IPA Better Life with IT

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

信州大学 SHINSHU UNIVERSITY

THE UNIVERSITY OF AIZU

会津大学

大規模複雑化した組み込みシステムのための障害診断における形式手法の適用事例報告

信州大学工学部
准教授 岡野浩三
okano@cs.shinshu-u.ac.jp

会津大学コンピュータ理工学部
教授　北道淳司
kitamiti@u-aizu.ac.jp

故障原因診断WGの活動

- 近年，大規模複雑化した組み込みシステムにおいて，ソフトウエアを起因とする障害が発生する
- ソフトウエアの原因調査は十分と言えない，障害に対する製造者の説明責任が発生

- 初動調査から設計・開発へのフィードバックにいたるまでの故障原因診断に調査と提言を行う

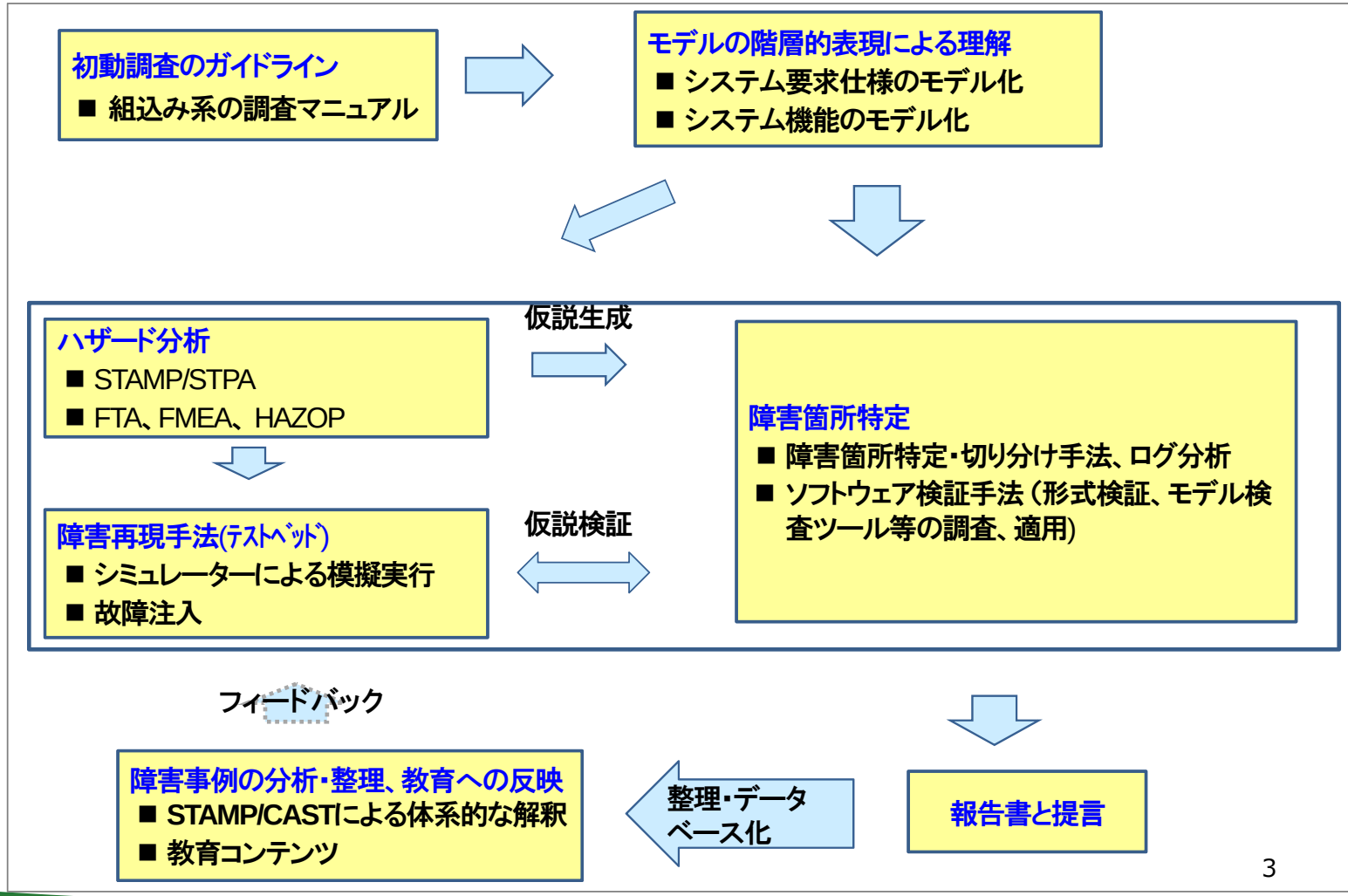
  IPA/SECとJASAによる　**障害原因診断WG**　が発足(2014.04)

  http://www.ipa.go.jp/sec/about/system.html

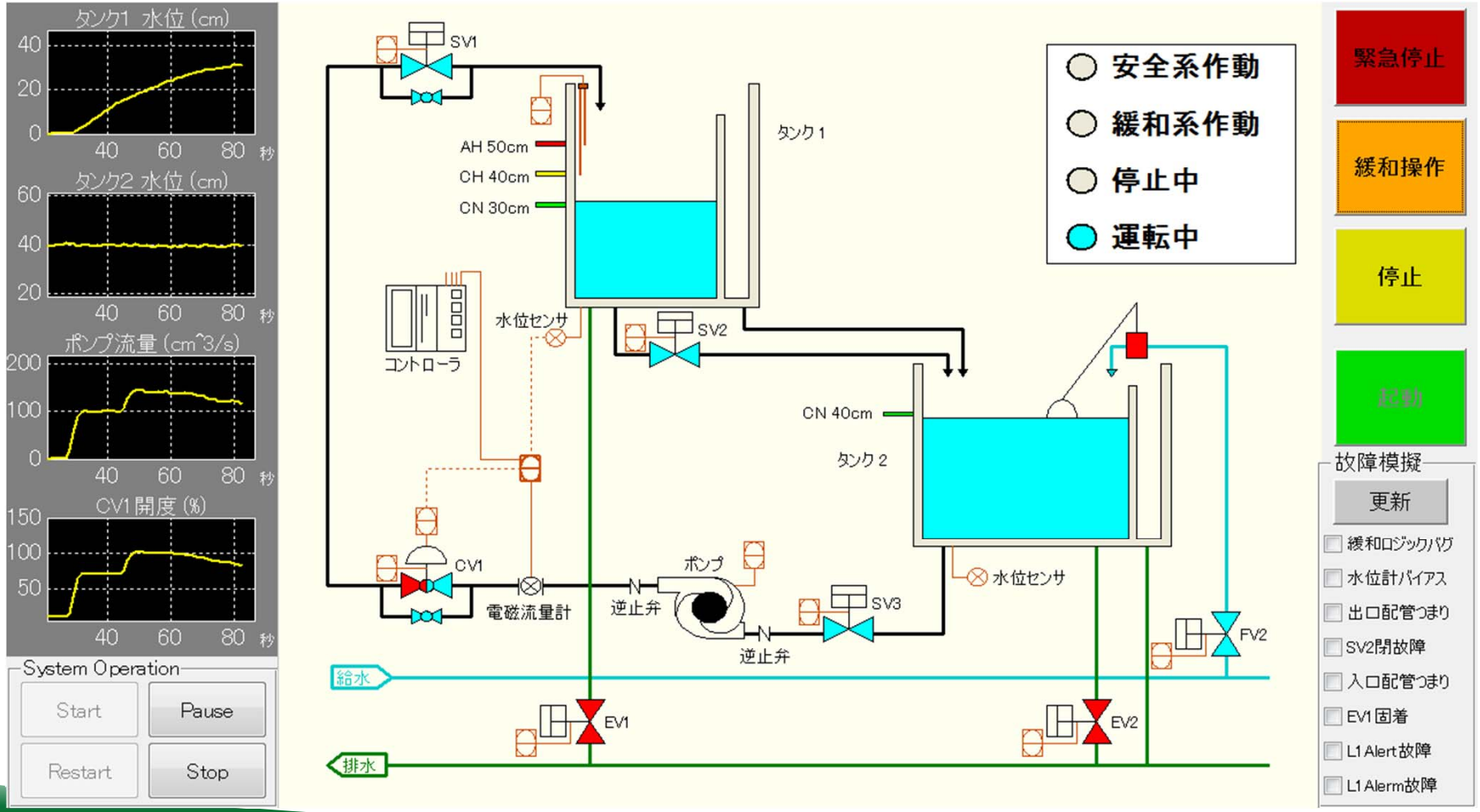
事後V＆Vの概要と形式手法の位置付け

- 障害発生原因究明に関するV(Verification)とV(Validation)が必要
- 故障箇所を特定するための手段の一つとして，形式手法の
  - ・形式的モデリング
  - ・モデル検査手法

が適用できないか検討



適用事例：化学プラントシステム



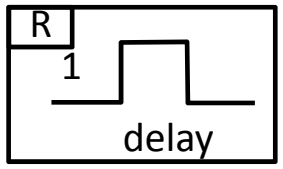
溢水防止のための機能と発生した障害

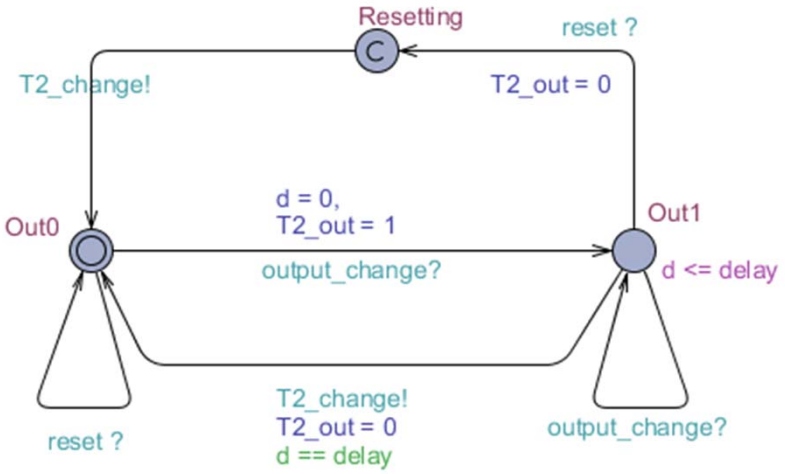
- アラートレベル(40cm)を越えると
  - 5秒間排出弁を開、同時に15秒間(含む5秒間)は新たな開指示を受け付けない
- 運転員の指示で、上記と同じ排出弁の操作を行う
- 運転員の指示は、常に優先する(15秒間の禁止区間でも受け付ける。自分自身の過去の指示に対しても優先する)

- 発生した障害:
  - センサがオンで、緩和期間をすぎているのに排水できない
  - マニュアルの操作も受け付けない

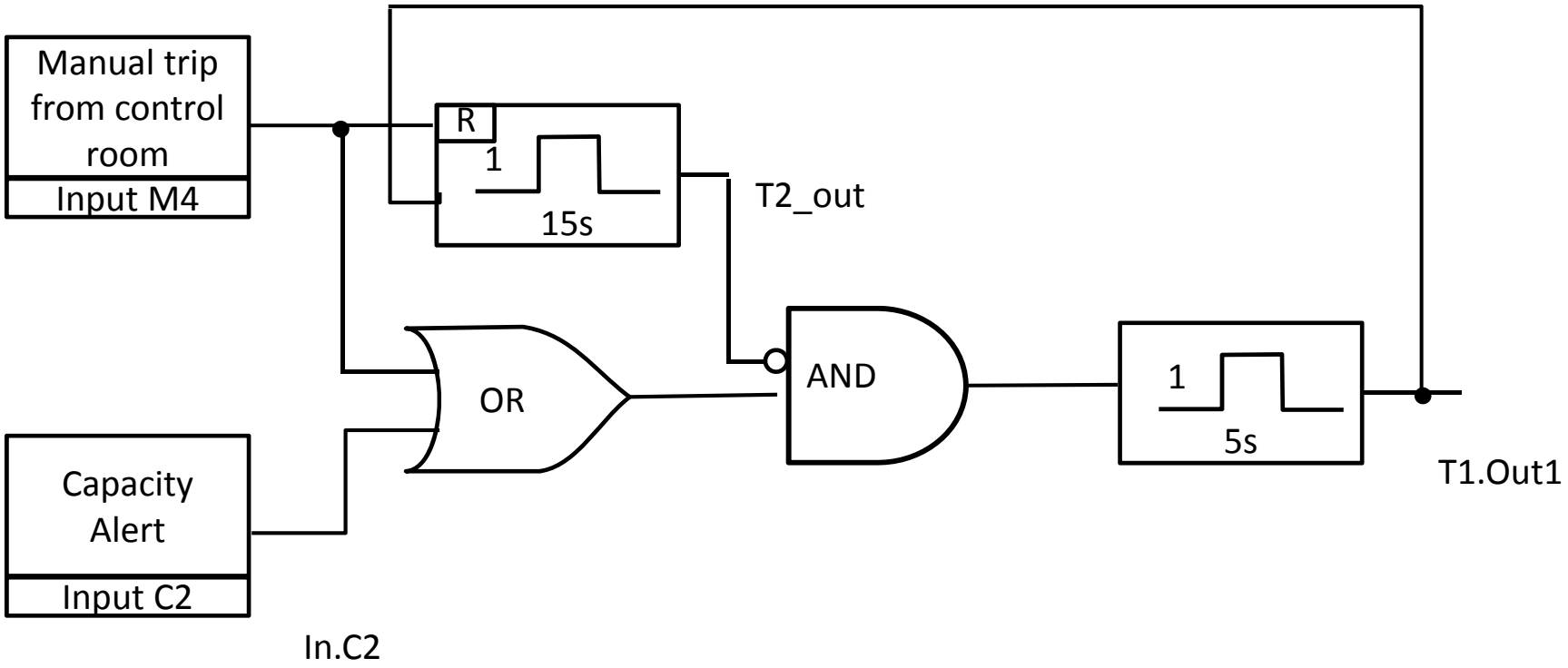
モデリング1：ディレイタイマwith Reset

- 入力　in 立ち上がり
  - 出力　out 0:　指定された時間*d*だけ1を出力
  - 出力　out 1:　何も変化無し
- 入力リセット　reset 立ち上がり
  - 出力　out 0: 何も変化無し
  - 出力　out 1:　出力0
- リセット後はin 立ち上がりで受け付け





モデリング２：制御システム（Design A）



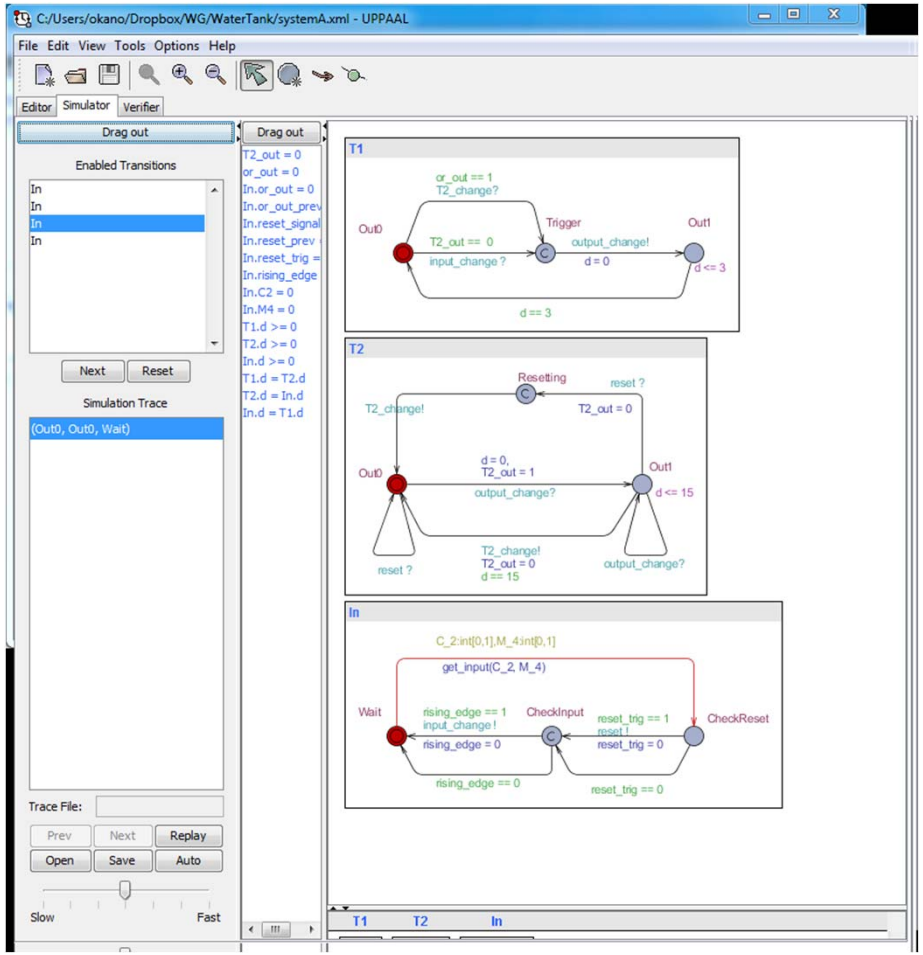
手動動作のときは強制排水開始の直後に15秒間
全体的にセンサ入力の伝達を禁止、を意図している

UPPAAL を用いたModelA

UPPAAL

時間オートマトンのモデル検査

シミュレーション



– モデル検査

- モデル(有限状態遷移)
- 時相論理式

- しらみつぶしに検査

システムにおいて成立する性質

- 通常の形式手法では，システムにおいて成立してほしい性質をモデル上で，成り立つか議論する
- ここでは，発生した障害の否定をシステムにおいて成立してほしい性質と考える　→　モデル検査に持ち込む

- 排水が抑制されていなく、かつ、水位レベルセンサが警告レベルの状態であるときに、いつか「排水モード」になるか
- (In.C2　and T2_out == 0) --> T1.Out1

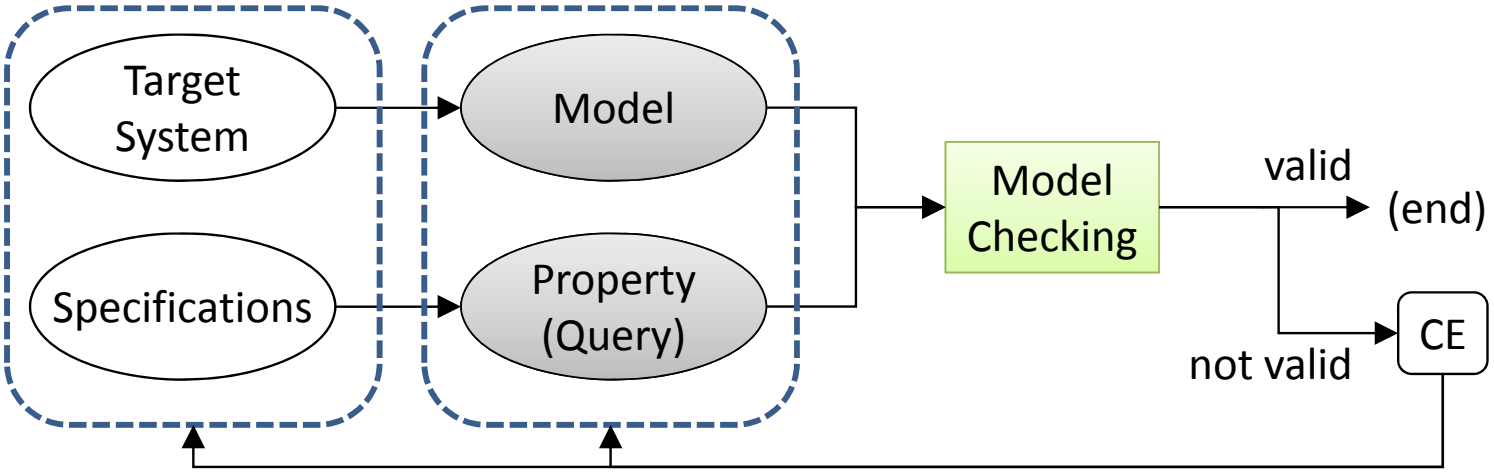
以下の(UPPPAAL上の)略記

$$A\Box\ ((In.C2\ and\ T2\_out == 0)\ imply\ A\Diamond\ T1.Out1)$$

モデル検査

モデル と 検証性質を与え

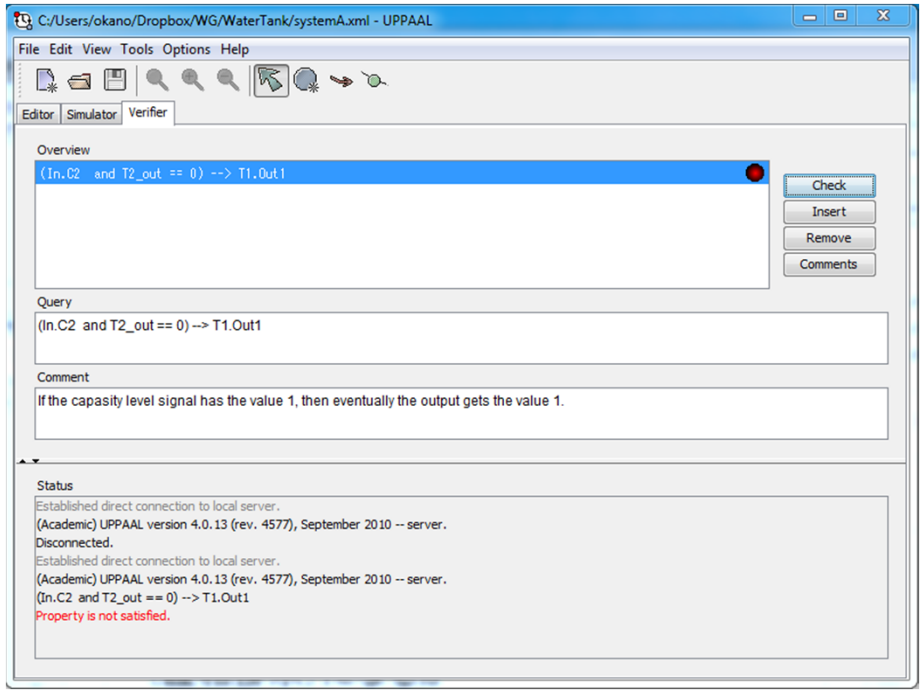
- モデル検査は
  - モデル上で検証性質が成り立つかを網羅的かつ論理的に調べる
  - 反例(CE)はバグ同定に役立つトレース情報



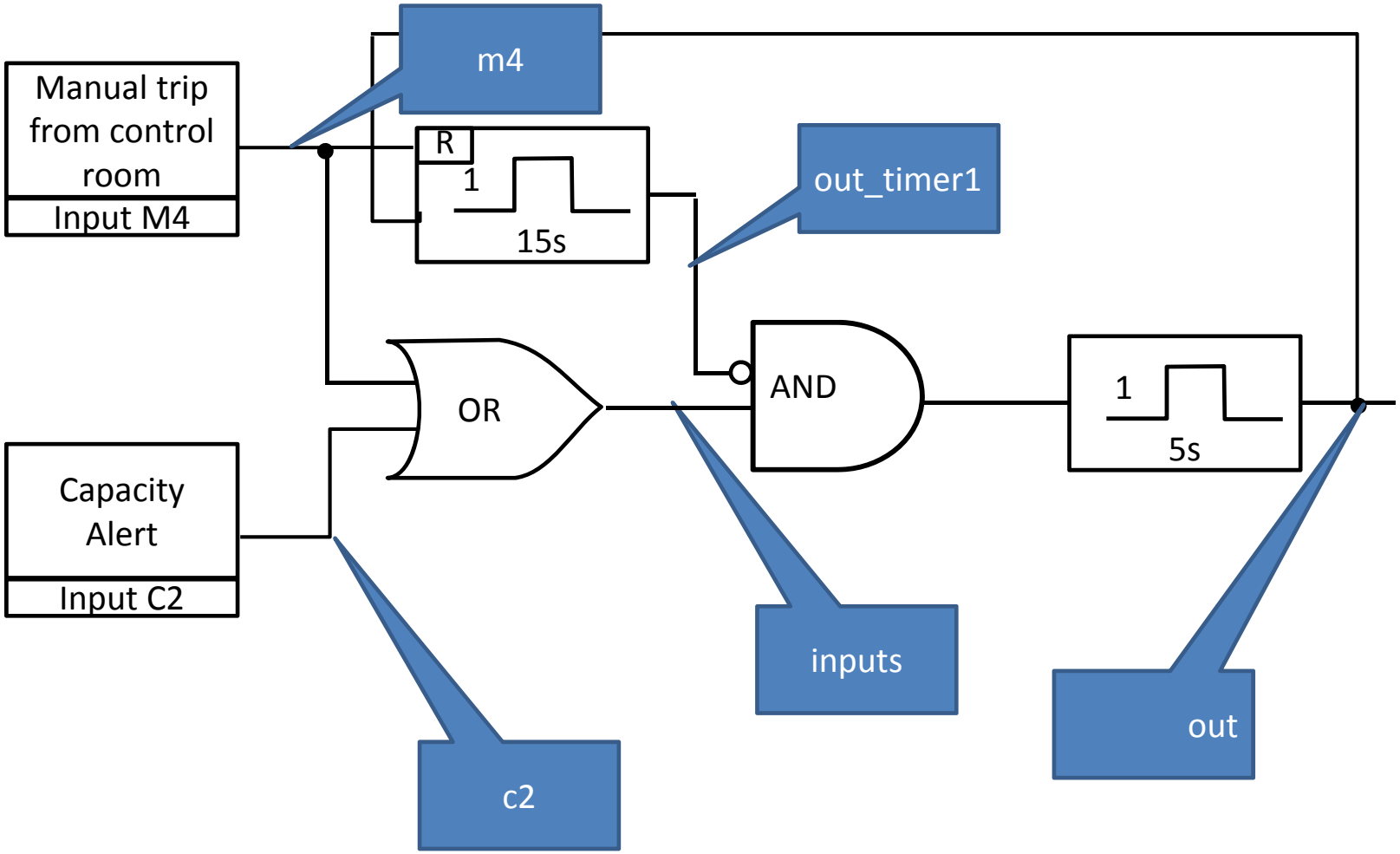
検証結果

- *性質P* は成立しないことがモデル検査で確認できる
  ＝障害発生

ツールが出力する反例を
障害診断に利用する



Design A


m4
Manual trip from control room
Input M4
R
1
15s
out_timer1
OR
AND
1
5s
Capacity Alert
Input C2
inputs
out
c2

反例をモデル上で追跡する

初期状態は0

C2 on

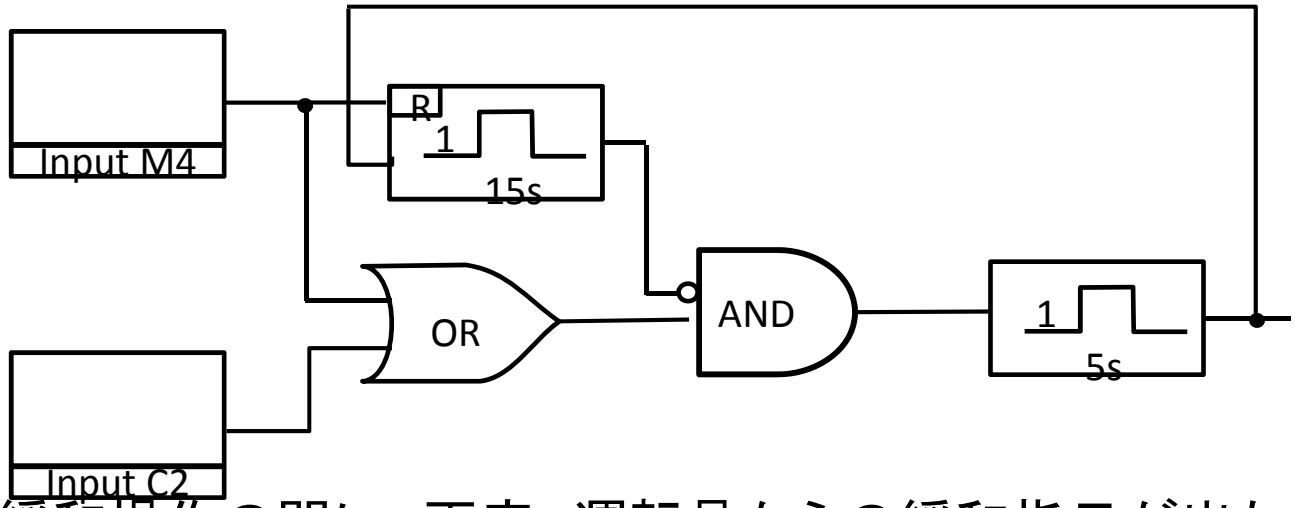
On(アラート)は1に

5sec 内にm4 on

これ以降水位レベルは異常値だが立ち上がりエッジが検出できないので出力が1にならない

tep	m4	c2	inputs	out_timer1	out	action
0	0	0	0	0	0	
						c2 on
1	0	1	0	0	0	
						0sec
2	0	1	1	0	1	
						0sec
3	0	1	1	1	1	
						m4 on
4	1	1	1	1	1	
						0sec
5	1	1	1	0	1	
						5sec
6	1	1	1	0	0	
						forever
7	0	1	1	0	0	

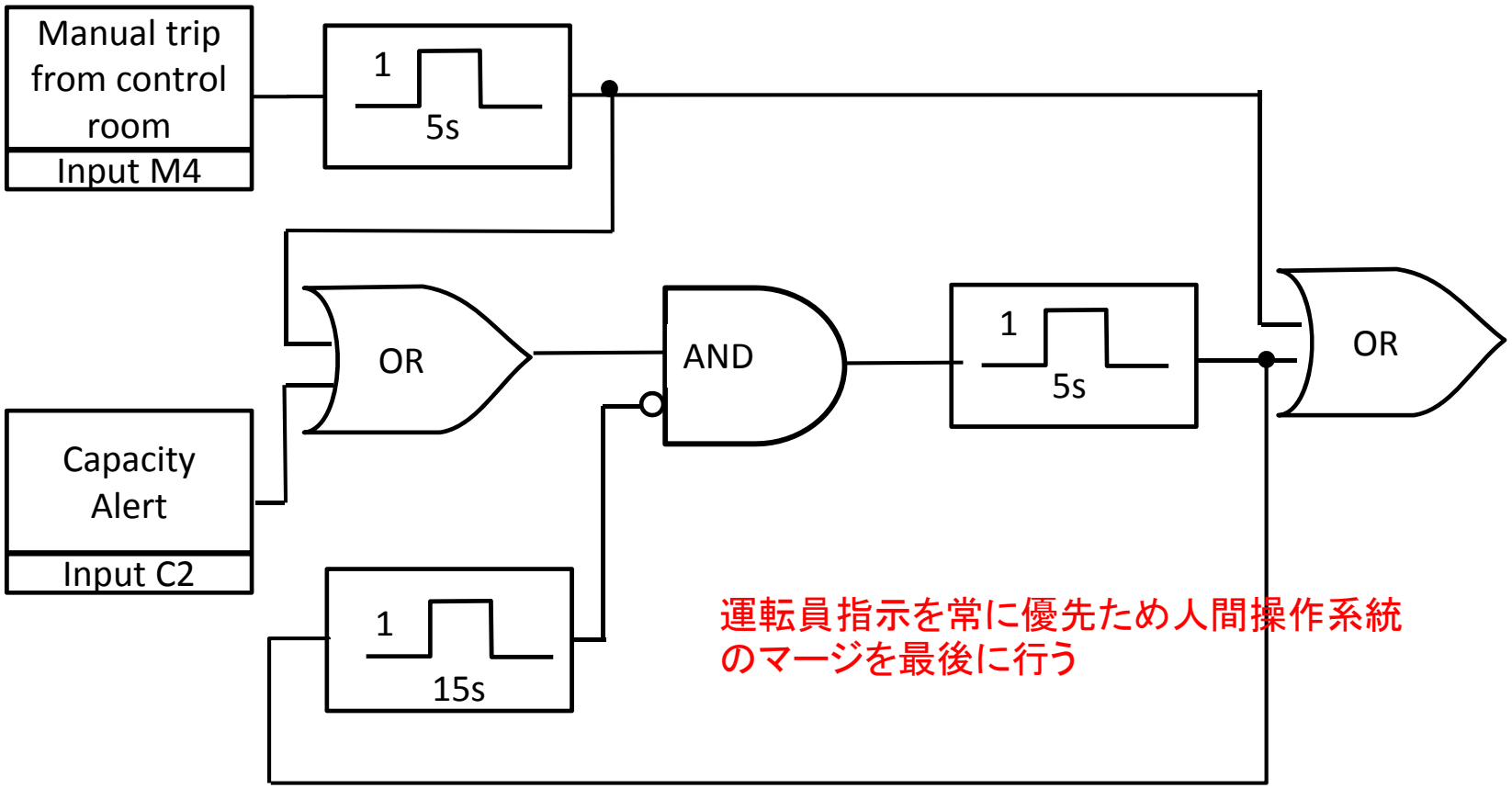
反例の解析＝障害診断



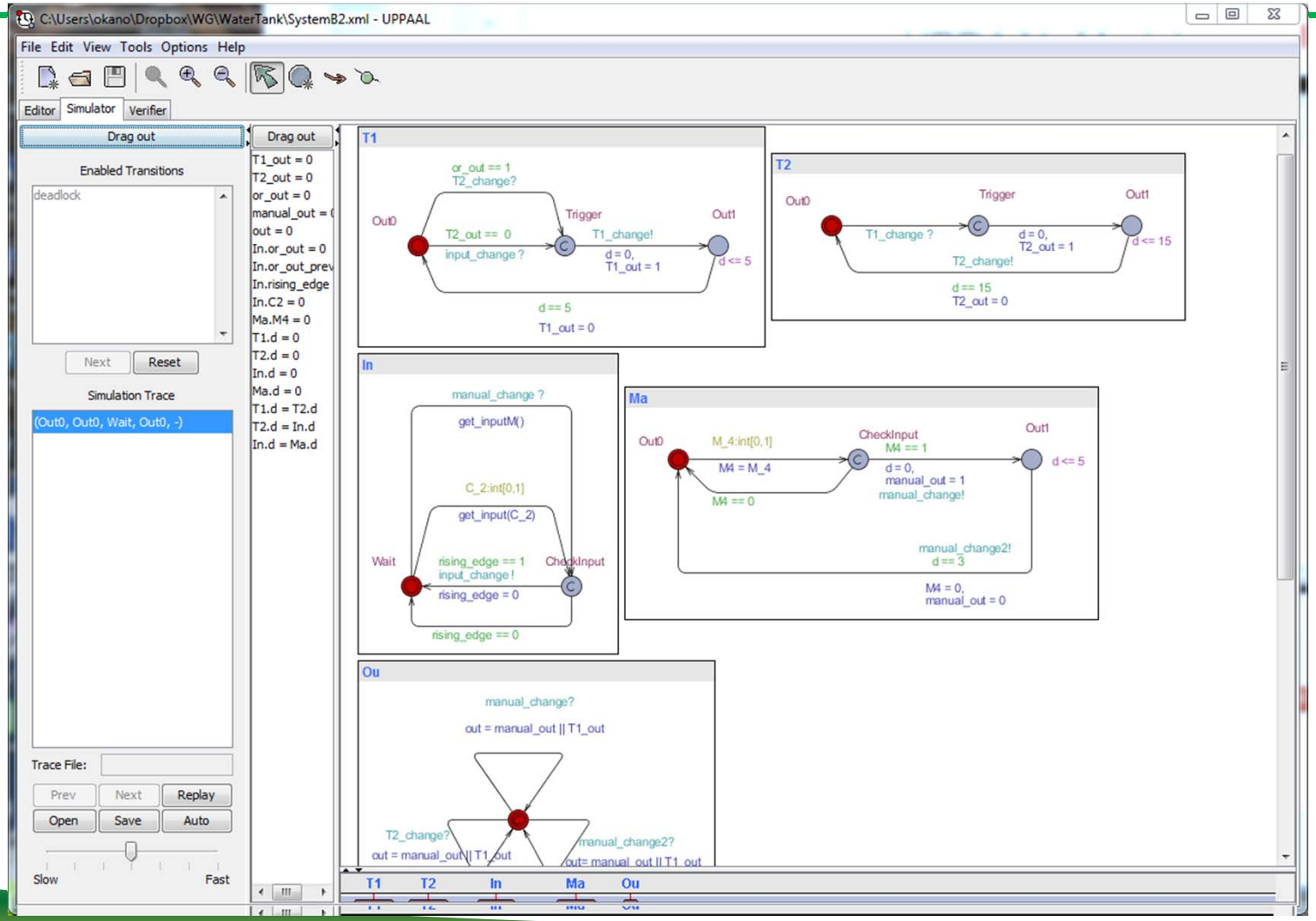
- 最初の5秒の緩和操作の間に、再度、運転員からの緩和指示が出た場合、15秒の操作禁止はリセットされるが、そのとき、水位がアラート越えの状態に留まっていた場合、AND出力は、0→1に立ち上がるが、5秒タイマは動作中で、これを受け付けない。5秒経過後も、AND出力が1で継続（水位アラート状態）の場合、AND出力は、1のままなので、5秒タイマは駆動されない。
- この状態で、運転員が緩和指示を出しても受け付けなくなる（運転員優先の逸脱）

障害原因が診断された

Design B (改善デザイン)



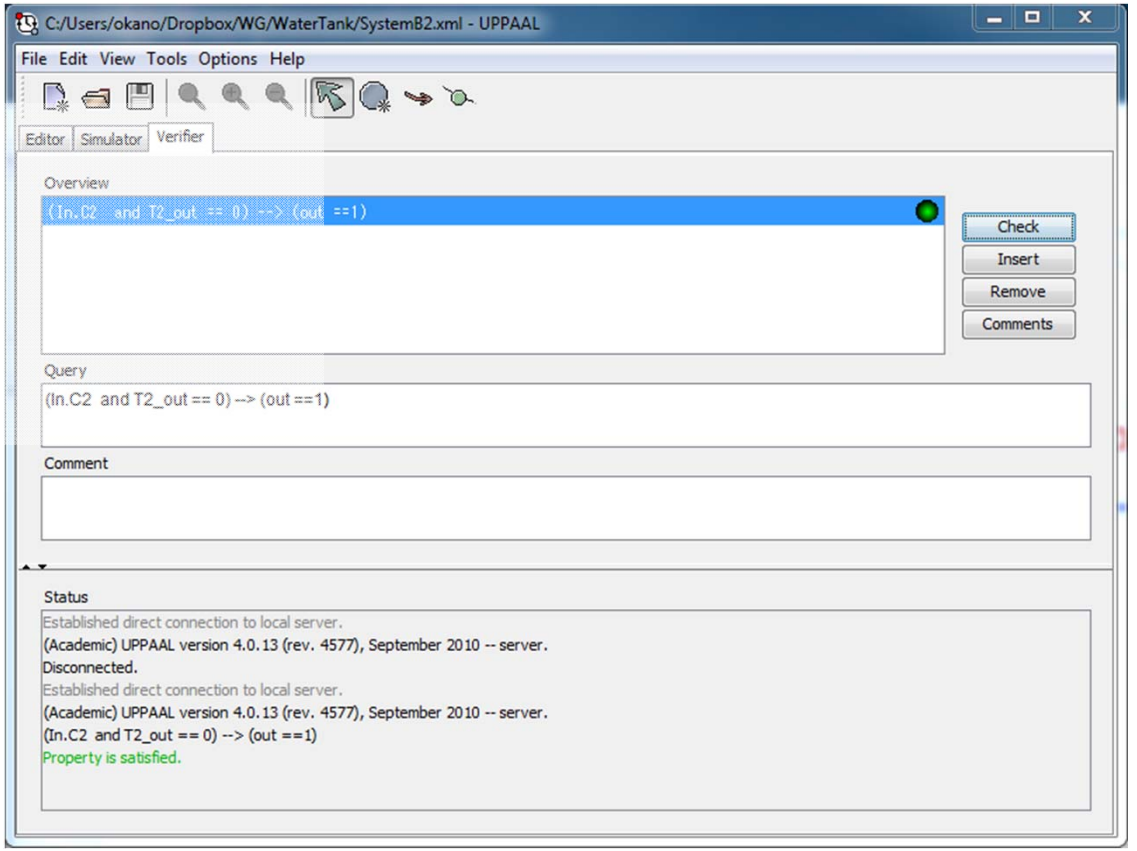
Design Bに対するUPPAAL Model



DesignBに対する検証結果

Design Bでは性質*P*が成立

Design Bでは性質*P*
に関する故障の原因が
取り除かれたと解釈できる



まとめ

- 故障原因診断WG，事後V＆Vとその中の形式手法の位置付け

- 化学プラントシステムを例に形式手法を用いて，モデリングおよびモデル検査による障害診断の例を示した．
- 通常，設計初期の抽象モデルへの形式手法の適用は多い．故障原因診断では，発生した障害，実際の開発物から形式手法の適用が始まる．参加者のご経験，ご意見を伺いたい