Using Part-Whole Statecharts for the Safe Modeling of Clinical Guidelines

Luca Pazzi & Marco Pradelli
Department of Information Engineering
University of Modena and Reggio Emilia
Via Vignolese 905,
I-41100 Modena,
Italy
Email: luca.pazzi@unimore.it

WHCM 2010

Medical guidelines as flow diagrams

- The focus of the research aims at coordinating medical teams through computer interpretable guidelines:
  - teams have to interact with patients and medical devices (Emergency Departments, Operating Rooms, etc.);
- A central real-time coordinating computer:
  - issues directives to team members;
  - interprets real time signals coming from patients, devices, and the environment;
- Different applications:
  - real-time monitoring (what is happening now is correct);
  - alternatives computed at real time given unexpected events;
  - models can being checked and simulated in advance in order to ensure safety-critical situations;

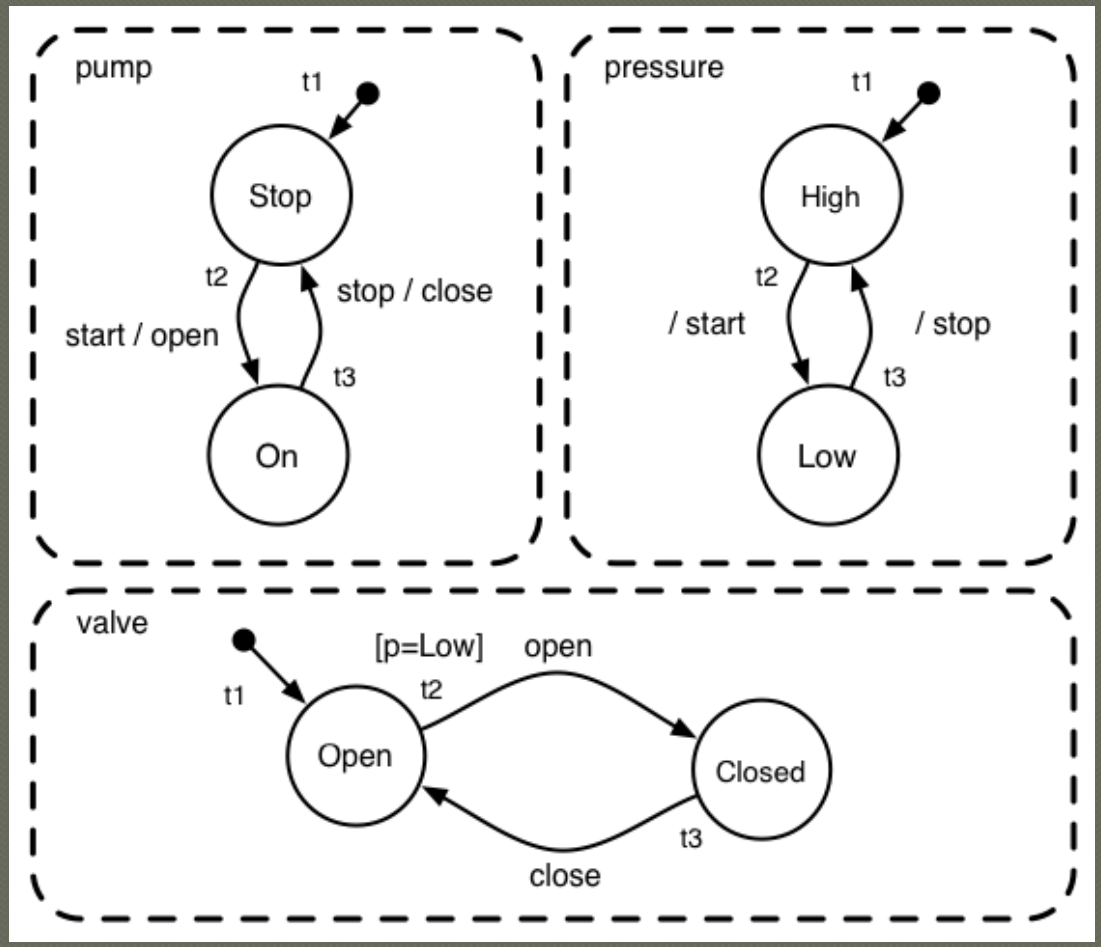
The safety problem

- Safety critical situations
  - mixed interaction of human operators, patients and computer controlled medical devices;
  - strict timing deadlines;
  - life support contexts;
- Safety depends in first analysis by:
  - timely execution of actions towards patients,
  - correct synchronization of the clinical agents involved in carrying out the different tasks;
  - late or incorrect interpretation of clinical data coming from monitoring devices may jeopardize patient's safety as well.
- Early research on medical embedded system safety showed that:
  - no (embedded) system is an island!
  - even the safest device, if used incorrectly or at the wrong time, may be dangerous!

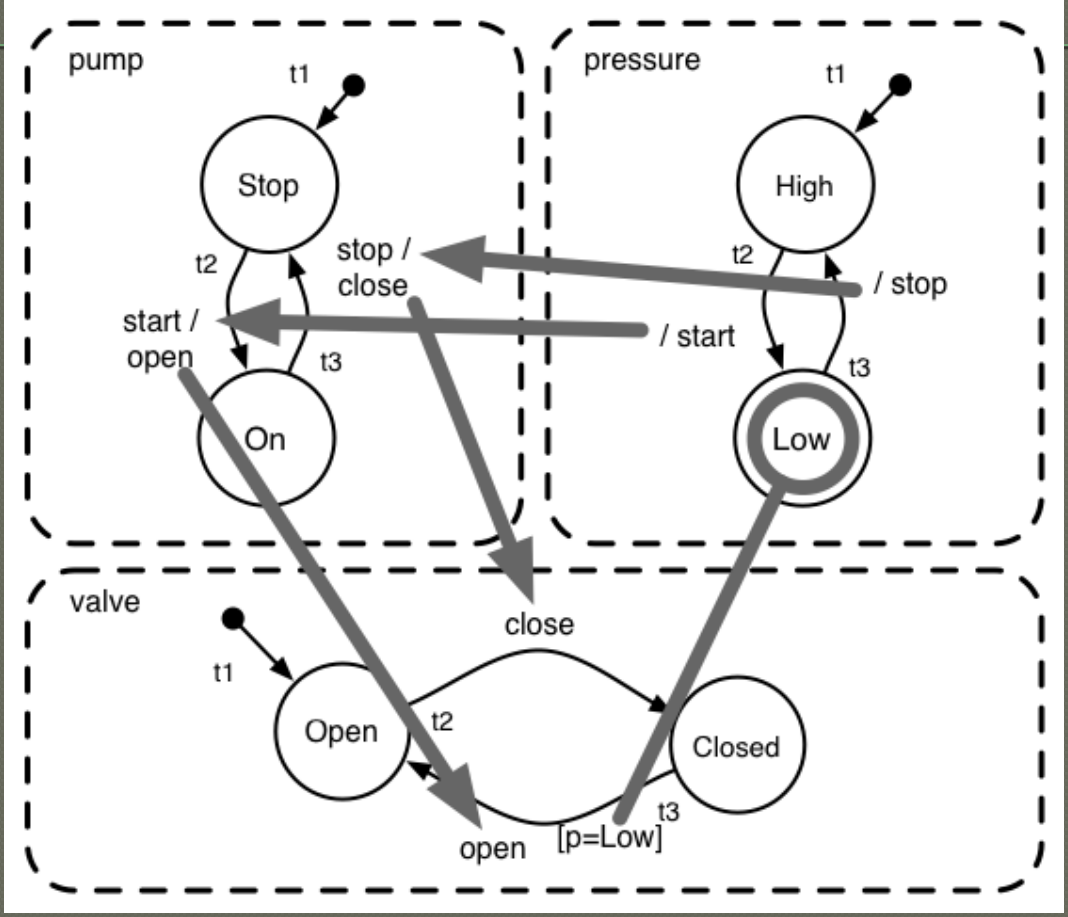
Safety as a systemic concept

- A system is safe once:
  1. it is assembled from safe/reliable components;
  2. its components interact in a safe manner.
- Easy to enounce, difficult to realize;
- Example [CBMS2008]:
  - a naive assemblage of a blood pump, a valve and a pressure monitor may be harmful under specific circumstances.

Example [CBMS2008]



Implicit dependencies amongst communicating modules



- **What if** we try to turn the infusion pump on when blood pressure is high?
  - system does not respond!

Algorithmic safety (I)

- Flowchart-like guideline models may lead to deadlocks or to non terminating loops;
- Medical teams adopting them may therefore be found in critical situations in which contradictory, inconsistent or cyclical actions are issued by the flowchart algorithm to the team members and to the medical devices involved;

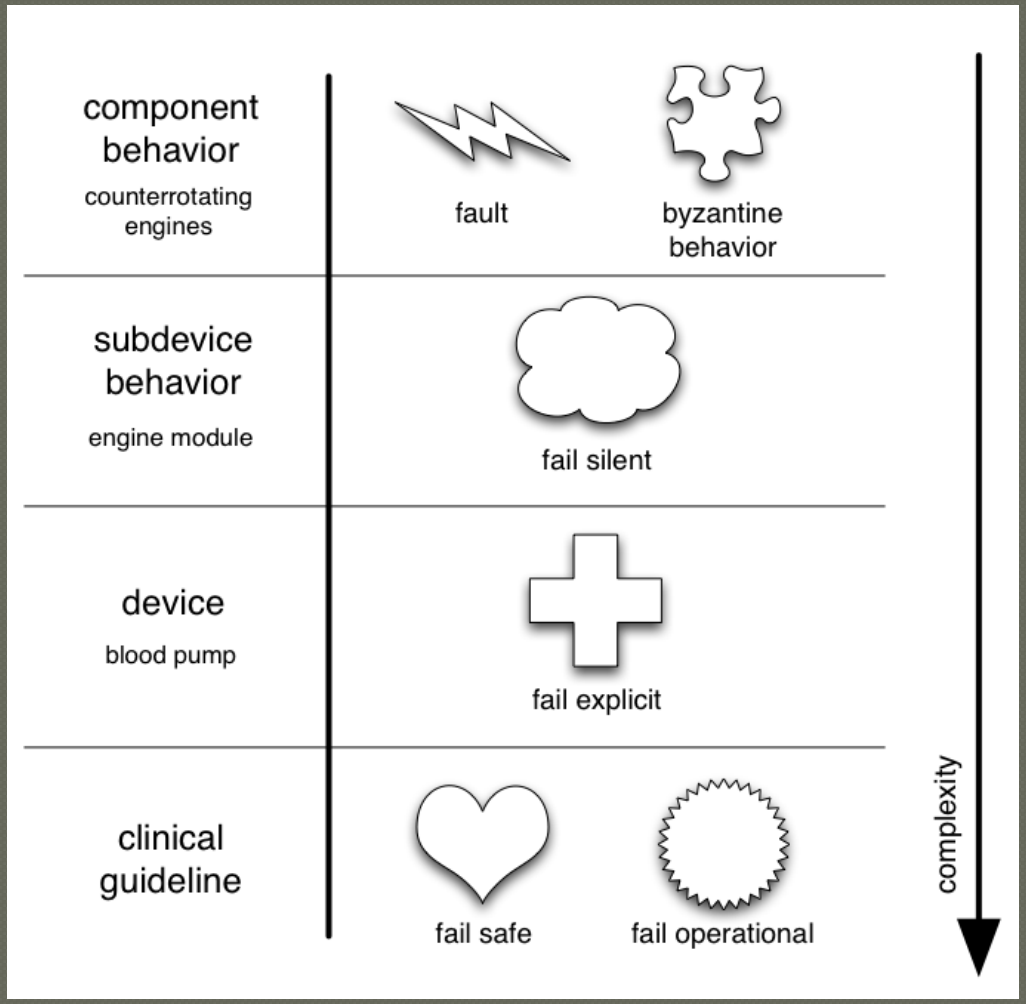
Algorithmic safety (II)

- Vice versa, wrong or exceptional actions and signals coming from both human and computer controlled agents have to be taken into account in order to undertake alternate recovery plans;
- Such events have to be exhaustively foreseen and considered by the flowchart algorithm in order to issue recovery actions accordingly.

Proposal

- The paper proposes to adopt a modular and hierarchical state based formalism for representing behavioral aspects in medical guidelines;
- Modular decomposition:
  - tasks decomposed into smaller tasks;
  - each task modelled, reused and checked separately;
  - medical guidelines models built incrementally.
- Fault management strategies may be assigned to each decomposition level in natural way;

Proposal at a glance

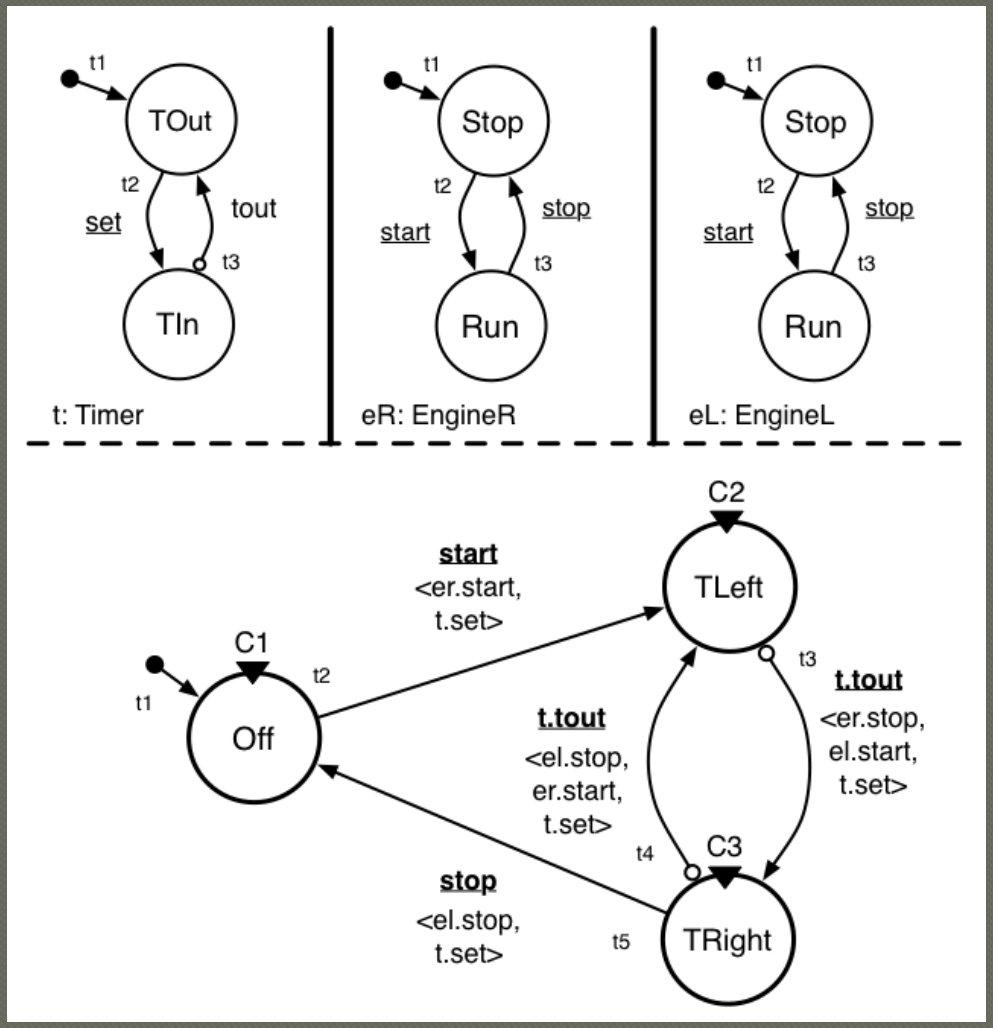


Example

- In the paper PW Statecharts are used to model, for instance, the safe behavior of a medical device at different specification levels, namely:

1. a component of the device (engines);
2. the device itself;
3. a portion of the medical guideline where the device is employed.

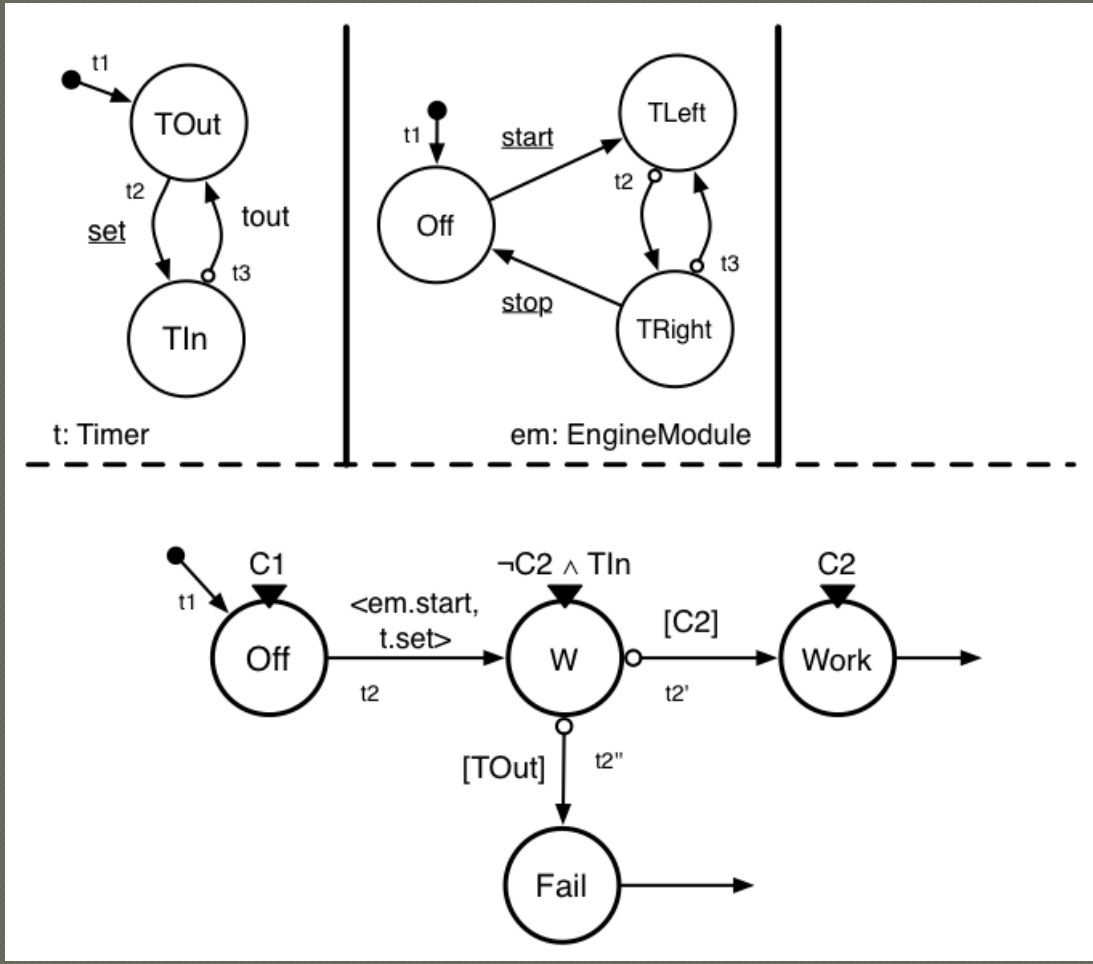
Sub-device behavior



fault behavior

fail silent behavior

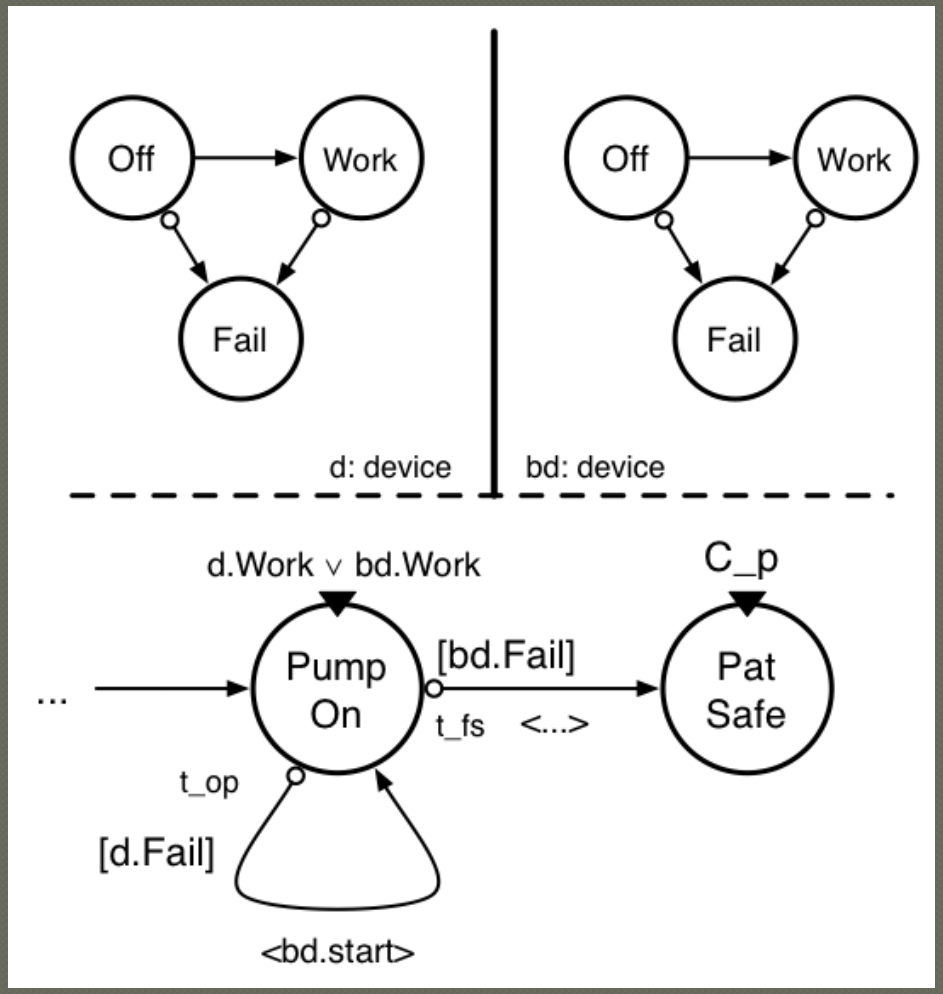
Device behavior



fail silent behavior

fail explicit behavior

Guideline behavior



fail explicit behavior

fail operational behavior

Conclusions

- The paper proposes to adopt a modular and hierarchical state based formalism for the sake of representing behavioral aspects in medical guidelines;
- PW Statecharts can be employed, homogeneously, at different description level.
- It can be observed that well-known fault management strategies fit inherently at the different decomposition levels, thus providing both an additional, empirical, confirmation of the validity of the approach and a stimulus for further research.