応用記述

宇宙環境応用のための安全管理

ATmegaS128

序説

この資料の狙いは宇宙空間安全応用を開発するために何れのﾊｰﾄﾞｳｪｱやｿﾌﾄｳｪｱの開発者によっても注意して扱われるべきATmegaS128の鍵となるﾊﾟﾗﾒｰﾀを紹介することです。

この資料は放射線環境に対して敏感になり得る機能と応用の段階で考慮されなければならない機能に集中します。加えて、全般的な応用の安全性を改善するためのいくつかの秘訣が提案されます。

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、Atmel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。

Rev. 41086A-05/2016, 41086AJ1-01/2021

1. フラッシュ/EEPROMメモリ管理

1.1. フラッシュ メモリ内容損失回避

ATmegaS128はフラッシュ メモリの内容を固定化するための施錠ビットを持ちます。

フラッシュ メモリ内容のどんな損失も防ぐために施錠ビットを使うことを推奨します。

助言: 書き換え機能が不要なら、(LBxビットを用いずに)BLB0xとBLB1xの施錠ビットを用いてデバイスの施錠を推奨します。

助言: ブートローダ機能が使われるなら、(LBxビットを用いずに)BLB1xの施錠ビットを用いてブートローダ領域の施錠を推奨します。

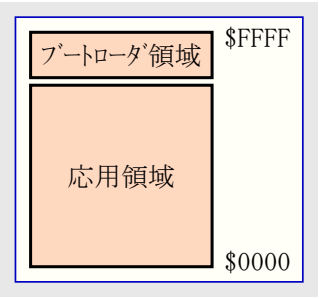
飛行中のプログラミングに関連する危険の完全な理解についてはこの資料の「ブートローダの考慮」章をご覧ください。

1.2. EEPROMメモリ内容損失回避

ATmegaS128はEEPROMメモリの内容を固定化するための施錠ビットを持ちます。

EEPROMメモリ内容のどんな損失も防ぐために施錠ビットを使うことを推奨します。

1.3. 飛行中書き換えの考慮



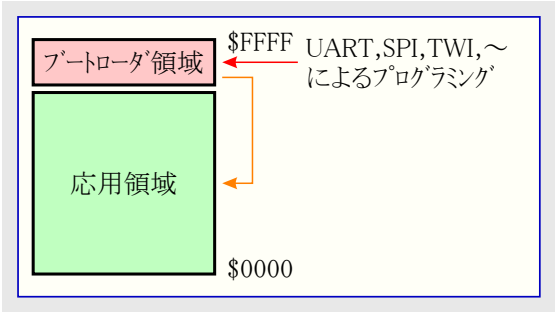
ATmegaS128の一般的な応用はフラッシュ メモリのブートローダ領域に合わせるブートローダとメモリの応用領域での使用者応用に依存します。

注意: 飛行中のフラッシュ メモリ書き換えを避けて、「フラッシュ メモリ内容損失回避」手順に従ってフラッシュ メモリ内容の施錠を強く推奨します。

メモリ(ブートローダと応用の両方)が完全に施錠されると、応用はどの書き込み操作に対しても保護され、故に予期せぬデータ損失を防ぎます。データ保持力も保証されます。施錠されている応用領域は応用書き換えが不能です。

飛行中のフラッシュ書き換えを使わないことを推奨しますが、デバイスを書き換える能力を使うことは可能です。最終使用者がこのような飛行中フラッシュ書き換えの使用を望む場合、この後で提案される可能な2つの構成設定の1つを頼ることができます。

1.3.1. ブート領域からの応用書き換え



この使用事例に対する参照基準構成設定の仮定は以下です。

- ブートローダ領域は施錠されます。 – 「フラッシュ メモリ内容損失回避」手順を参照
- 応用領域は施錠されません。

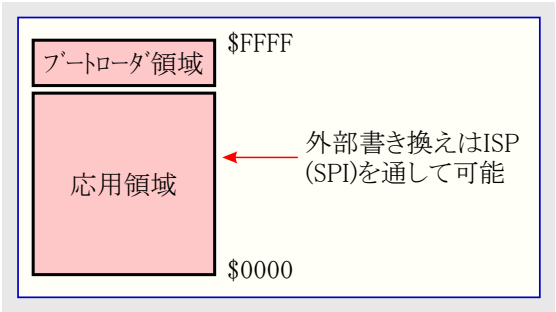
ソフトウェアの重要な領域でのどんな不正も避けるためにブート領域が施錠されると、ATmegaS128は未だブート領域から応用を書き換えることを許します。

ブートローダは予期せぬ損失に対して常に保護されます。ブートローダ領域のデータ保持力は保証されます。

応用領域は予期せぬデータ損失に対して保護されません。

飛行中プログラミング後の応用領域のデータ保持力はATmegaS128放射線報告で提供された書き込み後TID特性付け結果に関して再評価されなければなりません。

1.3.2. ISPインターフェースからの応用書き換え



この使用事例に対する参照基準構成設定の仮定は以下です。

- ブートローダ領域は施錠されます。 – 「フラッシュ メモリ内容損失回避」手順を参照
- 応用領域は施錠されます。 – 「フラッシュ メモリ内容損失回避」手順を参照

ブート領域と応用領域の両方が施錠されると、ブートローダを通して応用領域をこれ以上書き換えるのは不可能で、応用を書き換える唯一の方法は外部ISPを通して書き換えを実行することです。

ブートローダと応用は予期せぬ損失に対して常に保護されます。

飛行中プログラミング後の応用領域のデータ保持力はATmegaS128放射線報告で提供された書き込み後TID特性付け結果に関して再評価されなければなりません。

1.4. ヒューズ ビットの考慮

ATmegaS128はデバイス パラメータの構成設定用ヒューズ ビットの完全な組を組み込みます。フラッシュ メモリ配列それ自身に関して、ヒューズ ビットはSEU耐性です。ヒューズの実用的な効果は電源ONで一度だけ有効で、それらは揮発性メモリ セルにラッチされます。それらの揮発性セルはSEUによって影響を及ぼされ得ます。

重イオンによってこのセルで異常が誘発された場合、障害状態から回復するための唯一の方法はデバイスに対して電源OFF/ON手順を適用することです。

ヒューズ ビット損失はヒューズ ビットが電源ONでだけ採取されるため内部ウォッチドッグによって回復されません。

助言: いくつかのヒューズ ビット機能はクロック選択、BODレベル、ブート リセットとして応用に対して重要です。デバイスの行き詰まりを避けるため、応用がもはや応答しない時にデバイスを電源OFFしてその後にONするための外部機構を実装することを推奨します。このような事象の発生は非常に低いです。より多くの詳細についてはATmegaS128放射線報告を参照してください。

注意: 放射線の考慮に関連しないとは言え、ヒューズ ビットの不正な構成設定は基板で回復するためのどの可能性もなしにデバイスの行き詰まりを引き起こすかもしれません。ヒューズ ビットのどの構成設定にも先立ってハードウェア/ソフトウェアの調整を行ってください。

2. ブートローダの考慮

ATmegaS128のブートローダはデバイスの寿命に沿って応用の書き換えを意図されます。最終使用者がブートローダを通して作業中にそれの応用を書き換えること(フラッシュへの飛行中書き込み)が必要な場合、以下の助言を注意して考慮すべきです。

- 前の項で言及したように、ブートローダ領域(書き換え用の重要なソフトウェア)でのどんな不正も避けるため、ブート コード領域は施錠されるべきです。 – 「フラッシュ メモリ内容損失回避」手順を参照
- 以下の始動手順は正しい使用者応用実行を保証するために特権を与えられるべきです。

  ブートローダ領域へリセットしてブートローダが要求されたかを調べてください。
  a. ブートローダが要求された場合、
     - ブートローダを走らせてください。
  b. ブートローダが要求されない(応用開始が求められる)場合、
     - 応用領域内容(CRCまたはチェックサム)を調べてください。
       - 結果が正しい(応用内容が変更されていない)場合、アドレス$0000へ飛ぶことによって応用を走らせてください。
       - 応用検査が不正の場合、正しい応用を外部から再書き込みするためにブートローダを走らせてください。

注意: 始動手順中にWDTONビットがプログラム(0)されている場合、特にウォッチドッグの動きに気を付けてください。 – ウォチドッグの動きでの推奨の詳細についてはこの後の「**ウォッチドッグの考慮**」章を参照してください。

3. ウォッチドッグの考慮

ATmegaS128はこの応用の予期せぬ制限時間超過を避けるためそのソフトウェア設計で使用者が気を付けなければならないウォッチドッグ起動を組み込みます。

WDTON(ウォッチドッグ常時ON)がプログラム(0)されると、ウォッチドッグはリセット後に(超過に先立つ16kクロック周期の既定構成設定で)直接走行しています。

助言: 偽の制限時間超過なしに応用の正しい動きを保証するため、他のどの実用的な作業のその前に、ウォッチドッグを解消して応用始動ファイルでの応用必要条件に合う値にウォッチドッグを設定することを推奨します。

温度でのウォッチドッグ変動が充分な余力を考慮されなければならないことを使用者に思い出させます。ウォッチドッグ変動の詳細についてはデータシートを参照してください。

4. 内部発振器の考慮

OSCCAL値はリセットで識票列から発振校正(OSCCAL)レジスタに複写されます。

応用でOSCCALレジスタを使う場合、応用の寿命に沿ってそれの整合性を制御できるようにRAMメモリにこのパラメータの複製を作ることを推奨します。SEU事象に対して敏感になるRAMは効果的な検査を許すためにOSCCALパラメータの複製として3つの位置が使われるべきです。

どの場合でもリセットは既定工場値でOSCCALレジスタを再構成します。

5. A/D変換器の考慮

SEUがADC変換結果に影響を及ぼし得るため、複数変換を実行して変換した値を考慮する前に処理することを推奨します。

6. 入出力の考慮

入出力の構成設定に使われるﾚｼﾞｽﾀはPIN/PORT方向ﾚｼﾞｽﾀと入出力値を変更することにより、SEUによって影響を及ぼされ得ます。各入出力ｱｸｾｽに対して最適化された入出力構成設定手順が推奨されます。

6.1. PIN/PORTﾚｼﾞｽﾀ読み込み

助言: どのﾎﾟｰﾄをも読む前にPIN/PORTを入力で規則正しく構成設定してください。

助言: 値を得るのにPIN/PORTの複数読み込みを実行してください。

6.2. PIN/PORTﾚｼﾞｽﾀ書き込み

助言: どのﾎﾟｰﾄをも読む前にPIN/PORTを出力で規則正しく構成設定してください。

6.3. 入出力衝突管理

ﾎﾟｰﾄ方向に影響を及ぼすSEUの場合、入出力線での衝突(同一線での複数駆動部の危険)が現れ得ます。このような衝突を避けるため、以下を推奨します。

- 入出力方向を出力に変更するSEUの場合での衝突を避けるために全ての入力ﾋﾟﾝに線抵抗器を追加してください。
- 誤った方向への長期切り替えを避けるために基本的に速い時間でﾎﾟｰﾄ方向を再設定してください。

7. 通信接続の考慮

7.1. USART

SEUがUSART通信に影響を及ぼし得るため、応用段階でのﾃﾞｰﾀ完全性検査機構の実装を推奨します。異常の場合、送信側は異常の警告をされて受信側へﾃﾞｰﾀ/ﾌﾚｰﾑを再送(するか否か)の決断を下すべきです。

- ﾊｰﾄﾞｳｪｱ段階で、USARTに於いてﾊﾟｲﾄ制御を活性にすることができます。 – USART構成設定の内側ﾊﾟﾘﾃｨ ﾋﾞｯﾄの使用
- 応用段階で、CRC、ﾁｪｯｸｻﾑ、安全検査などを持つﾌﾚｰﾑ制御を実体(ｲﾝｽﾀﾝｽ)化することができます。

7.2. SPI

SEUがSPI通信に影響を及ぼし得るため、応用段階でのﾃﾞｰﾀ完全性検査機構の実装を推奨します。異常の場合、送信側は異常の警告をされて受信側へﾃﾞｰﾀ/ﾌﾚｰﾑを再試行(するか否か)の決断を下すべきです。

- 応用段階で、CRC、ﾁｪｯｸｻﾑ、安全検査などを持つﾌﾚｰﾑ制御を実体(ｲﾝｽﾀﾝｽ)化することができます。

助言: ﾒﾓﾘ ｱｸｾｽにSPIを使う場合、正しいﾃﾞｰﾀ読み込みを保証するために求めるﾒﾓﾘ ｾﾙの数回読み込み実行を推奨します。

7.3. TWI

SEUがTWI通信に影響を及ぼし得るため、応用段階でのﾃﾞｰﾀ完全性検査機構の実装を推奨します。異常の場合、送信側は異常の警告をされて受信側へﾃﾞｰﾀ/ﾌﾚｰﾑを再試行(するか否か)の決断を下すべきです。

- 応用段階で、CRC、ﾁｪｯｸｻﾑ、安全検査などを持つﾌﾚｰﾑ制御を実体(ｲﾝｽﾀﾝｽ)化することができます。

助言: ﾒﾓﾘ ｱｸｾｽにSPIを使う場合、正しいﾃﾞｰﾀ読み込みを保証するために求めるﾒﾓﾘ ｾﾙの数回読み込み実行を推奨します。

8. 全般的な考慮

8.1. コードの動きとコード制限

8.1.1. フラッシュ メモリの既定状態

PCまたはSPの予期せぬ損失の場合、応用はフラッシュ メモリ内の何処でも取得し得ます。

既定により、フラッシュ メモリに於ける未書き込みバイトは$FFに設定されます。$FFFF(16ビット命令符号)はATmegaS128命令一式で有効な次の命令符号に対応します。

“BRS R31,7”　(R31レジスタのビット7が設定(1)なら次を飛ばす。)

PCの損失の場合、PCが書き込んだプログラムの最後以上に行くなら、$0000に転換するまで全てのフラッシュ メモリの取得と実行を続けるでしょう。

助言: 無限繰り返しを許してウォッチドッグ超過をさせる命令符号でフラッシュ メモリの未使用バイトを満たすことを推奨します。$FCFF命令符号の”RJMP @PC”は無限繰り返し命令符号です。

情報: PCは常に語(2バイト)で整列されます。全ての未使用コード メモリが$FCFFで満たされた場合、プロセッサは決して$FFFCを取得しません。

8.1.2. 未知の命令符号

SEU事象のため、データは実行されるべき命令を取得している間に不正にされるかもしれません。予期せぬ命令符号(ATmegaS128命令一式で許されない命令符号)の取得の場合、コアはNOPを実行します。

8.2. 割り込み

予期せぬ割り込み(例えば未使用周辺機能からの割り込み)の場合、使用者ソフトウェアはこのルーチンの内側で何も行わず、単にその割り込みサブルーチンに入って出ることができます。使用者ソフトウェアはデバイスをリセットするためにウォッチドッグを待つ終わり無き繰り返しに移行ように決めることもできます。

助言: 例えそれらが使われなくても、割り込みベクタを全て初期化することを推奨します。

8.3. SFR/レジスタ定期更新

SFRでの全てのSEUの影響を修正するために周期的に全てのSFRをそれらの望まれた値に再設定することを使用者に推奨します。

8.4. システム段階でのFMEA

システム段階に於いて、最終使用者は応用の連続する再設定間で充分な軽減を入念に練るため、ATmegaS128によって管理される各種の信号/事象の重要性について考えるべきです。

すべきこと: 答えられるべき鍵となる点は、

- ➢ 短期間に対して信号が失われた場合に何が起こるか?
- ➢ 短期間に対して信号が不正な場合に何が起こるか?

9. 改訂履歴

資料改訂	日付	注釈
41086A	2016年5月	初版資料公開

本応用記述はAtmelの41086応用記述(Rev.41086A-05/2016)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。