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

EPFL Workshop on Logic Synthesis & Verification, December 10-11, 2015

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

[1] To Err Is Human: Building a Safer Health System (2000), Linda T. Kohn, Janet M. Corrigan, and Molla S. Donaldson

Better “safe” than “sorry”

The gap between medical and engineering domains

[1] To Err Is Human: Building a Safer Health System (2000), Linda T. Kohn, Janet M. Corrigan, and Molla S. Donaldson

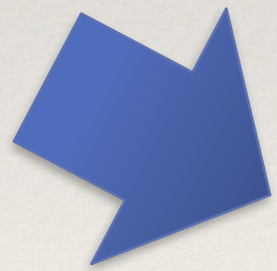
On the one hand

- 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*

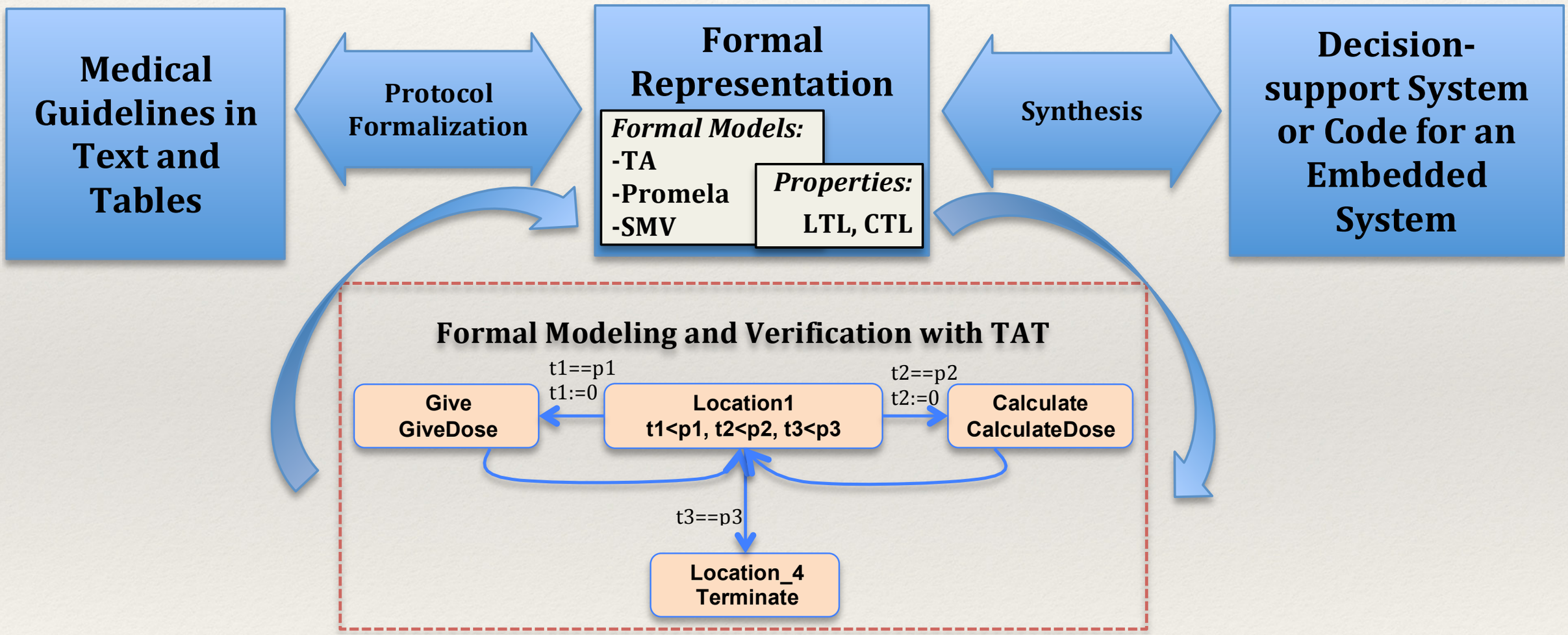


Formalize

Verify

Compose

From GLs to Executable Code



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)*
  - *PROforma (1992 - 2000)*
  - *SAGE (2002)*
  - *Stepper (2001 - 2003)*

Common practice

translation

- ***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 -

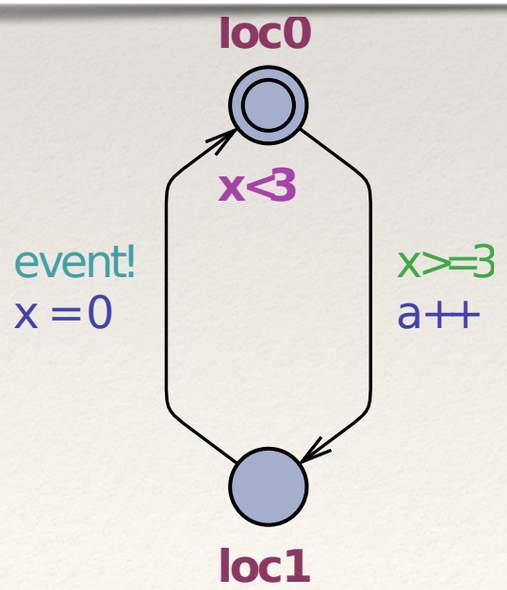
Timed Automata (TA)

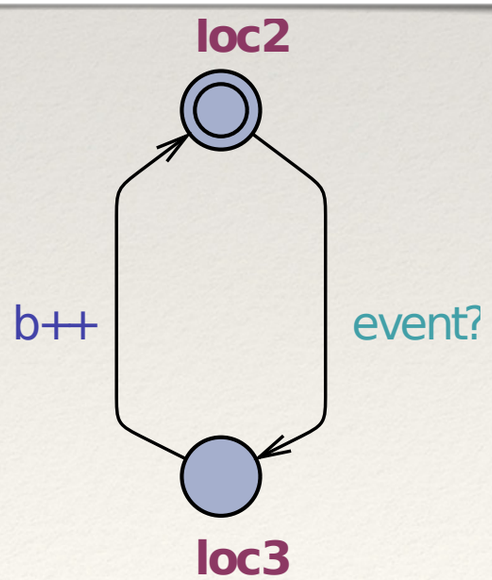
Definition

Timed Automata (TA) over actions (Act) and clocks (C) is a tuple $\langle Loc, Loc_0, \hookrightarrow \rangle$, where

- Loc is a set of finite location
- $Loc_0 \subseteq Loc$ is a set of initial location
- $\hookrightarrow \subseteq Loc \times \mathcal{B}(C) \times Act \times 2^C \times Loc$ is a set of edge relations

When $\langle Loc, g, a, r, Loc' \rangle \in \hookrightarrow$, we write $Loc \xrightarrow{g,a,r} Loc'$



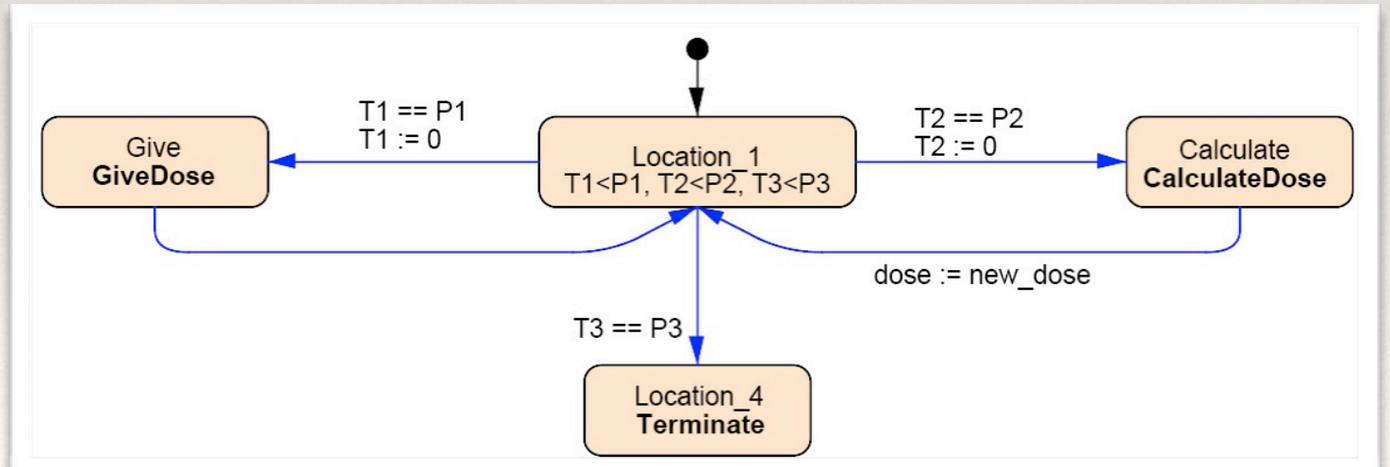


Timed Automata extended with Tasks (TAT)

Definition

Timed Automata extended with tasks (TAT) over actions (Act), clocks (C) and tasks (P) is a tuple $\langle Loc, Loc_0, \hookrightarrow, M \rangle$, where

- Loc is a set of finite location
- $Loc_0 \subseteq Loc$ is a set of initial location
- $\hookrightarrow \subseteq Loc \times \mathcal{B}(C) \times Act \times 2^C \times M \times Loc$ is a set of edge relations
- $M : Act \to P$ is a partial function assigning tasks to actions



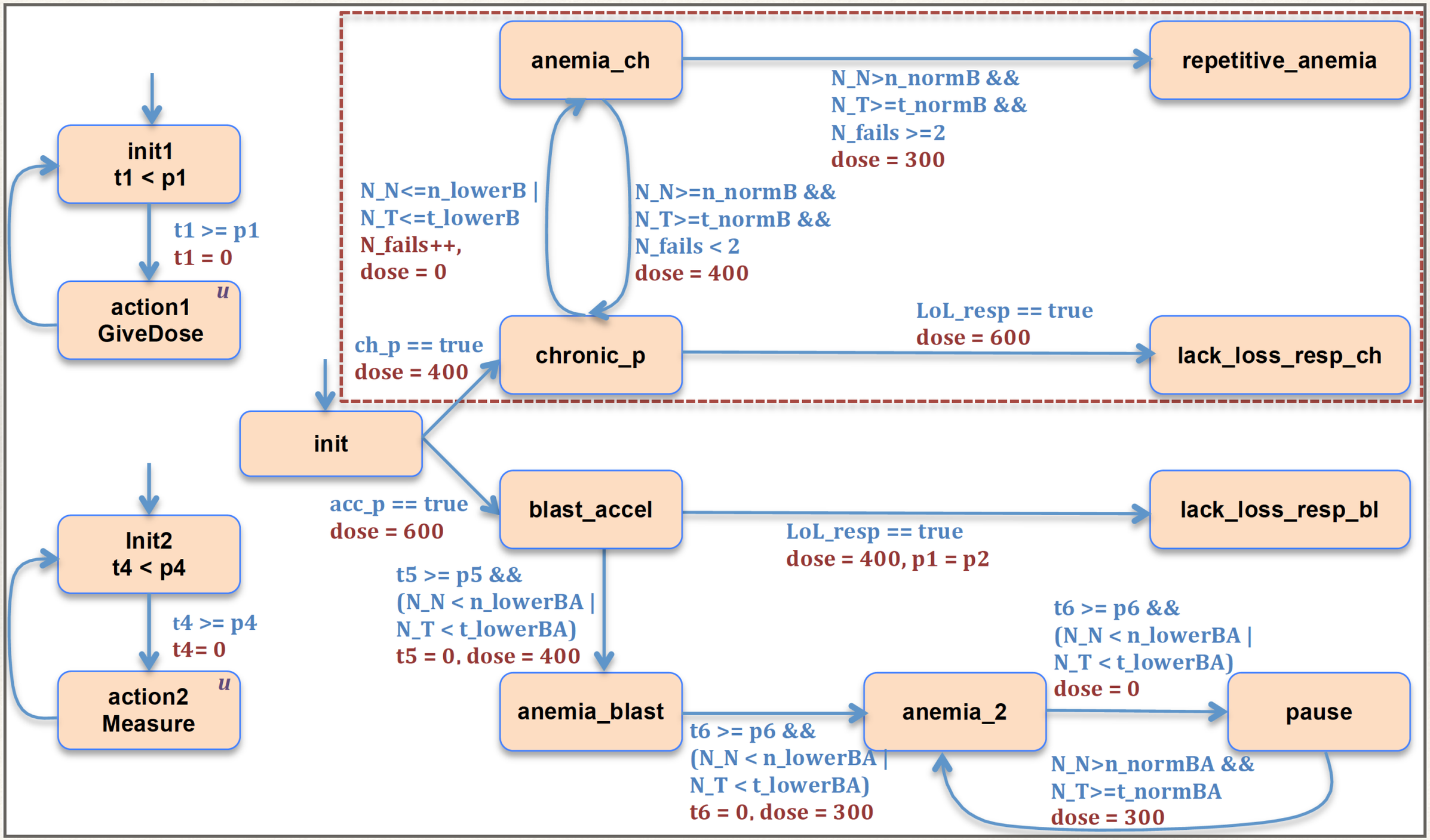
Task queue:

CalculateDose
GiveDose
CalculateDose
GiveDose
...
Terminate

Agenda

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

Imatinib GL modeling



Agenda

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

Response definition

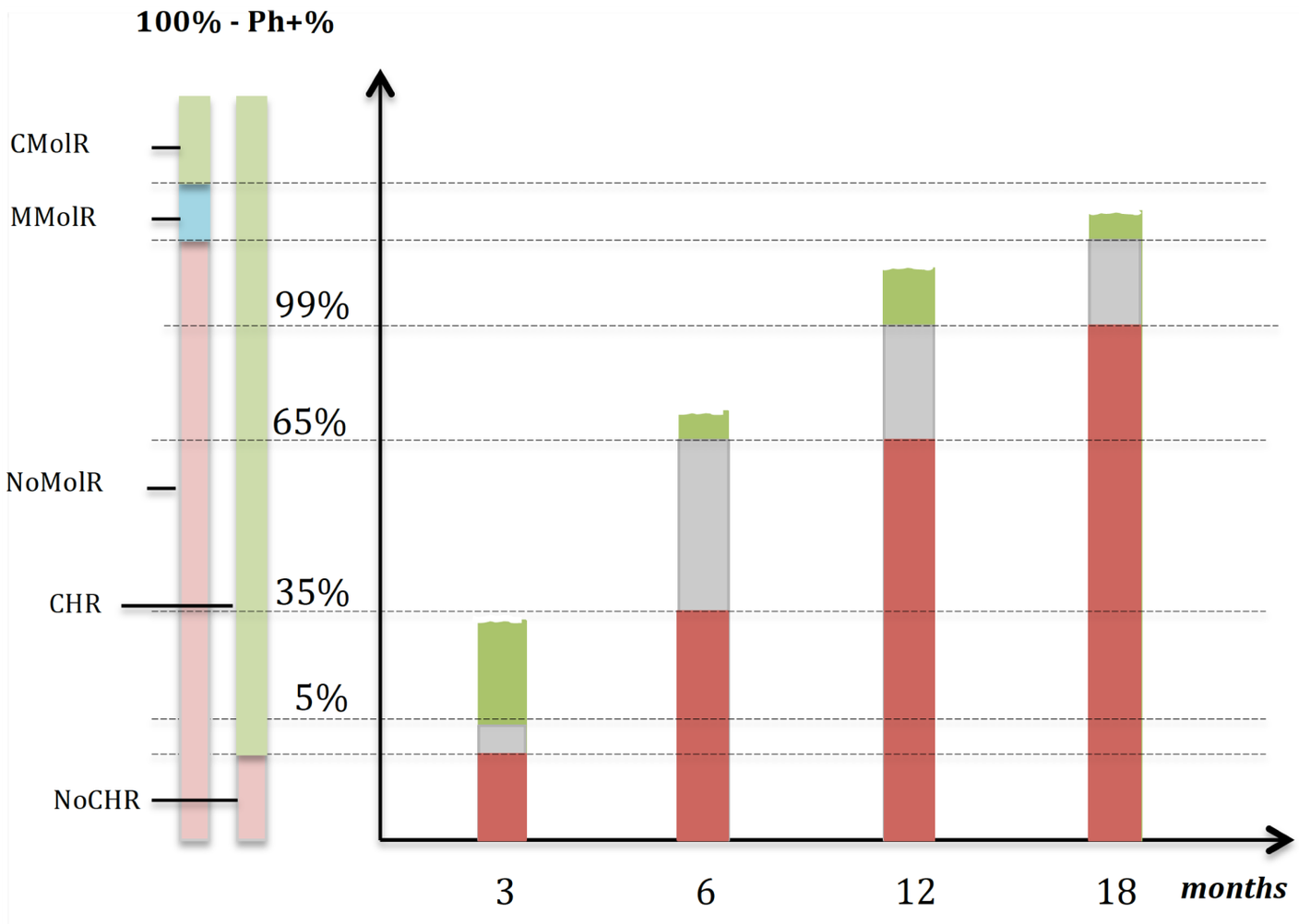
	Warnings	Failure	Suboptimal response	Optimal response
BASELINE	- High risk[a] - CCA/Ph + [b]	/	/	/
3 months	/	- Non CHR	- No CgR (Ph+ > 95%)	- At least minor CgR (Ph+ ≤ 65%)
6 months	/	- No CgR (Ph+ > 95%)	- Less than PCgR (Ph+ > 35%)	- At least PCgR (Ph+ ≤ 35%)
12 months	- Less than MMolR[b]	- Less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

Definition of haematologic, cytogenetic and molecular response.

Complete Hematologic Response (CHR)	- WBC< 10×10^9/L, no immature granulocytes, less than 5% basophils, platelets< 450x10^9/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 (MMolR)	- BCR-ABL: ABL ≤ 0.1% on the International Scale
Complete Molecular Response (CMolR)	- BCR-ABL transcript undetectable by RT-Q-PCR

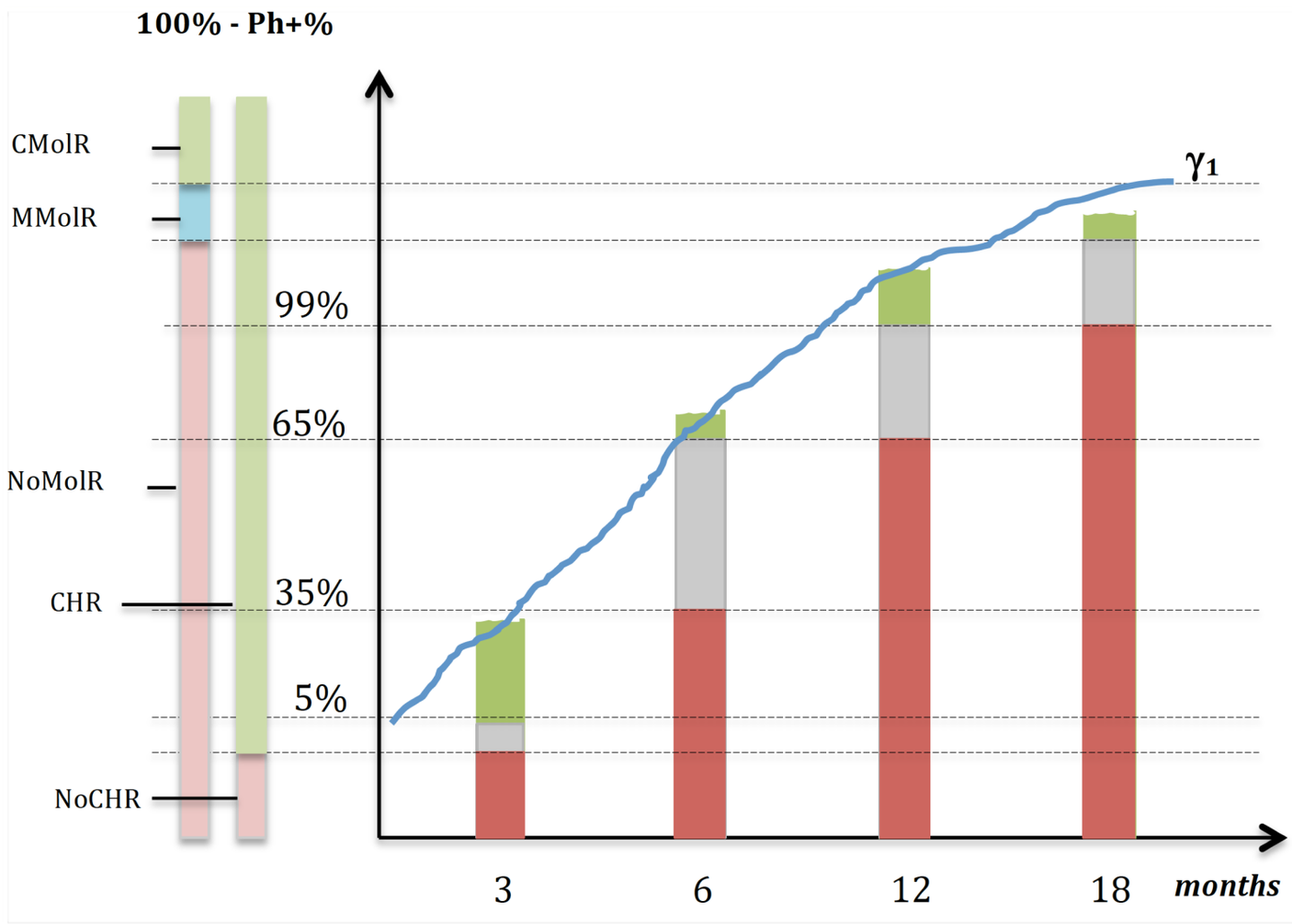
M. Baccarani, F. Castagnetti, G. Gugliotta, F. Palandri, and S. Soverini. Response definitions and european leukemia management recommendations. Best Pract Res Clin Haematol, 22(3):331–41, 2009.

Response definition - graph



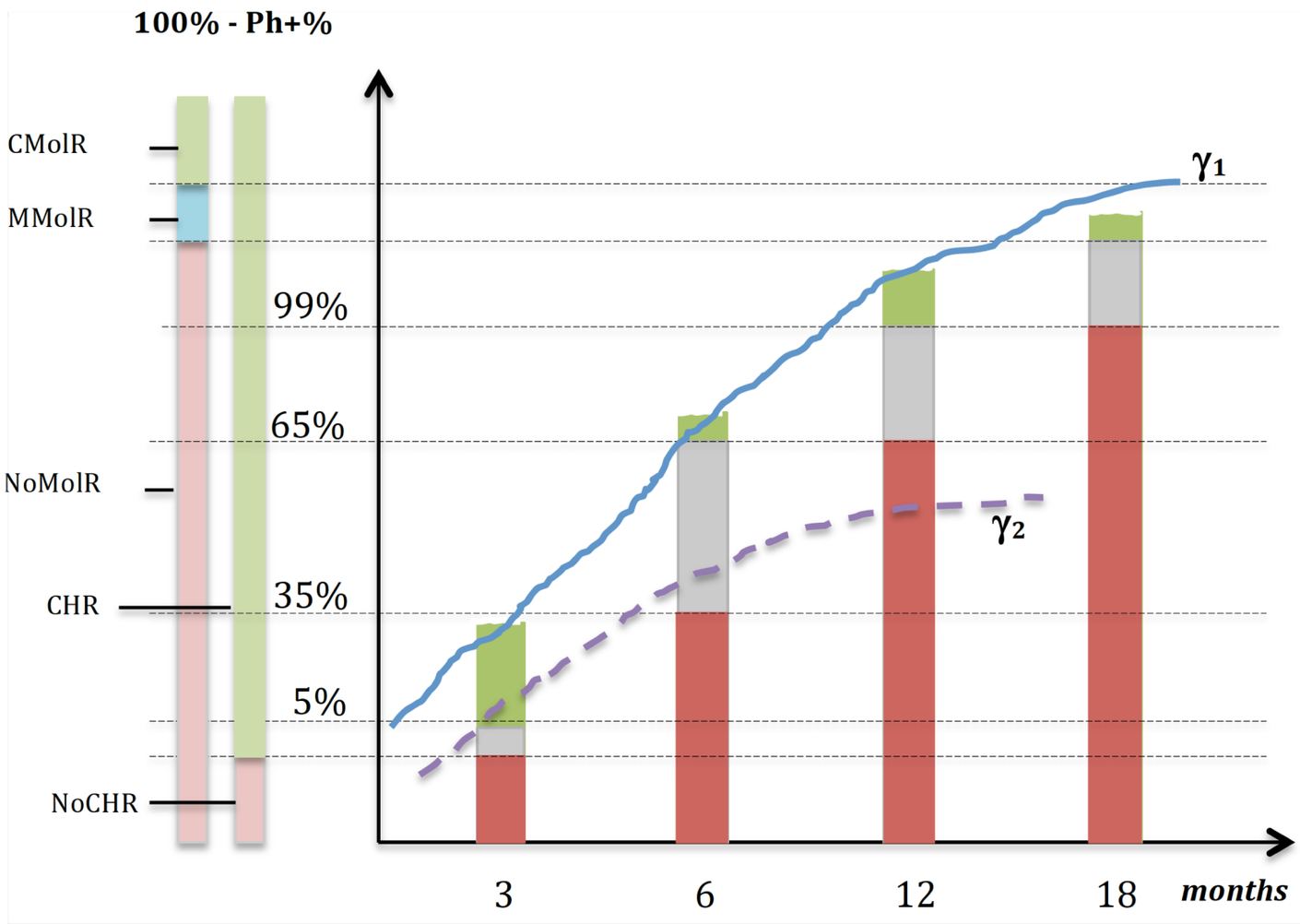
Complete Hematologic Response (CHR)	1. WBC < 10x10⁹/L; 2. Immature granulocytes <= 0 3. Basophils < 5%; 4. Platelets < 450 x 10⁹/L 5. Spleen non palpable
Complete Cytogenetic Response (CCgR)	No Ph+ metaphases
Partial Cytogenetic Response (PCgR)	1-35% Ph+ metaphases (65-99% in 100% - Ph+%)
Minor Cytogenetic 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 (MMolR)	BCL-ABL: ABL <= 0.1% on the Internal Scale
Complete Molecular Response (CMolR)	BCR-ABL transcript undetectable

Response definition - optimal response



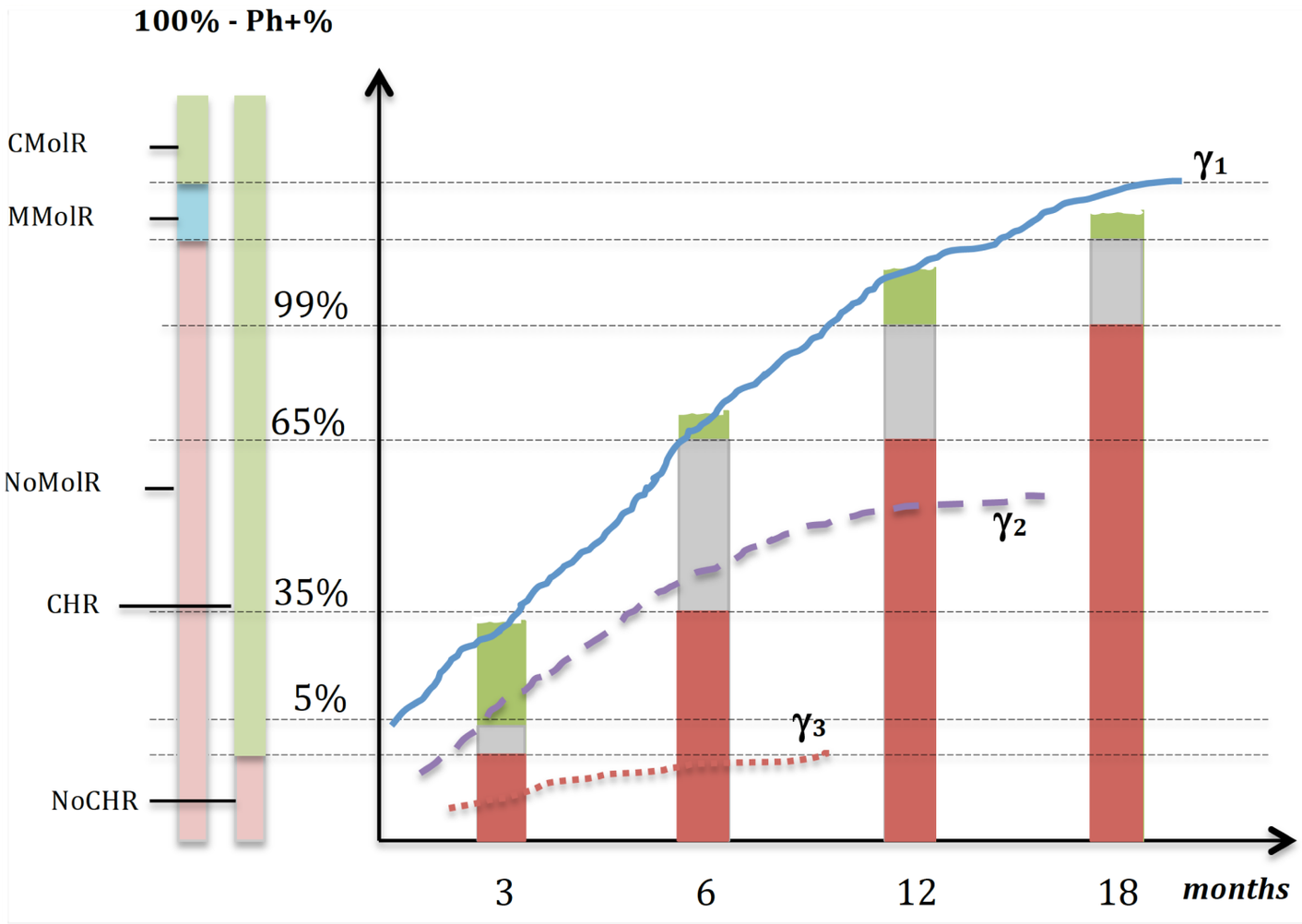
Complete Hematologic Response (CHR)	1. WBC < 10x10⁹/L; 2. Immature granulocytes <= 0 3. Basophils < 5%; 4. Platelets < 450 x 10⁹/L 5. Spleen non palpable
Complete Cytogenetic Response (CCgR)	No Ph+ metaphases
Partial Cytogenetic Response (PCgR)	1-35% Ph+ metaphases (65-99% in 100% - Ph+%)
Minor Cytogenetic 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 (MMolR)	BCL-ABL: ABL <= 0.1% on the Internal Scale
Complete Molecular Response (CMolR)	BCR-ABL transcript undetectable

Response definition - loss of response



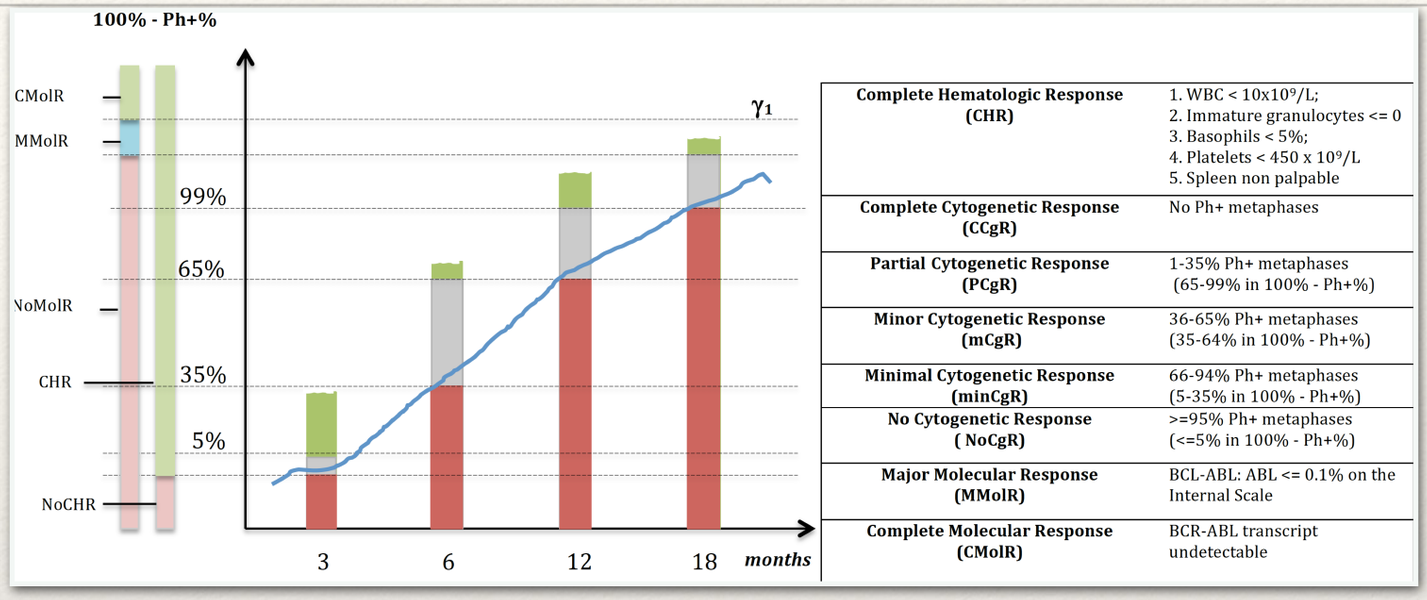
Complete Hematologic Response (CHR)	1. WBC < 10x10⁹/L; 2. Immature granulocytes <= 0 3. Basophils < 5%; 4. Platelets < 450 x 10⁹/L 5. Spleen non palpable
Complete Cytogenetic Response (CCgR)	No Ph+ metaphases
Partial Cytogenetic Response (PCgR)	1-35% Ph+ metaphases (65-99% in 100% - Ph+%)
Minor Cytogenetic 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 (MMolR)	BCL-ABL: ABL <= 0.1% on the Internal Scale
Complete Molecular Response (CMolR)	BCR-ABL transcript undetectable

Response definition - lack of response

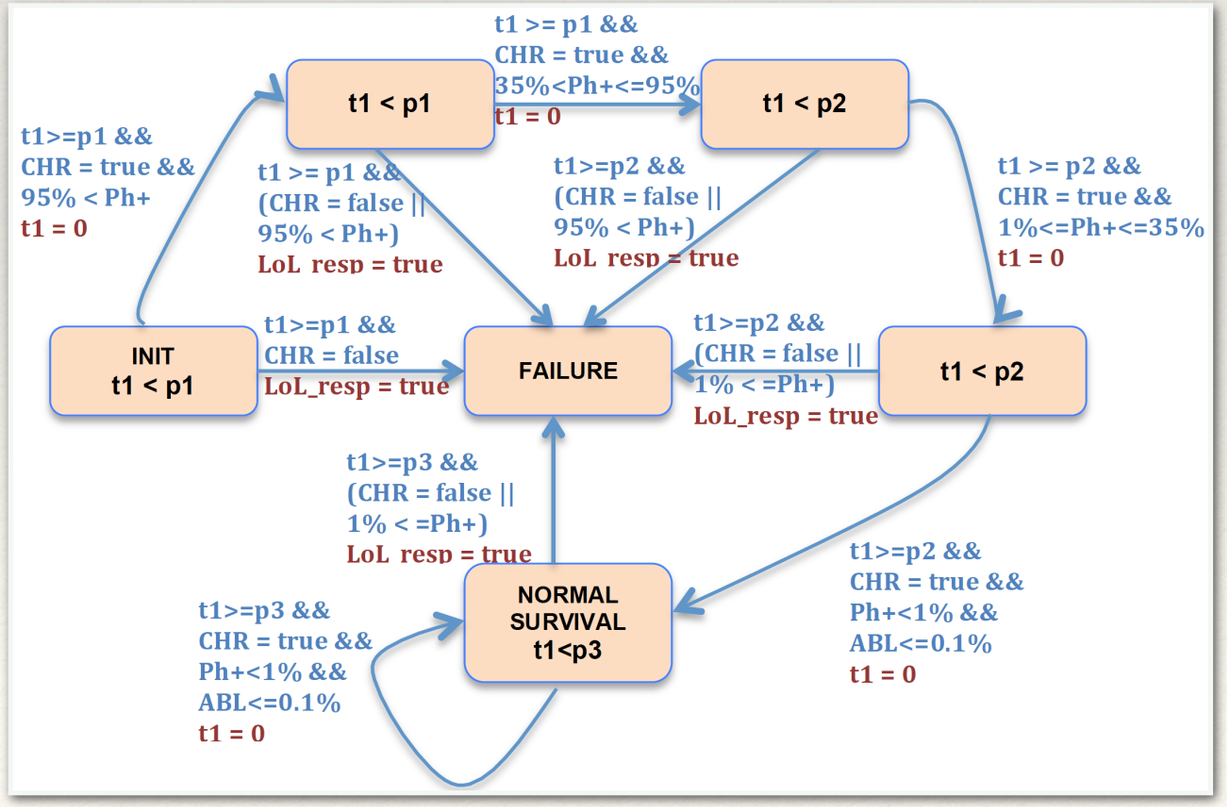


Complete Hematologic Response (CHR)	1. WBC < 10x10⁹/L; 2. Immature granulocytes <= 0 3. Basophils < 5%; 4. Platelets < 450 x 10⁹/L 5. Spleen non palpable
Complete Cytogenetic Response (CCgR)	No Ph+ metaphases
Partial Cytogenetic Response (PCgR)	1-35% Ph+ metaphases (65-99% in 100% - Ph+%)
Minor Cytogenetic 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 (MMolR)	BCL-ABL: ABL <= 0.1% on the Internal Scale
Complete Molecular Response (CMolR)	BCR-ABL transcript undetectable

Response observer



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 (MMolR)	BCL-ABL: ABL <= 0.1% on the Internal Scale
Complete Molecular Response (CMolR)	BCR-ABL transcript undetectable



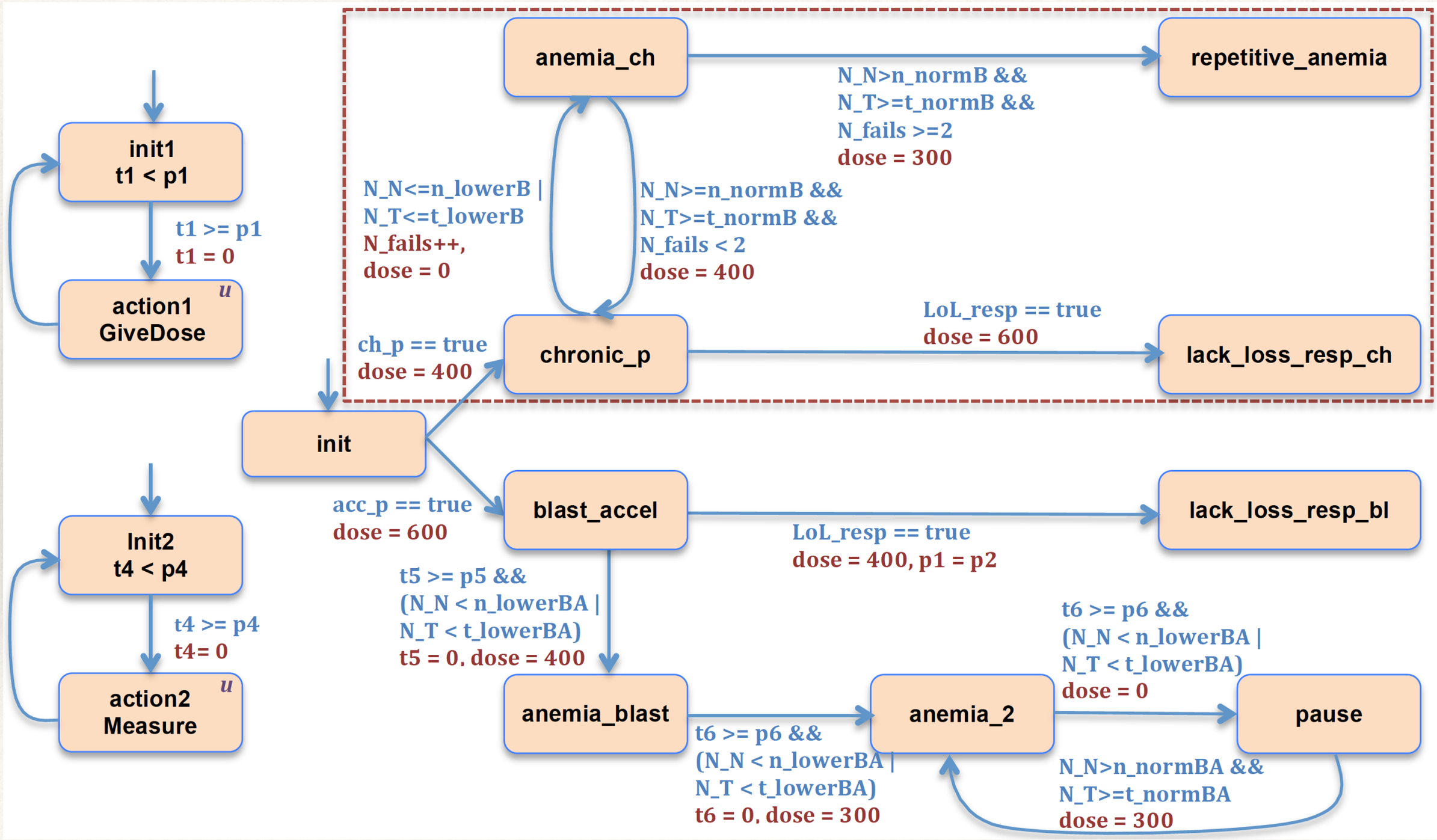
Observer TAT:

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.

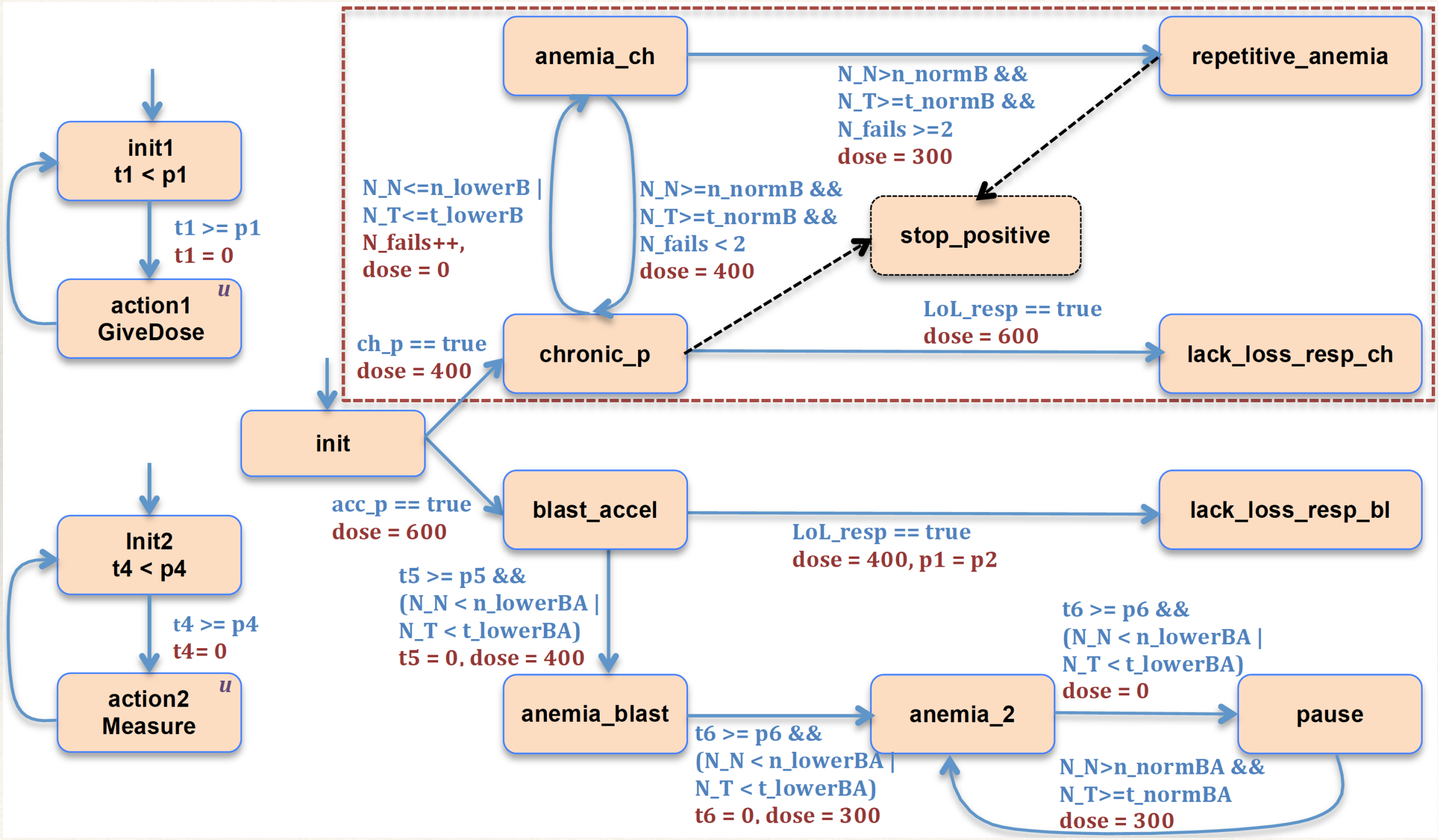
Agenda

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

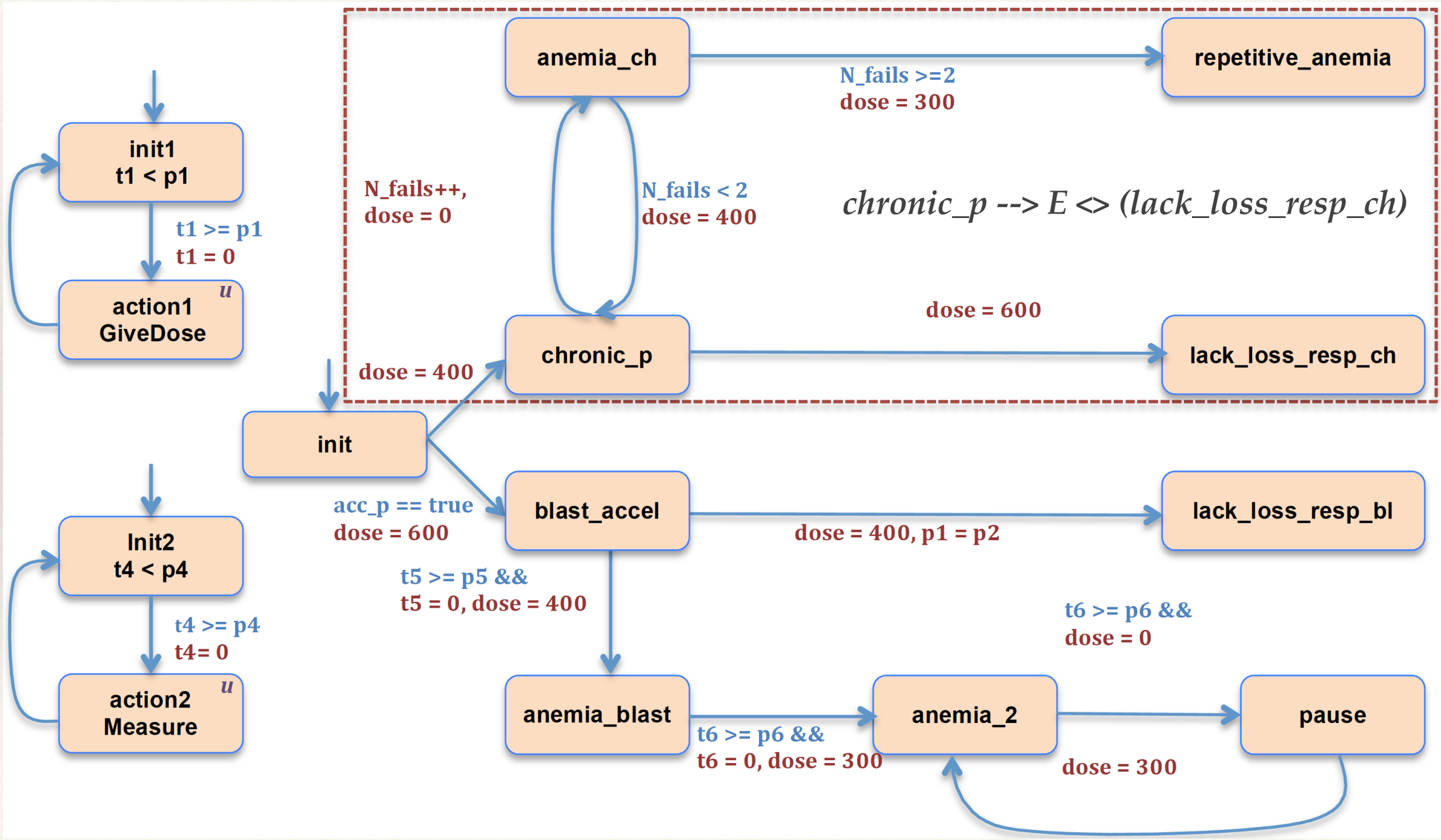
Imatinib GL extended



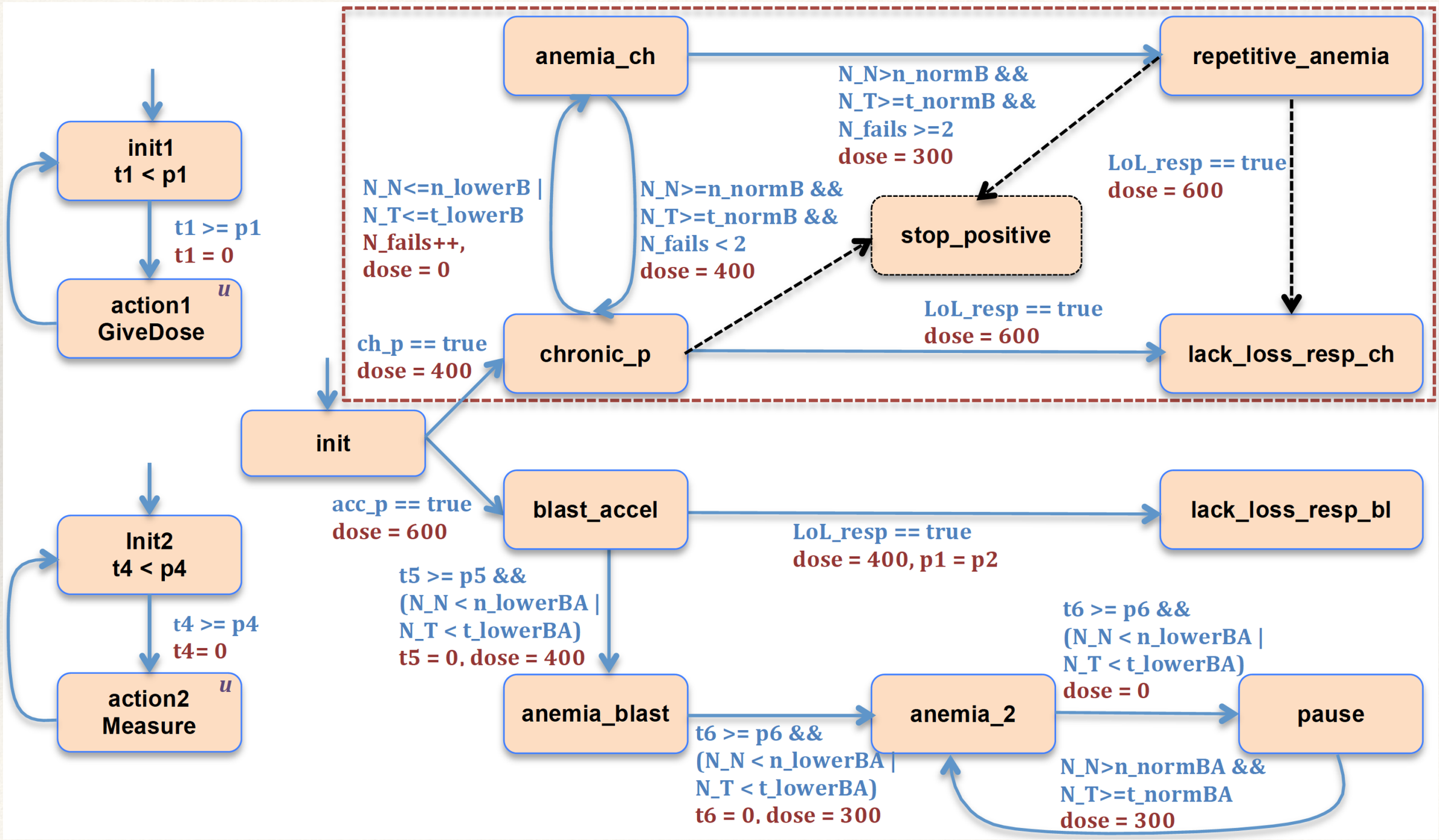
Imatinib GL extended



Imatinib GL extended



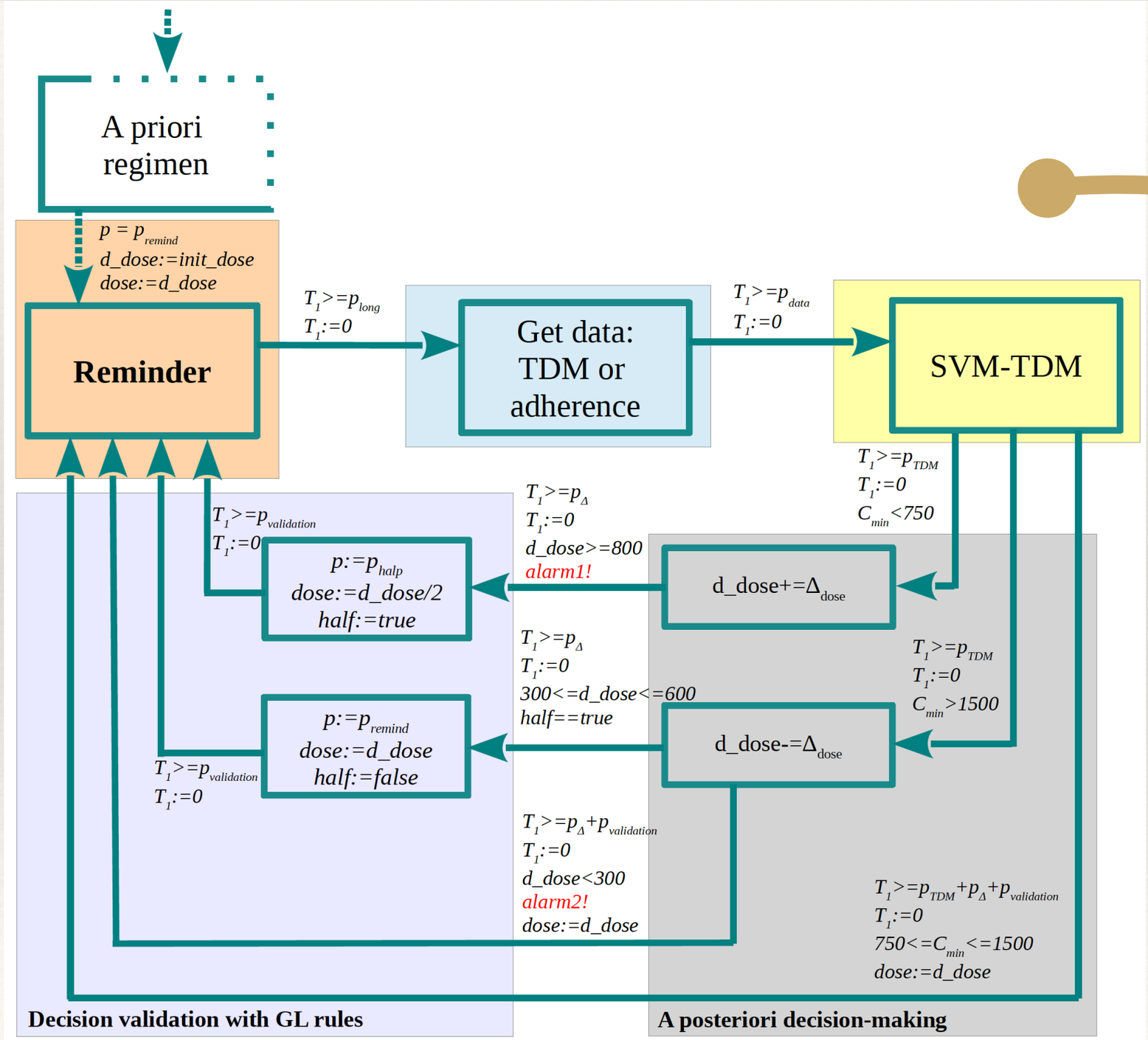
Imatinib GL extended



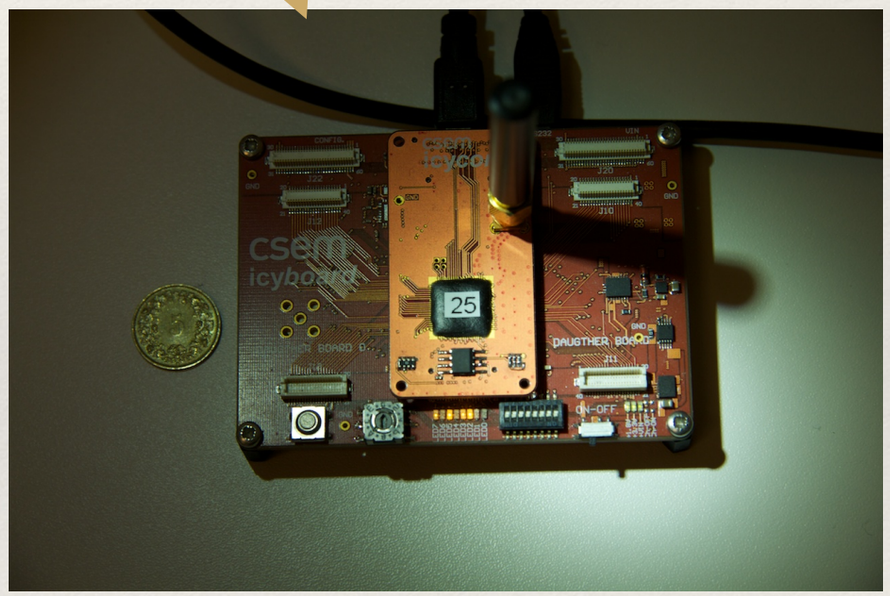
Agenda

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

Conclusion: drug delivery reminder



code generation



The Icycom platform by CSEM SA, Switzerland

Conclusion

- **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.**