デバイスからの異常注入が指定可能な CPU エミュレータ

東 誠†，山本 哲男‡，早瀬 康裕†，石尾 隆†，井上 克郎†
†大阪大学大学院情報科学研究科，‡立命館大学総合理工学院情報理工学部
連絡先:m-higasi@ist.osaka-u.ac.jp, tetsuo@cs.ritsumei.ac.jp
ESS2009:Embedded Systems Symposium 2009

1 背景

組込みソフトウェアで発生する故障の 1 つとして，組込みソフトウェアが特定の状況で特定のデバイスから入力を受け取った際に，組込みソフトウェアが正常に動作しなくなるという故障が挙げられる．例えば，携帯電話である FOMA P901i では，着信時に終了キーを連続押下した場合などに，稀に着信履歴が表示されない，または同じ着信履歴が 2 回表示されるという故障が報告されている．また，同じく携帯電話である FOMA D901i では，メール作成中に,「題名」を入力した直後に素早く「本文」にカーソルを合わせて「本文」を入力すると，操作ができなくなる場合があるという故障が報告されている．上記のような組込みソフトウェアの故障を引き起こす可能性のある入力を，以降は**異常**と呼ぶことにする．

このような故障を発見するには，ソフトウェアに異常を注入するテストが効果的だが，そのようなテストは困難である．その理由は以下の 3 つが挙げられる．

1.異常は発生頻度の低い入力であるため，そのような異常を用いたテストを実行するのは困難である

2.デバッガで入力値を書き換えて異常を注入することは可能だが，デバッガを使うには多くの手作業を必要とし，手間がかかる

3.組込みソフトウェアがデバイスから受け取る入力値と，それを受け取る状況の組み合わせの数は膨大であるため，全ての組み合わせを網羅してテストすることが困難である

そこで本展示では，組込みソフトウェアを効率的にテストするために，ソフトウェアに異常を注入する機構を加えた CPU エミュレータを展示する．具体的には，ソフトウェアが入力を受け取るデバイスや，そのデバイスから受け取る値をソフトウェアの実行前に予め指定しておく．そして，ソフトウェアの実行中に，デバイスから受け取る入力値を指定内容に従って変更することにより，ソフトウェアに異常を注入する．このような注入を行う機能を ARM の CPU エミュレータである skyeye に実装することで，skyeye で動作する様々なソフトウェアに異常を自動的に注入することができるようになる．

2 提案手法

異常注入機構を実装する箇所は，CPU エミュレータがロード命令を実装している箇所である．その理由は，本展示で異常注入機構を加えた CPU エミュレータがデバイスから入力を受け取る手

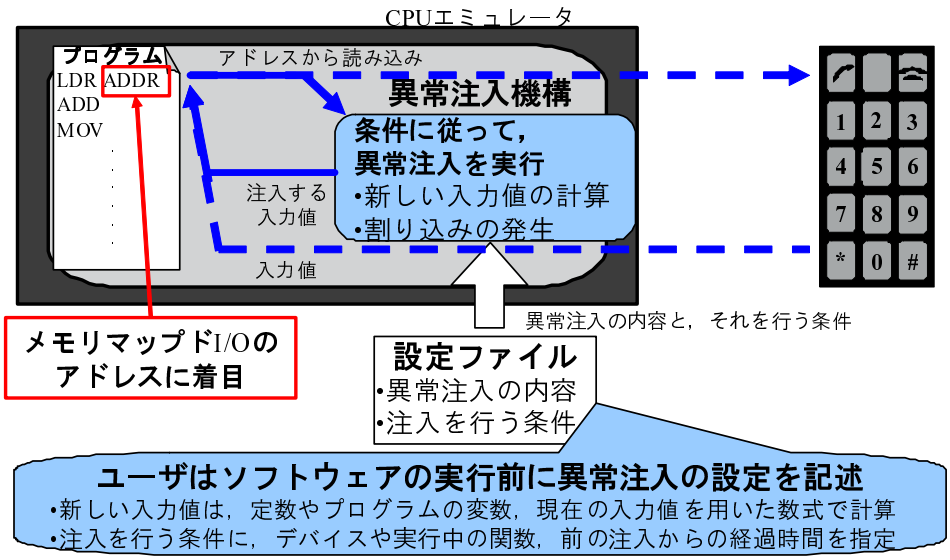

図 1: 異常注入の概要

段が，メモリから値を読み出すロード命令だからである．他の CPU エミュレータがデバイスから入力を受け取る手段としては，入出力ポートから値を読み出すイン命令が挙げられるが，その場合でも同様の方法で実装が可能である．

そして，CPU エミュレータが異常を注入するには，図 1 のように，CPU エミュレータがロード命令でデバイスから受け取る値を変更する．これにより，組込みソフトウェアが受け取る可能性の低い入力を発生させることができるため，その入力に対する処理が実装されていない組込みソフトウェアで故障が発生する可能性が高くなる．

この異常注入を用いたテストの内容をユーザが指定するには，ソフトウェアの実行前にユーザはテストの設定をファイルに記述する．このファイルに記述可能なテストの設定は，テストの内容と，そのテストを行う条件である．そして，ソフトウェアの実行中に，テストを行う条件が成立するかを判断し，成立するならテストの内容を実行する．

テストの内容には，異常として用いる新しい入力値の計算と，割り込みの発生が挙げられる．割り込みの発生を実装した理由は，利用時に割り込み用関数が必要になるデバイスから異常な入力を受け取るために必要となるからである．

新しい入力値の計算方法としては，現在の入力値を用いた演算やプログラムの変数の値や定数の代入が挙げられる．これらのうち，現在の入力値を用いて演算を行い，センサデバイスから受け取った入力値を壊すことで，ノイズへの対策がソフトウェアでなされているかをテストすることができる．また，定数や変数の値を代入することによって，デバイスで滅多に発生しない入力をソフトウェアに受け取らせるテストが可能になる．

また，割り込みの発生タイミングには，一定時間の経過や，特定の CPU 命令の実行前が指定できる．これらのうち，一定時間経過ごとに連続で割り込みを発生させることで，終了キーなどのキー入力デバイスを連打する状況を模倣し，FOMA P901i の故障などをテストすることができる．

さらに，テストを実行する条件には，値を読み取るデバイスや，現在実行中の関数，現在の入力値やプログラムの変数を用いた数式の成立が指定できる．これらのうち，現在実行中の関数を用いることにより，その関数に対応する特定の機能のみをテストすることができる．また，入力値や変数を用いた数式を用いることで，プログラム中の条件分岐を考慮してテストすることができる．