Software Design, Modelling and Analysis in UML

Lecture 19: Live Sequence Charts III

2016-02-02

Prof. Dr. Andreas Podelski, **Dr. Bernd Westphal**

Albert-Ludwigs-Universität Freiburg, Germany

Contents & Goals

Last Lecture:

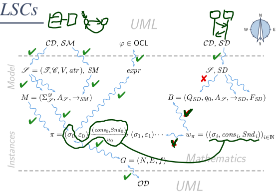
- Symbolic Büchi Automata
- Language of a UML Model
- Cuts

This Lecture:

- **Educational Objectives:** Capabilities for following tasks/questions.
  - How is the semantics of LSCs constructed?
  - What is a cut, fired-set, etc.?
  - Construct the TBA for this LSC.
  - Give one example which (non-)trivially satisfies this LSC.
- **Content:**
  - Cut Examples, Firedset
  - Automaton construction
  - Transition annotations
  - Forbidden scenarios

Live Sequence Charts — Semantics

TBA-based Semantics of LSCs



Plan:

- Given an LSC L with body

$$(I, (\mathscr{L}, \preceq), \sim, \mathscr{S}, \mathsf{Msg}, \mathsf{Cond}, \mathsf{LocInv}),$$

- construct a TBA $\mathcal{B}_L$, and
- define language $\mathcal{L}(L)$ of L in terms of $\mathcal{L}(\mathcal{B}_L)$,
  in particular taking activation condition and activation mode into account.
- Then $\mathcal{M} \models L$ (universal) if and only if $\mathcal{L}(\mathcal{M}) \subseteq \mathcal{L}(L)$.
  And $\mathcal{M} \models L$ (existential) if and only if $\mathcal{L}(\mathcal{M}) \cap \mathcal{L}(L) \neq \emptyset$.

Formal LSC Semantics: It's in the Cuts!

Definition.
Let $(I, (\mathscr{L}, \preceq), \sim, \mathscr{S}, \mathsf{Msg}, \mathsf{Cond}, \mathsf{LocInv})$ be an LSC body.
A non-empty set $\emptyset \neq C \subseteq \mathscr{L}$ is called a **cut** of the LSC body iff

- it is **downward closed**, i.e. $\forall\, l, l' \bullet l' \in C \wedge l \preceq l' \implies l \in C$,
- it is **closed** under **simultaneity**, i.e.

$$\forall\, l, l' \bullet l' \in C \wedge l \sim l' \implies l \in C, \text{ and}$$

- it comprises at least **one location per instance line**, i.e.

$$\forall\, i \in I\ \exists\, l \in C \bullet i_l = i.$$

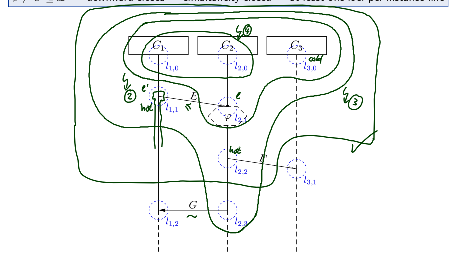
A cut C is called **hot**, denoted by $\theta(C) = \mathsf{hot}$, if and only if at least one of its maximal elements is hot, i.e. if

$$\exists\, l \in C \bullet \theta(l) = \mathsf{hot} \wedge \nexists\, l' \in C \bullet l \prec l'$$

Otherwise, C is called **cold**, denoted by $\theta(C) = \mathsf{cold}$.

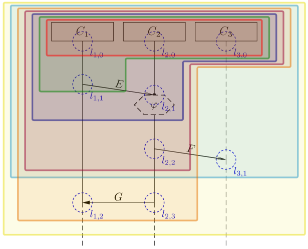
Cut Examples

$\emptyset \neq C \subseteq \mathscr{L}$ — downward closed — simultaneity closed — at least one loc. per instance line



Cut Examples

$\emptyset \neq C \subseteq \mathscr{L}$ — downward closed — simultaneity closed — at least one loc. per instance line



A Successor Relation on Cuts

The partial order of $(\mathscr{L}, \preceq)$ and the simultaneity relation "$\sim$" induce a **direct successor relation** on cuts of $\mathscr{L}$ as follows:

Definition. Let $C, C' \subseteq \mathscr{L}$ bet cuts of an LSC body with locations $(\mathscr{L}, \preceq)$ and messages Msg.

C' is called **direct successor** of C **via fired-set** F, denoted by $C \rightsquigarrow_F C'$, if and only if

include (*) from slide 9

- $F \neq \emptyset$,
- $C' \setminus C = F$,
- for each asynchronous (!) message reception in F, the corresponding sending is already in C,

$$\forall (l, E, l') \in \mathsf{Msg}, l \not\sim l' : l' \in F \implies l \in C, \text{ and}$$

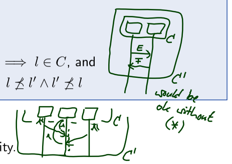
- locations in F, that lie on the same instance line, are pairwise unordered, i.e.

$$\forall l, l' \in F : l \neq l' \wedge i_l = i_{l'} \implies l \not\preceq l' \wedge l' \not\preceq l$$

Properties of the Fired-set

$C \rightsquigarrow_F C'$ if and only if

- $F \neq \emptyset$,
- $C' \setminus C = F$,
- $\forall (l, E, l') \in \mathsf{Msg}, l \not\sim l' : l' \in F \implies l \in C$, and
- $\forall l, l' \in F : l \neq l' \wedge i_l = i_{l'} \implies l \not\preceq l' \wedge l' \not\preceq l$

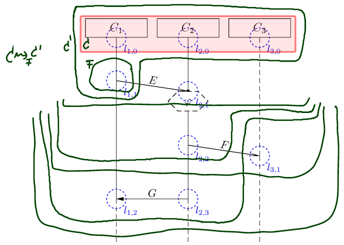


- **Note**: F is closed under simultaneity.
- **Note**: locations in F are direct $\preceq$-successors of locations in C, i.e.

$$\forall l' \in F \; \exists l \in C : l \prec l' \wedge \nexists l'' \in C : l \prec l'' \prec l' \quad (*)$$

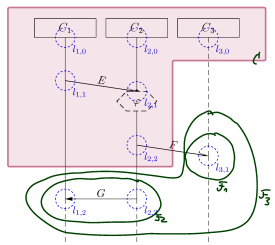
Successor Cut Example

$C \cap F = \emptyset$ — $C \cup F$ is a cut — only direct $\prec$-successors — same instance line on front pairwise unordered — sending of asynchronous reception already in

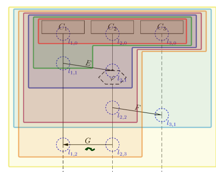


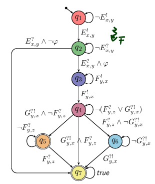
Successor Cut Example

$C \cap F = \emptyset$ — $C \cup F$ is a cut — only direct $\prec$-successors — same instance line on front pairwise unordered — sending of asynchronous reception already in



Language of LSC Body: Example





The TBA $\mathcal{B}_L$ of LSC L over Φ and $\mathcal{E}$ is $(Expr_B(X), X, Q, q_{ini}, \rightarrow, Q_F)$ with

- Q is **the set of cuts** of L, q_{ini} is the **instance heads** cut,
- $Expr_B(X) = Expr_{\mathscr{S}}(\mathscr{E}, X)$ (for considered signature $\mathscr{S}$),
- $\rightarrow$ consists of **loops**, **progress transitions** (by $\rightsquigarrow_F$), and **legal exits** (cold cond./local inv.),
- $Q_F = \{C \in Q \mid \Theta(C) = \text{cold} \vee C = \mathscr{L}\}$ is the set of cold cuts and the maximal cut.

TBA Construction Principle

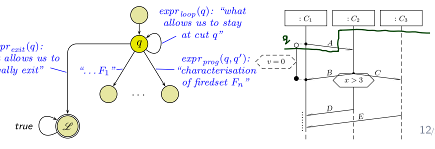
Recall: The TBA $\mathcal{B}(L)$ of LSC L is $(Expr_{\mathcal{B}}(X), X, Q, q_{ini}, \rightarrow, Q_F)$ with

- Q is **the set of cuts** of L, q_{ini} is the **instance heads** cut,
- $Expr_{\mathcal{B}}(X) = Expr_{\mathscr{S}}(\mathscr{E}, X)$ (for considered signature $\mathscr{S}$),
- $\rightarrow \subseteq Q \times Expr_{\mathscr{S}}(\mathscr{E}, X) \times Q$ consists of

  loops, **progress transitions** (by $\rightsquigarrow_F$), and **legal exits** (cold conditions / cold local invariants),
- $F = \{C \in Q \mid \Theta(C) = \text{cold} \vee C = \mathscr{L}\}$ is the set of cold cuts.

So in the following, we "only" need to construct the transitions' labels:

$\rightarrow = \{(q, expr_{loop}(q), q) \mid q \in Q\} \cup \{(q, expr_{prog}(q, q'), q') \mid q \rightsquigarrow_F q'\} \cup \{(q, expr_{exit}(q), \mathscr{L}) \mid q \in Q\}$



TBA Construction Principle

So in the following, we "only" need to construct the transitions' labels:

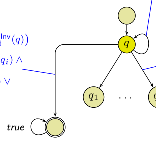
$\rightarrow = \{(q, expr_{loop}(q), q) \mid q \in Q\} \cup \{(q, expr_{prog}(q, q'), q') \mid q \rightsquigarrow_F q'\} \cup \{(q, expr_{exit}(q), \mathscr{L}) \mid q \in Q\}$

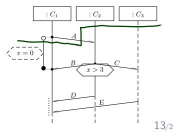
$$expr_{loop}(q) = \underbrace{expr^{\mathsf{Msg}}(q) \wedge expr^{\mathsf{LocInv}}_{\mathsf{hot}}(q)}_{=: expr^{\mathsf{hot}}_{loop}(q)} \wedge expr^{\mathsf{LocInv}}_{\mathsf{cold}}(q)$$

$$expr_{exit}(q) = \left(expr^{\mathsf{hot}}_{loop}(q) \wedge \neg expr^{\mathsf{LocInv}}_{\mathsf{cold}}(q)\right) \vee \bigvee_{1 \le i \le n} expr^{\mathsf{hot}}_{prog}(q, q_i) \wedge \left(\neg expr^{\mathsf{LocInv},\bullet}_{\mathsf{cold}}(q, q_i) \vee \neg expr^{\mathsf{Cond}}_{\mathsf{cold}}(q, q_i)\right)$$

$$expr_{prog}(q, q_n) = expr^{\mathsf{hot}}_{prog}(q, q_n) \wedge expr^{\mathsf{Cond}}_{\mathsf{cold}}(q, q_n) \wedge expr^{\mathsf{LocInv},\bullet}_{\mathsf{cold}}(q, q_n)$$

$$expr^{\mathsf{hot}}_{prog}(q, q_n) = expr^{\mathsf{Msg}}(q, q_n) \wedge expr^{\mathsf{Cond}}_{\mathsf{hot}}(q, q_n) \wedge expr^{\mathsf{LocInv},\bullet}_{\mathsf{hot}}(q, q_n)$$

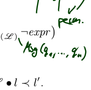




Loop Condition

$$expr_{loop}(q) = expr^{\mathsf{Msg}}(q) \wedge expr^{\mathsf{LocInv}}_{\mathsf{hot}}(q) \wedge expr^{\mathsf{LocInv}}_{\mathsf{cold}}(q)$$

none of any firedset messages is observed

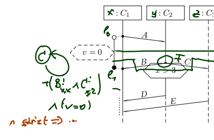


- $expr^{\mathsf{Msg}}(q) = \neg \bigvee_{1 \le i \le n} expr^{\mathsf{Msg}}(q, q_i) \wedge \left(strict \implies \bigwedge_{expr \in \mathcal{E}_{!?} \cap \mathsf{Msg}(\mathscr{L})} \neg expr\right)$

  \ Msg($q_1, \ldots, q_n$)
- $expr^{\mathsf{LocInv}}_{\theta}(q) = \bigwedge_{\ell = (l, \iota, \phi, l', \iota') \in \mathsf{LocInv},\ \Theta(\ell) = \theta,\ \ell \text{ active at } q} \phi$

  A location l is called **front location** of cut C if and only if $\nexists\, l' \in \mathscr{L} \bullet l \prec l'$.

  Local invariant $(l_0, \iota_0, \phi, l_1, \iota_1)$ is **active** at cut (!) q if and only if $l_0 \preceq l \preceq l_1$ for some front location l of cut (!) q.
- $\mathsf{Msg}(F) = \{E^{!}_{i_l, i_{l'}} \mid (l, E, l') \in \mathsf{Msg},\ l \in F\} \cup \{E^{?}_{i_l, i_{l'}} \mid (l, E, l') \in \mathsf{Msg},\ l' \in F\}$
- $\mathsf{Msg}(F_1, \ldots, F_n) = \bigcup_{1 \le i \le n} \mathsf{Msg}(F_i)$



Progress Condition

$$expr^{\mathsf{hot}}_{prog}(q, q_i) = expr^{\mathsf{Msg}}(q, q_n) \wedge expr^{\mathsf{Cond}}_{\mathsf{hot}}(q, q_n) \wedge expr^{\mathsf{LocInv},\bullet}_{\mathsf{hot}}(q_n)$$

$\wedge\ expr^{\mathsf{Cond}}_{\mathsf{cold}}(q, q_n) \wedge expr^{\mathsf{LocInv},\bullet}_{\mathsf{cold}}(q_n)$

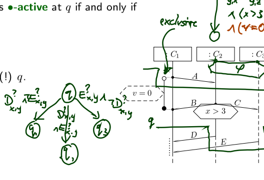
forgotten in the lecture

- $expr^{\mathsf{Msg}}(q, q_i) = \bigwedge_{expr \in \mathsf{Msg}(q_i \setminus q)} expr \wedge \bigwedge_{j \ne i} \bigwedge_{expr \in (\mathsf{Msg}(q_j \setminus q) \setminus \mathsf{Msg}(q_i \setminus q))} \neg expr$

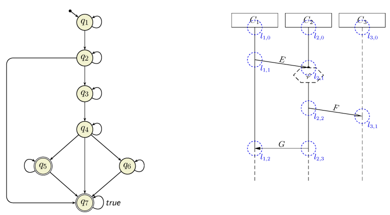
  $\wedge \left(strict \implies \bigwedge_{expr \in (\mathcal{E}_{!?} \cap \mathsf{Msg}(\mathscr{L})) \setminus \mathsf{Msg}(F_i)} \neg expr\right)$
- $expr^{\mathsf{Cond}}_{\theta}(q, q_i) = \bigwedge_{\gamma = (L, \phi) \in \mathsf{Cond},\ \Theta(\gamma) = \theta,\ L \cap (q_i \setminus q) \ne \emptyset} \phi$
- $expr^{\mathsf{LocInv},\bullet}_{\theta}(q, q_i) = \bigwedge_{\lambda = (l, \iota, \phi, l', \iota') \in \mathsf{LocInv},\ \Theta(\lambda) = \theta,\ \lambda\ \bullet\text{-active at } q_i} \phi$

  Local invariant $(l_0, \iota_0, \phi, l_1, \iota_1)$ is **•-active** at q if and only if
  - $l_0 \prec l \prec l_1$, or
  - $l = l_0 \wedge \iota_0 = \bullet$, or
  - $l = l_1 \wedge \iota_1 = \bullet$

  for some front location l of cut (!) q.



Example

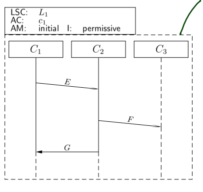


Finally: The LSC Semantics

A **full LSC** $L = ((I, (\mathscr{L}, \preceq), \sim, \mathscr{S}, \mathsf{Msg}, \mathsf{Cond}, \mathsf{LocInv}), ac_0, am, \Theta_L)$ consist of

- **body** $(I, (\mathscr{L}, \preceq), \sim, \mathscr{S}, \mathsf{Msg}, \mathsf{Cond}, \mathsf{LocInv})$,
- **activation condition** $ac_0 : Bool \in Expr_{\mathscr{S}}$, **strictness flag** $strict$ (otherwise called **permissive**)
- **activation mode** $am \in \{\text{initial}, \text{invariant}\}$,
- **chart mode existential** ($\Theta_L = \text{cold}$) or **universal** ($\Theta_L = \text{hot}$).

Concrete syntax:



Finally: The LSC Semantics

A **full LSC** $L = ((I, (\mathscr{L}, \preceq), \sim, \mathscr{S}, \mathsf{Msg}, \mathsf{Cond}, \mathsf{LocInv}), ac_0, am, \Theta_L)$ consist of

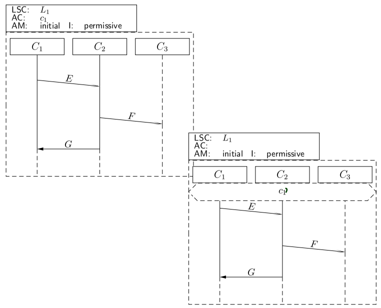
- **body** $(I, (\mathscr{L}, \preceq), \sim, \mathscr{S}, \mathsf{Msg}, \mathsf{Cond}, \mathsf{LocInv})$,
- **activation condition** $ac_0 : Bool \in Expr_{\mathscr{S}}$, **strictness flag** *strict* (otherwise called **permissive**)
- **activation mode** $am \in \{\mathsf{initial}, \mathsf{invariant}\}$,
- **chart mode existential** ($\Theta_L = \mathsf{cold}$) or **universal** ($\Theta_L = \mathsf{hot}$).

A **set of words** $W \subseteq (\Sigma_{\mathscr{S}}^{\mathscr{D}} \times \tilde{A})^\omega$ is **accepted** by L if and only if

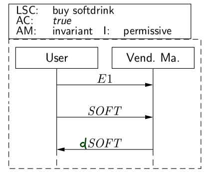
Θ_L	$am = \mathsf{initial}$	$am = \mathsf{invariant}$
cold	$\exists w \in W\ \exists \beta \bullet w^0 \models_\beta ac \wedge$ $w^0 \models_\beta expr_{\mathsf{hot}}^{\mathsf{Cond}}(\emptyset, C_0) \wedge w/1 \in \mathcal{L}(\mathcal{B}(L))$	$\exists w \in W\ \exists \beta\ \exists k \in \mathbb{N}_0 \bullet w^k \models_\beta ac \wedge$ $w^k \models_\beta expr_{\mathsf{hot}}^{\mathsf{Cond}}(\emptyset, C_0) \wedge w/k{+}1 \in \mathcal{L}(\mathcal{B}(L))$
hot	$\forall w \in W\ \forall \beta \bullet w^0 \models_\beta ac \implies$ $w^0 \models_\beta expr_{\mathsf{hot}}^{\mathsf{Cond}}(\emptyset, C_0) \wedge w/1 \in \mathcal{L}(\mathcal{B}(L))$	$\forall w \in W\ \forall \beta\ \forall k \in \mathbb{N}_0 \bullet w^k \models_\beta ac \implies$ $w^k \models_\beta expr_{\mathsf{hot}}^{\mathsf{Cond}}(\emptyset, C_0) \wedge w/k{+}1 \in \mathcal{L}(\mathcal{B}(L))$

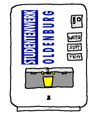
where $ac = ac_0 \wedge expr_{\mathsf{cold}}^{\mathsf{Cond}}(\emptyset, C_0) \wedge expr^{\mathsf{Msg}}(\emptyset, C_0)$; C_0 is the minimal (or **instance heads**) cut.

Activation Condition

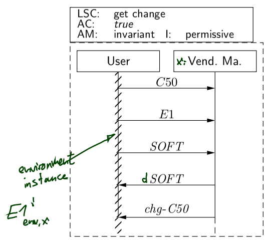


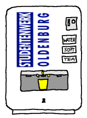
Existential LSC Example: Buy A Softdrink





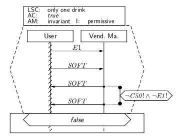
Existential LSC Example: Get Change





Live Sequence Charts — Precharts

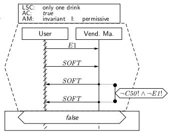
Pre-Charts



A **full LSC** $L = (PC, MC, ac_0, am, \Theta_L)$ **actually** consist of

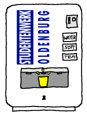
- **pre-chart** $PC = (I_P, (\mathscr{L}_P, \preceq_P), \sim_P, \mathscr{S}, \mathsf{Msg}_P, \mathsf{Cond}_P, \mathsf{LocInv}_P)$ (possibly empty),
- **main-chart** $MC = (I_M, (\mathscr{L}_M, \preceq_M), \sim_M, \mathscr{S}, \mathsf{Msg}_M, \mathsf{Cond}_M, \mathsf{LocInv}_M)$ (non-empty),
- **activation condition** $ac_0 : Bool \in Expr_{\mathscr{S}}$, **strictness flag** *strict* (otherwise called **permissive**)
- **activation mode** $am \in \{\mathsf{initial}, \mathsf{invariant}\}$,
- **chart mode existential** ($\Theta_L = \mathsf{cold}$) or **universal** ($\Theta_L = \mathsf{hot}$).

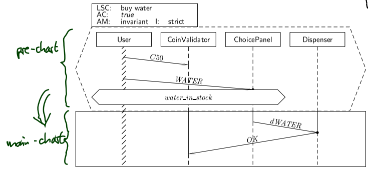
Pre-Charts Semantics



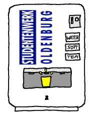
Θ_L	am = initial	am = invariant
cold	$\exists\, w \in W\ \exists\, \beta\ \exists\, m \in \mathbb{N}_0 \bullet w^0 \models_\beta ac$ $\wedge\, w^0 \models_\beta expr^{\mathsf{Cond}}_{\mathsf{hot}}(\emptyset, C_0^P)$ $\wedge\, w/1, \dots, w/m \in \mathcal{L}(\mathcal{B}(PC))$ $\wedge\, w^{m+1} \models_\beta expr^{\mathsf{Cond}}_{\mathsf{hot}}(\emptyset, C_0^M)$ $\wedge\, w/m+1 \in \mathcal{L}(\mathcal{B}(MC))$	$\exists\, w \in W\ \exists\, \beta\ \exists\, k < m \in \mathbb{N}_0 \bullet w^k \models_\beta ac$ $\wedge\, w^k \models_\beta expr^{\mathsf{Cond}}_{\mathsf{hot}}(\emptyset, C_0^P)$ $\wedge\, w/k+1, \dots, w/m \in \mathcal{L}(\mathcal{B}(PC))$ $\wedge\, w^{m+1} \models_\beta expr^{\mathsf{Cond}}_{\mathsf{hot}}(\emptyset, C_0^M)$ $\wedge\, w/m+1 \in \mathcal{L}(\mathcal{B}(MC))$
hot	$\forall\, w \in W\ \forall\, \beta \bullet w^0 \models_\beta ac$ $\wedge\, w^0 \models_\beta expr^{\mathsf{Cond}}_{\mathsf{hot}}(\emptyset, C_0^P)$ $\wedge\, w/1, \dots, w/m \in \mathcal{L}(\mathcal{B}(PC))$ $\wedge\, w^{m+1} \models_\beta expr^{\mathsf{Cond}}_{\mathsf{cold}}(\emptyset, C_0^M)$ $\implies w^{m+1} \models_\beta expr^{\mathsf{Cond}}_{\mathsf{cold}}(\emptyset, C_0^M)$ $\wedge\, w/m+1 \in \mathcal{L}(\mathcal{B}(MC))$	$\forall\, w \in W\ \forall\, \beta\ \forall\, k \le m \in \mathbb{N}_0 \bullet w^k \models_\beta ac$ $\wedge\, w^k \models_\beta expr^{\mathsf{Cond}}_{\mathsf{hot}}(\emptyset, C_0^P)$ $\wedge\, w/k+1, \dots, w/m \in \mathcal{L}(\mathcal{B}(PC))$ $\wedge\, w^{m+1} \models_\beta expr^{\mathsf{Cond}}_{\mathsf{hot}}(\emptyset, C_0^M)$ $\implies w^{m+1} \models_\beta expr^{\mathsf{Cond}}_{\mathsf{cold}}(\emptyset, C_0^M)$ $\wedge\, w/m+1 \in \mathcal{L}(\mathcal{B}(MC))$

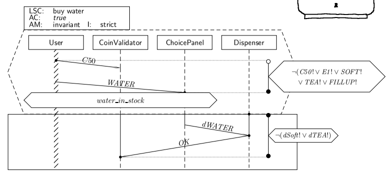
Universal LSC: Example



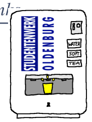


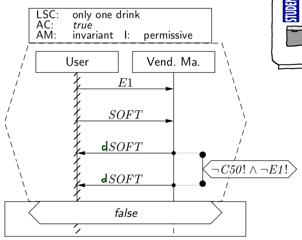
Universal LSC: Example



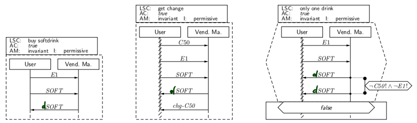


Forbidden Scenario Example: Don't Give Two Drinks





Note: Scenarios and Acceptance Test



- **Existential** LSCs* may hint at **test-cases** for the **acceptance test**!
  (∗: as well as (positive) scenarios in general, like use-cases)
- **Universal** LSCs (and negative/anti-scenarios) in general need **exhaustive analysis**!
  (Because they require that the software **never ever** exhibits the unwanted behaviour.)

References

References

OMG (2011a). Unified modeling language: Infrastructure, version 2.4.1. Technical Report formal/2011-08-05.

OMG (2011b). Unified modeling language: Superstructure, version 2.4.1. Technical Report formal/2011-08-06.