
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ド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の鍵となるパ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。

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用することを推奨します。

 **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用されるなら、(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用することを推奨します。

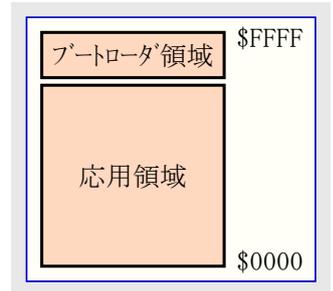
1.3. 飛行中書き換えの考慮

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用し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

この使用場面に対する参照基準形態設定の仮定は以下です。

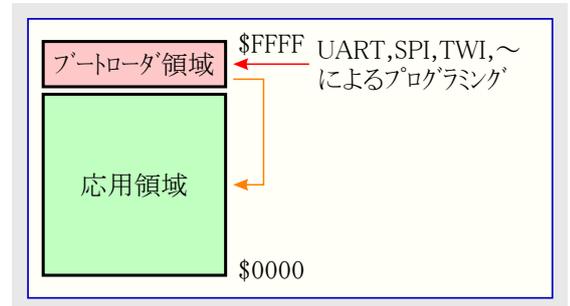
- ブートローダ領域は施錠されます。 - 「フラッシュメモリ内容損失回避」手順を参照
- 応用領域は施錠されません。

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

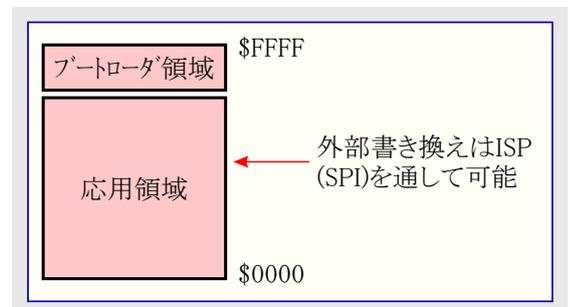
この使用場面に対する参照基準形態設定の仮定は以下です。

- 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 パラメータの形態設定用ヒューズ 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 ビットの不正な形態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 ビットのどの形態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。 - ウォッ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形態設定で)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十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)レジスタに複製されます。

応用でOSCCALレジスタを使用する場合、応用の寿命に沿ってそ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つの位置が使用されるべきです。

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

入出力の形態設定に使用されるレジスタはPIN/PORT方向レジ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形態設定手順が推奨されます。

6.1. PIN/PORTレジスタ読み込み

 **助言:** どのポートをも読む前にPIN/PORTを入力で規則正しく形態設定してください。

 **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レジスタ書き込み

 **助言:** どのポートをも読む前にPIN/PORTを出力で規則正しく形態設定してください。

6.3. 入出力衝突管理

ポ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ピ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ポ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、応用段階でのデ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データ/フレームを再送(するか否か)の決断を下すべきです。

- ・ ハードウェア段階で、USARTに於いてバイト制御を活性化することができます。 - USART形態設定の内側パリティビットの使用
- ・ 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、応用段階でのデ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データ/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を使用する場合、正しいデータ読み込みを保証するために求めるメモリセルの複数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、応用段階でのデ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データ/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を使用する場合、正しいデータ読み込みを保証するために求めるメモリセルの複数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の移行ように決めることもできます。

 **助言:** 例えそれらが使用されなくても、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十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



Atmel® | Enabling Unlimited Possibilities®



Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA TEL:(+1)(408) 441-0311 FAX: (+1)(408) 436-4200 | www.atmel.com

© 2016 Atmel Corporation. / 改訂:Atmel-41086A-AERO- Safety_Management_for_Space_Environment_Application-ApplicationNote_05/2016

Atmel機密: 秘密保持契約(NDA)下でのみ公開用

Atmel®, Atmelロゴとそれらの組み合わせ、Enabling Unlimited Possibilities®とその他は米国と他の国に於けるAtmel Corporationの登録商標または商標です。ARM®, ARM Connected®ロゴとその他はARM Ltdの登録商標または商標です他の用語と製品名は一般的に他の商標です。

お断り: 本資料内の情報はAtmel製品と関連して提供されています。本資料またはAtmel製品の販売と関連して承諾される何れの知的所有権も禁反言あるいはその逆によって明示的または暗示的に承諾されるものではありません。Atmelのウェブサイトに表示する販売の条件とAtmelの定義での詳しい説明を除いて、商品性、特定目的に関する適合性、または適法性の暗黙保証に制限せず、Atmelはそれらを含むその製品に関連する暗示的、明示的または法令による如何なる保証も否認し、何ら責任がないと認識します。たとえAtmelがそのような損害賠償の可能性を進言されたとしても、本資料を使用できない、または使用以外で発生する(情報の損失、事業中断、または利益と損失に関する制限なしの損害賠償を含み)直接、間接、必然、偶然、特別、または付随して起こる如何なる損害賠償に対しても決してAtmelに責任がないでしょう。Atmelは本資料の内容の正確さまたは完全性に関して断言または保証を行わず、予告なしでいつでも製品内容と仕様の変更を行う権利を保留します。Atmelはここに含まれた情報を更新することに対してどんな公約も行いません。特に別の方法で提供されなければ、Atmel製品は車載応用に対して適当ではなく、使用されるべきではありません。Atmel製品は延命または生命維持を意図した応用での部品としての使用に対して意図、認定、または保証されません。

安全重視、軍用、車載応用のお断り: Atmel製品はAtmelが提供する特別に書かれた承諾を除き、そのような製品の機能不全が著しく人に危害を加えたり死に至らしめることがかなり予期されるどんな応用(“安全重視応用”)に対しても設計されず、またそれらとの接続にも使用されません。安全重視応用は限定なしで、生命維持装置とシステム、核施設と武器システムの操作の装置やシステムを含みます。Atmelによって軍用等級として特に明確に示される以外、Atmel製品は軍用や航空宇宙の応用や環境のために設計も意図もされていません。Atmelによって車載等級として特に明確に示される以外、Atmel製品は車載応用での使用のために設計も意図もされていません。

© HERO 2016.

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。