Formal Approaches to Safe Software Development for Medical Devices

by Alena Simalatsar
RiSD, EPFL

In collaboration with:
Nicolas Widmer, Thierry Buclin, CHUV
Romain Bornet, Yann Thoma, HEIG-VD
Dechao Sun, Wenqi You, Giovanni De Micheli, EPFL
Better “safe” than “sorry”

“The problem in medical errors is not bad people in health care—it is that good people are working in bad systems that need to be made safer”[1]

The gap between medical and engineering domains

Better “safe” than “sorry”

The gap between medical and engineering domains

On the one hand

- Nowadays, there exist a large set of electronic medical devices to support medical doctors in the process of patients:
  - Monitoring
  - Controlling
  - Treatment

- These devices are controlled by software: 1) drivers  2) decision-support

- Software developers have no medical knowledge:
  - Assume the requirements
  - Produce open interface devices that need to be further used and programmed
  - By medical doctors with now engineering background
On the other hand

❖ When treating patients practitioners are following Medical Guidelines
  • A Medical Guideline (GL) – is a document used to guiding decisions and criteria regarding diagnosis, management and treatment in specific areas of healthcare

❖ However, GLs are often:
  • Non formally represented (text form and likely tables), therefore
  • Suffer from such structural problems as: incompleteness, inconsistency, ambiguity and redundancy

❖ Which:
  • Source of errors when applying them
  • Make automatisation of the GLs hard

Formalize
Compose
Verify
From GLs to Executable Code

- Medical Guidelines in Text and Tables
- Protocol Formalization
- Formal Representation
  - Formal Models: TA, Promela, SMV
  - Properties: LTL, CTL
- Synthesis
- Decision-support System or Code for an Embedded System
Agenda

❖ Existing formalisms
❖ Imatinib GL modelling
❖ Response to the treatment definition
❖ Protocol formal analysis
❖ Conclusion: drug delivery reminder
Medical Records

• **Formal Modeling**
  - Arden (1989)
  - Asbru (1998)
  - EON (1996)
  - GLARE (1997)
  - GLIF (1998)
  - GUIDE (1998)
  - Prestige (1996)
  - PRODIGY (1996)
  - SAGE (2002)

Common practice

• **Formal Verification**
  - SPIN (Promela);
  - SMV symbolic model checker;

Some are discontinued -
No support for verification -
Trace back the counterexamples is hard -
Notion of time only in flow-chart order -
Timed Automata (TA)

Definition

Timed Automata (TA) over actions (Act) and clocks (C) is a tuple \( \langle \text{Loc}, \text{Loc}_0, \rightarrow \rangle \), where

- \( \text{Loc} \) is a set of finite location
- \( \text{Loc}_0 \subseteq \text{Loc} \) is a set of initial location
- \( \rightarrow \subseteq \text{Loc} \times B(C) \times \text{Act} \times 2^C \times \text{Loc} \) is a set of edge relations

When \( \langle \text{Loc}, g, a, r, \text{Loc}' \rangle \in \rightarrow \), we write \( \text{Loc} \xrightarrow{g,a,r} \text{Loc}' \)
Timed Automata extended with Tasks (TAT)

Definition
Timed Automata extended with tasks (TAT) over actions ($\text{Act}$), clocks ($\text{C}$) and tasks ($\text{P}$) is a tuple $\langle \text{Loc}, \text{Loc}_0, \rightarrow, \text{M} \rangle$, where

- $\text{Loc}$ is a set of finite location
- $\text{Loc}_0 \subseteq \text{Loc}$ is a set of initial location
- $\rightarrow \subseteq \text{Loc} \times \mathcal{B}(\text{C}) \times \text{Act} \times 2^\text{C} \times \text{M} \times \text{Loc}$ is a set of edge relations
- $\text{M} : \text{Act} \rightarrow \text{P}$ is a partial function assigning tasks to actions
Agenda

- Existing formalisms
- Imatinib GL modelling
- Response to the treatment definition
- Protocol formal analysis
- Conclusion: drug delivery reminder
Imatinib GL modeling

**Diagram Details:**
- **Init1:** t1 < p1
- **Action1:** GiveDose
  - t1 >= p1
  - t1 = 0
- **Init2:** t4 < p4
  - t4 >= p4
  - t4 = 0
- **Action2:** Measure
- **Init:**
  - acc_p = true
  - dose = 600
- **Blast_accel:**
  - t5 >= p5 && (N_N < n_lowerBA | N_T < t_lowerBA)
  - t5 = 0, dose = 400
- **Anemia_ch:**
  - N_N <= n_lowerB && N_T <= t_lowerB
  - N_fails++, dose = 0
- **Chronic_p:**
  - ch_p = true
  - dose = 400
- **Repetitive_anemia:**
  - N_N >= n_normB && N_T >= t_normB && N_fails >= 2
  - dose = 300
- **Lack_loss_resp_ch:**
  - LoL_resp = true
  - dose = 600
- **Lack_loss_resp_bl:**
  - LoL_resp = true
  - dose = 400, p1 = p2
- **Anemia_blast:**
  - N_N >= n_normB && N_T >= t_normB && N_fails < 2
  - dose = 400
- **Anemia_2:**
  - t6 >= p6 && (N_N < n_lowerBA | N_T < t_lowerBA)
  - t6 = 0, dose = 300
- **Pause:**
  - N_N > n_normBA && N_T >= t_normBA
  - dose = 300
Agenda

❖ Existing formalisms
❖ Imatinib case study modelling
❖ Response to the treatment definition
❖ Protocol formal analysis
❖ Conclusion: drug delivery reminder
### Response definition

<table>
<thead>
<tr>
<th>Warnings</th>
<th>Failure</th>
<th>Suboptimal response</th>
<th>Optimal response</th>
</tr>
</thead>
</table>
| BASELINE | - High risk<sup>a</sup>  
- CCA/Ph +<sup>b</sup> | / | / | / |
| 3 months | / | - Non CHR | - No CgR (Ph+ > 95%) | - At least minor CgR (Ph+ ≤ 65%) |
| 6 months | / | - No CgR (Ph+ > 95%) | - Less than PCgR (Ph+ > 35%) | - At least PCgR (Ph+ ≤ 35%) |
| 12 months | - Less than MMoI<sup>c</sup> | - Less than PCgR (Ph+ > 35%) | - PCgR (Ph+ 1–35%) | - CgR |
| 18 months | / | - Less than CcgR | - Less than MMoI<sup>c</sup> | - MMoI<sup>c</sup> |
| Any Time, during treatment | - Rise in transcript levels  
- CCA/Ph−<sup>d</sup> | - Loss of CHR  
- Loss of CcgR  
- Mutations<sup>e</sup>  
- CCA/Ph +<sup>b</sup> | - Loss of MMoI<sup>c</sup>  
- Mutations<sup>f</sup> | - Stable or improving MMoI<sup>c</sup> |

#### Definition of hematologic, cytogenetic and molecular response.

- **Complete Hematologic Response (CHR)**  
- WBC < 10×10<sup>9</sup>/L, no immature granulocytes, less than 5% basophils, platelets < 450×10<sup>9</sup>/L, spleen non palpable
- **Complete Cytogenetic Response (CCgR)**  
- No Ph+ metaphases
- **Partial Cytogenetic Response (PCgR)**  
- 1–35% Ph+ metaphases
- **Minor Cytogenetic Response (mCgR)**  
- 36–65% Ph+ metaphases
- **Minimal Cytogenetic Response (minCgR)**  
- 66–94% Ph+ metaphases
- **No Cytogenetic Response (NoCgR)**  
- ≥ 95% Ph+ metaphases
- **Major Molecular Response (MMoI<sup>c</sup>)**  
- BCR-ABL: ABL ≤ 0.1% on the International Scale
- **Complete Molecular Response (CMoI<sup>c</sup>)**  
- BCR-ABL transcript undetectable by RT-Q-PCR

---

Response definition - graph
Response definition - optimal response

**Complete Hematologic Response (CHR)**
1. WBC < 10^9/L;
2. Immature granulocytes <= 0
3. Basophils < 5%
4. Platelets < 450 x 10^9/L
5. Spleen non palpable

**Complete Cytogenetic Response (CCgR)**
No Ph+ metaphases

**Partial Cytogenetic Response (PCgR)**
1-35% Ph+ metaphases
(65-99% in 100% - Ph+)

**Minor Cytogenetic Response (mCgR)**
36-65% Ph+ metaphases
(35-64% in 100% - Ph+)

**Minimal Cytogenetic Response (minCgR)**
66-94% Ph+ metaphases
(5-35% in 100% - Ph+)

**No Cytogenetic Response (NoCgR)**
>=95% Ph+ metaphases
(<=5% in 100% - Ph+)

**Major Molecular Response (MMoIR)**
BCL-ABL: ABL <= 0.1% on the Internal Scale

**Complete Molecular Response (CMoIR)**
BCR-ABL transcript undetectable
Response definition - loss of response

- **Complete Hematologic Response (CHR)**
  1. WBC < 10x10⁹/L;
  2. Immature granulocytes <= 0
  3. Basophils < 5%
  4. Platelets < 450 x 10⁹/L
  5. Spleen non palpable

- **Complete Cytogenetic Response (CCgR)**
  No Ph+ metaphases

- **Partial Cytogenetic Response (PCgR)**
  1-35% Ph+ metaphases (65-99% in 100% - Ph+%)

- **Minor Cytogenetic Response (mCgR)**
  36-65% Ph+ metaphases (35-64% in 100% - Ph+%)

- **Minimal Cytogenetic Response (minCgR)**
  66-94% Ph+ metaphases (5-35% in 100% - Ph+)

- **No Cytogenetic Response (NoCgR)**
  >=95% Ph+ metaphases (<=5% in 100% - Ph+)

- **Major Molecular Response (MMoR)**
  BCL-ABL: ABL <= 0.1% on the Internal Scale

- **Complete Molecular Response (CMoIR)**
  BCR-ABL transcript undetectable

[Graph showing response definition with stages: CMoIR, MMoIR, NoMoIR, CHR, NoCHR over months 3, 6, 12, 18 with percentages: 100% - Ph+%: 100%, 99%, 65%, 35%, 5%]
Response definition - lack of response

**Complete Hematologic Response (CHR)**
1. WBC < 10^9/L
2. Immature granulocytes <= 0
3. Basophils < 5%
4. Platelets < 450 x 10^9/L
5. Spleen non palpable

**Complete Cytogenetic Response (CCgR)**
No Ph+ metaphases

**Partial Cytogenetic Response (PCgR)**
1-35% Ph+ metaphases (65-99% in 100% - Ph+ %)

**Minor Cytogenetic Response (mCgR)**
36-65% Ph+ metaphases (35-64% in 100% - Ph+ %)

**Minimal Cytogenetic Response (minCgR)**
66-94% Ph+ metaphases (5-35% in 100% - Ph+ %)

**No Cytogenetic Response (NoCgR)**
>=95% Ph+ metaphases (<=5% in 100% - Ph+ %)

**Major Molecular Response (MMolR)**
BCL-ABL: ABL <= 0.1% on the Internal Scale

**Complete Molecular Response (CMolR)**
BCR-ABL. transcript undetectable
Response observer

Observer TAT:

TAT insures that the progressive patient reaction to the treatment will always remain at least above the failure level, at the level of suboptimal response and higher.
Agenda

❖ Existing formalisms
❖ Imatinib case study modelling
❖ Response to the treatment definition
❖ Protocol formal analysis
❖ Conclusion: drug delivery reminder
Imatinib GL extended

- **init1**: t1 < p1
  - t1 >= p1
  - t1 = 0
  - **action1**: GiveDose

- **Init2**: t4 < p4
  - t4 >= p4
  - t4 = 0
  - **action2**: Measure

- **init**
  - acc_p == true
  - dose = 600

- **chronic_p**
  - N_N <= n_lowerB | N_T <= t_lowerB
  - N_fails++, dose = 0
  - ch_p == true
  - dose = 400

- **anemia_ch**
  - N_N > n_normB & N_T > t_normB & N_fails >= 2
  - dose = 300

- **lack_loss_resp_ch**
  - LoL_resp == true
  - dose = 600

- **lack_loss_resp_bl**
  - LoL_resp == true
  - dose = 400, p1 = p2

- **anemia_blast**
  - t5 >= p5 & (N_N < n_lowerBA | N_T < t_lowerBA)
  - t5 = 0, dose = 400

- **anemia_2**
  - t6 >= p6 & (N_N < n_lowerBA | N_T < t_lowerBA)
  - t6 = 0, dose = 300

- **repetitive_anemia**
  - N_N > n_normB & N_T > t_normB & N_fails >= 2
  - dose = 300

- **stop_positive**
  - LoL_resp == true
  - dose = 600

- **pause**
  - N_N > n_normBA & N_T >= t_normBA
  - dose = 300
Imatinib GL extended

chronic_p —> E <> (lack_loss_resp_ch)
Imatinib GL extended
Agenda

❖ Existing formalisms
❖ Imatinib case study modelling
❖ Response to the treatment definition
❖ Protocol formal analysis
❖ Conclusion: drug delivery reminder
Conclusion: drug delivery reminder

The Icycom platform by CSEM SA, Switzerland
TAT is suitable for action and definition based GLs modelling;

Structural problems of GLs can be fixed;

The verification of life-cycle properties requires a patient or a model:
- Pharmacokinetic (PK) - pharmacodynamic (PD) modeling

Formally models of GLs must be complemented with other functionality;

TAT is compositional and synthesisable.