple Blocker、SAM-ICE、Serial Quad I/O、SMART-I.S.、SQI、SuperSwitcher、SuperSwitcher II、Total Endurance、TSHARC、USBCheck、VariSense、View Sense、WiperLock、Wireless DNA、ZENAは米国と他の国に於けるMicrochip Technology Incorporatedの商標です。

SQTPは米国に於けるMicrochip Technology Incorporatedの役務標章です。

Adaptecﾛｺﾞ、Frequency on Demand、Silicon Storage Technology、Symmcomは他の国に於けるMicrochip Technology Inc.の登録商標です。

GestICは他の国に於けるMicrochip Technology Inc.の子会社であるMicrochip Technology Germany II GmbH & Co. KGの登録商標です。

ここで言及した以外の全ての商標はそれら各々の会社の所有物です。

© 2019年、Microchip Technology Incorporated、米国印刷、不許複製

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http://www.microchip.com/qualityを訪ねてください。

日本語© *HERO* 2021.

本応用記述はMicrochipのAN2747応用記述(DS00002747C-2019年11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: http://www.microchip.com/support ｳｪﾌﾞｱﾄﾞﾚｽ: http://www.microchip.com **ｱﾄﾗﾝﾀ** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **ｵｰｽﾁﾝ** TX Tel: 512-257-3370 **ﾎﾞｽﾄﾝ** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **ｼｶｺﾞ** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **ﾀﾞﾗｽ** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **ﾃﾞﾄﾛｲﾄ** Novi, MI Tel: 248-848-4000 **ﾋｭｰｽﾄﾝ** TX Tel: 281-894-5983 **ｲﾝﾃﾞｱﾅﾎﾟﾘｽ** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **ﾛｻﾝｾﾞﾙｽ** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **ﾛｰﾘｰ** NC Tel: 919-844-7510 **ﾆｭｰﾖｰｸ** NY Tel: 631-435-6000 **ｻﾝﾎｾ** CA Tel: 408-735-9110 Tel: 408-436-4270 **ｶﾅﾀﾞ - ﾄﾛﾝﾄ** Tel: 905-695-1980 Fax: 905-695-2078	**ｵｰｽﾄﾗﾘｱ - ｼﾄﾞﾆｰ** Tel: 61-2-9868-6733 **中国 - 北京** Tel: 86-10-8569-7000 **中国 - 成都** Tel: 86-28-8665-5511 **中国 - 重慶** Tel: 86-23-8980-9588 **中国 - 東莞** Tel: 86-769-8702-9880 **中国 - 広州** Tel: 86-20-8755-8029 **中国 - 杭州** Tel: 86-571-8792-8115 **中国 - 香港特別行政区** Tel: 852-2943-5100 **中国 - 南京** Tel: 86-25-8473-2460 **中国 - 青島** Tel: 86-532-8502-7355 **中国 - 上海** Tel: 86-21-3326-8000 **中国 - 瀋陽** Tel: 86-24-2334-2829 **中国 - 深圳** Tel: 86-755-8864-2200 **中国 - 蘇州** Tel: 86-186-6233-1526 **中国 - 武漢** Tel: 86-27-5980-5300 **中国 - 西安** Tel: 86-29-8833-7252 **中国 - 厦門** Tel: 86-592-2388138 **中国 - 珠海** Tel: 86-756-3210040	**ｲﾝﾄﾞ - ﾊﾝｶﾞﾛｰﾙ** Tel: 91-80-3090-4444 **ｲﾝﾄﾞ - ﾆｭｰﾃﾞﾘｰ** Tel: 91-11-4160-8631 **ｲﾝﾄﾞ - ﾌﾟﾈｰ** Tel: 91-20-4121-0141 **日本 - 大阪** Tel: 81-6-6152-7160 **日本 - 東京** Tel: 81-3-6880-3770 **韓国 - 大邱** Tel: 82-53-744-4301 **韓国 - ｿｳﾙ** Tel: 82-2-554-7200 **ﾏﾚｰｼｱ - ｸｱﾗﾙﾝﾌﾟｰﾙ** Tel: 60-3-7651-7906 **ﾏﾚｰｼｱ - ﾍﾟﾅﾝ** Tel: 60-4-227-8870 **ﾌｨﾘﾋﾟﾝ - ﾏﾆﾗ** Tel: 63-2-634-9065 **ｼﾝｶﾞﾎﾟｰﾙ** Tel: 65-6334-8870 **台湾 - 新竹** Tel: 886-3-577-8366 **台湾 - 高雄** Tel: 886-7-213-7830 **台湾 - 台北** Tel: 886-2-2508-8600 **ﾀｲ - ﾊﾞﾝｺｸ** Tel: 66-2-694-1351 **ﾍﾞﾄﾅﾑ - ﾎｰﾁﾐﾝ** Tel: 84-28-5448-2100	**ｵｰｽﾄﾘｱ - ｳﾞｪﾙｽ** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **ﾃﾞﾝﾏｰｸ - ｺﾍﾟﾝﾊｰｹﾞﾝ** Tel: 45-4450-2828 Fax: 45-4485-2829 **ﾌｨﾝﾗﾝﾄﾞ - ｴｽﾎﾟｰ** Tel: 358-9-4520-820 **ﾌﾗﾝｽ - ﾊﾟﾘ** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **ﾄﾞｲﾂ - ｶﾞﾙﾋﾝｸﾞ** Tel: 49-8931-9700 **ﾄﾞｲﾂ - ﾊｰﾝ** Tel: 49-2129-3766400 **ﾄﾞｲﾂ - ﾊｲﾙﾌﾞﾛﾝ** Tel: 49-7131-72400 **ﾄﾞｲﾂ - ｶｰﾙｽﾙｰｴ** Tel: 49-721-625370 **ﾄﾞｲﾂ - ﾐｭﾝﾍﾝ** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **ﾄﾞｲﾂ - ﾛｰｾﾞﾝﾊｲﾑ** Tel: 49-8031-354-560 **ｲｽﾗｴﾙ - ﾗｰﾅﾅ** Tel: 972-9-744-7705 **ｲﾀﾘｱ - ﾐﾗﾉ** Tel: 39-0331-742611 Fax: 39-0331-466781 **ｲﾀﾘｱ - ﾊﾟﾄﾞﾊﾞ** Tel: 39-049-7625286 **ｵﾗﾝﾀﾞ - ﾃﾞﾙｰﾈﾝ** Tel: 31-416-690399 Fax: 31-416-690340 **ﾉﾙｳｪｰ - ﾄﾛﾝﾊｲﾑ** Tel: 47-72884388 **ﾎﾟｰﾗﾝﾄﾞ - ﾜﾙｼｬﾜ** Tel: 48-22-3325737 **ﾙｰﾏﾆｱ - ﾌﾞｶﾚｽﾄ** Tel: 40-21-407-87-50 **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