高レジリエンス・システムの
モデル化による検証例

ETアワード（2011）
最優秀賞受賞
高レジリエンス・マイコン紹介

Resilience →　回復、柔軟性

止まらないマイコン、FUJIMI

PCT特許申請中

（株）エルイーテック

高レジリエンスシステム FUJIMIの意義

コンピュータ、マイコンは広く現代社会に使われており、そのトラブルは生活の質のみでなく、金銭、生命にも関わる

- 遊戯機器の対策技術を改良して汎用化した技術

- コンピュータのトラブルの防止策としてソフトウェアの検証ツールが充実し、バグによるトラブルは減ってきている（自動車業界）
- マイコンの開発、進化は、低消費電力、高速化に向いている

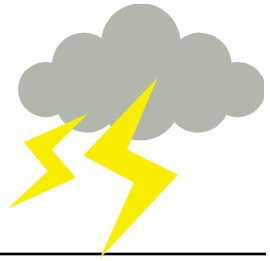
→ コンピュータの安定動作の方向には向いていない

- FUJIMIは、マイコンのトラブル、暴走への対策
- FUJIMIは、ウォッチドッグといった最終安全策に入る前の中間的な暴走への対策システム全般の名称

マイコンの基本問題、暴走

- 種々の原因で、マイコンは正常な動作をしなくなる事がある
  - ー　これを暴走、フリーズ、固まる、停止、と言っている
- 電源を一度、切って、入れ直すと正常な動作を行う様になる
  - 家電のサービス窓口の標準的な対応になっている
  - 人間で言えば「気絶」、破壊には至っていない場合が殆ど
- 動作不良は、再現しない、よって異常の理由は分からない
  - 自動車メーカーの電装品の不良根絶のできない理由の1つ
- 異常を起こした理由が分からないので、対策も立てられない
- 開発時、製造時の試験では起きない

暴走は何故おきるか？



- 半導体で作られている以上、動作範囲を超える電気ショックで
  半導体の回路（特にF/F）が異常を起こすのは当然
- 動作周波数を超える周波数の電波が入り込むと正常に動作できないの
  も当然
- プログラムとデーターが混在しているのだから、何かの原因で
  実行する位置がずれれば何をするのか分からない
  - オペランドを命令語として読んで実行してしまう
- マイコンのCPUは内部に複数のシーケンサがあり、これらが
  同期して動作しているが、同期がずれると停止してしまう
- 暴走を引き起こす外因の大きさに規定は無いので完璧な対策は無い

○ 結論：暴走は防げない

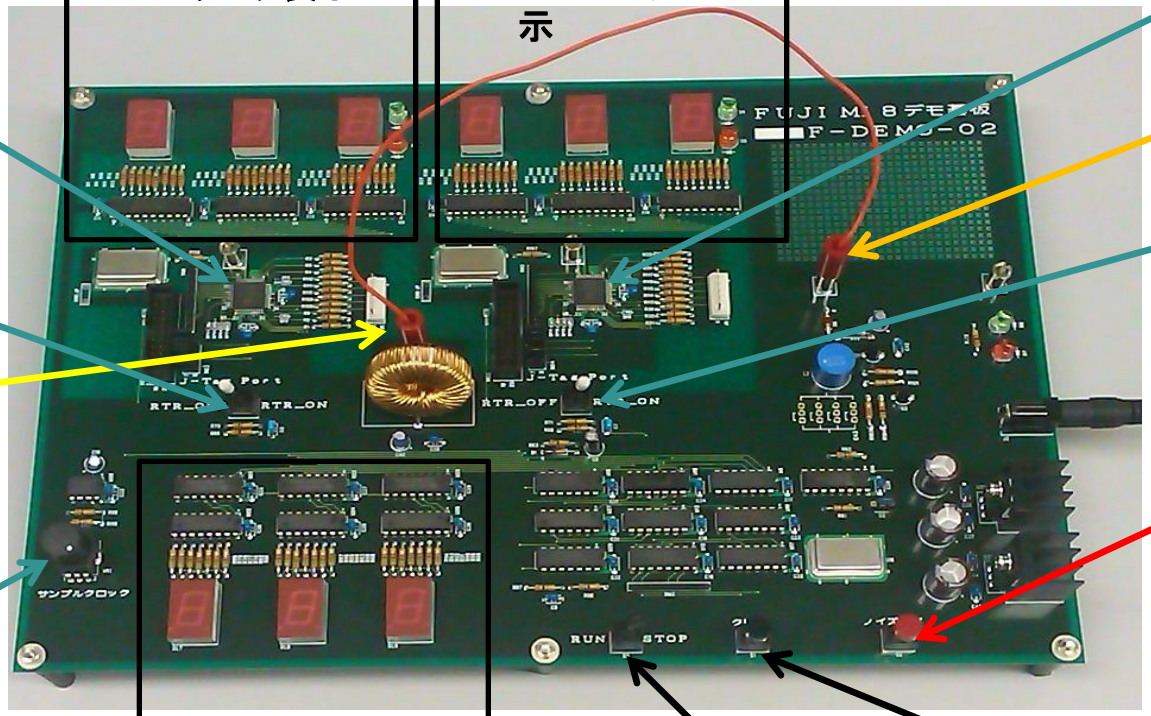
暴走は防げない、では、どうする

- 暴走したら、**リセット**、すればよい
  - ウォッチドッグ・タイマーにより、**リセット**する
  - 違法命令（存在しない命令）の検出で**リセット**する
  - 無効空間（メモリ、I／Oの無いアドレス）へのアクセスで**リセット**する
  - 別のマイコンで監視して、異常時に**リセット**する
- **リセット**以外に確実に動作が戻る方法は無い

対策としての高レジリエンス・システム

- ウォッチドッグ、他の対策はシステム初期化
  - システムはカタストロフィとして初期起動から
- 高レジリエンス・システムは動作継続
  - コンピュータの動作を止めない事が特徴
  - ウォッチドッグでの初期化以前の、暴走への対策
  - ハードでトリガ、ソフトで処理を行う
  - 対策方法はソフトで自由に決められる
    - 動作継続　　何が何でも仕事をします
    - フェールセーフ　　安全第一で処理します
    - エラーの外部への通知

FUJIMI8 デモ基板の機能説明



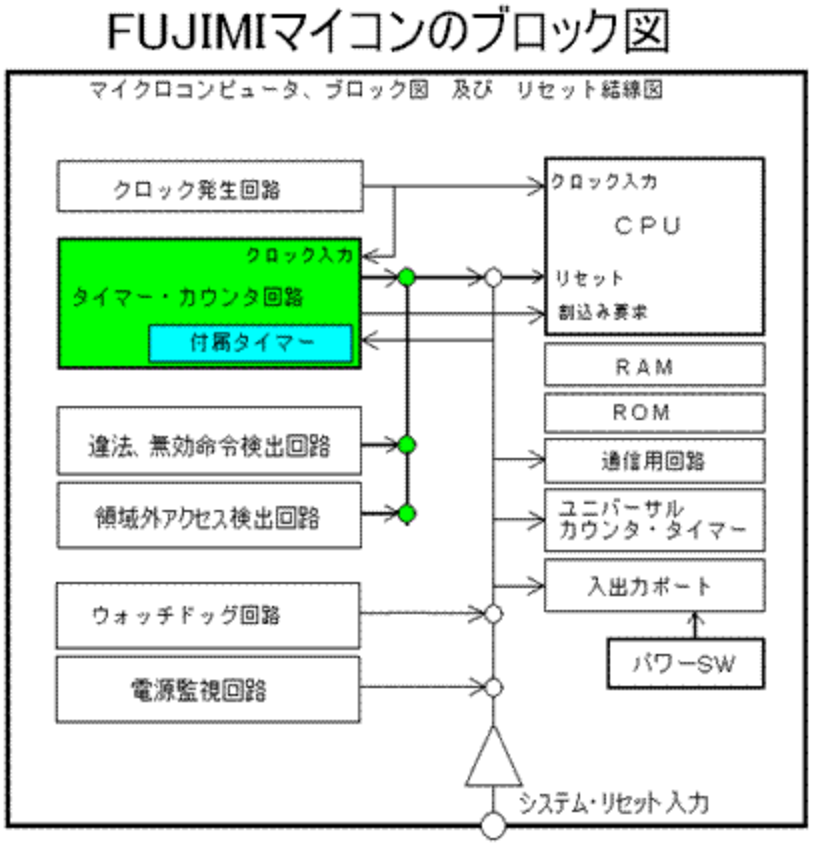
デモ・ムービー


FUJIMI-8 デモビデオ
8051コアのFUJIMIマイコン
緑色LED FUJIMIモード
赤色LED 初期化中
CR発振器からのパルスを数えて
3ケタの7骨具LEDで表示します
(株)エルイーテック

FUJIMI
高レジリエンス・システムのコア技術

- 暴走したマイコンはリセットするしかない
  - しかし、マイコン全体をリセットする必要はない
- 機能不全を起こしているのは、主にCPU
  - では、CPUだけをリセットすればよい！
    - RAMの情報は正しいはず
    - I／Oはソフトで再設定できる
    - 周期的にCPUをリセットすれば、暴走は見えなくなる
- しかしリセットが掛かっては、ソフトの実行に問題
  - リセットを割込処理の一部にすれば問題なし！

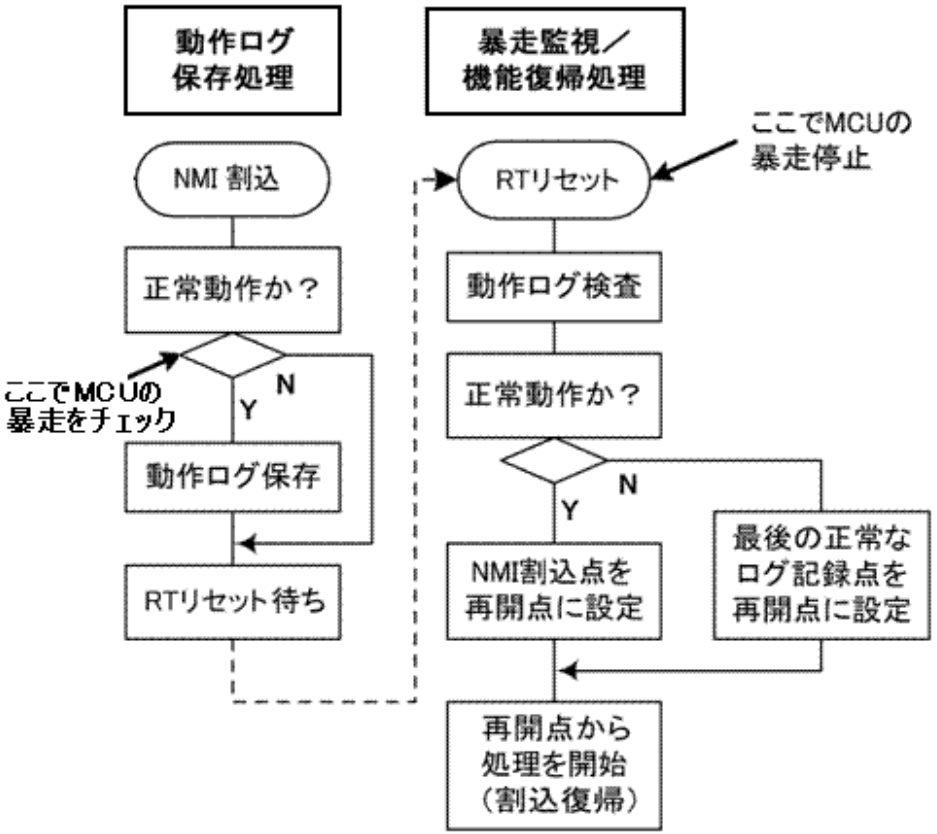
FUJIMIマイコンの構造



- **リセットが2系統化する**
  - 通常と同じ、システム・リセット
    - 電源監視
    - ウォッチドッグ
  - **CPUコア専用のリセット**

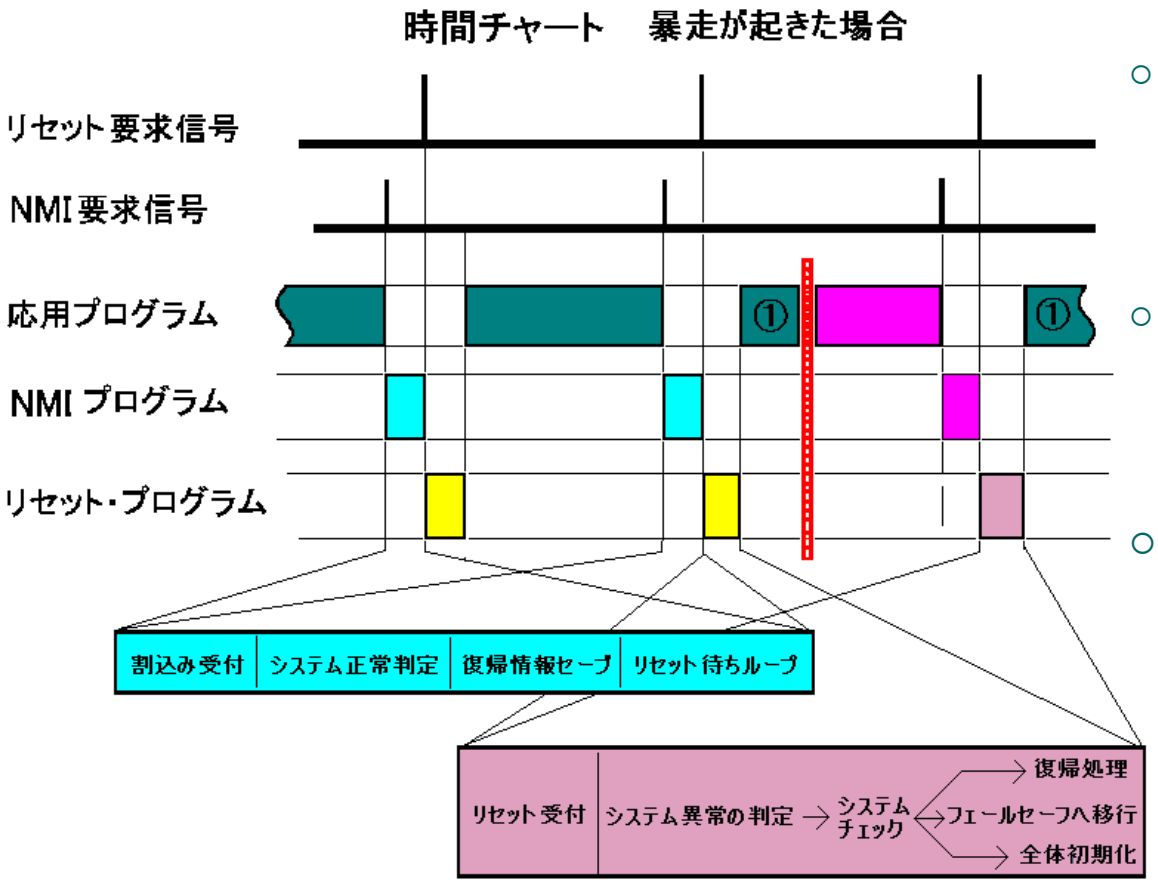
    命令実行の異常を検出
    - 違法命令の検出
    - 無効な空間のアクセス
    - 定時タイマー

FUJIMIのフローチャート



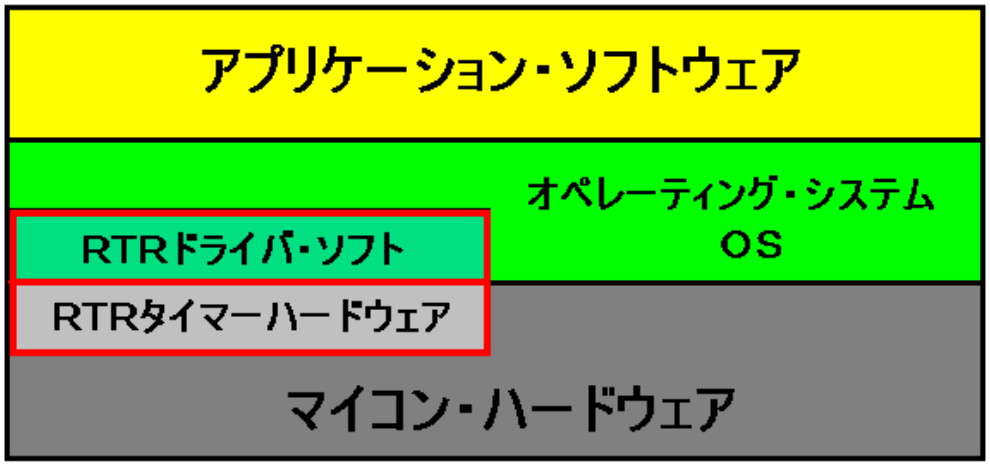
- リセットを割込の中で行い、割込みからの復帰をシミュレートする
- 割込み処理の開始時に暴走のチェックを行う
- リセットでCPUは初期化されて暴走は停止する
- 周期的にCPUの状態が記録されるのでログとして使用可

FUJIMIの動作タイミング



- 暴走が起きても、CPUはリセットされ以前にセーブした復帰用データーを用いて、動作を復帰させる
- ①と、①は同じ動作を繰り返すことになる
  - ソフトで問題になる点を予め排除しておく必要がある。
- 異常時には、対応する処理を選択する事も可能

高レジリエンスの実体



- **高レジリエンスは；**

1）マイコンのハードに
組み込まれたRTRタイマ

2）OSに組み込まれた
RTRドライバ・ソフト

この2つが組み合わさって
実現します。

- **高レジリエンス・マイコンは専用のマイコンが必要です**
- **ワンチップ・フォールト・トレラント・コンピュータとなります**

FUJIMIの長所、短所

- メリット
  - 見かけ上、暴走は見えなくなる
  - リアルタイム割込みの代替とする（例：4mS）
  - システムが暴走する最長時間が規定できる
  - 初期化をしない再スタート（ホットスタート）が可能となる
  - RAM，I/Oは初期化されないので、状態が保持される
- デメリット
  - ソフトウェアの作成が難しい
  - システムの検証が難しい－ハードとソフトが絡む
- 形式手法による検証中

高レジリエンス・マイコンの長所

- マイコンをICと考えた場合に、ICコストの上昇は無い
- 追加技術なので従来技術の移植が難しくはない
- ESDへの保護部品が減らせるので、システムではコスト・ダウンとできる
- 誤動作しても自動で短時間の内に回復して、全体に影響が及ばない様にできる
- オプションで、動作記録がとれるので、停止する前の状態を調べることも可能

止まらないマイコンを必要とする分野

- 航空・宇宙用 （日本の人工衛星には採用）
- 海底、山奥、等、人が関与できない場所の施設
  - 気象観測機、海底ケーブルの中継器、放射線モニター
- 故障しても、人間が関与できない装置
  - 自動車のマイコン
  - 新幹線、等、電車の通信装置・制御装置
  - エレベータの制御装置
  - 自動製造装置、等、FA装置
  - 医療用機器
- 家庭電化製品（プラグを抜いてください、が不要）
  - 録画装置 （予約録画が出来なかった、の解消）
  - 冷蔵庫 （スイッチが無いので対処不能）
  - 省電力・スマートパワー装置

まとめ

- 高レジリエンス・システム、FUJIMIは検証中です
  - （独）産業技術総合研究所の協力で完成度が向上しました
- ET2012でも展示、セミナー開催を行います
  - 明後日より横浜パシフィコで開催です
- 風速風向計では採用が決まっています
  - ドラゴンチップ社製8bitマイコン
- 2013年4月より富士通セミコン社よりFUJIMIマイコンが発売されます
- iTRON準拠のOSを製作中です