トップエスイー修了制作

リスク分析手法とモデル検査を組合わせた高信頼設計プロセスの提案

若林　昇
Noboru Wakabayashi

開発における問題点

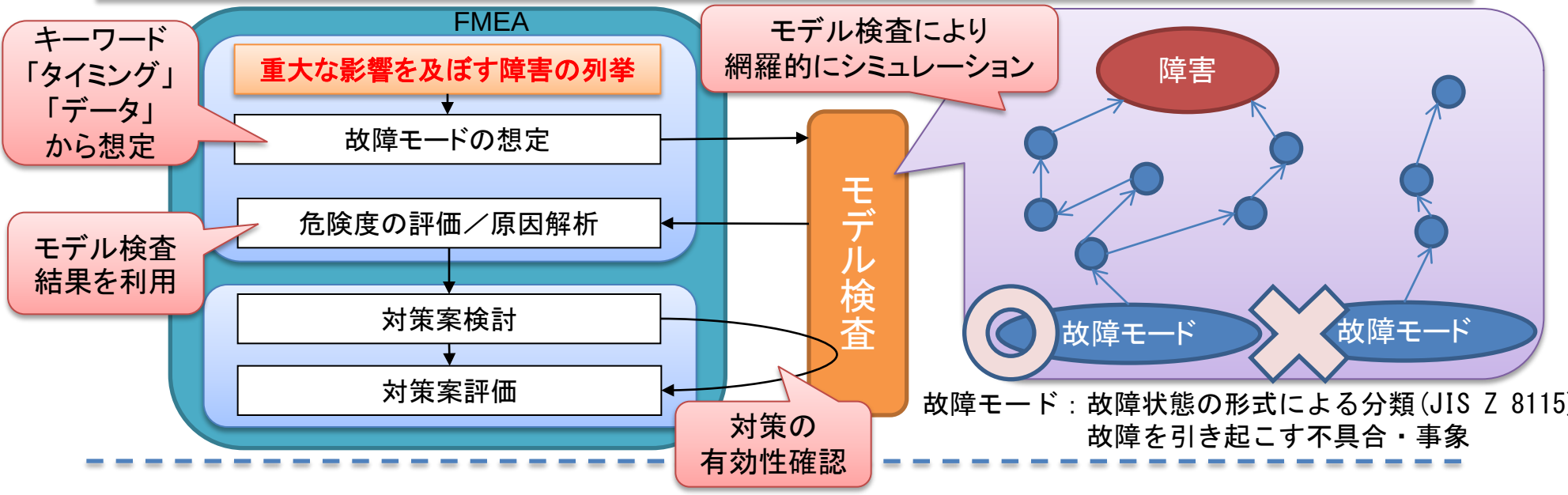
■機器のネットワーク化／オープン化
⇒運用後の振舞いを完全には予測不可能
⇒効率的な不具合対策が十分にできない
■FMEA：検討漏れが起きにくいが課題あり
・障害に至らない故障モードも列挙
・故障モードの影響度見積もりが困難
・影響解析に時間がかかる

FMEA ： Failure Mode and Effect Analysis

手法･ツールの適用による解決

部品に対する故障を列挙し上位機能に及ぼす影響を解析することで，故障に対する検討漏れが起こりにくいリスク分析手法FMEAと，あらゆる状態遷移を網羅的に自動検証するモデル検査を組合わせる
⇒列挙した故障モードが重大な障害に至るかを網羅的に検証し，効率的な対策を実施する

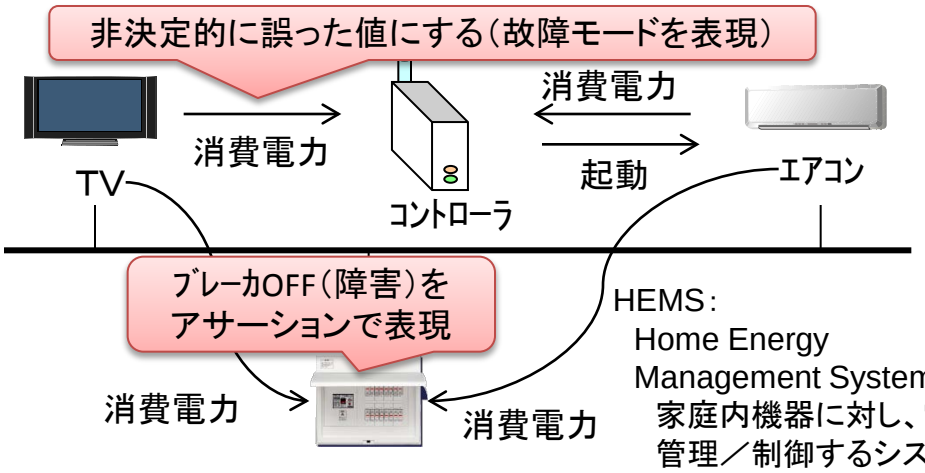
提案手法



故障モード：故障状態の形式による分類(JIS Z 8115)
故障を引き起こす不具合・事象

適用事例

HEMSシステムにおけるエアコン起動サービス
・コントローラが宅内の総使用電力を勘案して，指定時刻にエアコン起動
・各機器は消費電力をコントローラに通知
障害：障害の状態をモデルに追加 or アサーション記述
故障モード：イベント／アクションを故意に変える



HEMS：
Home Energy Management System
家庭内機器に対し、電力管理／制御するシステム

適用結果

アサーションエラーが出ないかモデル検査で網羅的に検証
【結果】
・アサーションエラー(=ブレーカOFF(障害)に至る)あり
⇒想定した故障モードが重大な影響を及ぼす障害に至ることが確認できた
・反例(具体的なパス)解析
⇒原因解析が容易であった
⇒障害に至る発生頻度検証が容易であった
・対策案の再モデル検査結果でエラーなし
⇒対策案の有効性を確認できた
【モデル検査を用いて判明したこと】
・(検証モデルのデバッグ過程で)違うパスが見つかった
⇒１つだけの対策では不十分．複数の対策が必要．
・検証モデルを正しく作ることが難しい
（検証モデルのデバッグに時間がかかる）
【今後の進め方】
・大規模な例題に適用し，本手法の有効性を確認