USC

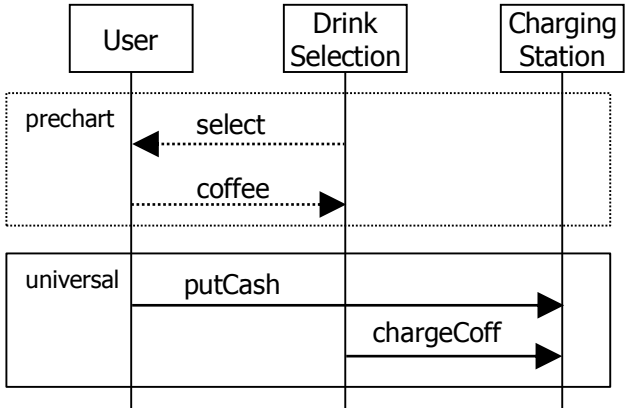
USC Viterbi
School of Engineering

# Distributing Refinements of a System-Level Partial Behavior Model

**Ivo Krka and Nenad Medvidović**
University of Southern California

# Overview

USC Viterbi School of Engineering




**chargeCoff precondition**

- CoffeeSelected ∧ Payment

**chargeCappuccino precondition**

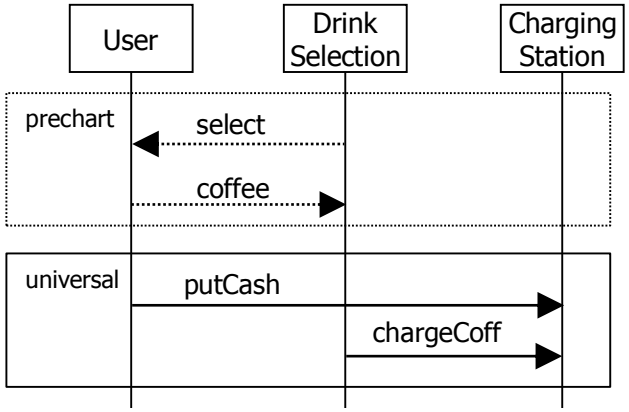
- CappuccinoSelected ∧ Payment

**Goal SelectionFirst**

- G (Payment => DrinkSelected)

# Overview

USC Viterbi School of Engineering

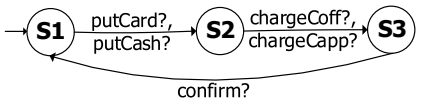



**chargeCoff precondition**
- CoffeeSelected ∧ Payment

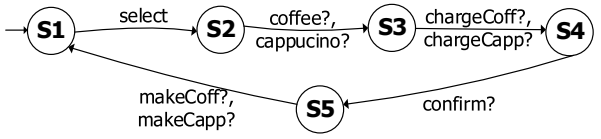
**chargeCappuccino precondition**
- CappuccinoSelected ∧ Payment

**Goal SelectionFirst**
- G (Payment => DrinkSelected)

**Charging Station**

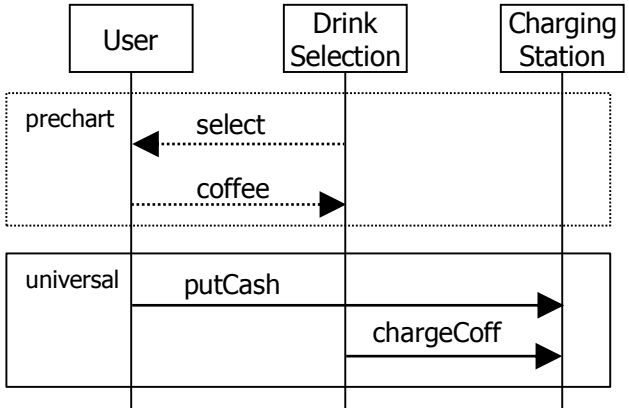


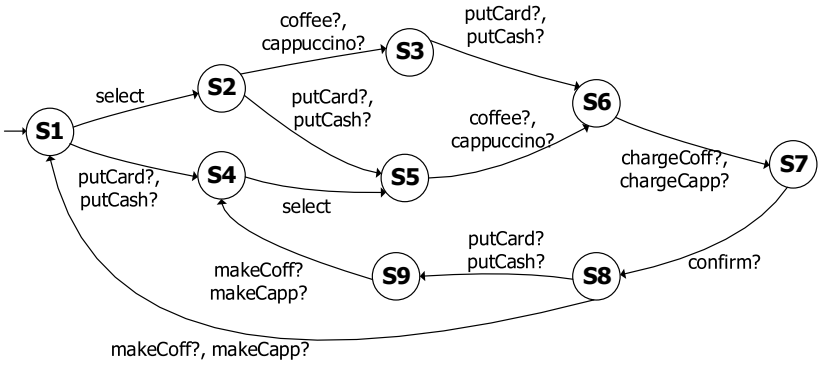

**Drink Selection**



# Overview

USC Viterbi School of Engineering




**chargeCoff precondition**

- CoffeeSelected ∧ Payment

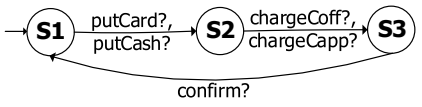
**chargeCappuccino precondition**

- CappuccinoSelected ∧ Payment

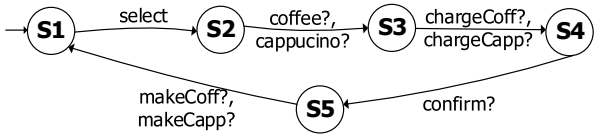
**Goal SelectionFirst**

- G (Payment => DrinkSelected)

**Charging Station**

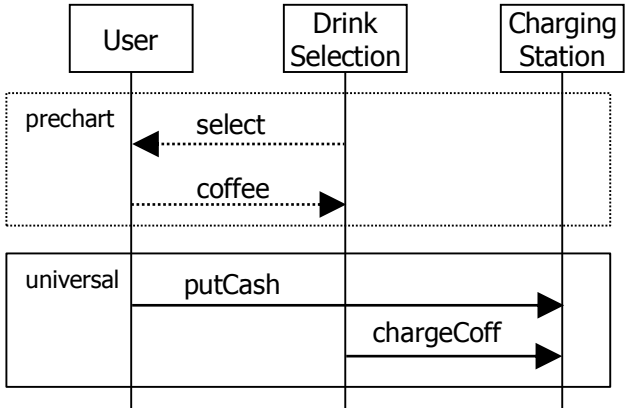


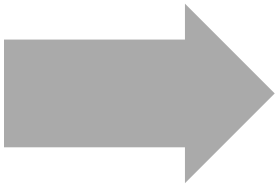

**Drink Selection**

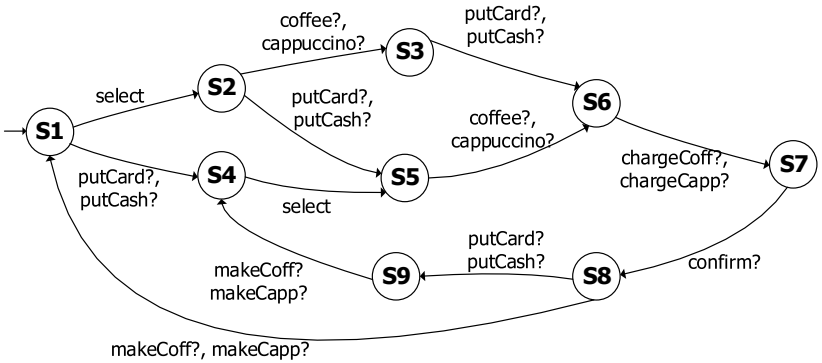


# Overview

USC Viterbi School of Engineering






**chargeCoff precondition**

- CoffeeSelected ∧ Payment

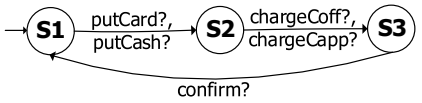
**chargeCappuccino precondition**

- CappuccinoSelected ∧ Payment

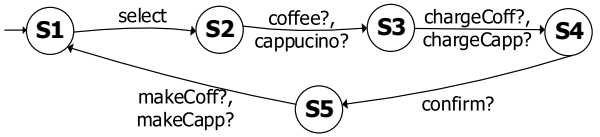
**Goal SelectionFirst**

- G (Payment => DrinkSelected)

**Charging Station**



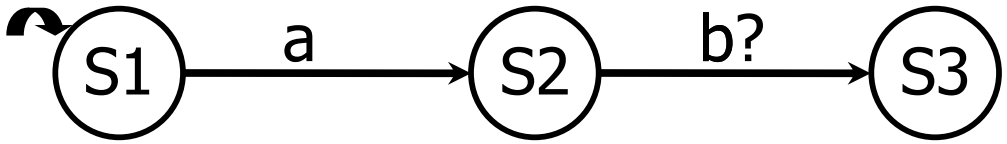

**Drink Selection**



# Modal Transition Systems and Fluents

USC Viterbi School of Engineering

**MTS M**

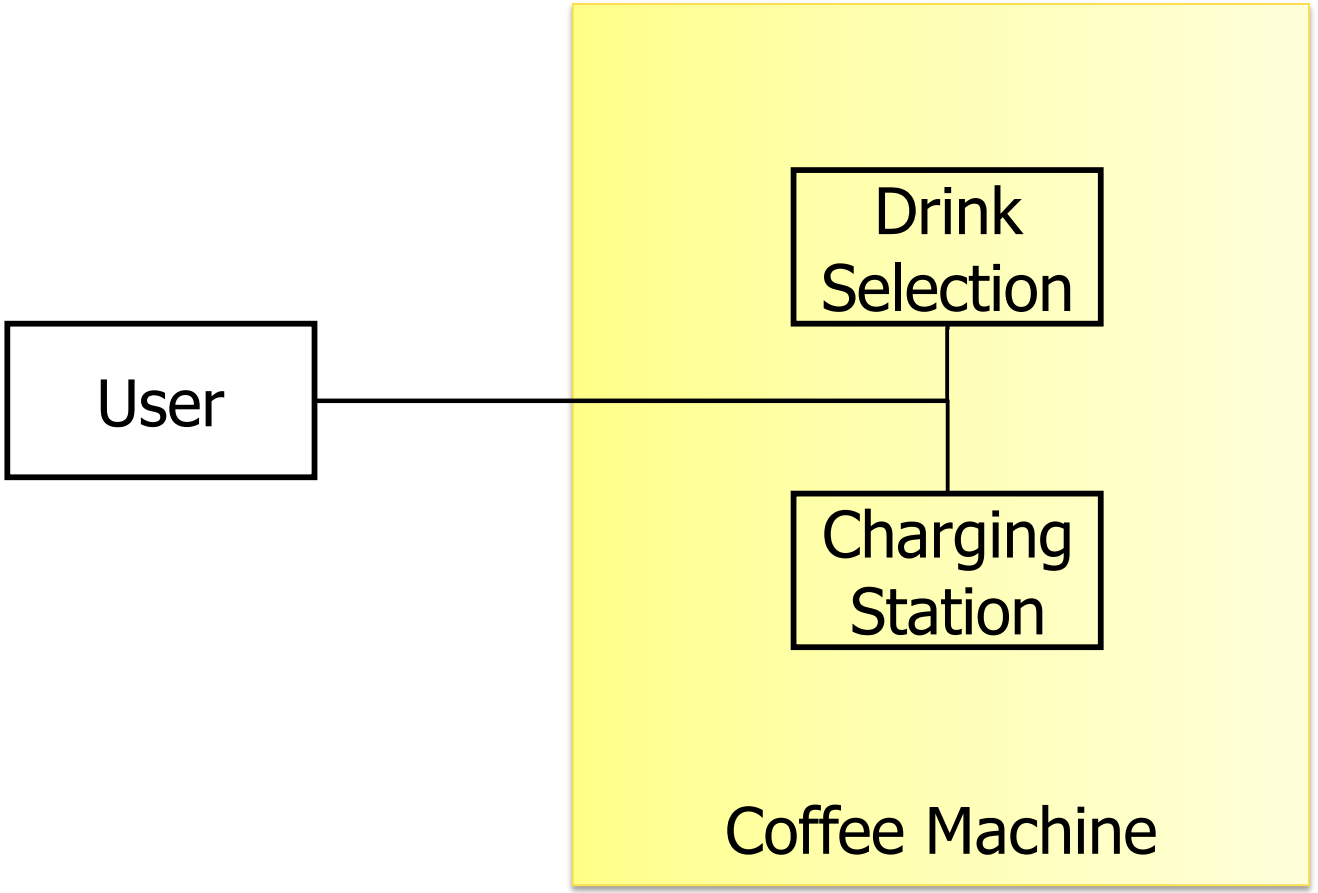



**Fluent P**

- <a,b> initially false

# Coffee Machine System

USC Viterbi School of Engineering



# Preliminary Requirements

USC Viterbi School of Engineering

**Precondition select**

- Idle

**Precondition coffee/cappuccino**

- WaitingForSelection

**Precondition putCard/putCash**

- WaitingForPayment

**Precondition chargeCoff/chargeCapp**

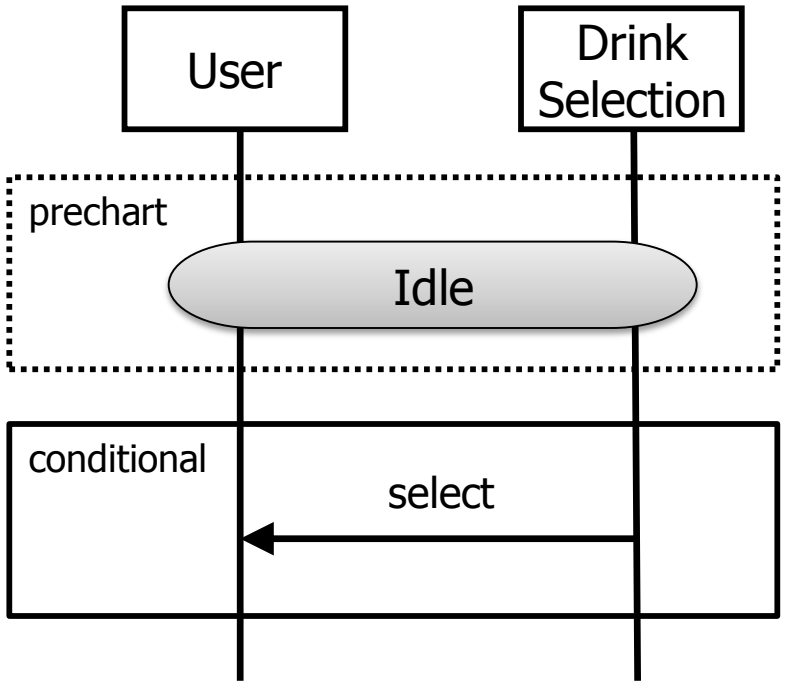
- DrinkSelected ∧ Payment

**Precondition confirm**

- PaymentSubmitted

**Precondition makeCoffee/makeCapp**

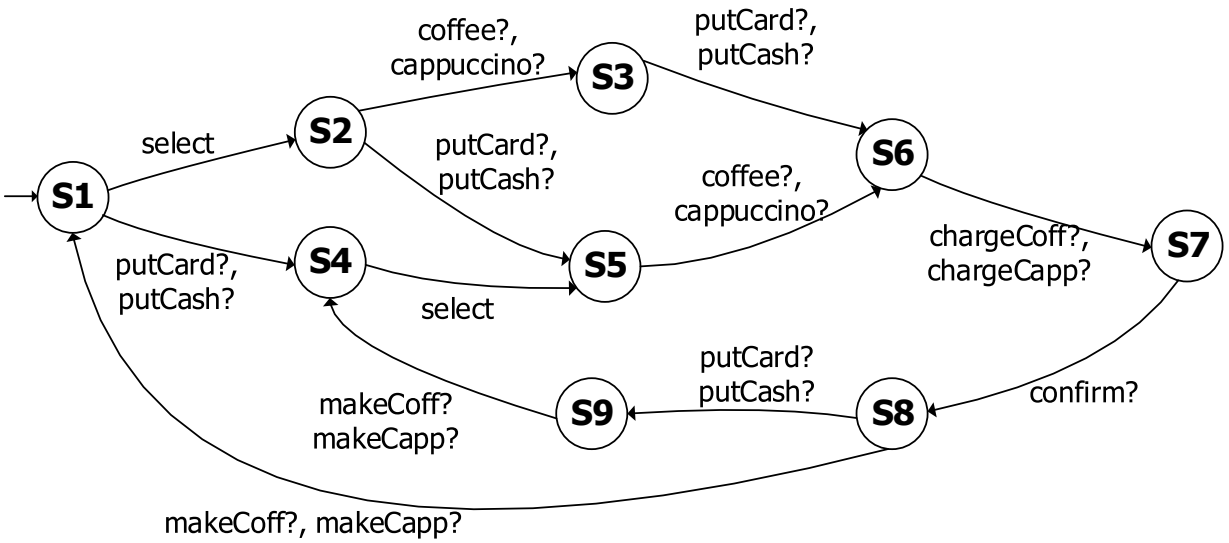
- PaymentConfirmed ∧ DrinkSelected



# Initial System and Component Models

USC Viterbi School of Engineering

**Coffee Machine**

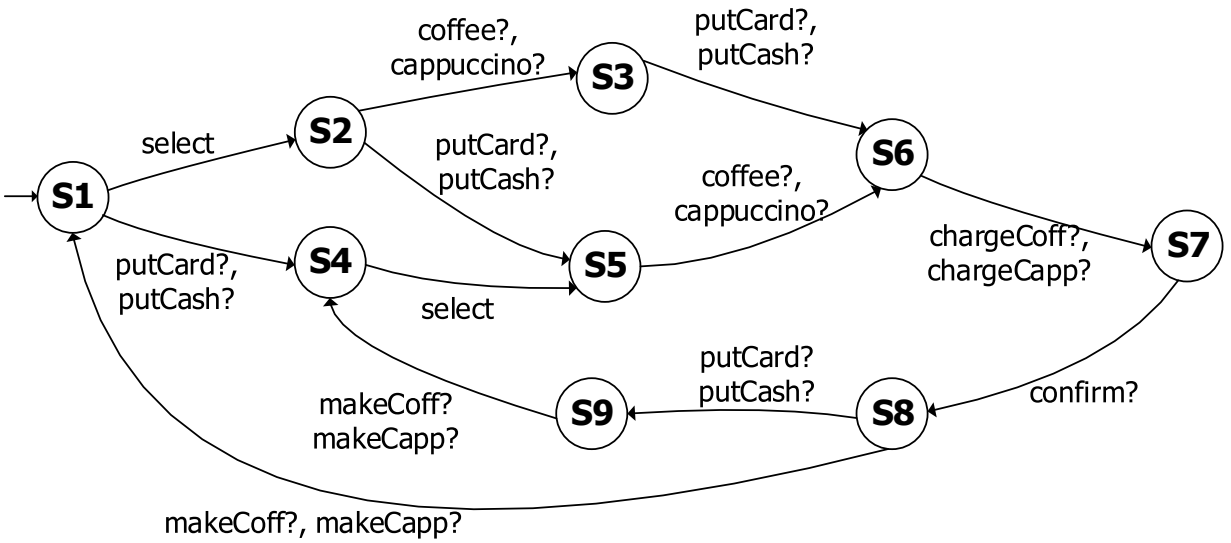



MTS distribution (Sibay-FM12)

# Initial System and Component Models

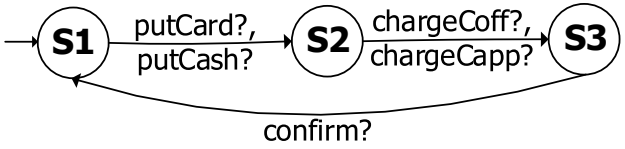
USC Viterbi School of Engineering

**Coffee Machine**

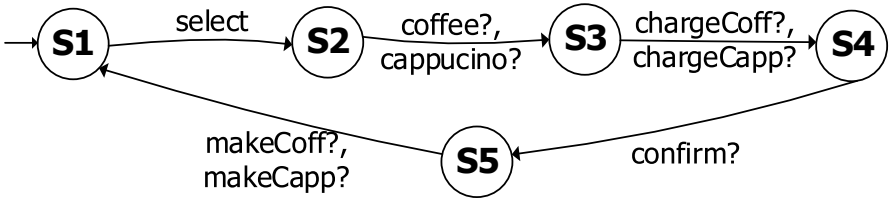



MTS distribution (Sibay-FM12)

**Charging Station**



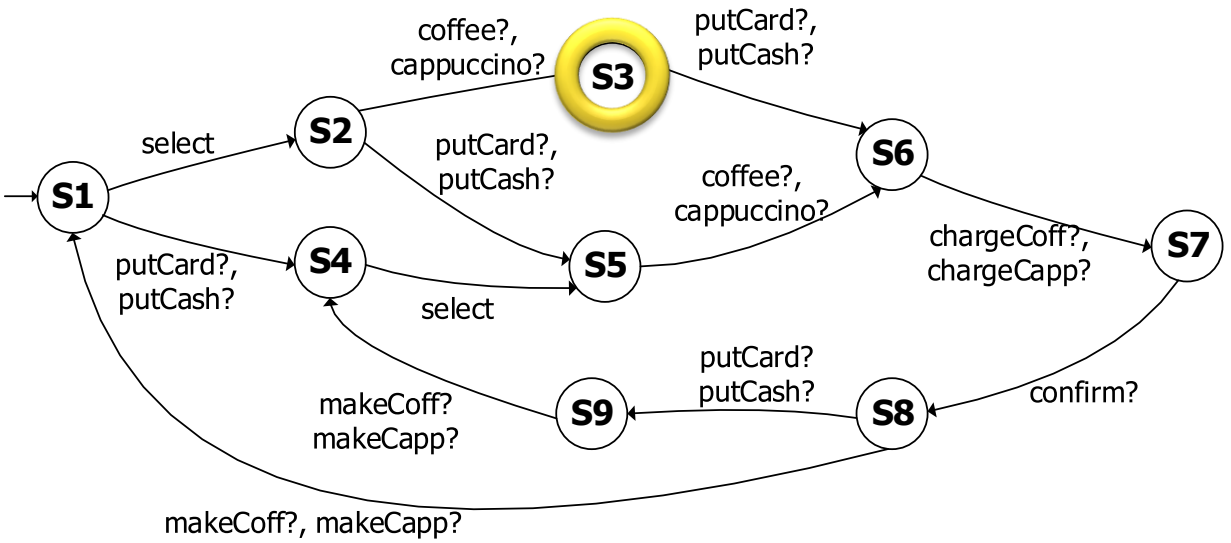

**Drink Selection**



# Initial System and Component Models

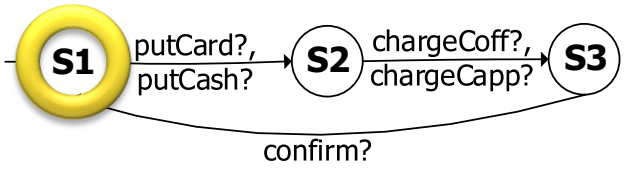
USC Viterbi School of Engineering

**Coffee Machine**

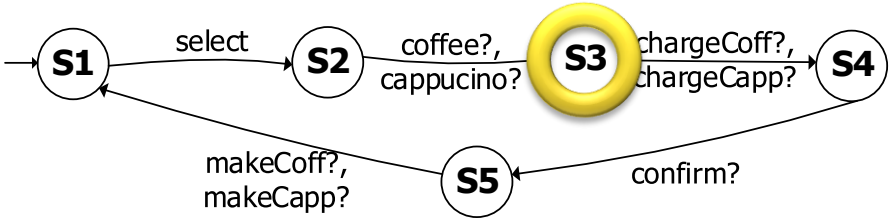



MTS distribution (Sibay-FM12)

**Charging Station**



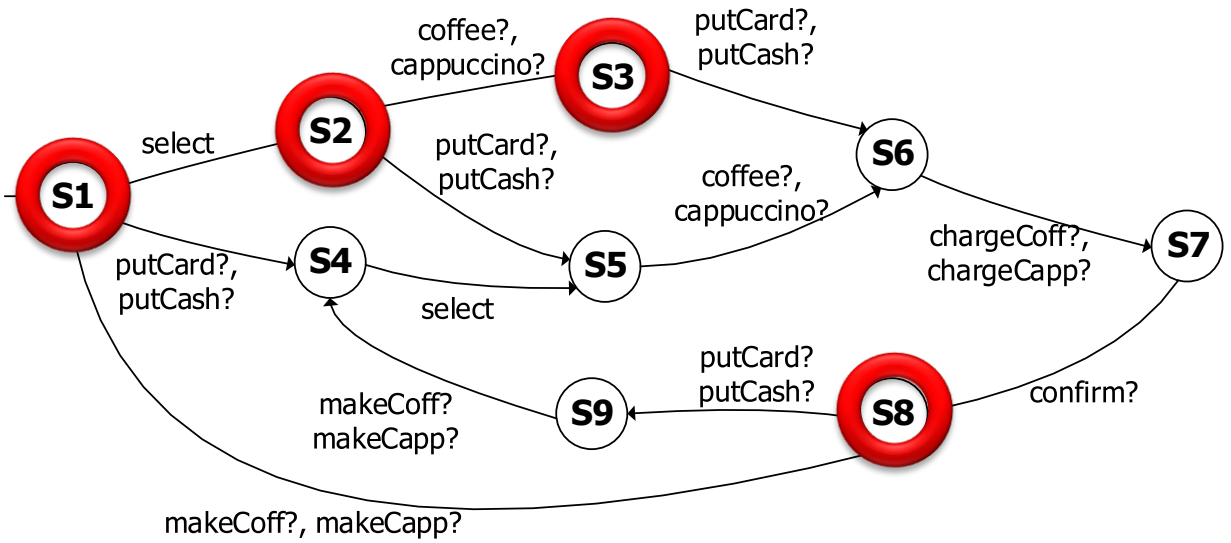

**Drink Selection**



# Initial System and Component Models

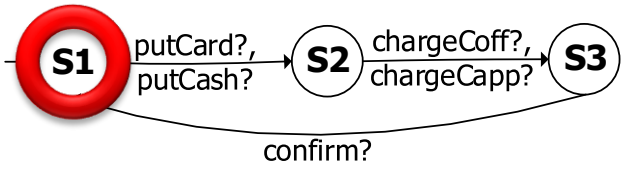
USC Viterbi School of Engineering

**Coffee Machine**

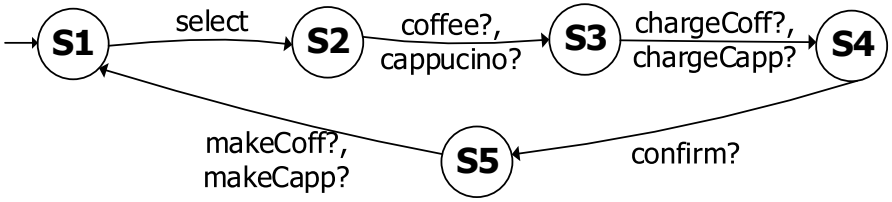



MTS distribution (Sibay-FM12)

**Charging Station**

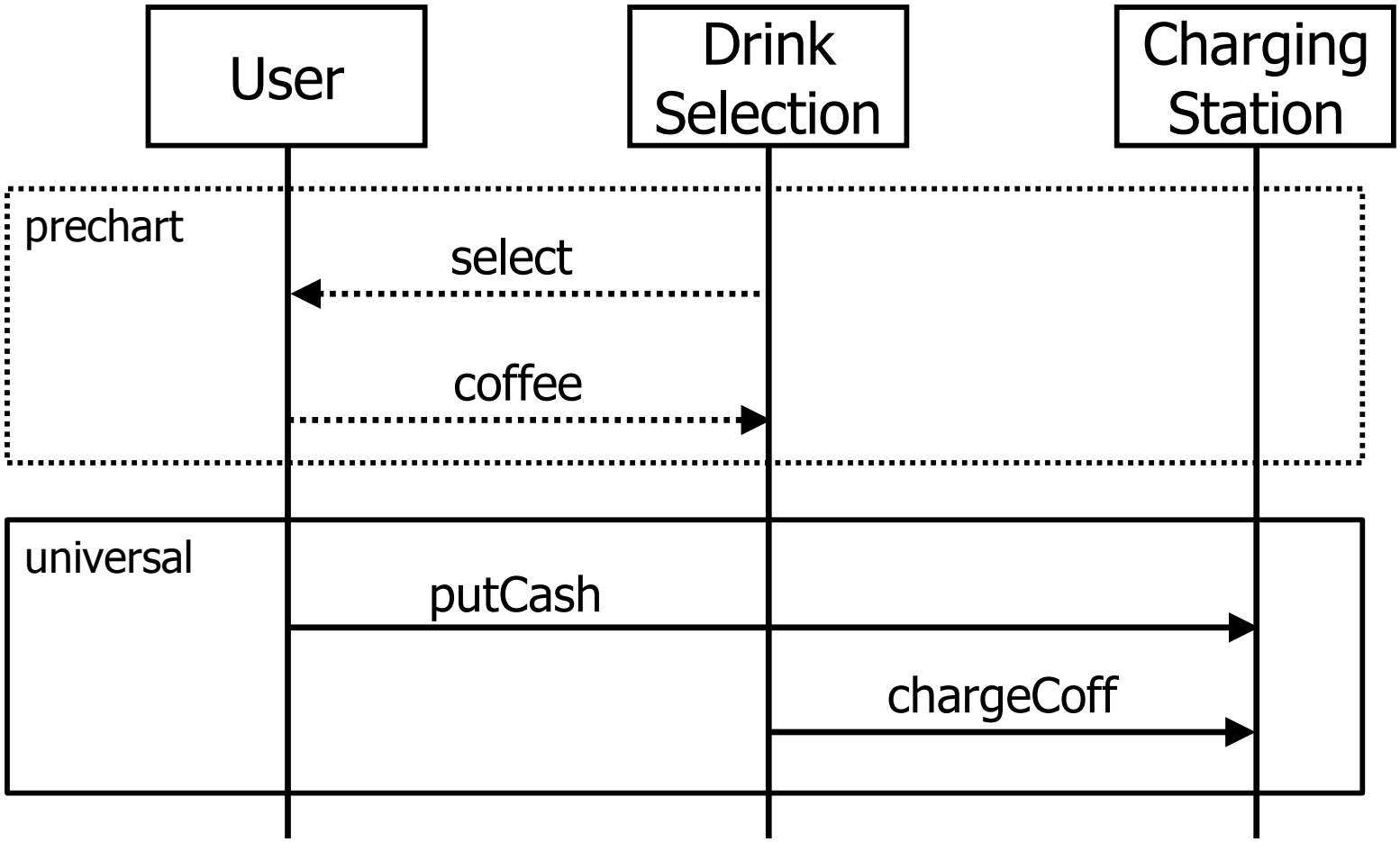



**Drink Selection**



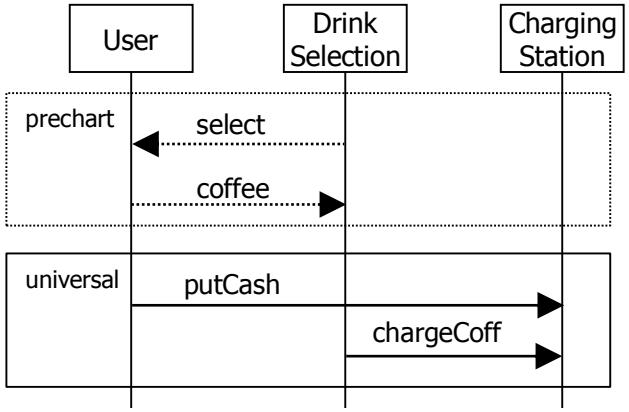
# Coffee Selection Scenario

USC Viterbi School of Engineering



# Coffee Machine Properties

USC Viterbi School of Engineering




**Precondition chargeCoff**

- CoffeeSelected ∧ Payment

**Precondition chargeCappuccino**

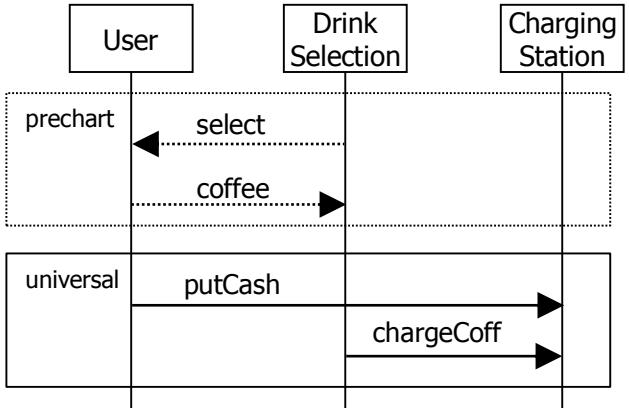
- CappuccinoSelected ∧ Payment

**Goal SelectionFirst**

- G (Payment => DrinkSelected)

# Coffee Machine Refinement

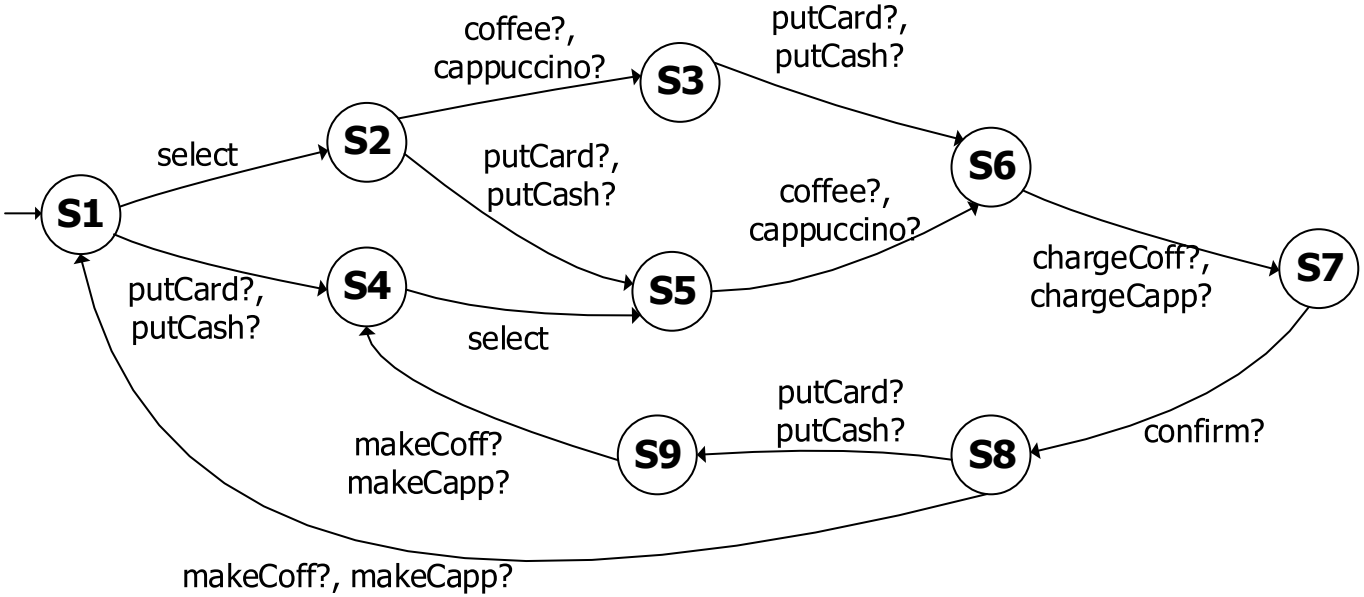
USC Viterbi School of Engineering




**Precondition chargeCoff**
- CoffeeSelected ∧ Payment

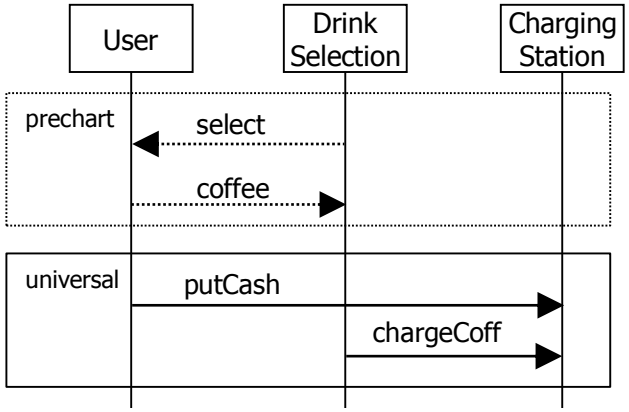
**Precondition chargeCappuccino**
- CappuccinoSelected ∧ Payment

**Goal SelectionFirst**
- G (Payment => DrinkSelected)



# Coffee Machine Refinement

USC Viterbi School of Engineering




**Precondition chargeCoff**

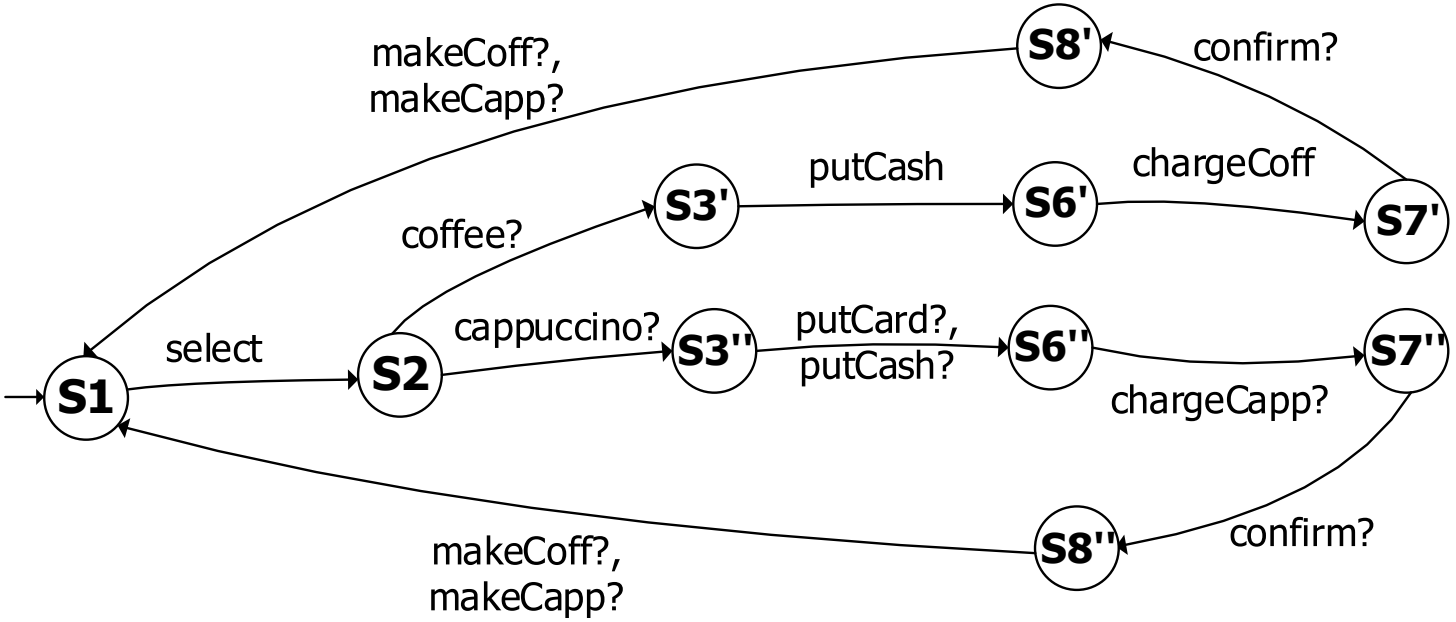
- CoffeeSelected ∧ Payment

**Precondition chargeCappuccino**

- CappuccinoSelected ∧ Payment

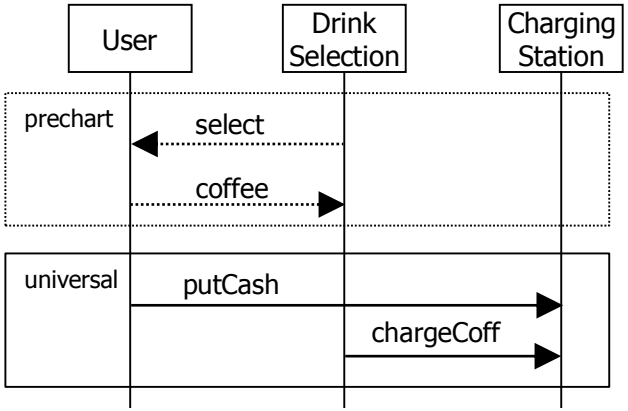
**Goal SelectionFirst**

- G (Payment => DrinkSelected)



# Coffee Machine Refinement

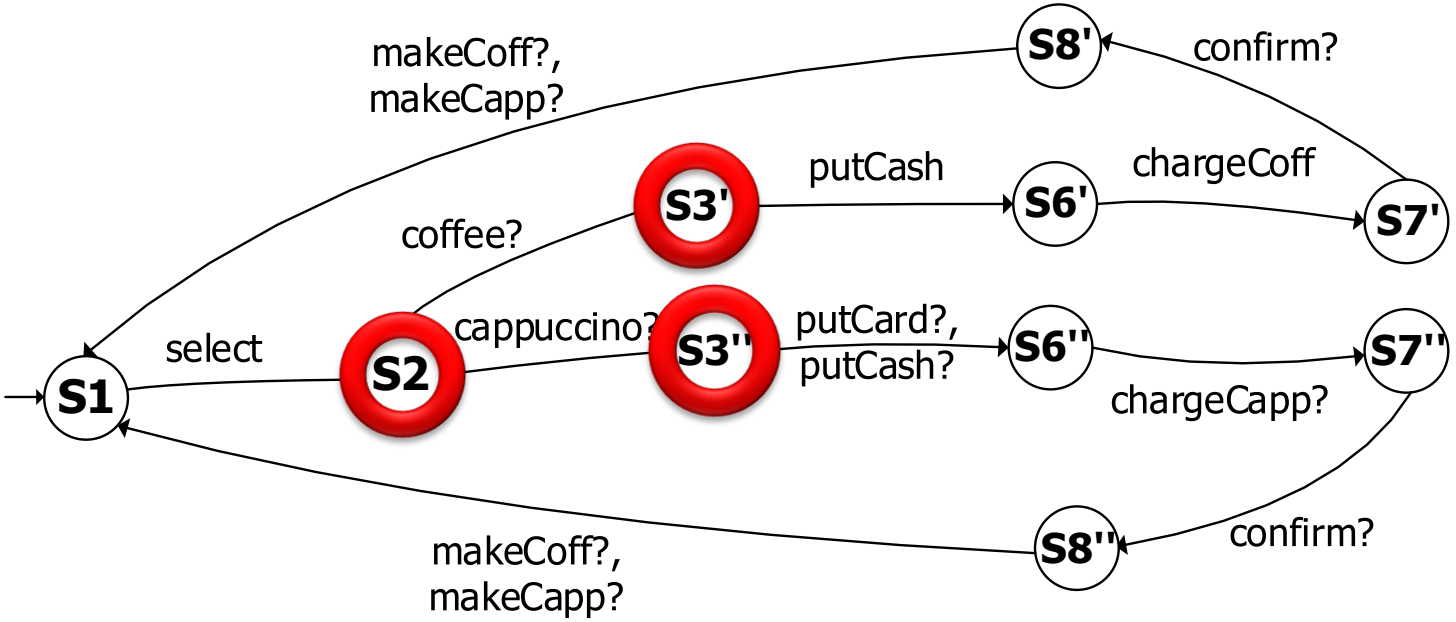
USC Viterbi School of Engineering




**Precondition chargeCoff**
- CoffeeSelected ∧ Payment

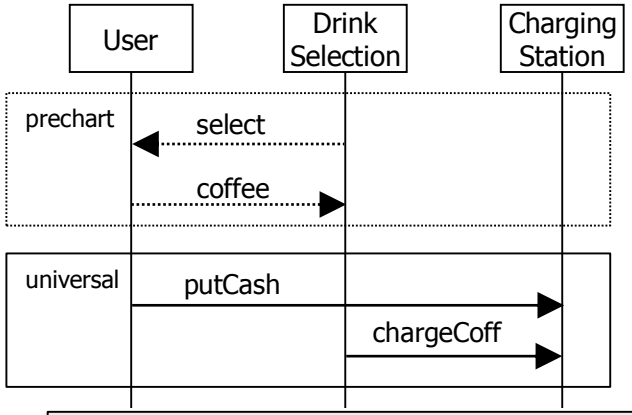
**Precondition chargeCappuccino**
- CappuccinoSelected ∧ Payment

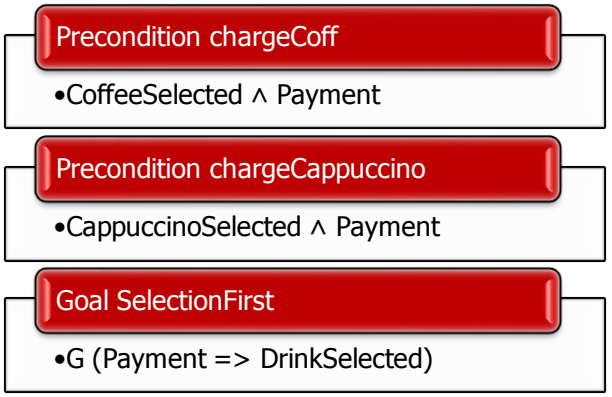
**Goal SelectionFirst**
- G (Payment => DrinkSelected)



# Coffee Machine Refinement

USC Viterbi School of Engineering




- Our insights
  1. *MTS refinements incremental*
  2. *Component-system state mapping*

➢ Can we gradually refine component models based on system requirements?

# Refinement Framework Design

USC Viterbi School of Engineering

1. Determine how MTS relates to requirements
2. Define finite set of refinement types
3. Devise methods to handle refinement types

# How MTS Relate to Requirements

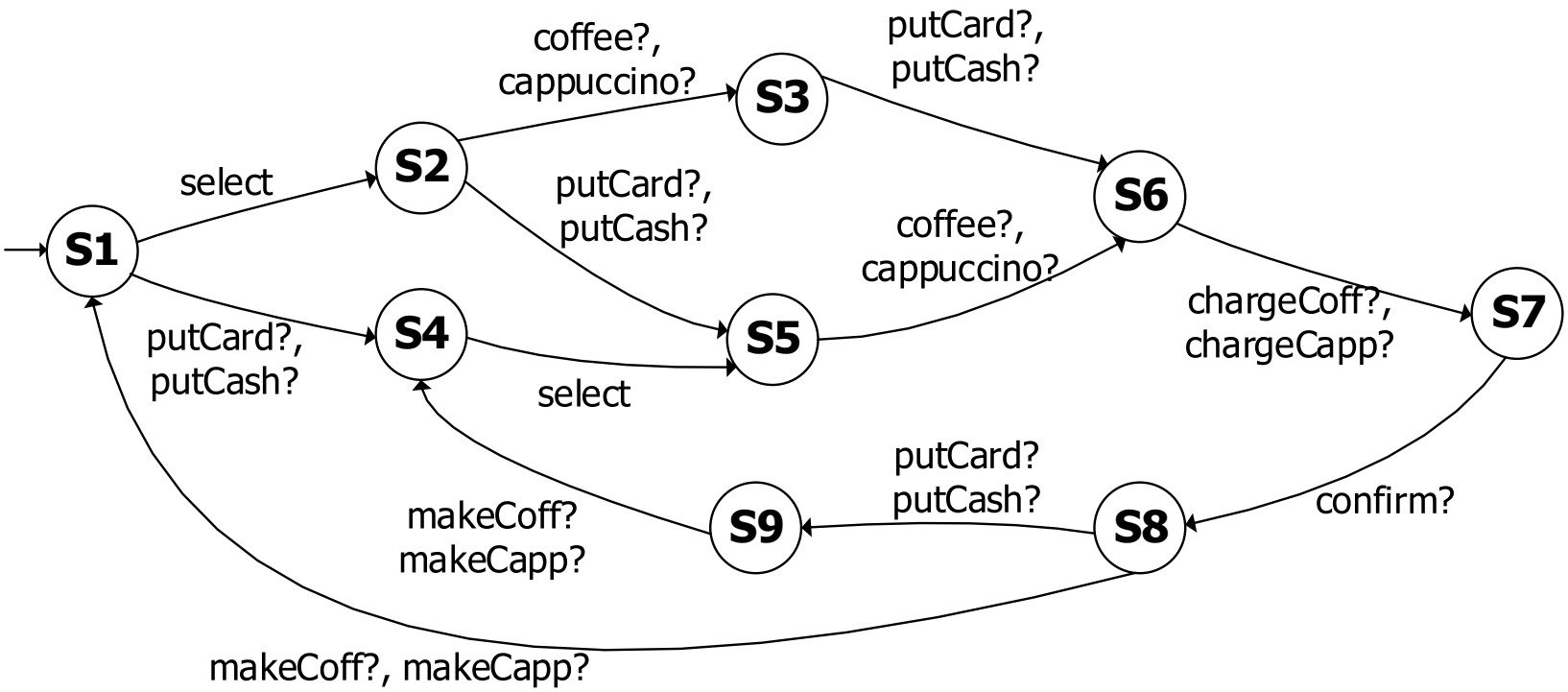
USC Viterbi School of Engineering

State **S3**

- DrinkSelected holds

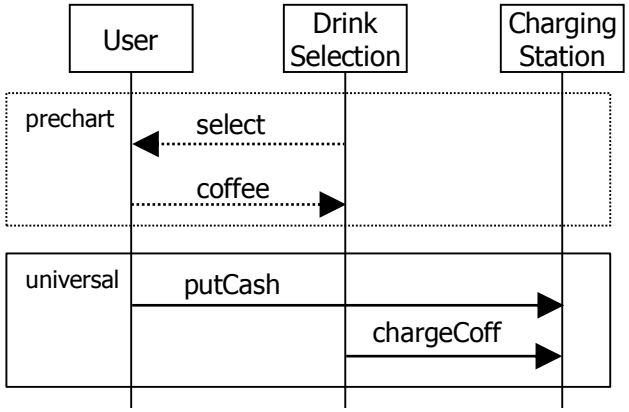
State **S6**

- DrinkSelected and Payment hold



# How MTS Relate to Requirements

USC Viterbi School of Engineering

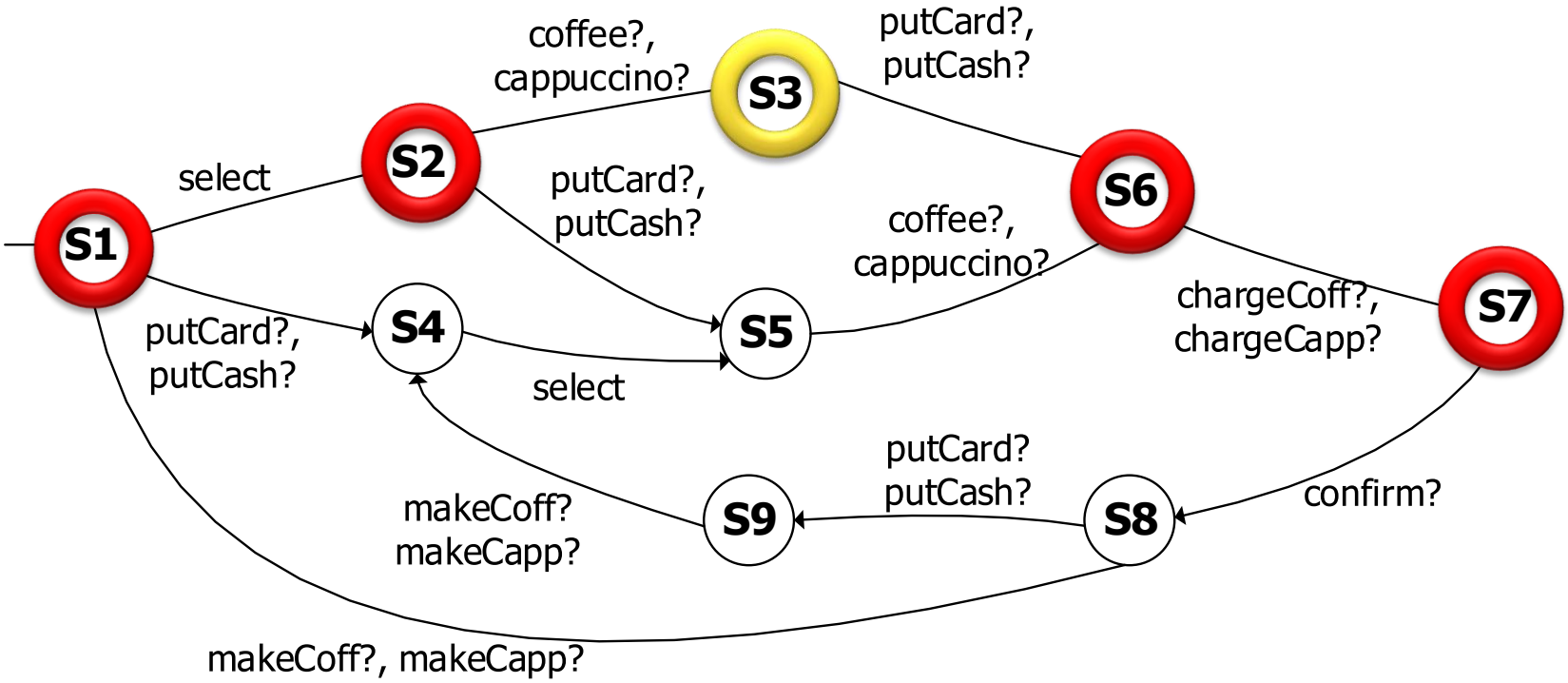



**State S3**

- DrinkSelected holds

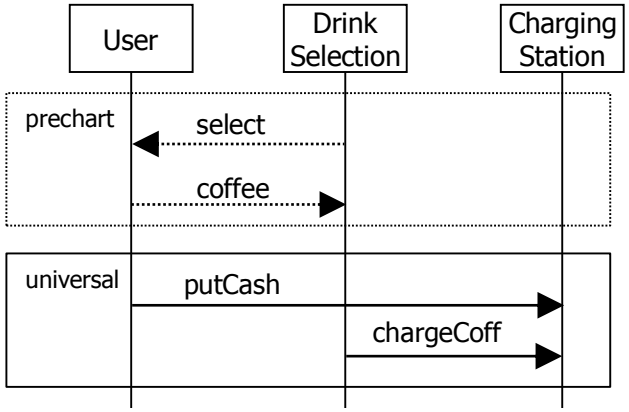
**State S6**

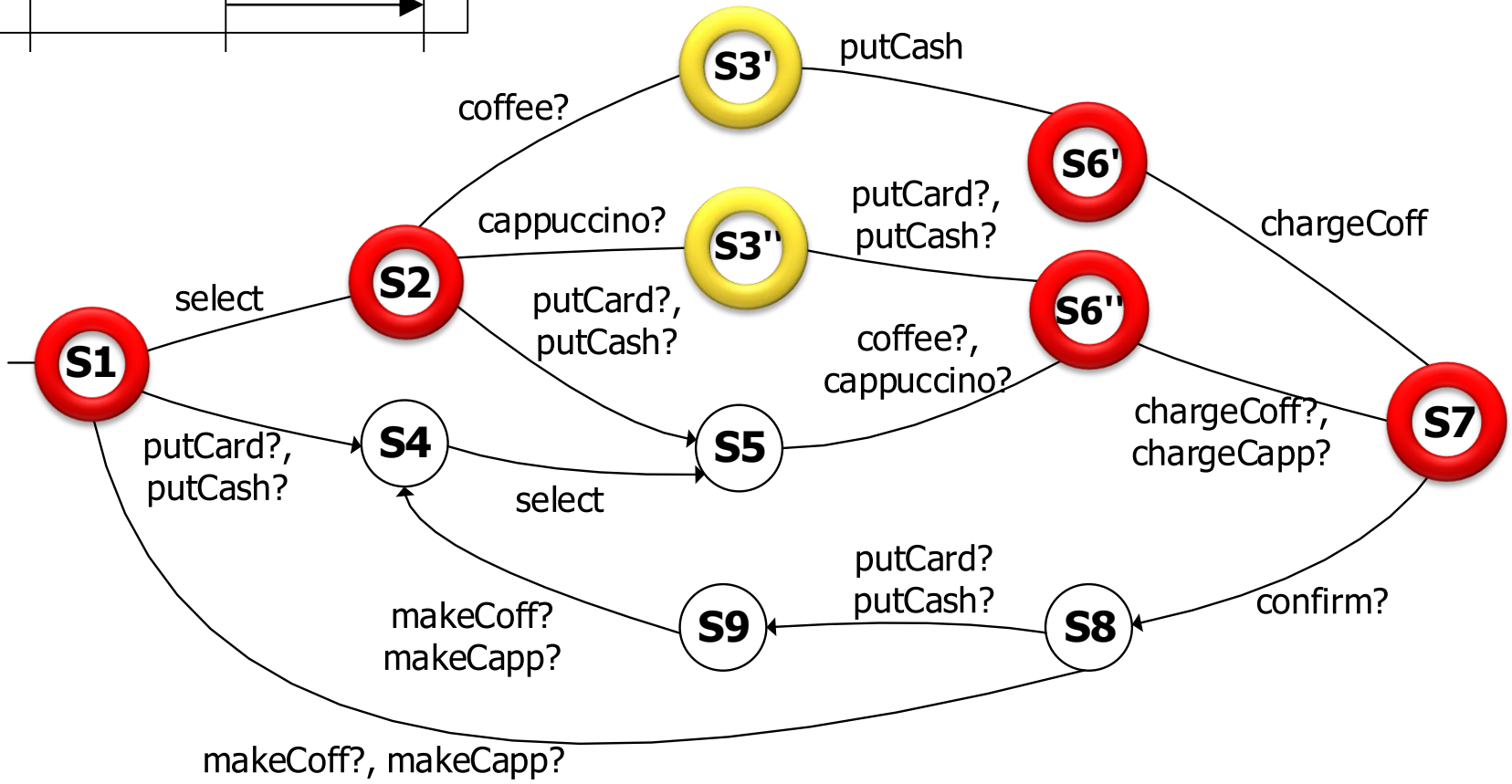
- DrinkSelected and Payment hold



# How MTS Relate to Requirements

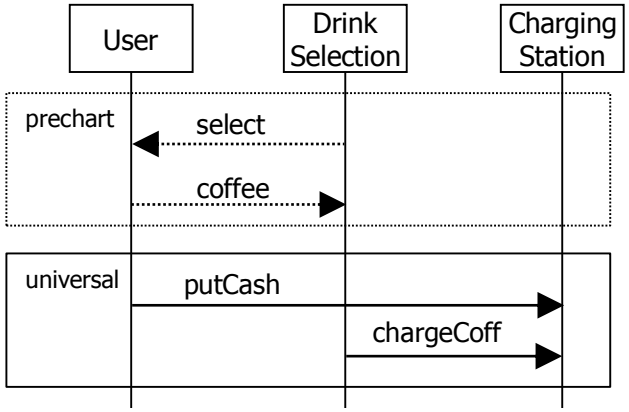
USC Viterbi School of Engineering



# How MTS Relate to Requirements

USC Viterbi School of Engineering

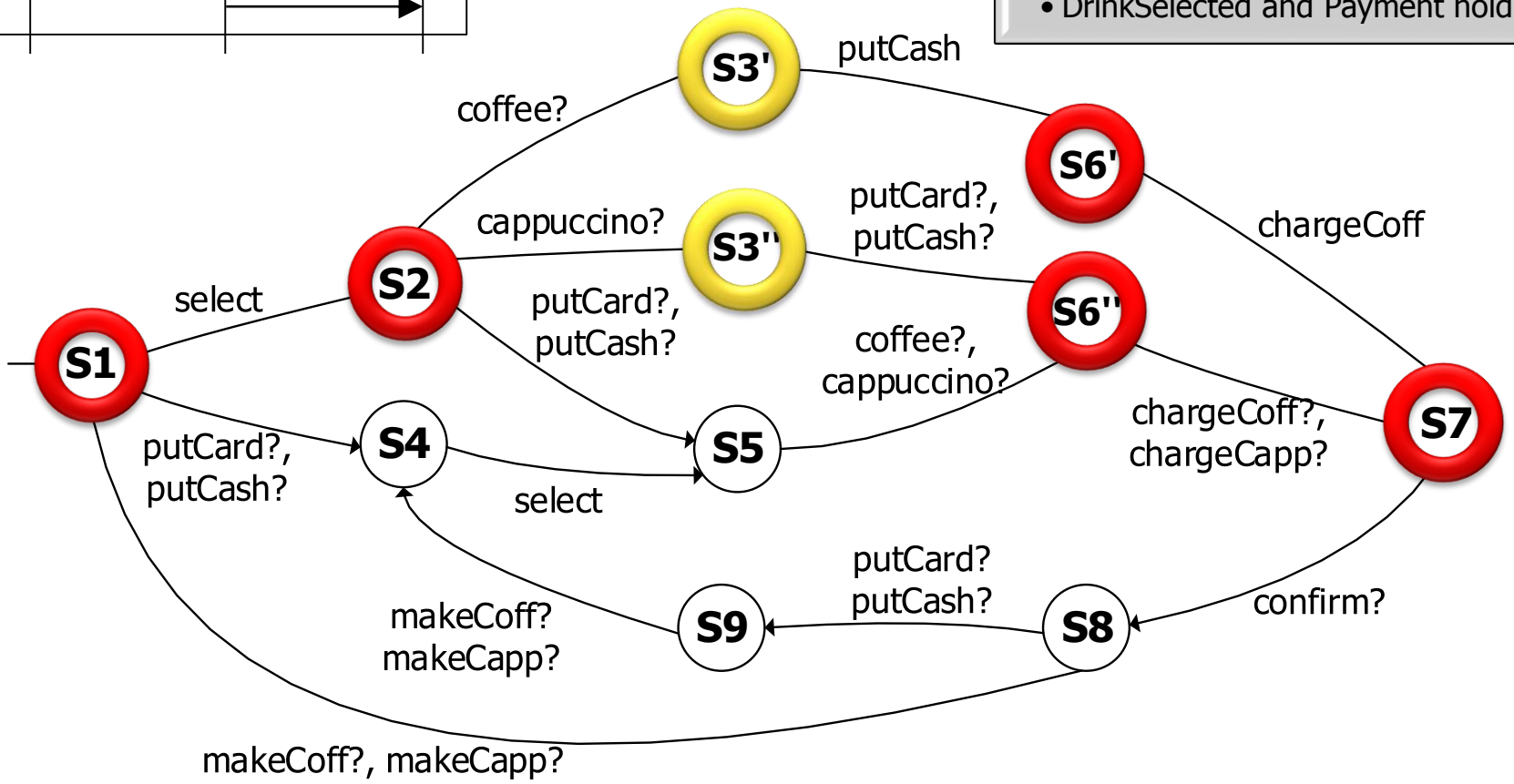



State **S3'**

- Step 2 of **Selection** scenario
- DrinkSelected and Payment hold

State **S3''**

- Step 0 of **Selection** scenario
- DrinkSelected and Payment hold



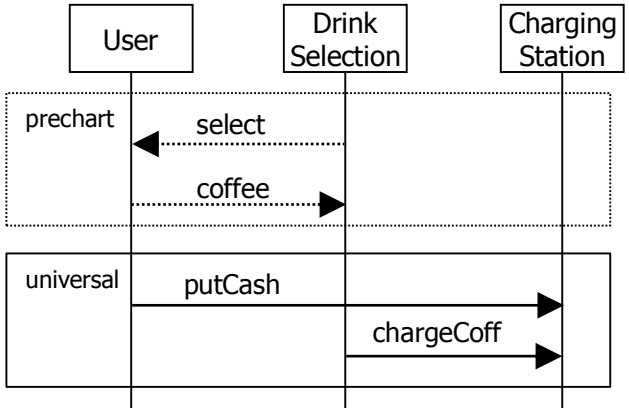
# Refinement Types

USC Viterbi School of Engineering

- Transition refinement
  - *Scenario steps and fluents captured*
  - *Prohibit or require particular behavior*
- Execution-tracking state refinement
  - *Scenario step not captured*
  - *Split state to track execution*
- Fluent-based state cloning
  - *Fluent of interest not tracked*
  - *Split states to track new fluent*

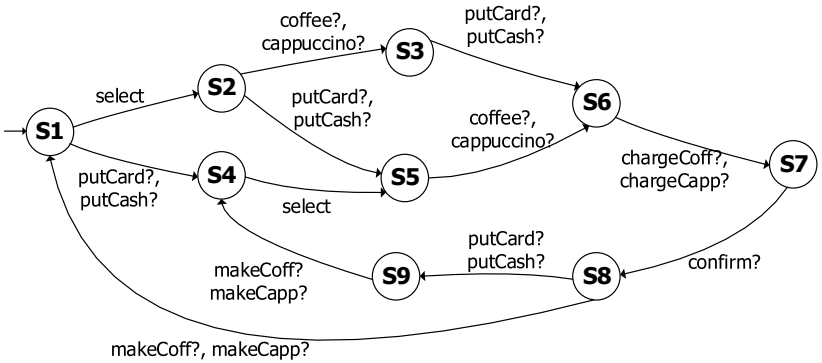
# Refinement Framework

USC Viterbi School of Engineering




1

4




2

3

**chargeCoff precondition**

- CoffeeSelected ∧ Payment

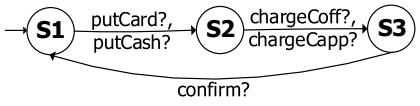
**chargeCappuccino precondition**

- CappuccinoSelected ∧ Payment

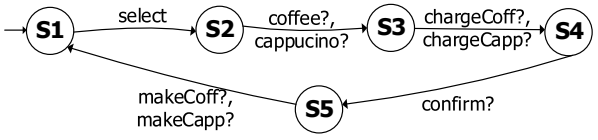
**Goal SelectionFirst**

- G (Payment => DrinkSelected)

**Charging Station**



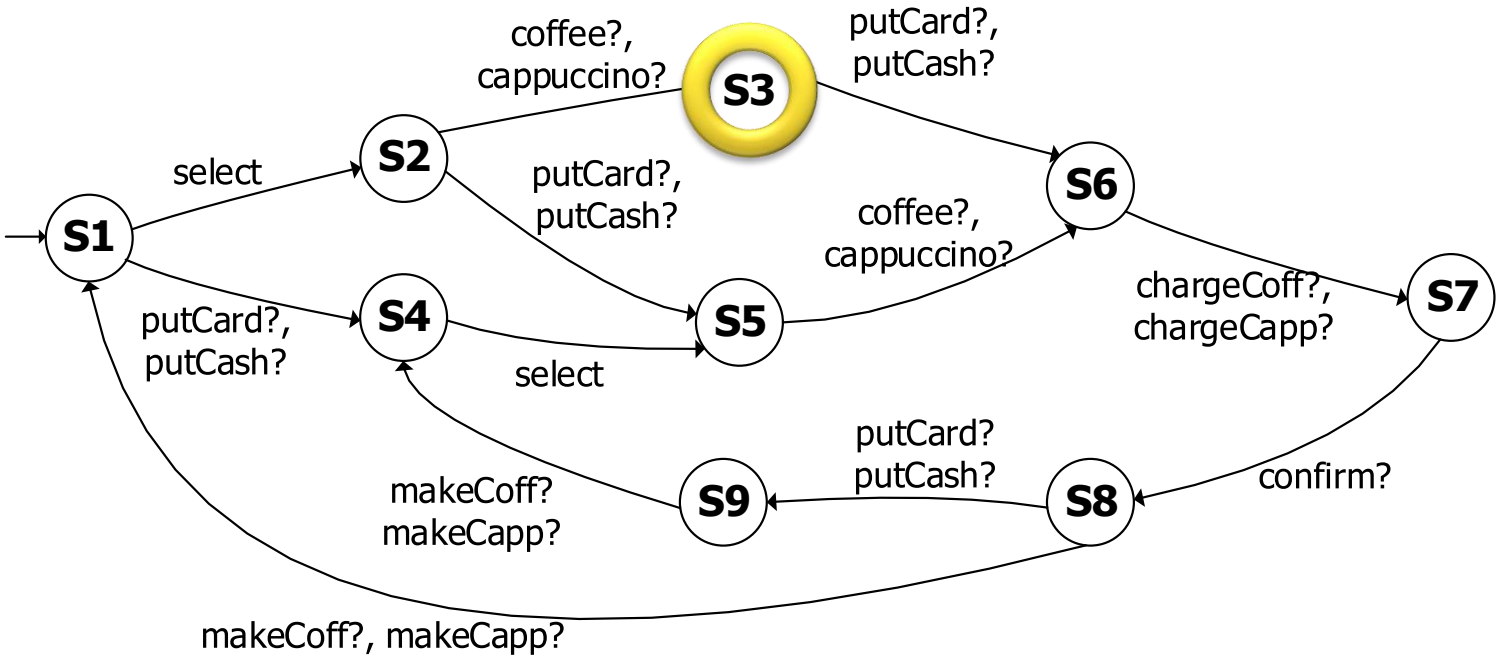

**Drink Selection**



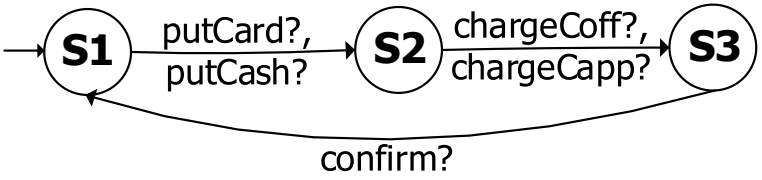
# Refine System State

USC Viterbi School of Engineering

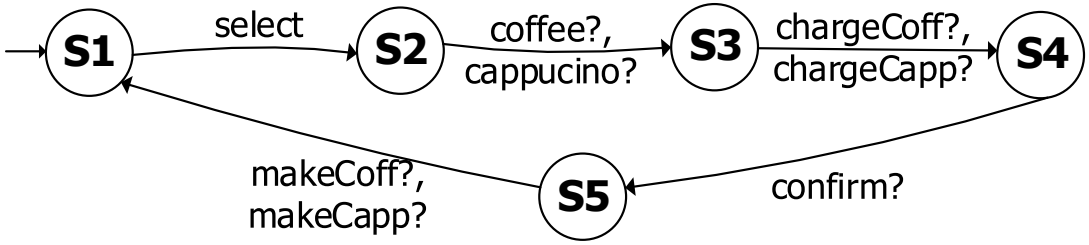
**Coffee Machine**




**Charging Station**



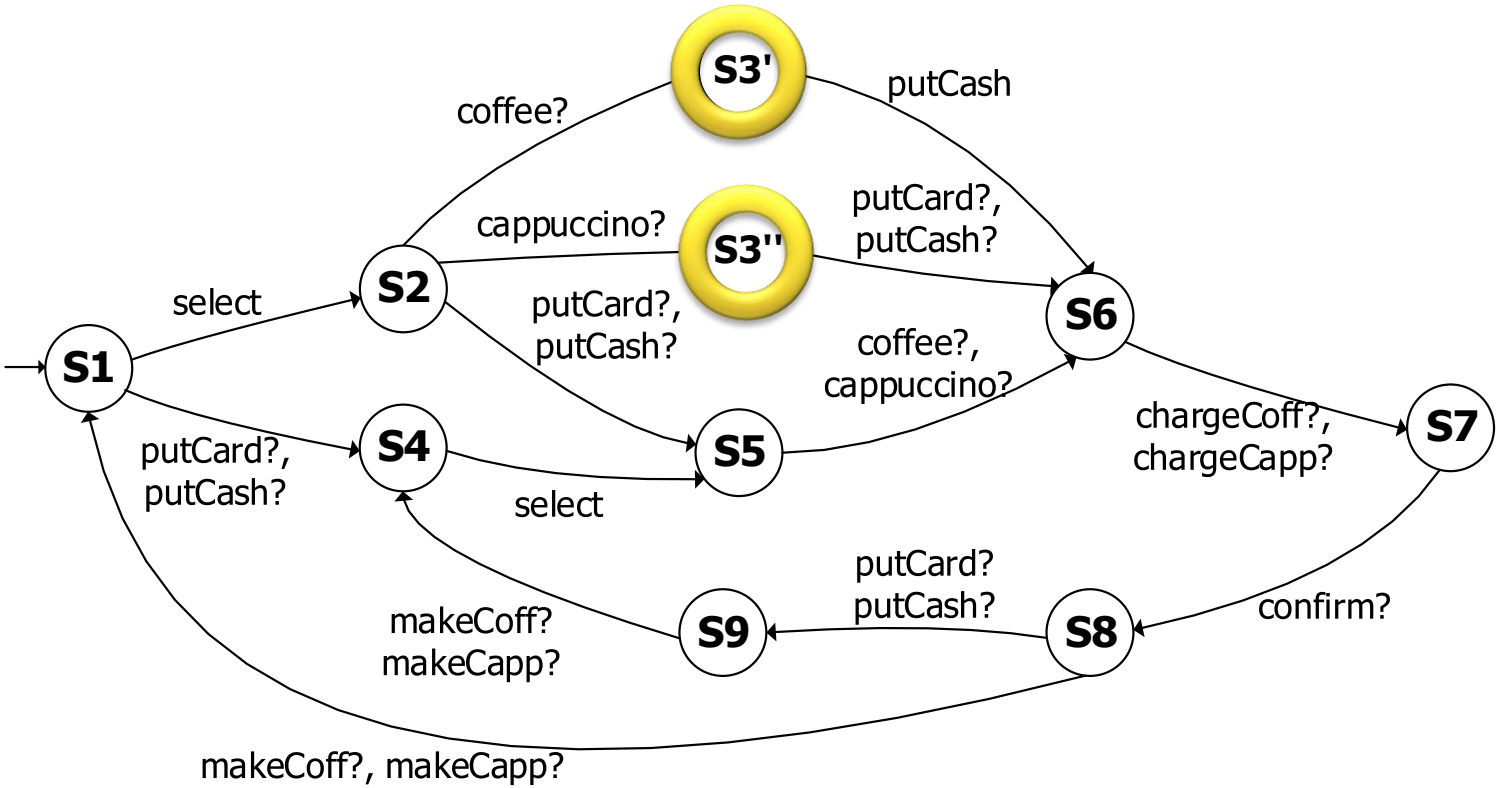

**Drink Selection**



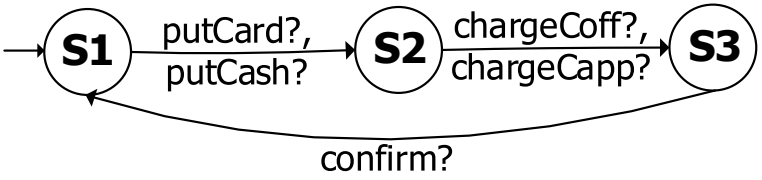
# Refine System State

USC Viterbi School of Engineering

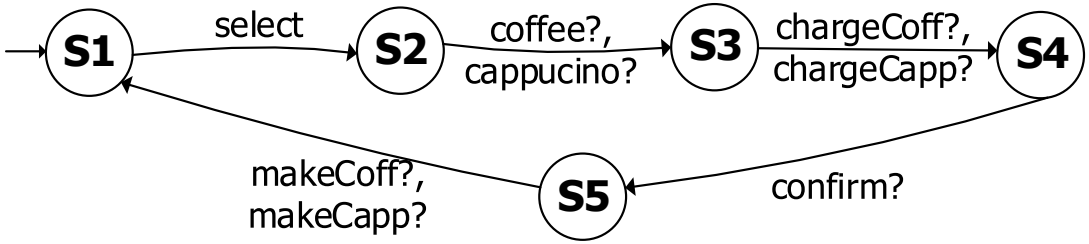
**Coffee Machine**




**Charging Station**



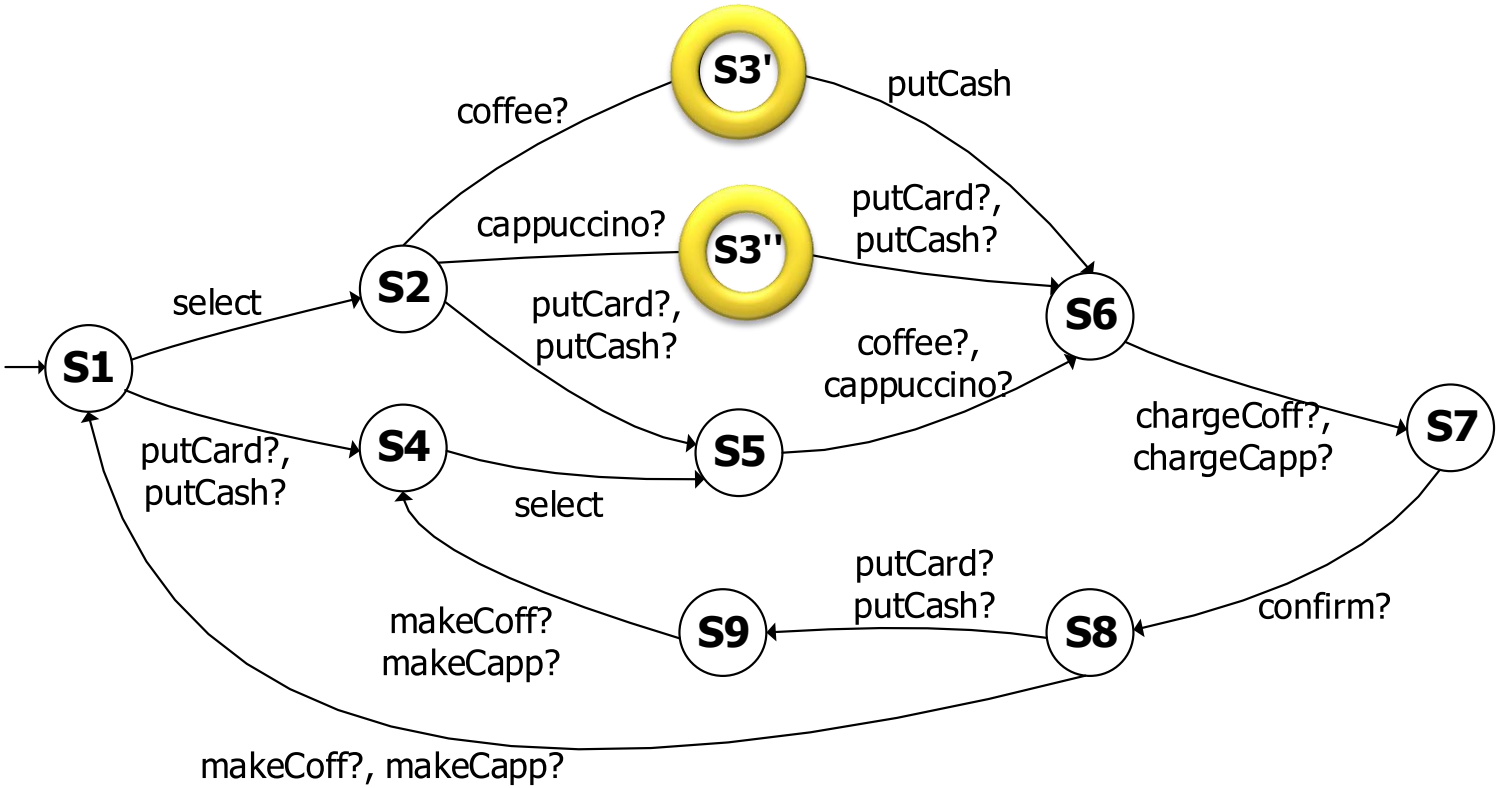

**Drink Selection**



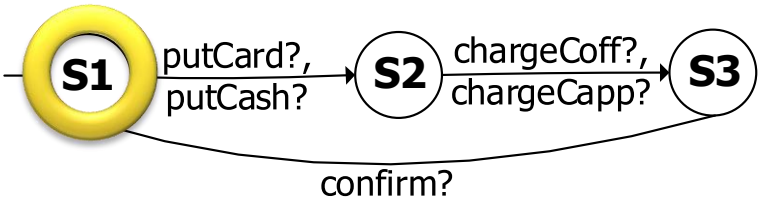
# Identify Affected Component States

USC Viterbi School of Engineering

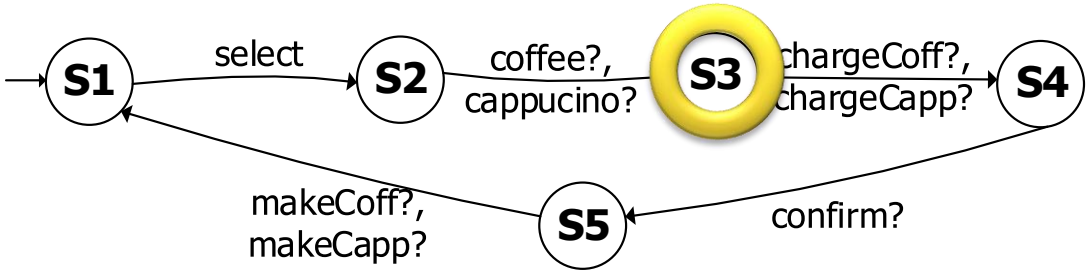
**Coffee Machine**




**Charging Station**



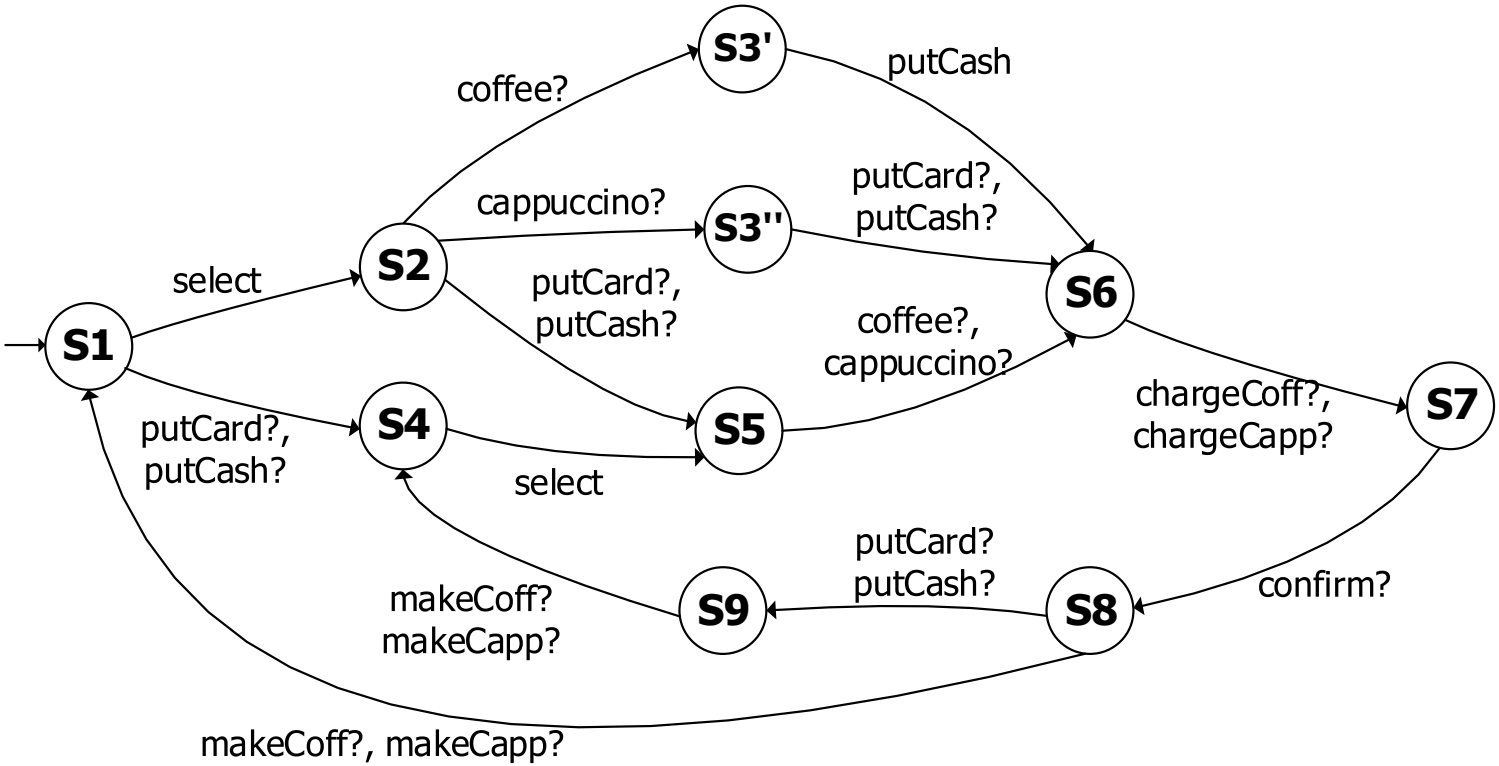

**Drink Selection**



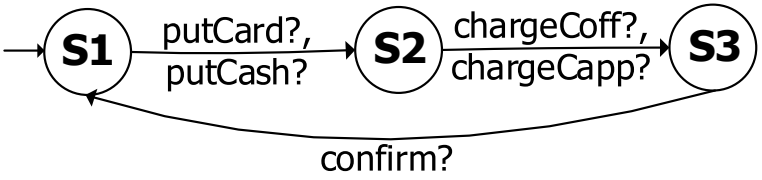
# Perform Component State Refinement

USC Viterbi School of Engineering

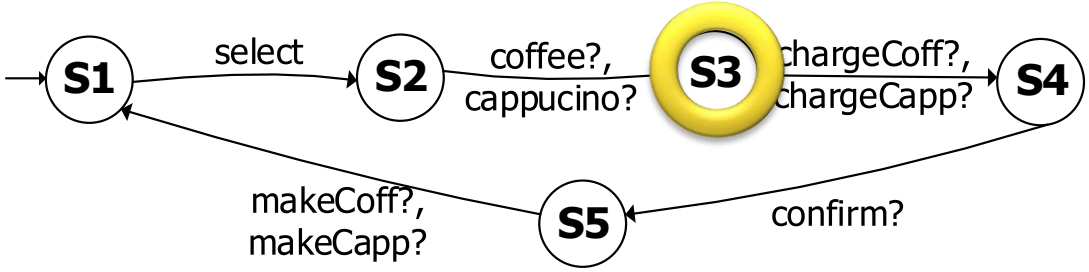
**Coffee Machine**




**Charging Station**



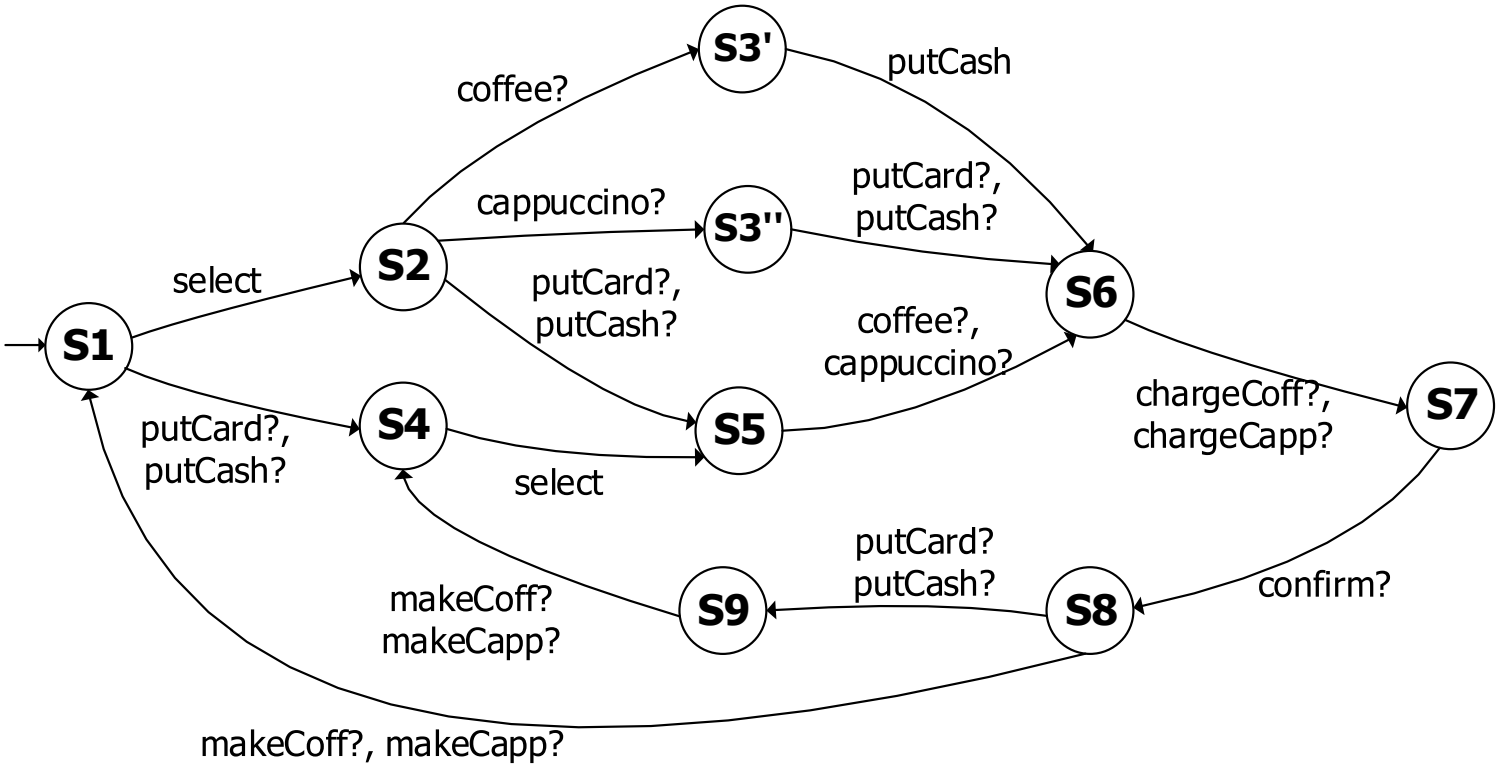

**Drink Selection**



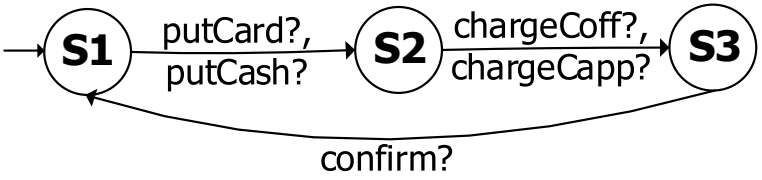
# Perform Component State Refinement

USC Viterbi School of Engineering

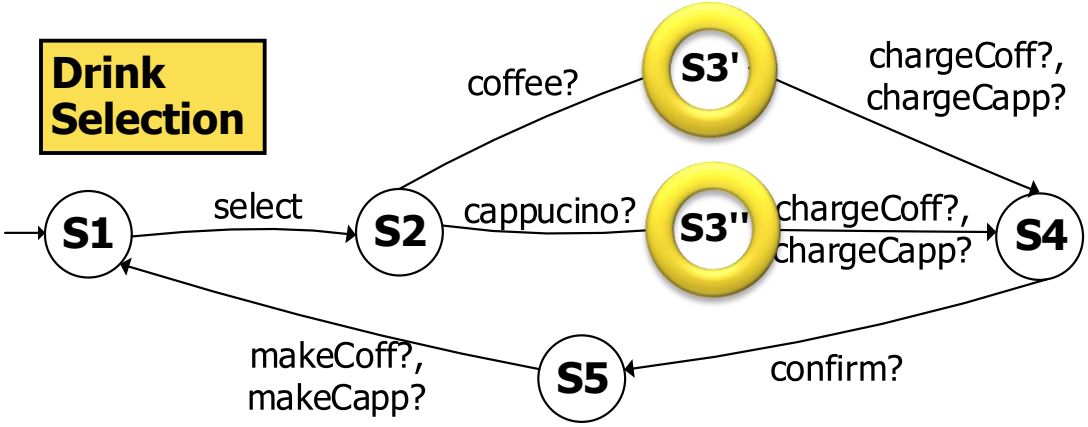
**Coffee Machine**




**Charging Station**



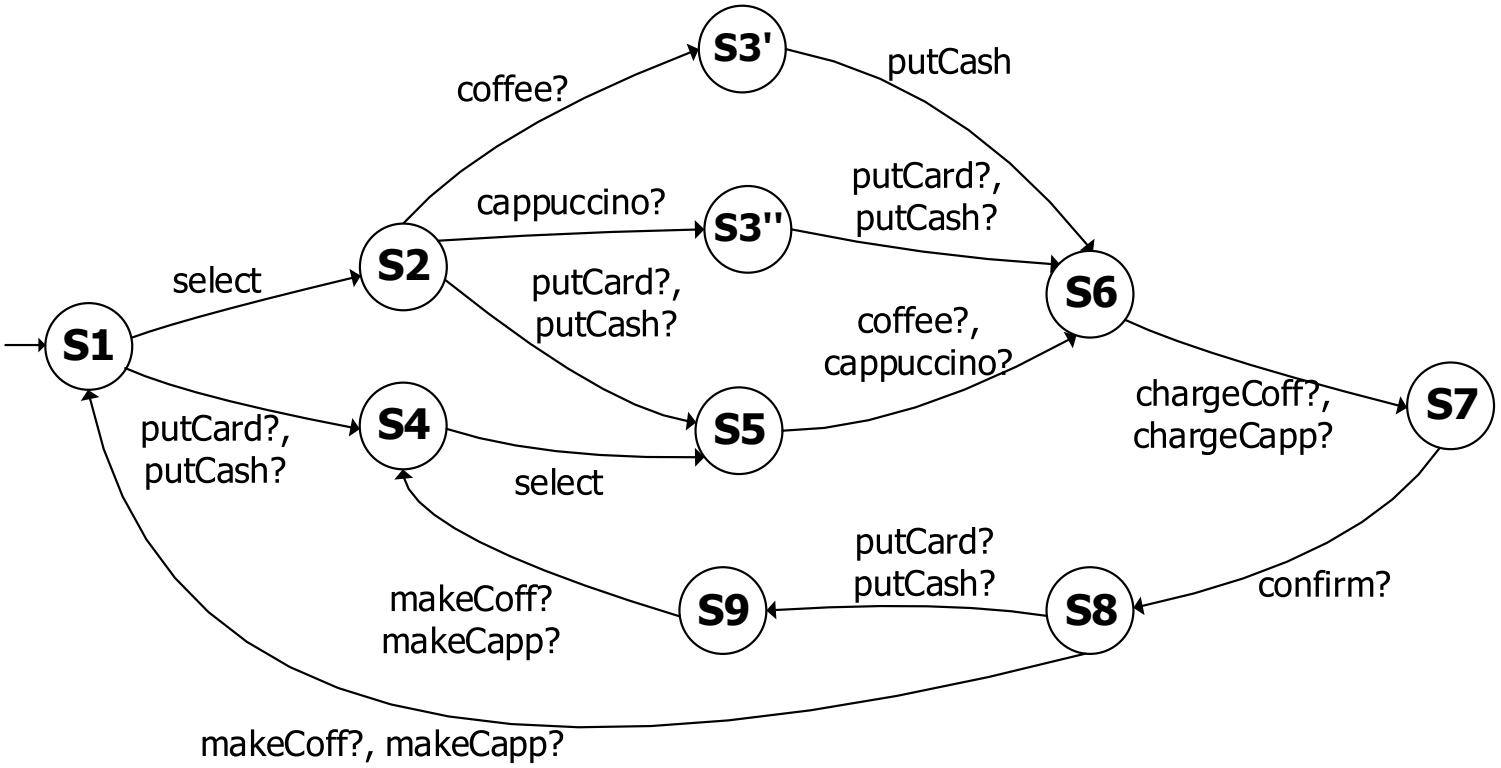

**Drink Selection**



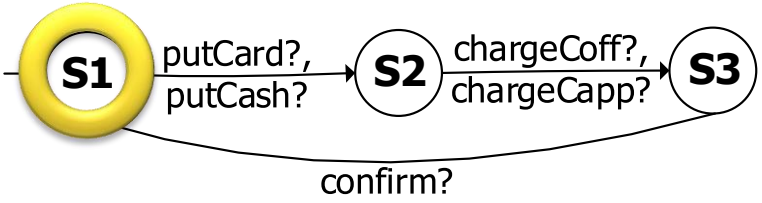
# Perform Component Transition Refinements

USC Viterbi School of Engineering

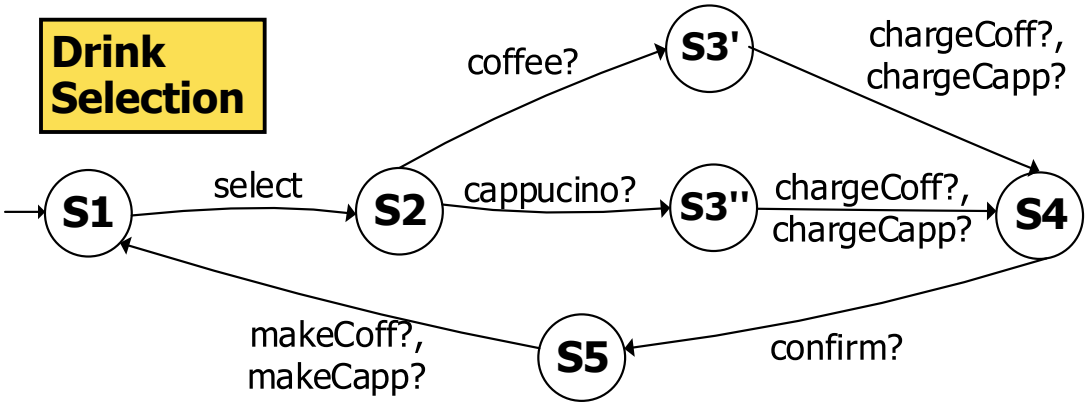
**Coffee Machine**




**Charging Station**



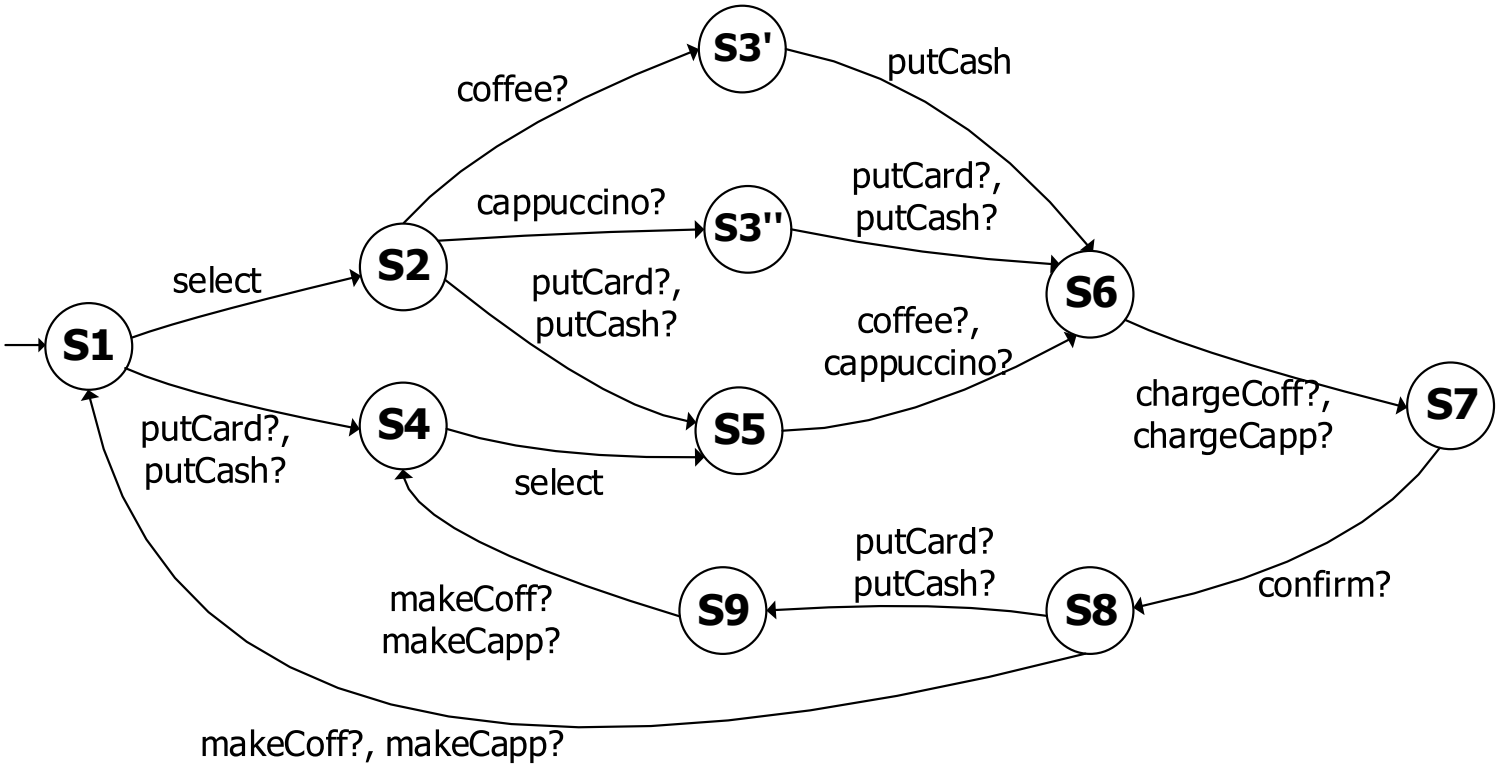

**Drink Selection**



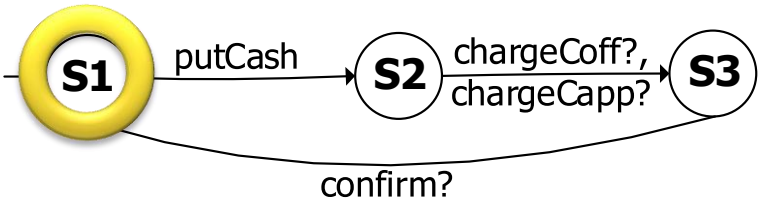
# Perform Component Transition Refinements

USC Viterbi School of Engineering

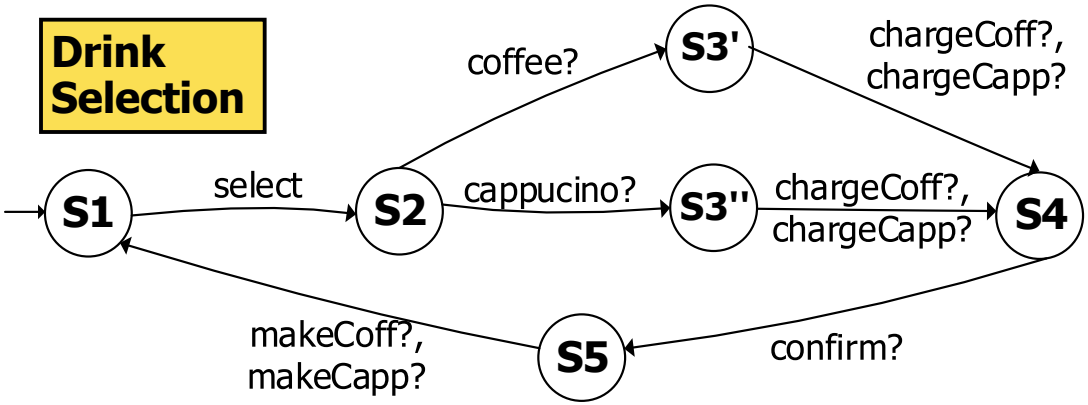
**Coffee Machine**




**Charging Station**



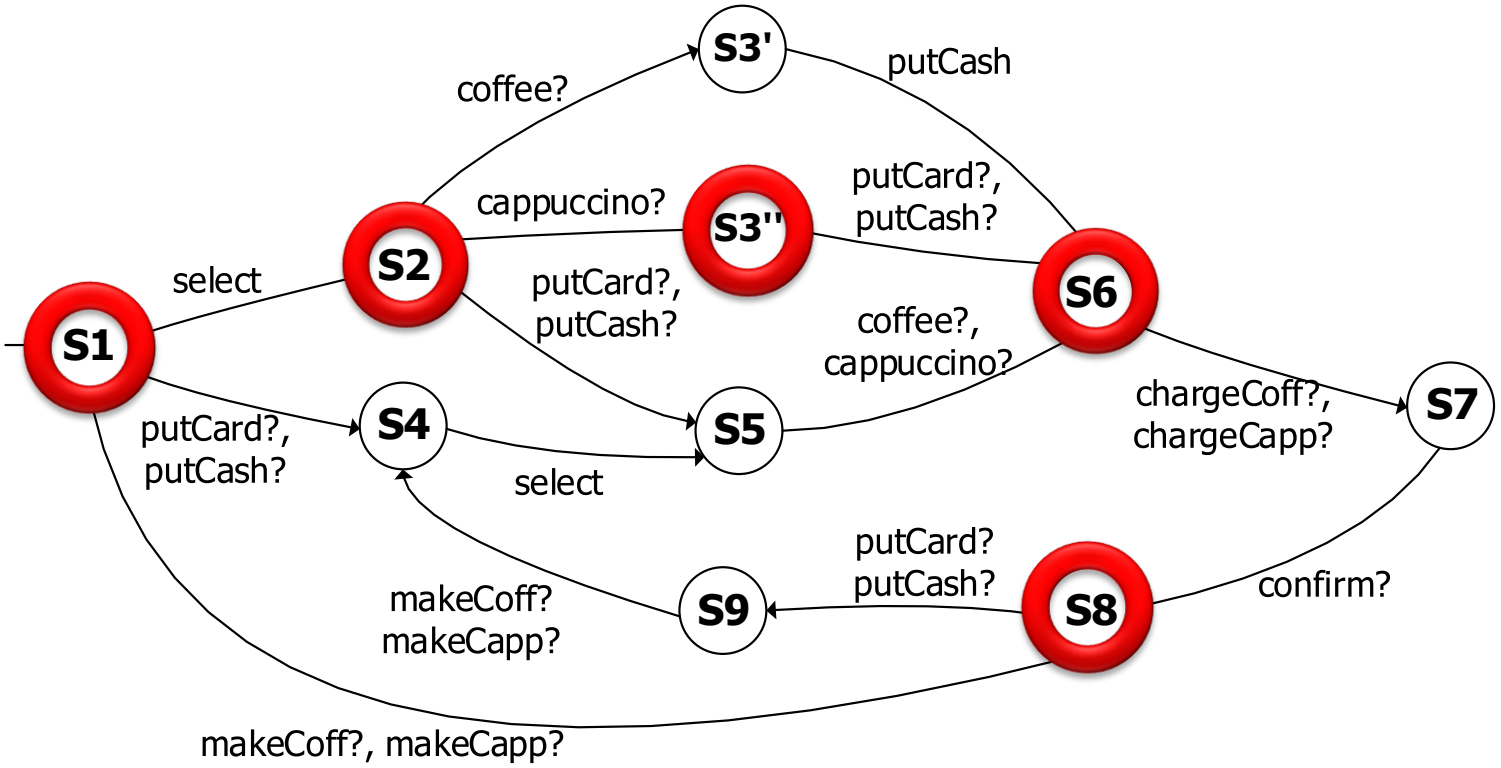

**Drink Selection**



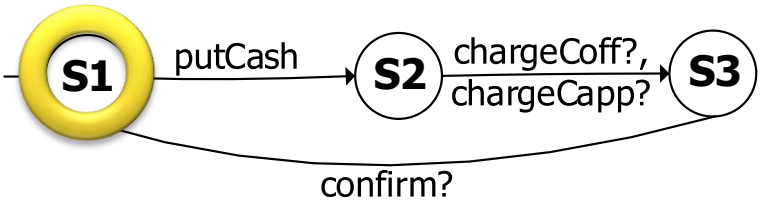
# Determine Affected System States

USC Viterbi School of Engineering

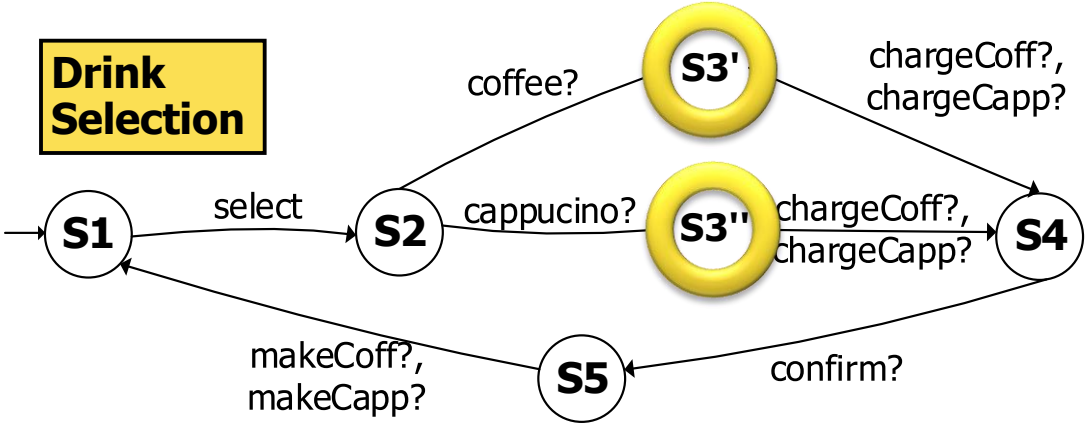
**Coffee Machine**




**Charging Station**



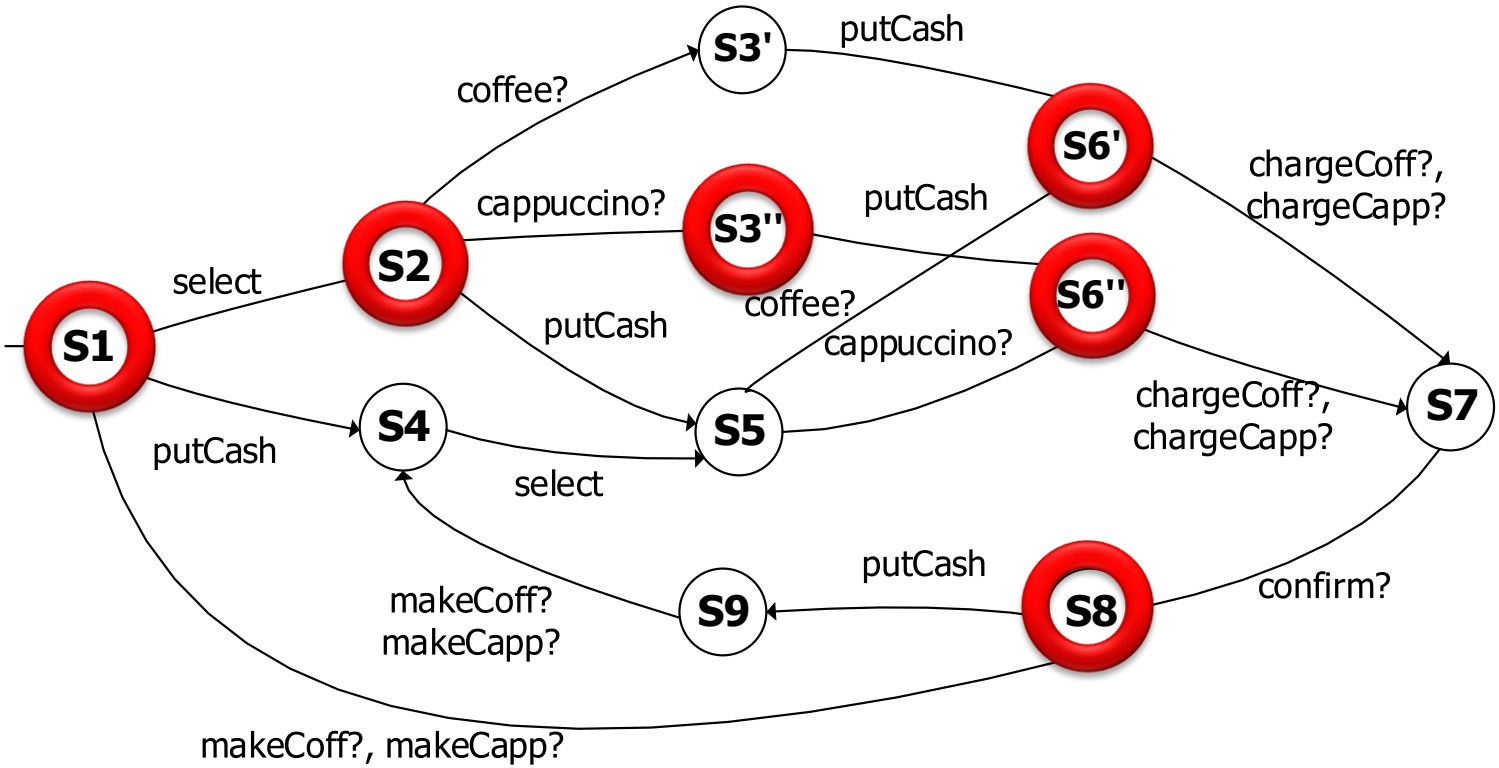

**Drink Selection**



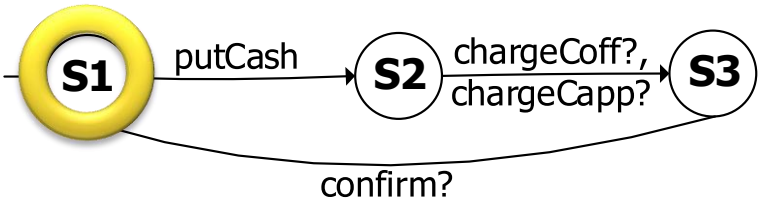
# Propagate Component Refinements

USC Viterbi School of Engineering

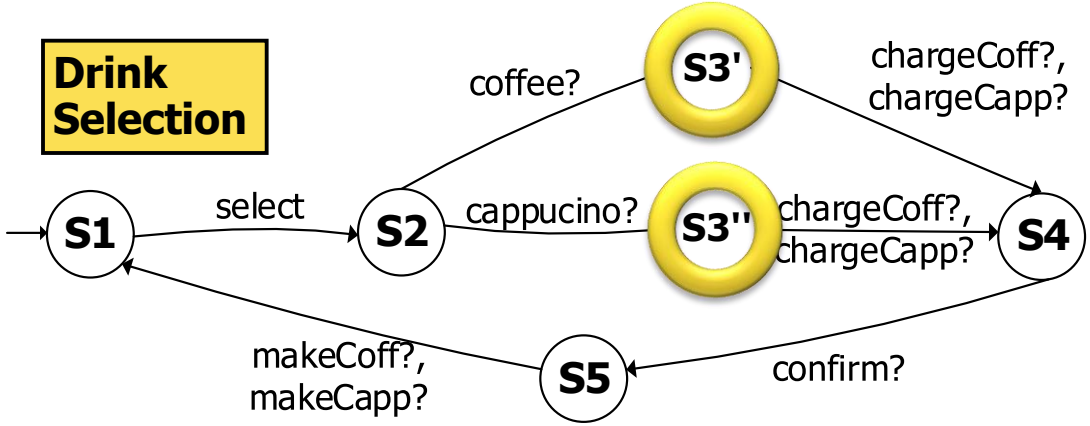
**Coffee Machine**




**Charging Station**

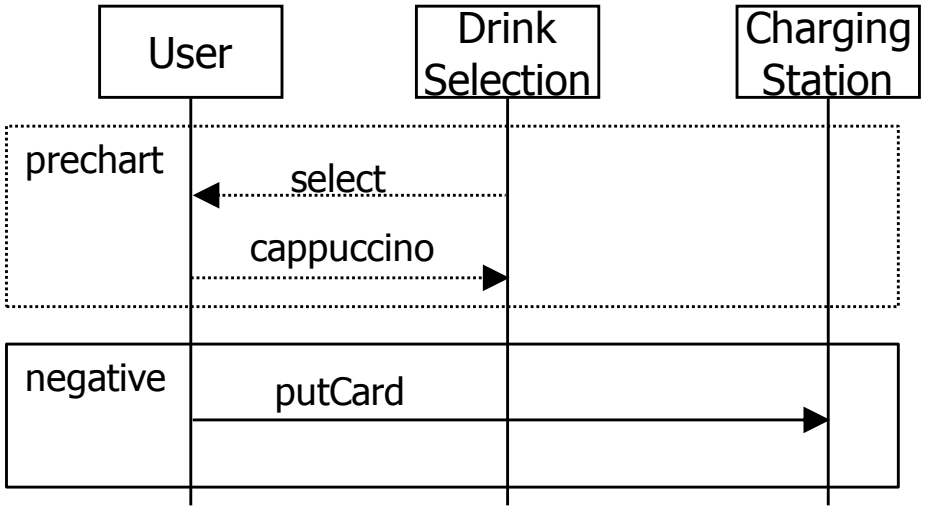


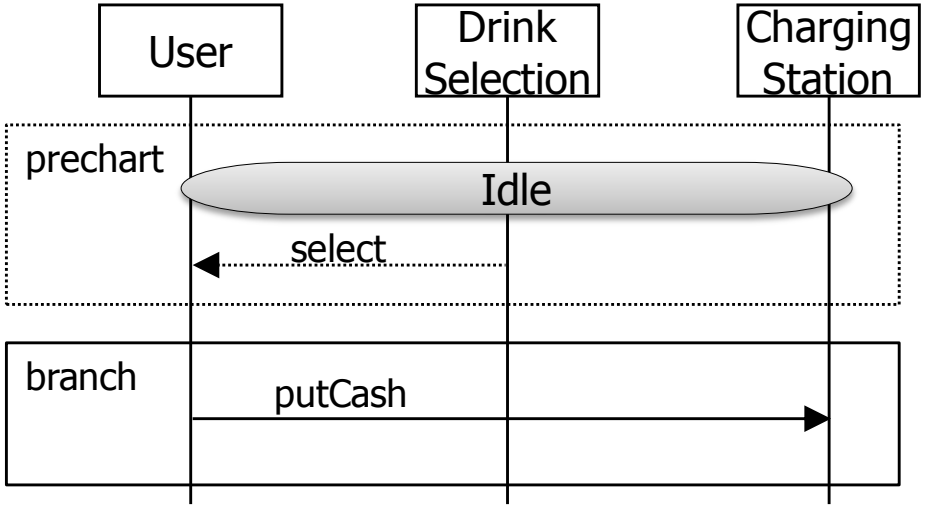

**Drink Selection**



# Induced Scenarios

USC Viterbi School of Engineering




- Analyze impact of requirement decomposition
- Avoid potentially costly errors

# Evaluation

USC Viterbi School of Engineering

- Theoretical aspects
  - *Soundness*
  - *Correctness*
- Case study
  - *Phillips TV specification (Sibay-TOSEM12)*

# Phillips TV - Findings

USC Viterbi School of Engineering

- Avoid errors
  - *Overly restrictive scenarios*
  - *Fluents that cannot be mapped to components*
- Elicitation of new requirements
  - *Behaviors not explored in original study*
- Easier model validation
  - *Small component vs. large system models*

# Conclusions

USC Viterbi School of Engineering

- Requirements-to-MTS mapping
- Refinement propagation framework
  - *Distinct refinement types*
  - *Analyze distribution impact*
  - *Avoid errors*
- Evaluation results

➢ Formalisms with requirements-based heuristics