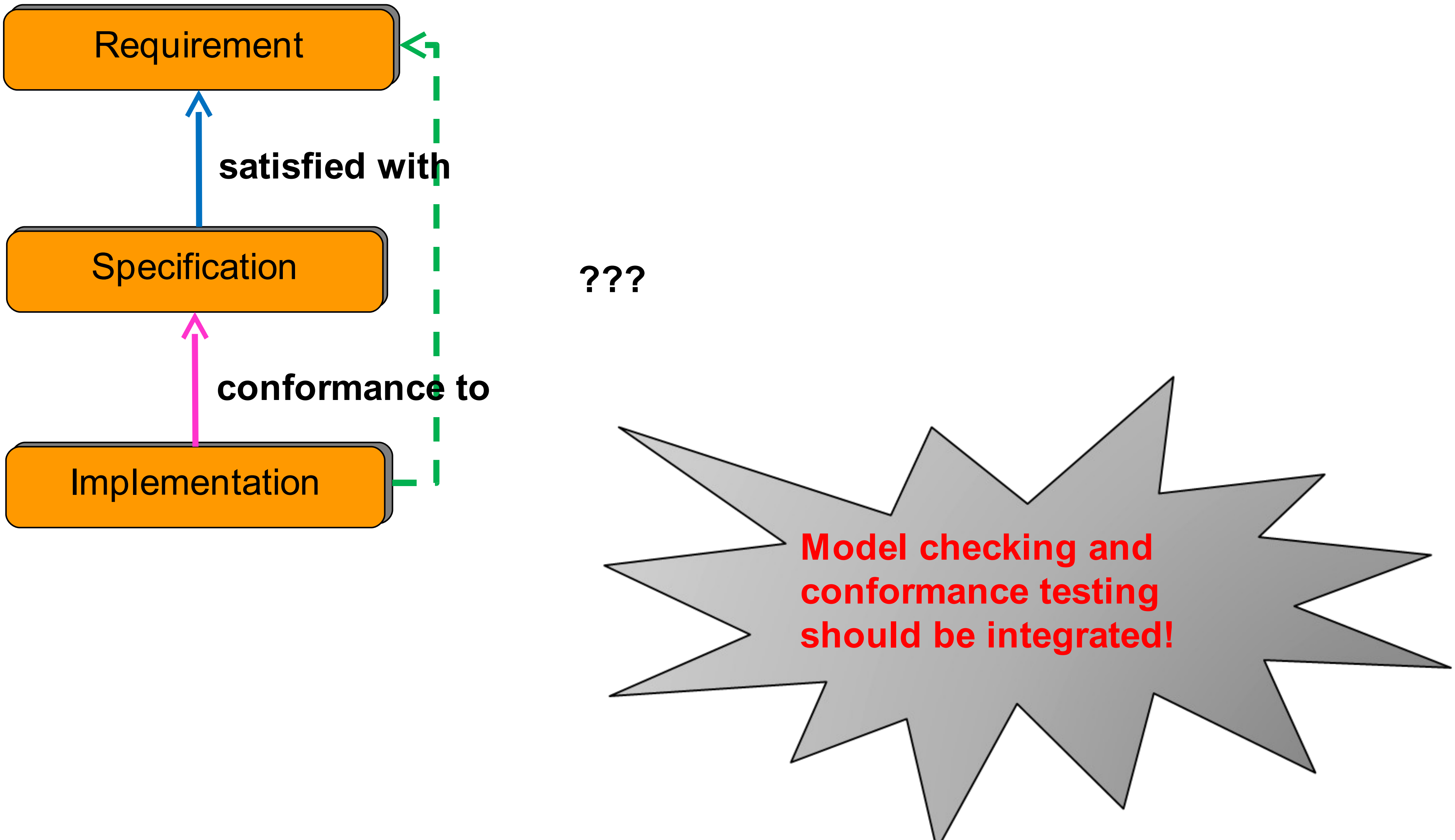
Integration of Safety Verification with Conformance Testing in Real-time Reactive System

Haiying Sun
Software Engineering Institute
East China Normal University
Shanghai, China
Email: hysun@sei.ecnu.edu.cn

Agenda

- Introduction
- Real-time system modeling and basic operators
- The Integration Method
  - Time-bounded input/output conformance relation
  - Safety Verification Based On Conformance Testing
  - Test generation based on safety observer
- Future work

Introduction



Introduction

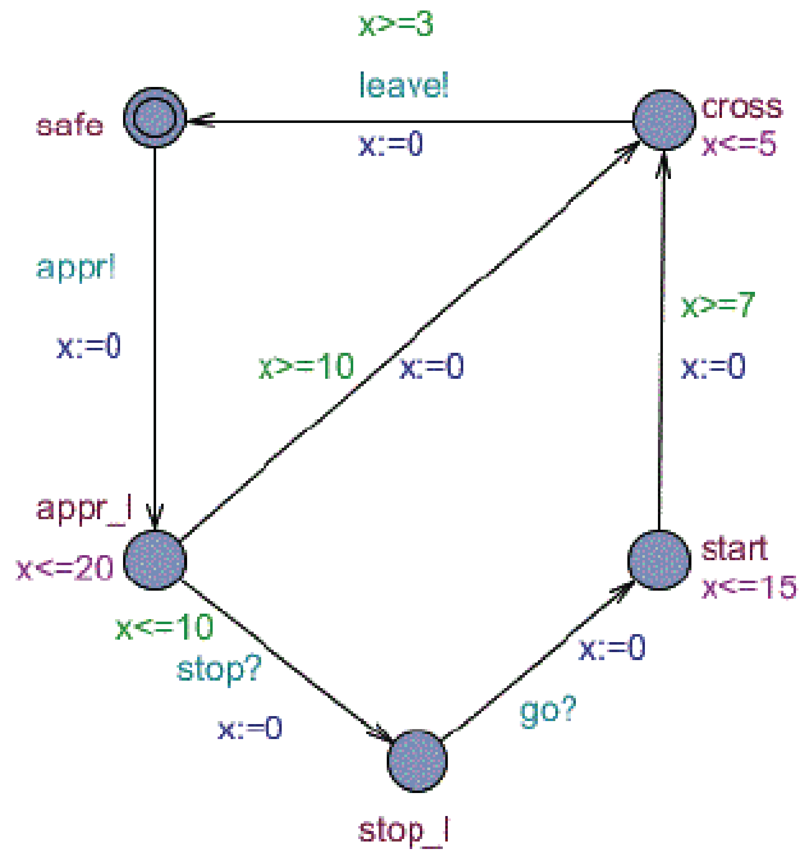
- The main work including
  - Formally defined the λ-bounded quiescence and the corresponding timed input output conformance relation;
  - proved that under the input enabled specification precondition, a real time implementation conforms to its specification if and only if the implementation satisfied with any of its safety properties
  - constructed a test case generation framework in which the test cases aim to lead the implementation into the error-prone execution paths.

Modeling

- Timed Automata

$\mathcal{T}$ is a tuple $(L, l_0, X, \Sigma, Inv, \rightarrow)$, where

- L is the set of locations, $l_0 \in L$ is the initial location
- X is a finite set of clock variables.
- Σ is a nonempty, observable finite set of actions which is a disjoint union of an input action set $\Sigma_?$ and an output action set $\Sigma_!$. Σ^τ is the internal action set, $\Sigma^\tau \cap \Sigma = \emptyset$, which can't be observed from the environment. Σ_τ denotes $\Sigma \cup \Sigma^\tau$.
- Inv is the set of invariant which maps each location $l \in L$ to some clock constraints in $\Phi(X)$. Here, we only consider downclosed time constraint in invariant: $\varphi := true | x \leq c | x < c | \varphi_1 \wedge \varphi_2$. Invariants restrict the amount of time passage in a location.
- $\rightarrow \subseteq L \times \Phi(X) \times \Sigma^\tau \times R(2^X) \times L$ is the transition relation. $l \xrightarrow{\varphi, a, \gamma} l'$ represents the location l change to l' on action a when the clock constraints φ is true. γ denotes the reset of clocks $\gamma \subseteq X$.



Modeling

- Timed input output labeled transition system(TIOS)

A TIOS $\mathcal{S}$ is a tuple (S, s_0, A, E)

- S is a set of states, $s_0 \in S$ is the initial state;
- A is the set of observable actions and $A = A_? \cup A_!$ satisfying $A_? \cap A_! = \emptyset$. A^τ is the internal action set and $A^\tau \cap A = \emptyset$. A_τ denotes $A \cup A^\tau$.
- $E : S \times A_\tau \cup R^{\geq 0} \times S$ is the transition relation which has two sets: $E^a = \{s \xrightarrow{a} s' | a \in A_\tau\}$ denotes the set of discrete transitions. $E^d = \{s \xrightarrow{d} s' | d \in R^{\geq 0}\}$ denotes the set of delay transitions which should satisfying the following constraints:
  1) time deterministic: $d \in R^{\geq 0}$, if $s \xrightarrow{d} s'$ and $s \xrightarrow{d} s''$ then $s' = s''$
  2) time additivity: $d_1, d_2 \in R^{\geq 0}$, if $s \xrightarrow{d_1} s'$ and $s' \xrightarrow{d_2} s''$ then $s \xrightarrow{d_1 + d_2} s''$
  3) zero-delay: $\forall s \in S, s \xrightarrow{0} s$

Modeling

The TIOS semantics of a TA $\mathcal{T} = (L, l_0, X, \Sigma, Inv, \rightarrow)$ is denoted as $\mathcal{S}_{\mathcal{T}} = (S, s_0, A, E)$ where

- $S = \{(l, v) | l \in L, v : X \rightarrow R^{\geq 0} \wedge Inv(l)(v)\}$ can be explained as: a state of $[\![T]\!]$ is a triple(l, v), v is a clock interpretation satisfying the invariant of l.
- $s_0 = (l_0, v_0)$, v_0 means $\forall x \in X, v(x) = 0$.
- The set of observable actions $A = \Sigma$, moreover, the set of internal actions $A^{\tau} = \Sigma^{\tau}$
- The set of transitions E is defined as the following:
  1) E^d: $\frac{d' \in R^{\geq 0}, \forall d' \leq d, Inv(l)(v+d')}{(l,v) \xrightarrow{d} (l, v+d)}$
  2) E^a: $\frac{l \xrightarrow{\varphi, a, \gamma} l' \wedge \varphi(v) \wedge Inv(l')(v'), v' = v[\gamma := 0]}{(l,v) \xrightarrow{a} (l', v')}$

Definition 1: A TIOS $\mathcal{S}_{\mathcal{T}}$ is said to be **Input-enabled** if $\forall s \in S_{\mathcal{T}}, \forall a \in A_? : s \stackrel{a}{\Longrightarrow}$.

Modeling

Definition 6: TA **Synchronized Composition**. Two compatible TA $\mathcal{T}_1 = (L_1, l_{10}, C_1, \Sigma_1, Inv_1, \rightarrow_1)$ and $\mathcal{T}_2 = (L_2, l_{20}, , C_2, \Sigma_2, Inv_2, \rightarrow_2)$ denoted as $\mathcal{T}_1 \parallel \mathcal{T}_2 = (L, l_0, C, \Sigma, Inv, \rightarrow)$ can be defined as following:

- The set of location $L = L_1 \times L_2$
- The initial location $l_0 = (l_{10}, l_{20})$
- The set of clocks $C = C_1 \cup C_2$
- The action set Σ remain the same as either Σ_1 or Σ_2 and the internal action set $\Sigma^{\tau} = \Sigma \cup \{\tau_1\} \cup \{\tau_2\}$
- $Inv(l_i, l_j) = Inv_1(l_i) \wedge Inv_2(l_j)$ is the invariant of location (l_i, l_j)
- The transition set $\rightarrow$ should satisfy the following rules:
  1) $\frac{(l_1,\varphi_1,a,\gamma_1,l_1')\in\rightarrow_1, a\in\{\tau_1\}, l_2\in L_2}{((l_1,l_2),\varphi_1,a,\gamma_1\cup\{c:=c\}_{(c\in C_2)},(l_1',l_2))\in\rightarrow}$
  2) $\frac{(l_2,\varphi_2,a,\gamma_2,l_2')\in\rightarrow_2, a\in\{\tau_2\}, l_1\in L_1}{((l_1,l_2),\varphi_2,a,\gamma_2\cup\{c:=c\}_{(c\in C_1)},(l_1,l_2'))\in\rightarrow}$
  3) $\frac{(l_1,\varphi_1,a,\gamma_1,l_1')\in\rightarrow_1, (l_2,\varphi_2,a,\gamma_2,l_2')\in\rightarrow_2}{((l_1,l_2),\varphi_1\wedge\varphi_2,a,\gamma_1\cup\gamma_2,(l_1',l_2'))\in\rightarrow}$

Real-time Conformance Testing

- check the conformance of SUT to a given specification only through the observable input and output actions.
- *"ioco"* relation is a standard conformance relation applied in untimed systems
- *δ* (quiescence): an additional observable output action modeling the absence of response
- What is the quiescence in real time system?
  - Time-bounded quiescence

Given a maximum time delay λ that a real time system may be allowed, time-bounded quiescence means if after λ time passage the system doesn't output any action, the real time quiescence occurs. .

$$\forall a \in A_!, \forall d \in R^{\geq 0} \wedge d > v(\lambda) : s \overset{\widehat{da}}{\not\Rightarrow}$$

Real-time Conformance Testing

Definition 9: $\lambda-$**Timed Conformance**. An input-enabled and non-blocking implementation TIOS $\mathcal{S}_{\mathcal{I}}$ has the same action interface set with the non-blocking specification $\mathcal{S}_{\mathcal{S}}$. Given λ which is the maximum duration, the $\lambda-$time bounded input output conformance relation between $\mathcal{S}_{\mathcal{I}}$ and $\mathcal{S}_{\mathcal{S}}$ is defined as:

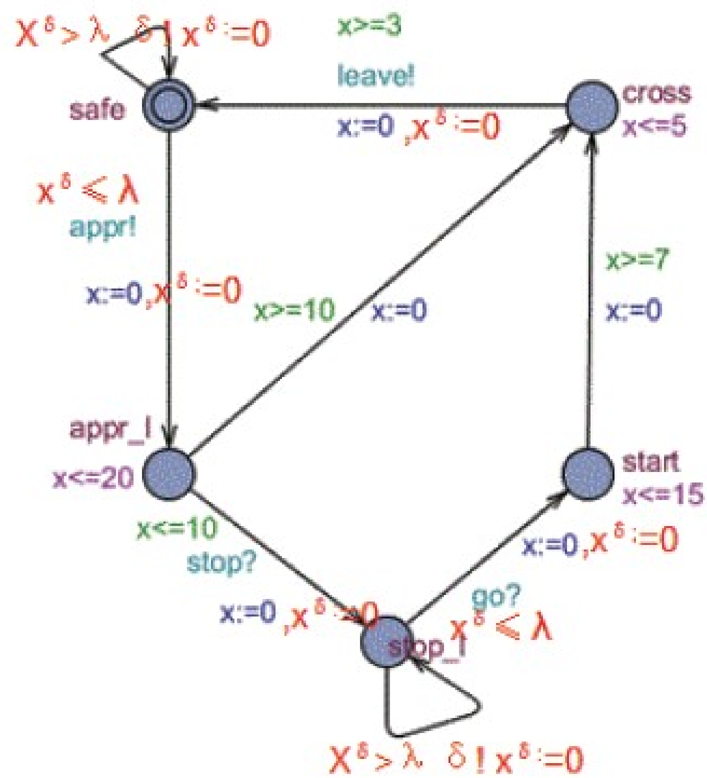
$$\mathcal{S}_I \ tioco^{\lambda} \ \mathcal{S}_S \Leftrightarrow \forall \sigma \in tTr(\mathcal{S}_S^{\delta^{\lambda}}), Out_t^{\lambda}(\mathcal{S}_I^{\delta^{\lambda}} \ After \ \sigma) \subseteq Out_t^{\lambda}(\mathcal{S}_s^{\delta^{\lambda}} \ After \ \sigma)$$

Definition 8: $\mathbf{Out}_t^{\lambda}(s) =_{def} \{(d,a) | d \in R^{\geq 0} \wedge a \in \Sigma_! \wedge s \stackrel{\widehat{da}}{\Longrightarrow}\} \cup \{(v(\lambda),\delta) | s \stackrel{\widehat{v(\lambda)\delta}}{\Longrightarrow}\}$.

λ- suspension TA

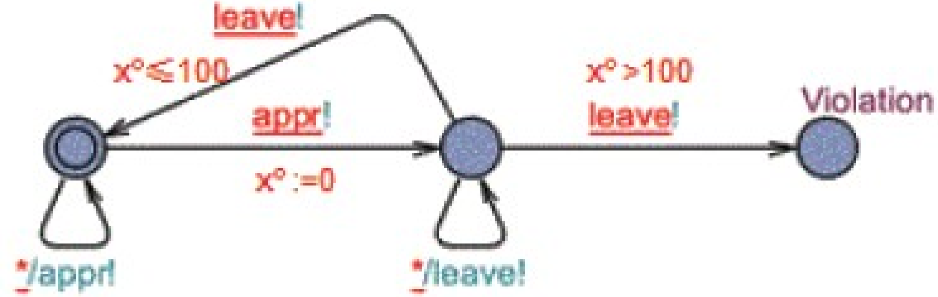
Definition 10: $\lambda-$**suspension TA**. The $\lambda-$suspension TA of a TA $\mathcal{T} = (L, l_0, C, \Sigma, Inv, \rightarrow)$ denoted as $\mathcal{T}^{\delta^\lambda} = (L^{\delta^\lambda}, l_0^{\delta^\lambda}, C^{\delta^\lambda}, \Sigma^{\delta^\lambda}, Inv^{\delta^\lambda}, \rightarrow^{\delta^\lambda})$ where

- $L^{\delta^\lambda} = L, l_0^{\delta^\lambda} = l_0$
- $C^{\delta^\lambda} = C \cup \{x^\delta\}$ where $x^\delta \notin C$ is the added clock to monitor time passage for the δ action.
- $\Sigma^{\delta^\lambda} = \Sigma \cup \{\delta\}$
- $Inv^{\delta^\lambda} = Inv(l)$
- $\rightarrow^{\delta^\lambda} = \rightarrow' \cup \rightarrow^\delta$ where
  1) $\rightarrow' = \{l \xrightarrow{\varphi, a, \gamma \cup x^\delta := 0} l^\delta | Inv(l^\delta) = true\} \cup \{l \xrightarrow{\varphi, a, \gamma} l' | Inv(l') \neq true\}$
  2) $\rightarrow^\delta = \{l^\delta \xrightarrow{x^\delta > \lambda, \delta!, x^\delta := 0} l^\delta | Inv(l^\delta) = true\}$



Model Checking Safety Properties

Definition 12: **Safety Observer.** A safety observer for a TA $\mathcal{T} = (L, l_0, C, \Sigma, Inv, \rightarrow)$ is a deterministic TA $\varphi = (L^o \cup \{Violation\}, l_0^o, C^o, \Sigma^o, Inv^o, \rightarrow^o)$ where $Violation$ is a specific location as its final location, $C^o \wedge C = \emptyset$, $\Sigma^o = \Sigma$. The set of safety observers for a TA $\mathcal{T}$ is denoted as $\Omega(\mathcal{T})$.



Lemma 2: $\mathcal{T} \models \varphi \Leftrightarrow tTr(\mathcal{T}) \cap tTr(\varphi, \{Violation\}) = \emptyset$

Lemma 3: $tTr(\mathcal{T}) \cap tTr(\varphi, Violation) = tTr(\mathcal{T} \parallel \varphi, Violation)$.

Safety Model Checking Based On Conformance Testing

Given a input enabled specification TIOS $\mathcal{S}_S$:

Lemma 4: $\mathcal{S}_I \ tioco^{\lambda} \ \mathcal{S}_S \Leftrightarrow tTr(\mathcal{S}_I^{\delta^{\lambda}}) \subseteq tTr(\mathcal{S}_S^{\delta^{\lambda}})$

Theorem 1: $\mathcal{S}_I \ tioco^{\lambda} \ \mathcal{S}_S \Leftrightarrow \forall \varphi \in \Omega(\mathcal{T}_S), \mathcal{S}_S^{\delta^{\lambda}} \models \mathcal{S}_{\varphi} \Rightarrow \mathcal{S}_I^{\delta^{\lambda}} \models \mathcal{S}_{\varphi}$

Proof:($\Rightarrow$) $\mathcal{S}_I \ tioco^{\lambda} \ \mathcal{S}_S \Rightarrow tTr(\mathcal{S}_I^{\delta^{\lambda}}) \subseteq tTr(\mathcal{S}_S^{\delta^{\lambda}})$, $\mathcal{S}_S \models \mathcal{S}_{\varphi}$ implies $tTr(\mathcal{S}_S^{\delta^{\lambda}}) \cap tTr(\mathcal{S}_{\varphi}) = \emptyset$. Thus, $tTr(\mathcal{S}_I^{\delta^{\lambda}}) \cap tTr(\mathcal{S}_{\varphi}) = \emptyset$ which equals $\mathcal{S}_I^{\delta^{\lambda}} \models \mathcal{S}_{\varphi}$ by the definition of safety model checking.

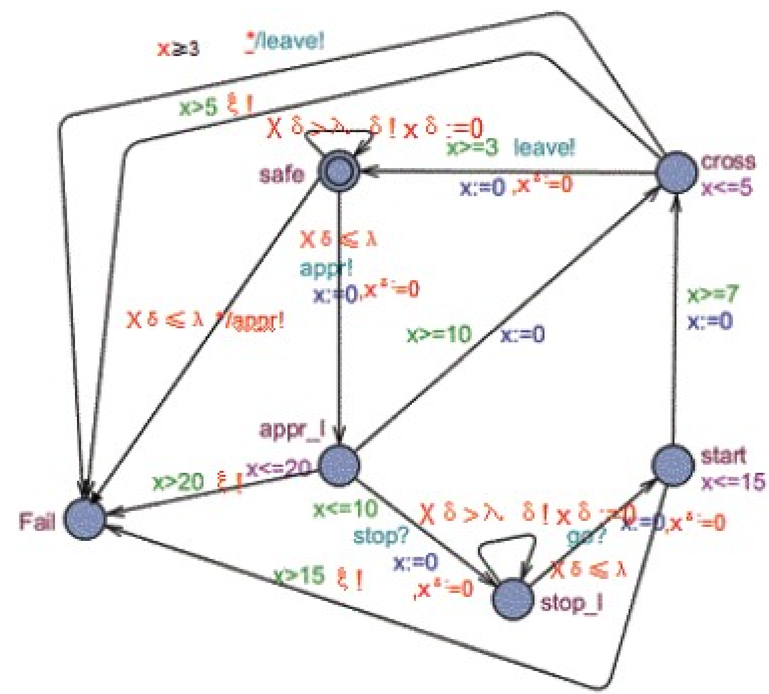
($\Leftarrow$) Suppose $\mathcal{S}_I \ \cancel{tioco^{\lambda}} \ \mathcal{S}_S$, this means $\exists \sigma \in (\Sigma \cup R^{\geq 0})^*$, $\sigma \in tTr(\mathcal{S}_I^{\delta^{\lambda}})$ but $\sigma \notin tTr(\mathcal{S}_S^{\delta^{\lambda}})$, construct an observer which include σ as one of its trace. Thus $tTr(\mathcal{S}_S^{\delta^{\lambda}}) \cap tTr(\mathcal{S}_{\varphi}) = \emptyset$ means $\mathcal{S}_S^{\delta^{\lambda}} \models \mathcal{S}_{\varphi}$, however $tTr(\mathcal{S}_I^{\delta^{\lambda}}) \cap tTr(\mathcal{S}_{\varphi}) \neq \emptyset$ means $\mathcal{S}_I^{\delta^{\lambda}} \not\models \mathcal{S}_{\varphi}$. This is contradict with the known condition. $\square$

Test Generation Based on Safety Observer

Definition 14: **Testable TA**. The testable TA of a TA $\mathcal{T} = (L, l_0, C, \Sigma, Inv, \rightarrow)$ denoted as $\Delta(\mathcal{T})$ is a TA can be defined as: $\Delta(\mathcal{T}) = (L \cup \{Fail\}, l_0, C, \Sigma \cup \{\xi!\}, Inv, \rightarrow^{\mathcal{A}})$ where

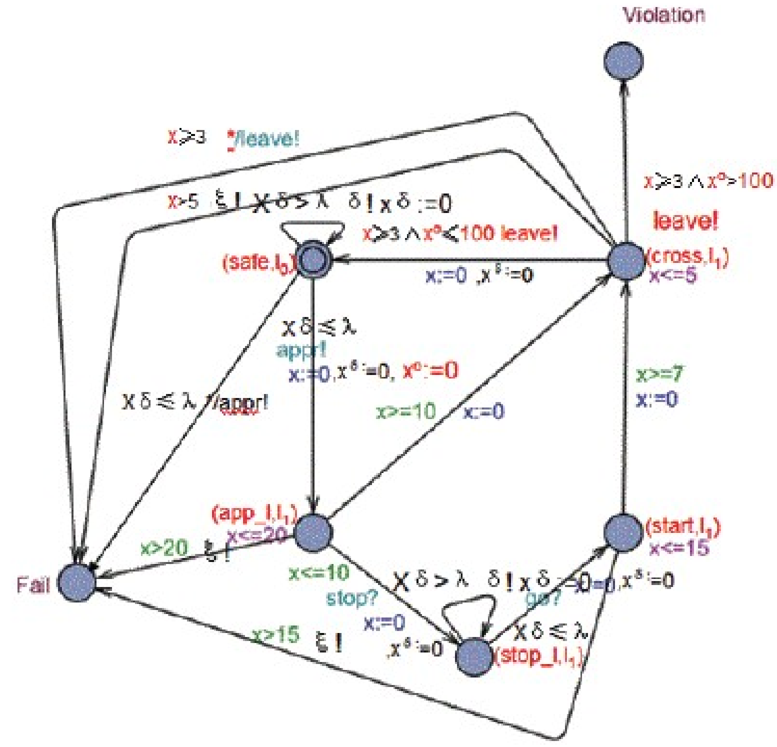
- $Fail \notin L$ is a verdict location with no time meaning.
- The added output action $\xi!$ implies time out which occurs when the time constrain is violated.
- $\rightarrow^{\mathcal{A}} = \rightarrow \cup \{l \xrightarrow{\neg Inv(l), \xi!} Fail | l \in L \wedge Inv(l) \neq true\} \cup \{l \xrightarrow{\varphi, a} Fail | l \in L \wedge Inv(l) \neq true \wedge a \in \Sigma_! \wedge l \not\xrightarrow{\varphi, a}\}$

Theorem 2: $if\ \exists \sigma \in tTr(\mathcal{T}_I^{\delta^\lambda}) \cap tTr(\Delta(\mathcal{T}_S^{\delta^\lambda}))$ and $Fail \in$ **Des**$(\Delta(\mathcal{T}_S^{\delta^\lambda})\ After\ \sigma) \Rightarrow \mathcal{T}_I\ \not{tioco}^{\lambda}\ \mathcal{T}_S$



Test Generation Based on Safety Observer

Definition 15: Given a specification $\mathcal{T}_S$ and a safety observer φ, the synchronized composition $\Delta(\mathcal{T}_S^{\delta^\lambda}) \parallel \varphi$ is the desired test specification for selecting test case to detect safety property violation between implementation and requirements and non-conformance between implementation and specification. $\Delta(\mathcal{T}_S^{\delta^\lambda}) \parallel \varphi$ is denoted as $tc(\mathcal{T}_S, \varphi)$.



Future work

- Faster than relation
- Non-deterministic
- Tools Development

Thank you for your listening