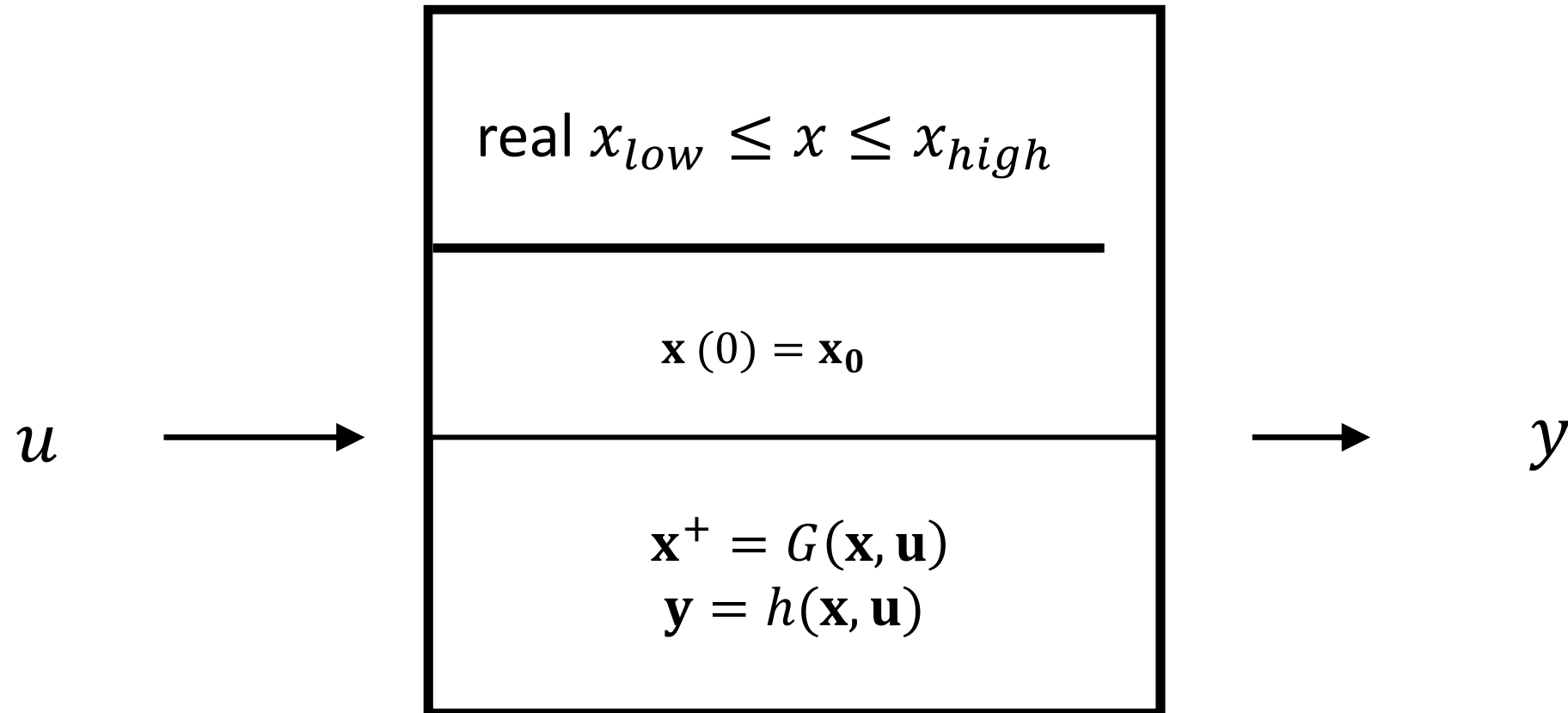# Cyber-Physical Systems

Laura Nenzi

Università degli Studi di Trieste
II Semestre 2022

Lecture 3: Concurrent Modeling

[Many Slides due to J. Deshmukh, Toyota]

Difference Equation

$$\text{real } x_{low} \leq x \leq x_{high}$$

$$\mathbf{x}\,(0) = \mathbf{x_0}$$

$$\mathbf{x}^+ = G(\mathbf{x}, \mathbf{u})$$
$$\mathbf{y} = h(\mathbf{x}, \mathbf{u})$$

u → → y

$$\mathbf{x}(k+1) = G(x(k), u(k))$$

Difference Equation

u_1, u_2 →

force, angular speed

real $-\pi \leq \theta \leq \pi$

$\mathrm{x}_1(0) = 0$
$\mathrm{x}_2(0) = 0$
$\theta(0) = 0$

$\mathrm{x}_1^+ = \mathrm{x}_1 + \mathrm{d}\sin(\theta)\mathrm{u}_1$
$\mathrm{x}_2^+ = \mathrm{x}_2 + \mathrm{d}\cos(\theta)\mathrm{u}_1$
$\theta^+ = \theta + \mathrm{c}\,u_2$
$\mathrm{y} = \theta$

→ y

Functional Components

1. *Classical* model of computation: Functional or Transformational Programs

   ▶ Start from a given input,

   ▶ Produce a certain output and then **terminate**

   ▶ Desired functionality can be described by a mathematical function

   ▶ Emphasis is on data computation

Reactive Components

2. Reactive Programs:

   ▶ It maintains and internal state

   ▶ Continuously interact with the environment at a rate decided by the environment

   ▶ Emphasis is on system-environment interaction; e.g. airline autopilot, mail-servers, etc.

Synchronous Models

▶ All components execute in a sequence of rounds in lock-step

▶ Example:
 ▶ Components in a digital hardware circuit with a central global clock

 ▶ Fixed-step Simulation Models of Discrete Components in Simulink
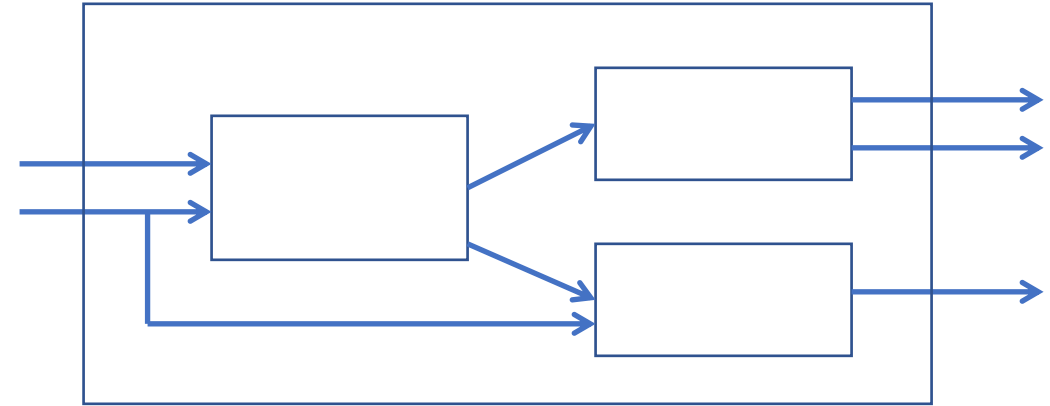
Synchronous languages

▶ Benefit: system design is simpler if we use a simple round-based computation

▶ Challenge: How do we ensure synchronous execution when components may execute on different hardware?

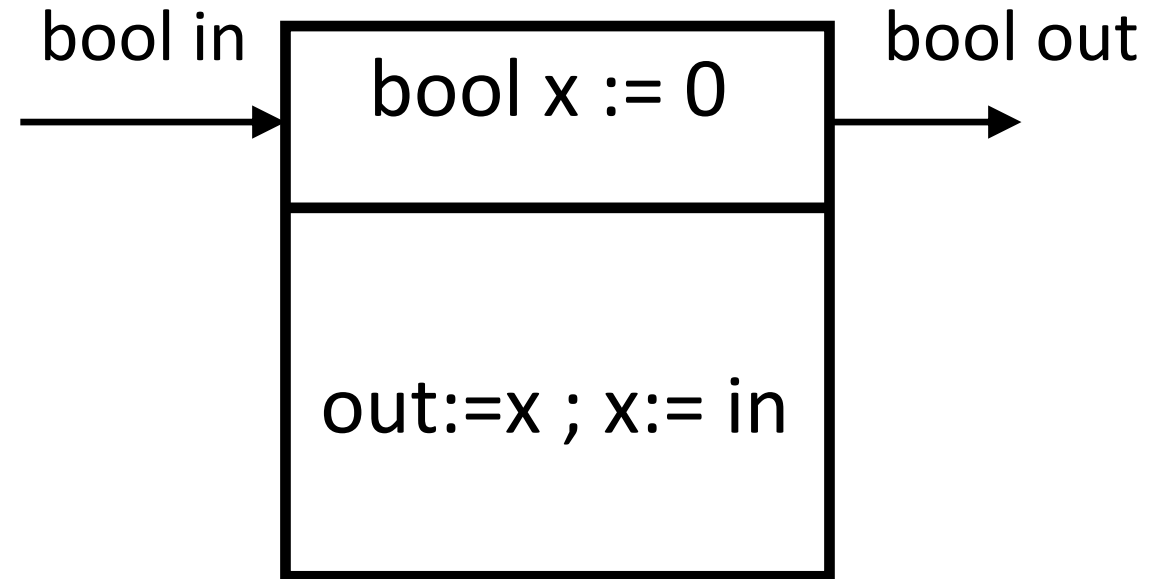# Simple Representation of a Synchronous Component
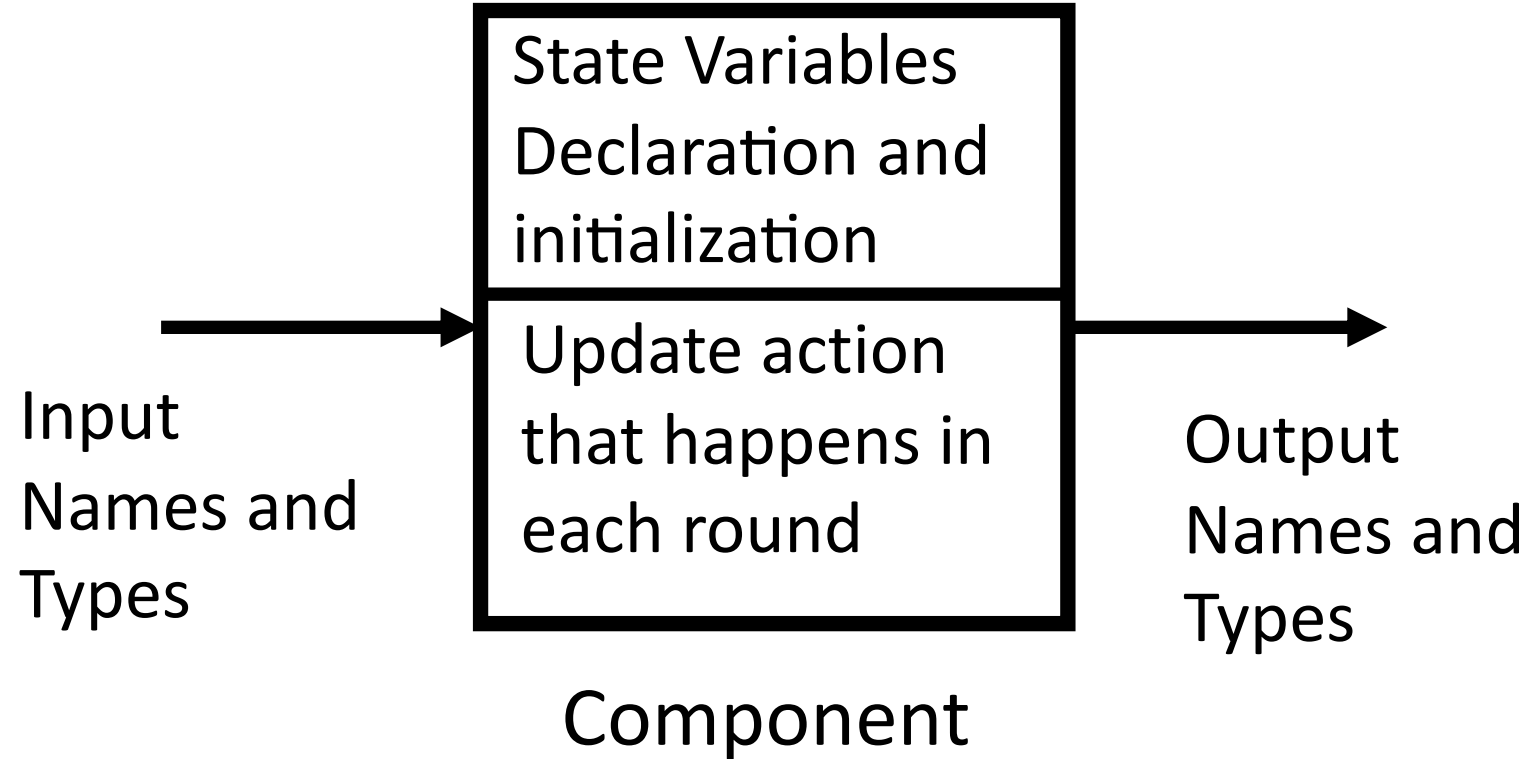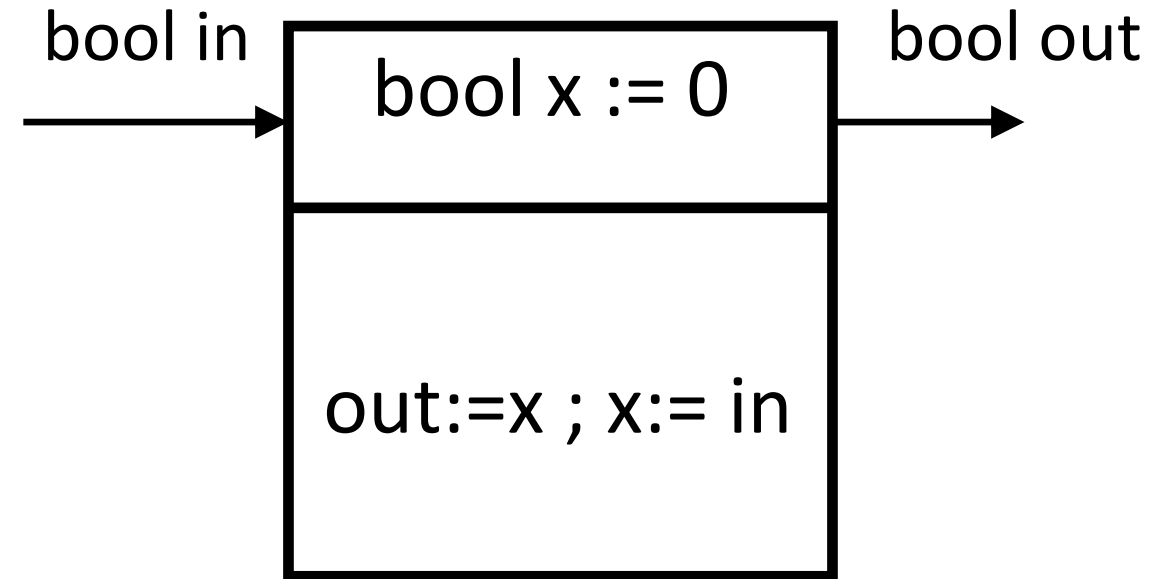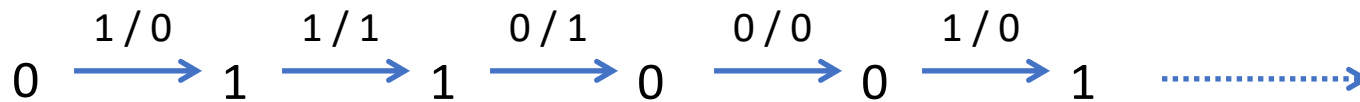
Simplest synchronous component: delay

(Boolean = { 0, 1})

▶ Input variable: in of type Boolean

▶ Output variable: out of type Boolean

▶ State variable: x of type Boolean, initialized to 0

▶ In each round, component updates output from the state and state from input

bool in → | bool x := 0 | → bool out

out:=x ; x:= in

Execution of "Delay"

▶ Initialize state to 0

▶ Repeatedly execute rounds

▶ In each round:
  ▸ Choose value for input (provided from environment, e.g. by user)
  ▸ Execute update code

bool in → [bool x := 0 / out:=x ; x:= in] → bool out

$$0 \xrightarrow{1/0} 1 \xrightarrow{1/1} 1 \xrightarrow{0/1} 0 \xrightarrow{0/0} 0 \xrightarrow{1/0} 1 \dashrightarrow$$

Synchrony hypothesis

▶ Time needed to execute update is negligible compared to arrival times between consecutive inputs

▶ Synchronous execution is a *logical abstraction*

- ▶ *Execution time of update code is 0*
- ▶ *Production of outputs, updates to state and arrival of inputs happen instantaneously*

▶ With multiple components, assume all execute synchronously and simultaneously
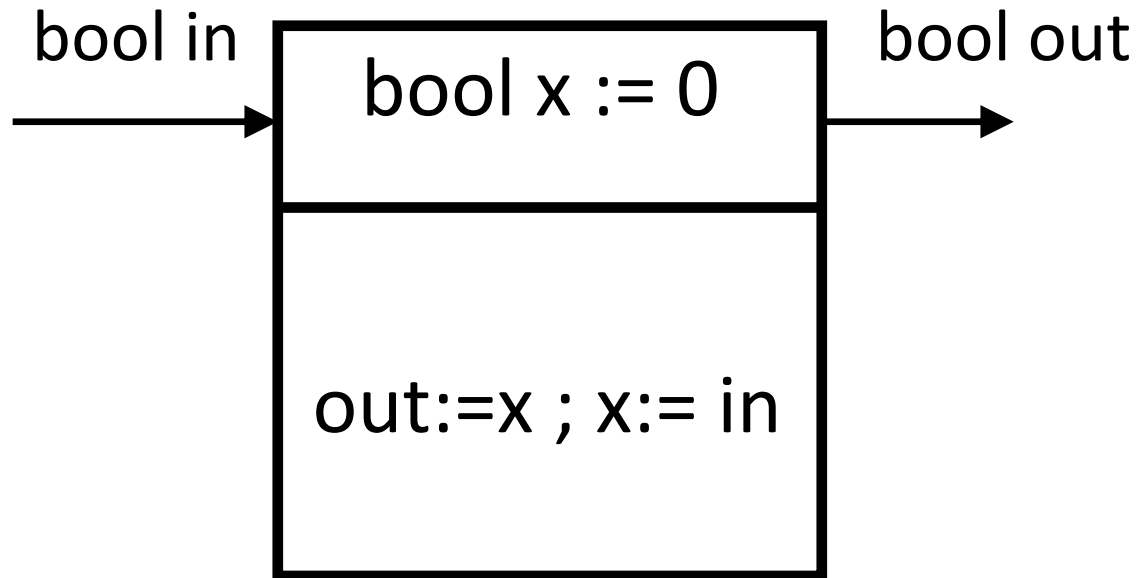
Let's Formalize an SRC

▶ SRC is defined as a tuple: $(Q_I, Q_x, Q_o, [\![init]\!], [\![react]\!])$, where:

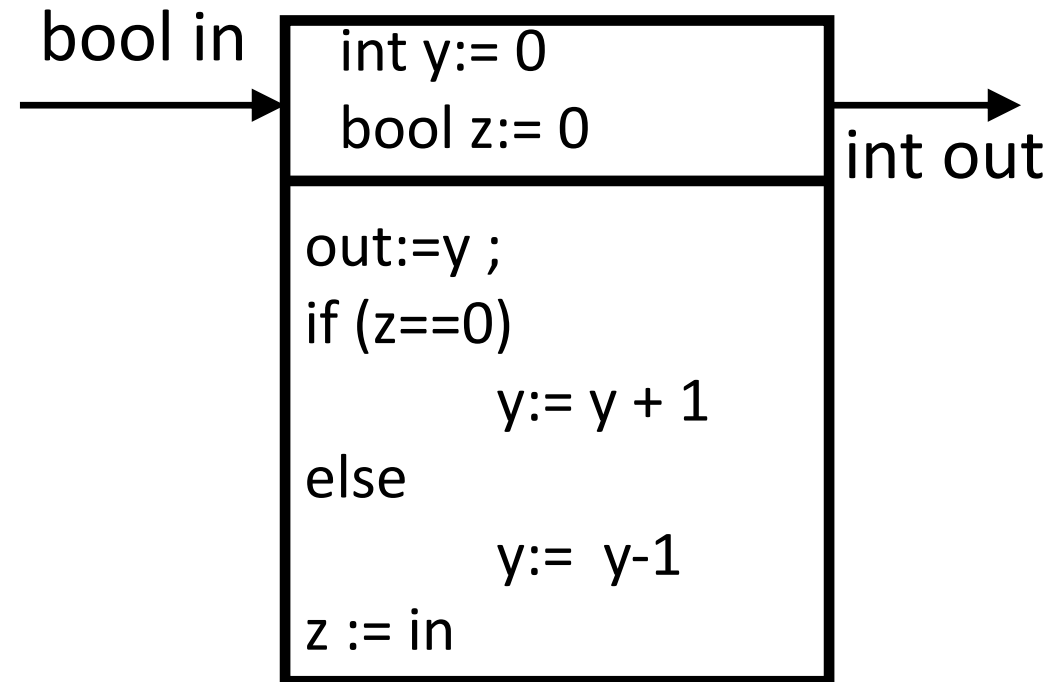| Symbol	Designation	Examples
Q_I	Set of Inputs	{bool in}
Q_X	Set of State Variables	$\{bool\ x\ \}$
Q_o	Set of Outputs	$\{bool\ out\}$
$[\![init]\!]$	Set of initial States	$x := 0$
$[\![react]\!]$	Set of Updates	$out := x$ $x := in$

Semantics of updates & initialization

▶ Let the set of input, output, and state values be Q_I, Q_O, Q_X

▶ Semantics of the initialization function:

  ▶ At time/round 0, maps the state variables to some specified value (or values) in Q_X

▶ Semantics of the update function (some sequence of conditionals and assignments):

  ▶ A set R of transitions where each transition is of the form: $q \xrightarrow{i/o} q'$, where q is the old value of the state variables, q' is the new value of the state variables, i is the value of the input in that round, and o is the value of the output

  ▶ R is a subset of $Q_X \times Q_I \times Q_O \times Q_X$

What are the Q_I, Q_O, Q_X for these SRCs?

bool in	
	bool x := 0
	out:=x ; x:= in

bool out

$$Q_I = \{0,1\}, Q_X = \{0,1\}, Q_O = \{0,1\}$$

bool in

```
int y:= 0
bool z:= 0
```

int out

```
out:=y ;
if (z==0)
            y:= y + 1
else
            y:= y-1
z := in
```

$$Q_I = \{0,1\}, Q_X = \text{int} \times \{0,1\}, Q_O = \text{int}$$

Transitions for Delay

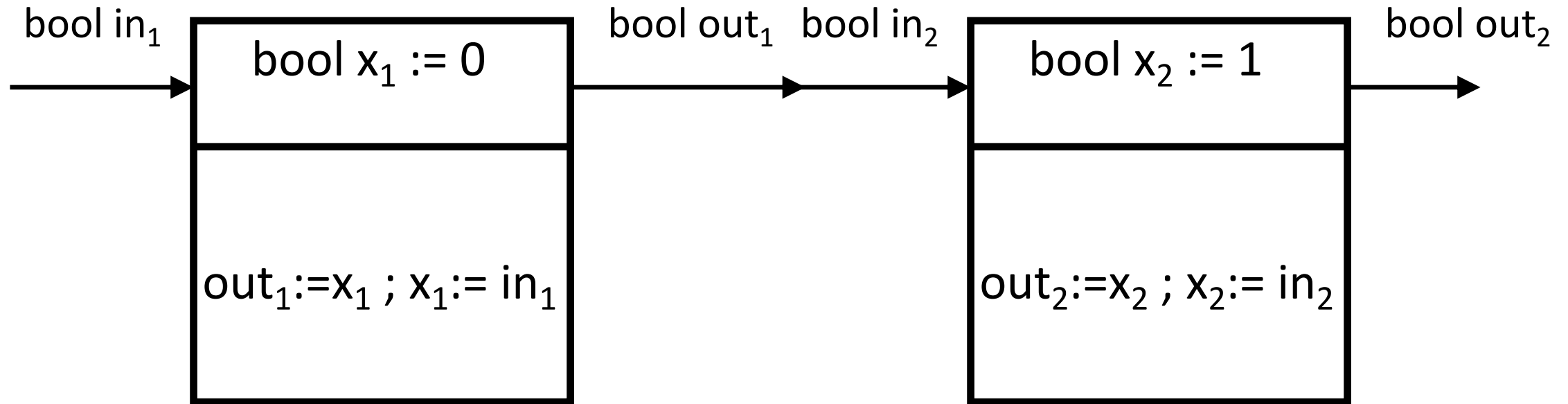bool in

bool x := 0

out:=x ; x:= in

bool out
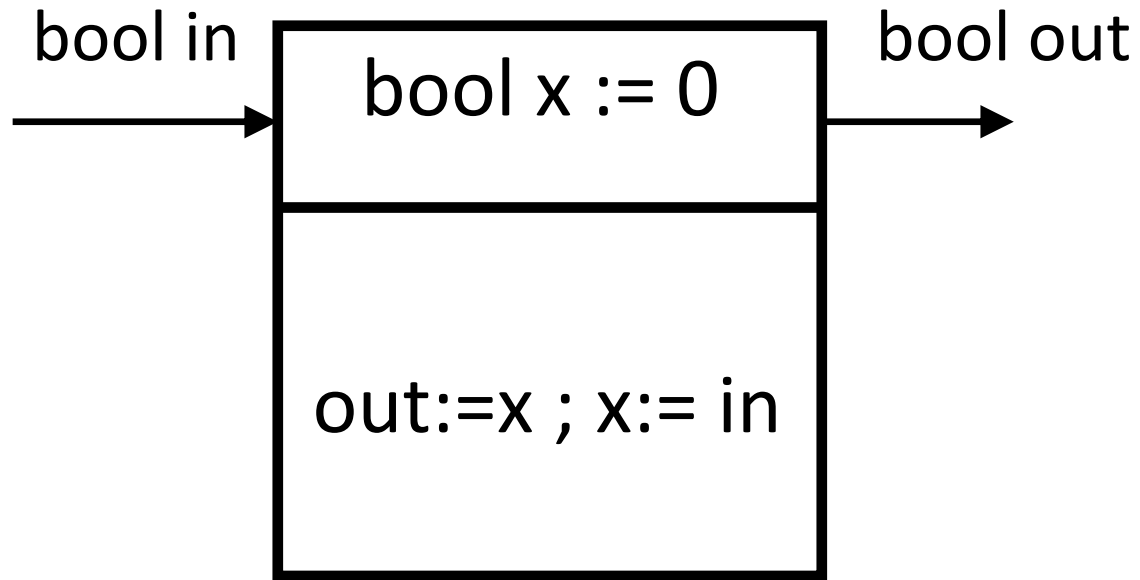
$$0 \xrightarrow{0/0} 0$$

$$0 \xrightarrow{1/0} 1$$

$$1 \xrightarrow{0/1} 0$$

$$1 \xrightarrow{1/1} 1$$

Composition of Synchronous Components

Delay sequentially composed with Delay

Composition of Synchronous Components
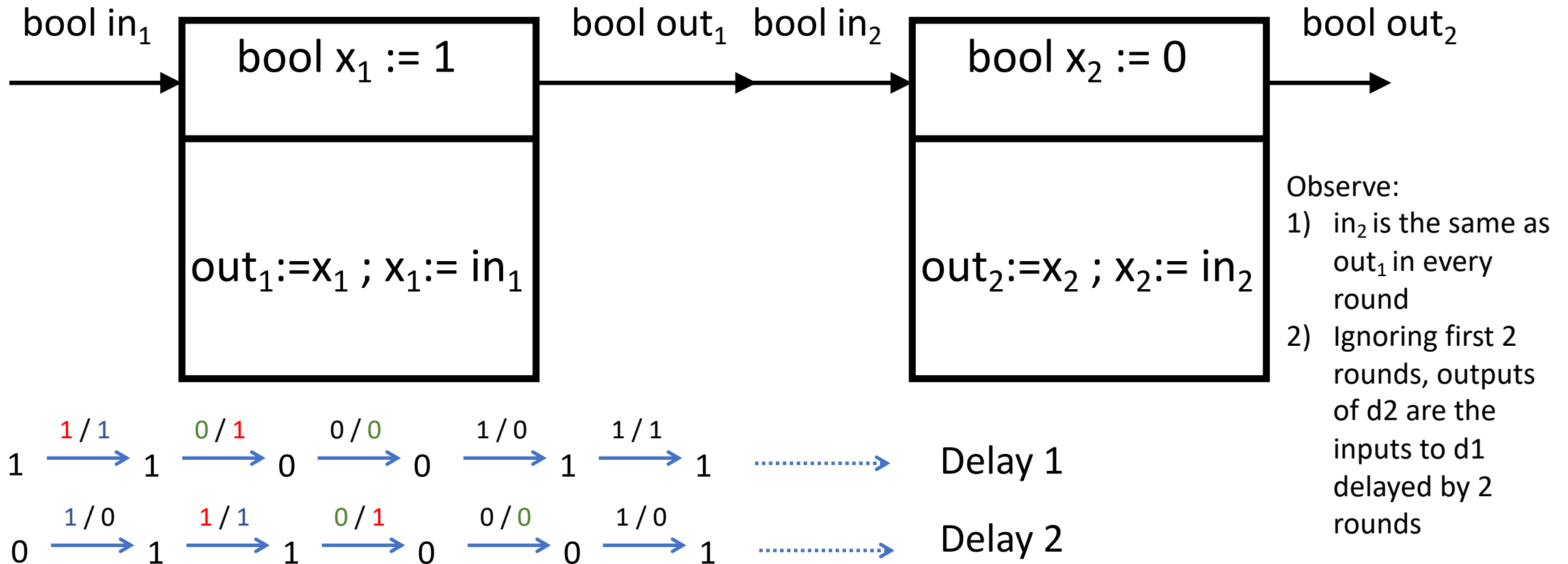
What does this model achieve?

bool in

int y:= 0

out:=y ;
if (in==0)
    y:= y + 1
else
    y:= y-1

int out

int c

bool d := 0

if (c $\geq$ 2)
    if (d != 0)
        warn:=1;
    else
        d := 1;
    end
else
    d := 0;
end

bool
warn
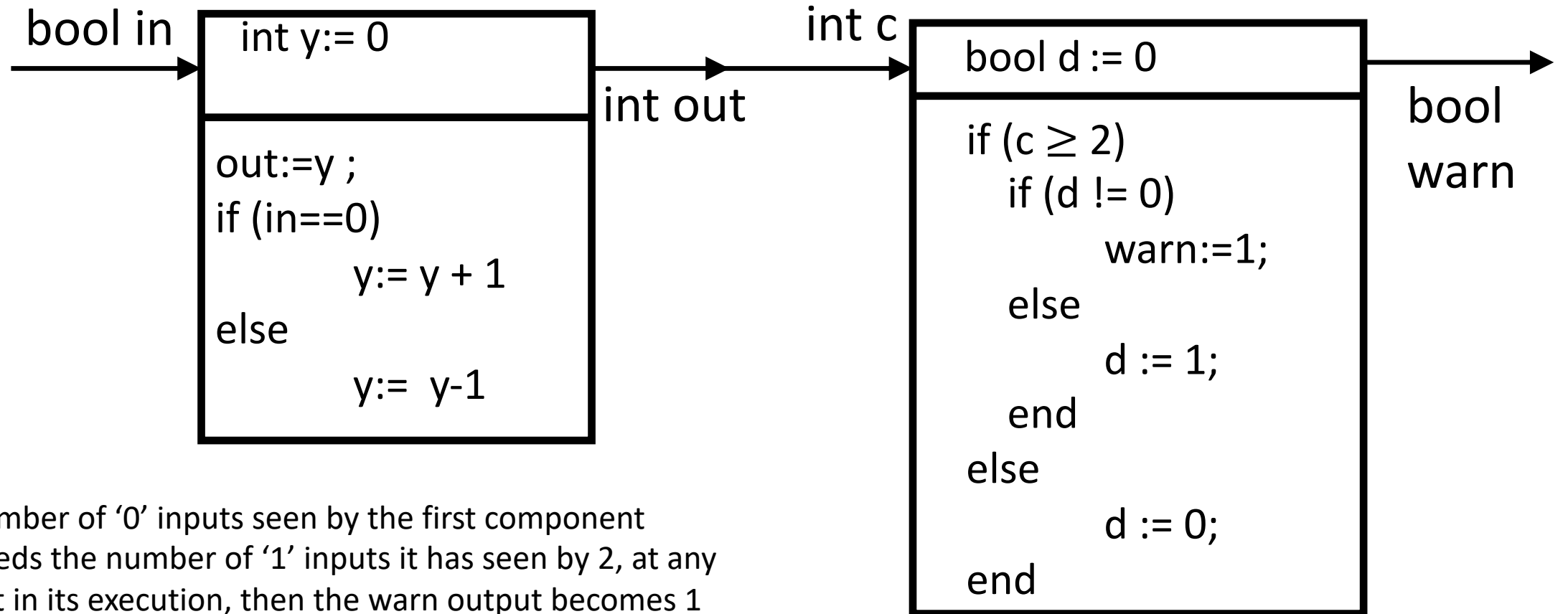
If number of '0' inputs seen by the first component exceeds the number of '1' inputs it has seen by 2, at any point in its execution, then the warn output becomes 1

Deterministic Component

▶ An SRC is deterministic if:
  ▸ It has a single initial state
  ▸ Updates ensure that for every state q and input i, there is a unique state q' and output o such that (q, i, o, q') is a transition

▶ Determinism means for same input sequence, you get same state/output sequence every single time

▶ Note:
  ▸ Nondeterminism is useful for modeling uncertainty/unknown and compactness
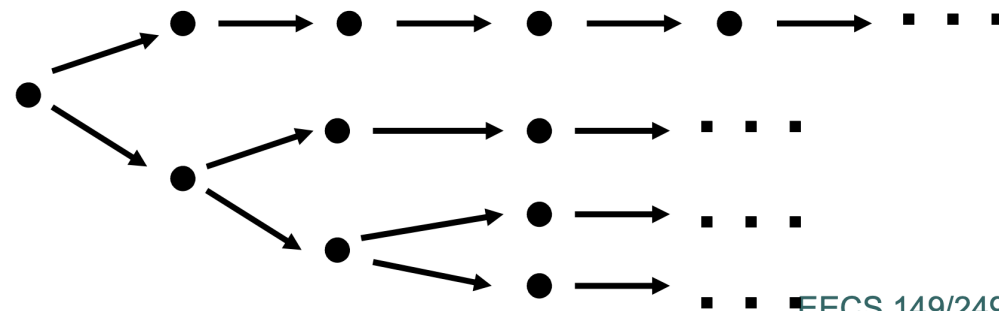
  ▸ It is not the same as probabilistic/random choice!

Extended State Machines

▶ Commonly used to describe behavior of MBD models
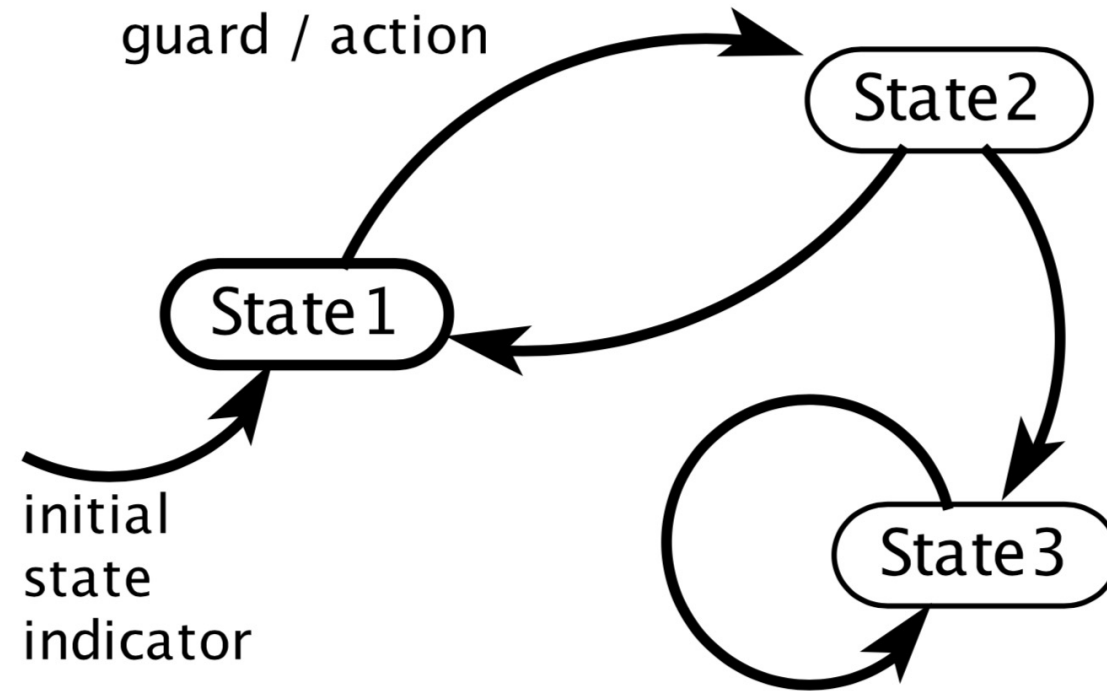
Extended State Machines

▶ Does this ESM remind you of something?
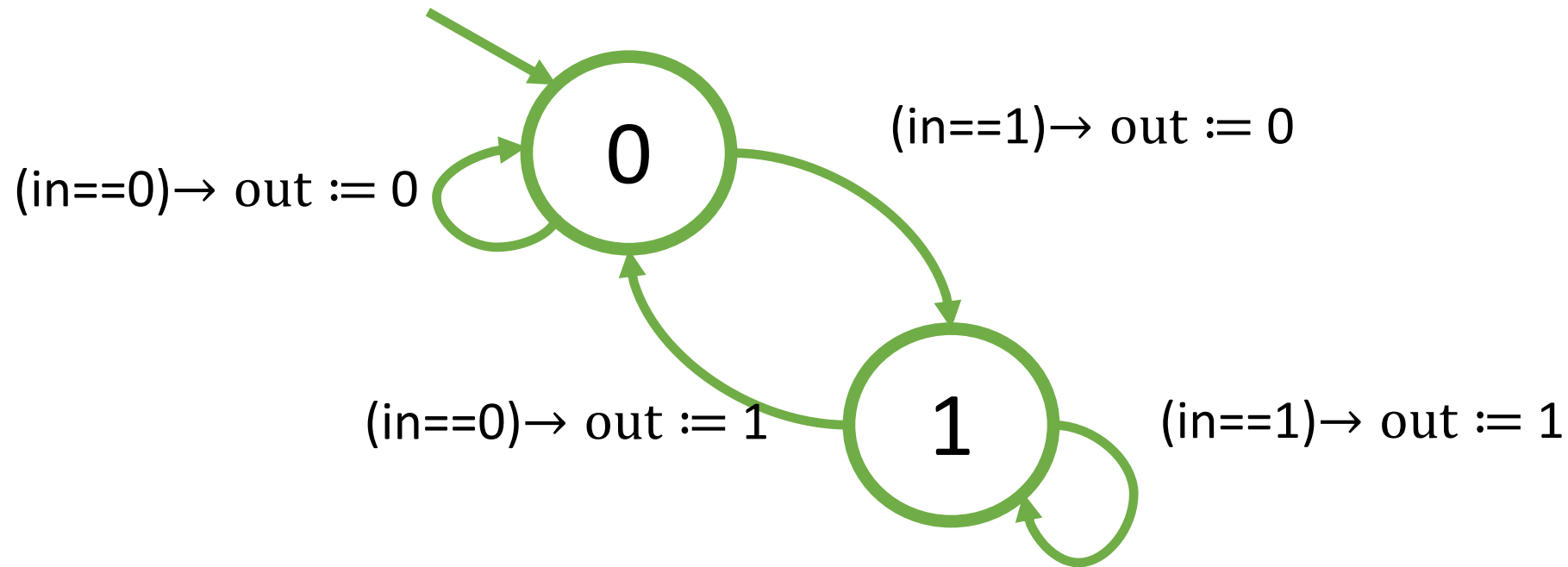
Component Switch: What does this do?

bool press

$\longrightarrow$

```
int x := 0
bool q := 0

switch (q)
  case 0: if (press==1) q:= 1
  case 1: if (press==0) & (x < 10)
              q:=1; x:= x+1
          elseif (press==1) or ( x >= 10)
              q:=0; x:= 0
          end
end
```

$\longrightarrow$
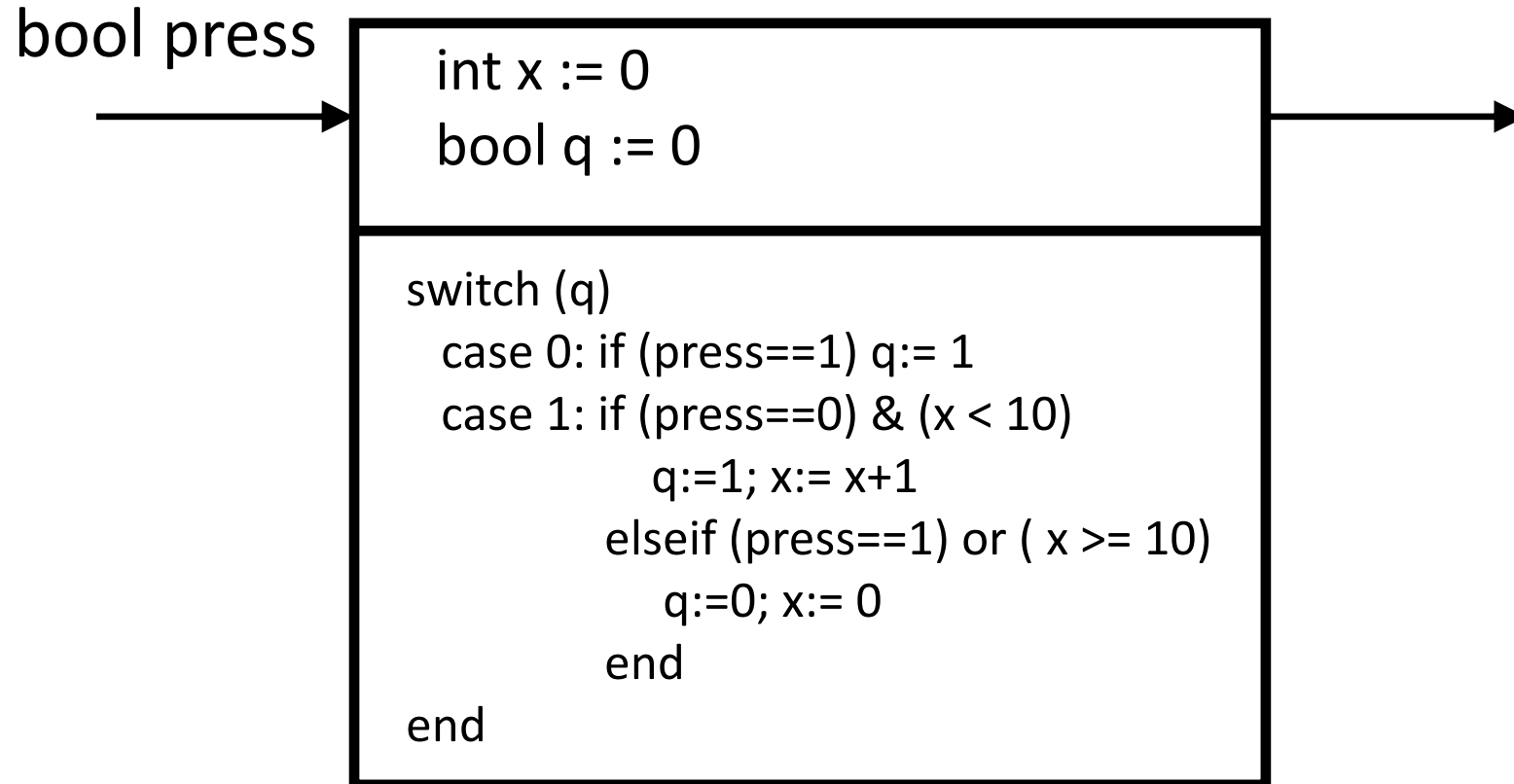
ESM corresponding to Switch SRC

int x := 0

off

(press==0)?

(press==1)?

on

(press==1) | (x≥10)
→ x := 0

(press==0) & (x<10)
→ x := x + 1

q = 0 : off
  = 1 : on
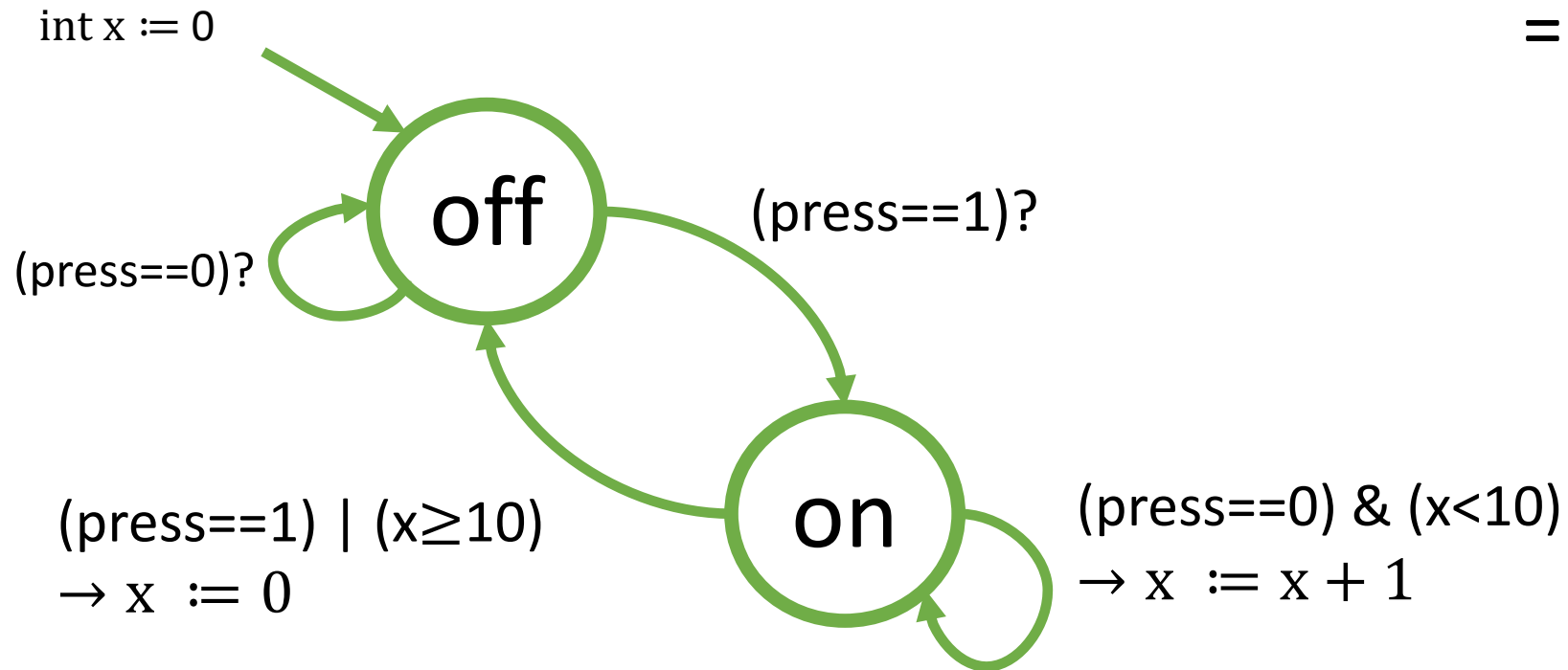
ESM notation
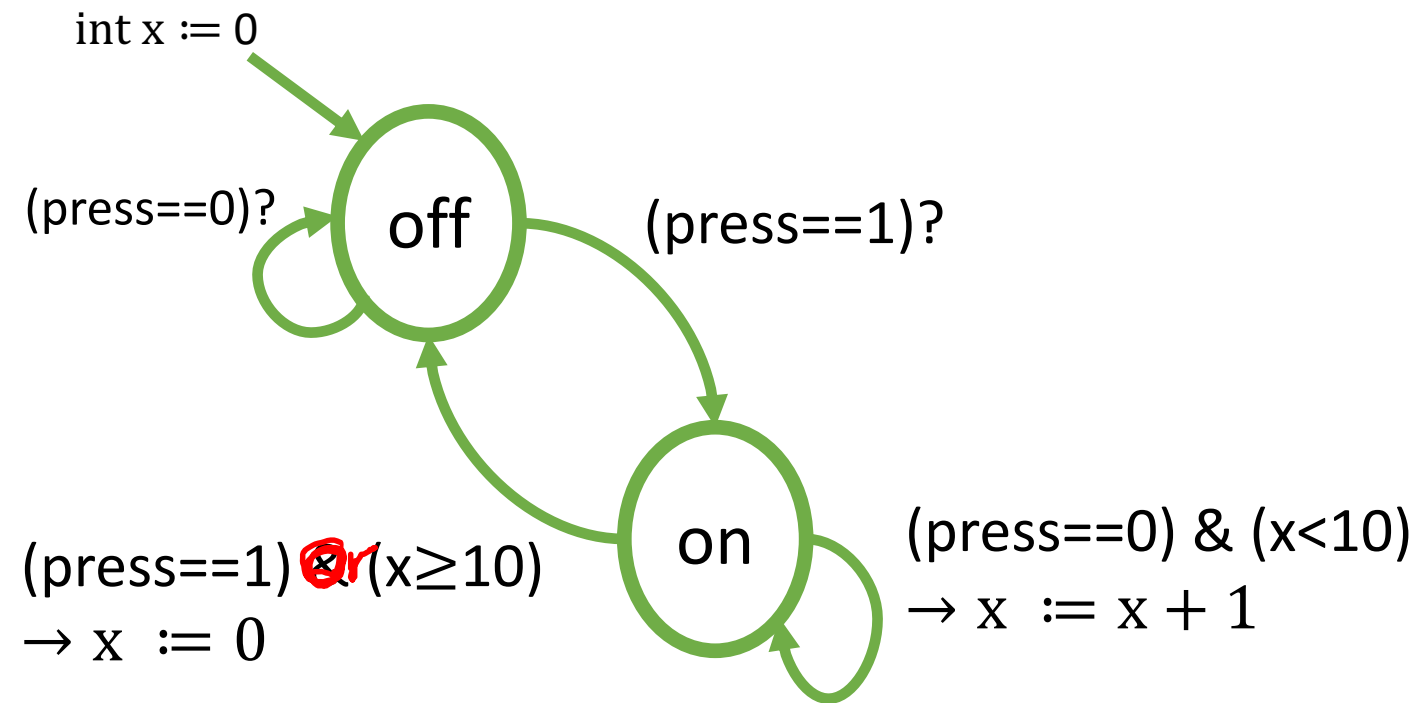
- Implicit variable called "mode" that is a *discrete* state variable over some finite enumeration. Here: {on, off}

- SRC transition may correspond to mode-switch

- Each mode-switch has guard/update. Example:
  - Guard: (press==0) & (x<10) and
  - Update: x:= x+1

ESM execution

int x := 0

(press==0)?

off

(press==1)?

(press==1) or (x≥10)
→ x := 0

on

(press==0) & (x<10)
→ x := x + 1
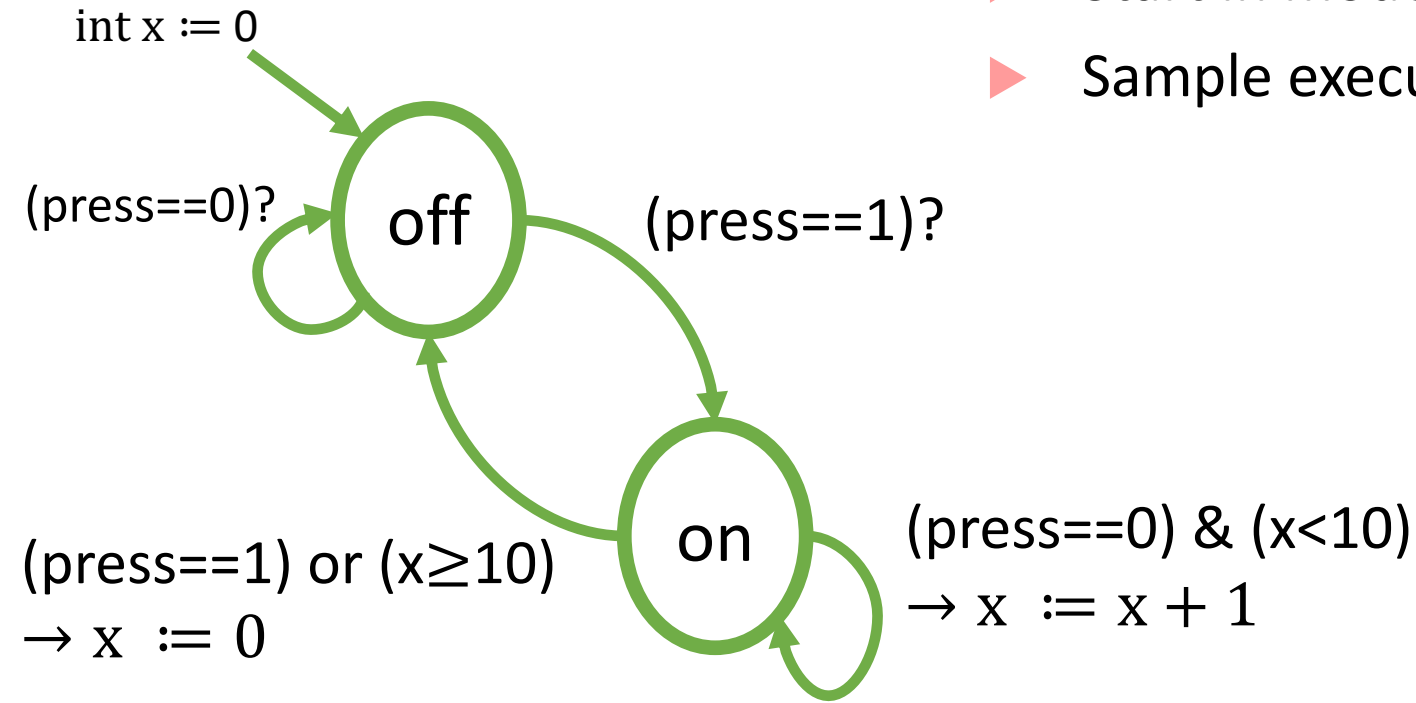
▶ Start in mode off; initial state = (off,0)

▶ Sample executions:

$$(off, 0) \qquad (off, 0)$$
$$\downarrow 0 \qquad\qquad \downarrow 0$$
$$(off, 0) \qquad (off, 0)$$
$$\downarrow 1 \qquad\qquad \downarrow 1$$
$$(on, 0) \qquad (on, 0)$$
$$\downarrow 0 \qquad\qquad \downarrow 0$$
$$(on, 1) \qquad (on, 1)$$
$$\vdots \qquad\qquad \vdots$$
$$\downarrow 0 \qquad\qquad \downarrow 0$$
$$(on, 10) \qquad (on, 5)$$
$$\downarrow 0 \qquad\qquad \downarrow 1$$
$$(off, 0) \qquad (off, 0)$$

ESM transitions could be nondeterministic!

int x := 0

(press==0)?

off

(press==1)?

on

(press==1) or (x≥10)
→ x := 0

(press==0) & (x≤10)
→ x := x + 1
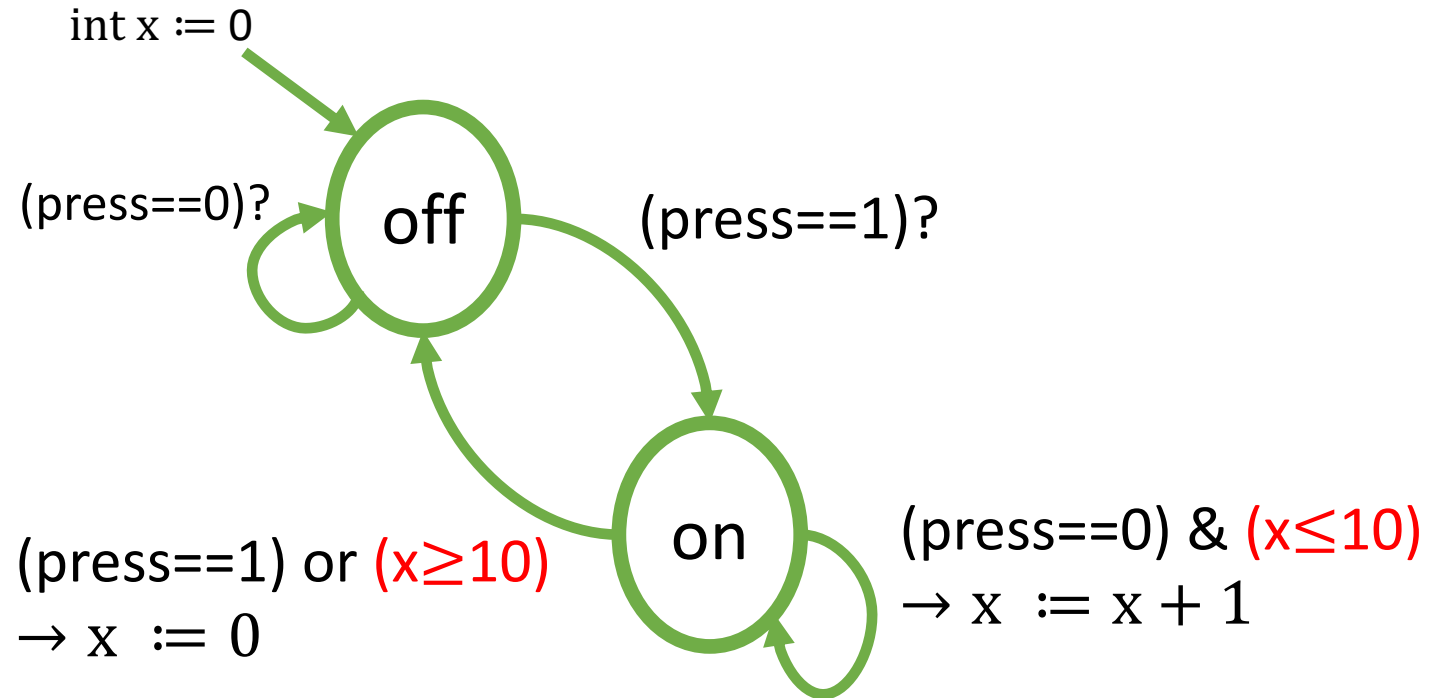
Event-triggered Components

▶ What to do if we want some components to *not* participate in some rounds?

▶ Event is a special input/output variable, which can be *absent* or *present*

▶ Event variable has value only if it is *present*

▶ Syntax:

e?	True if e is present
e!a	e gets the value of the assignment a

Event-triggered Copy

event(bool) out

nat x := 0

event(bool) in

if in? then
  {out!in; x:=x+1}
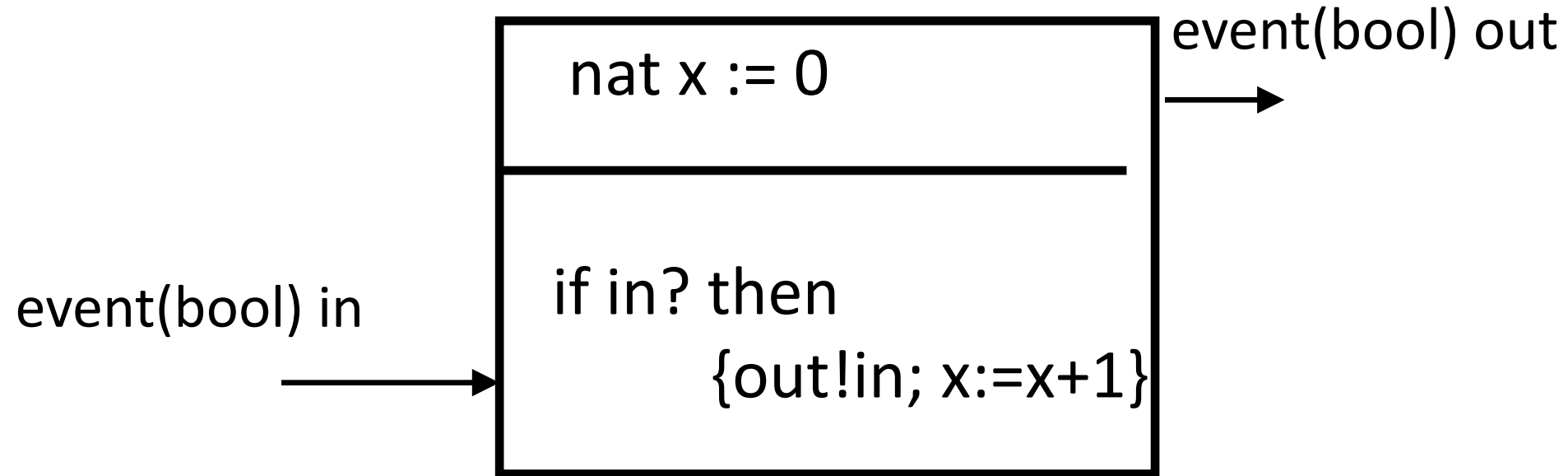
Event-triggered ClockedCopy

bool in →

event(bool) flag →

event(bool) clock →

bool x := 0

if clock? then
  flag!x; x:=in
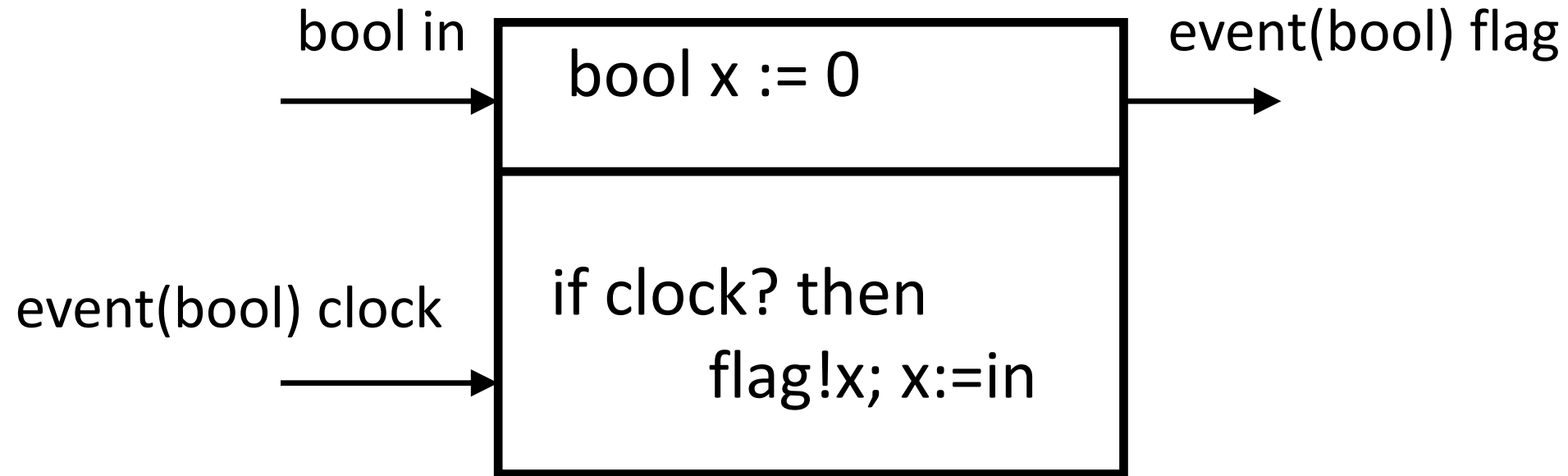
Event-triggered Components

▶ No need to execute in a round where triggering events are absent

event(bool) sec ⟶

```
nat x := 0
─────────────────
if sec? then
    x:=x+1;
    if (x==60)
      min! 1;
       x:=0
    end
end
```

⟶ event(bool) min
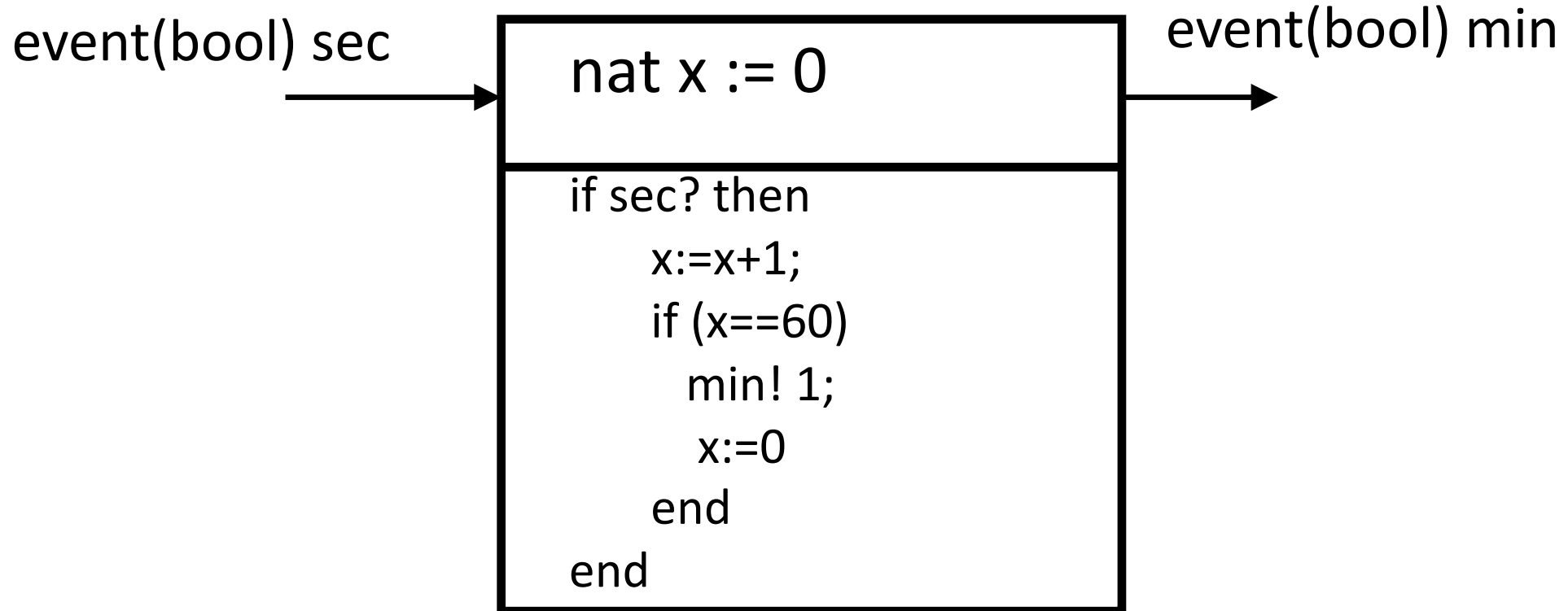
Finite-state Components

▶ Component is finite state if all variables are over finite types

bool in → [bool x := 0 | out:=x ; x:= in] → bool out   **FS**

bool in → [int y:= 0 ; bool z:= 0 | out:=y ; if (z==0) y:= y + 1 else y:= y-1 ; z := in] → int out   **Not FS!**
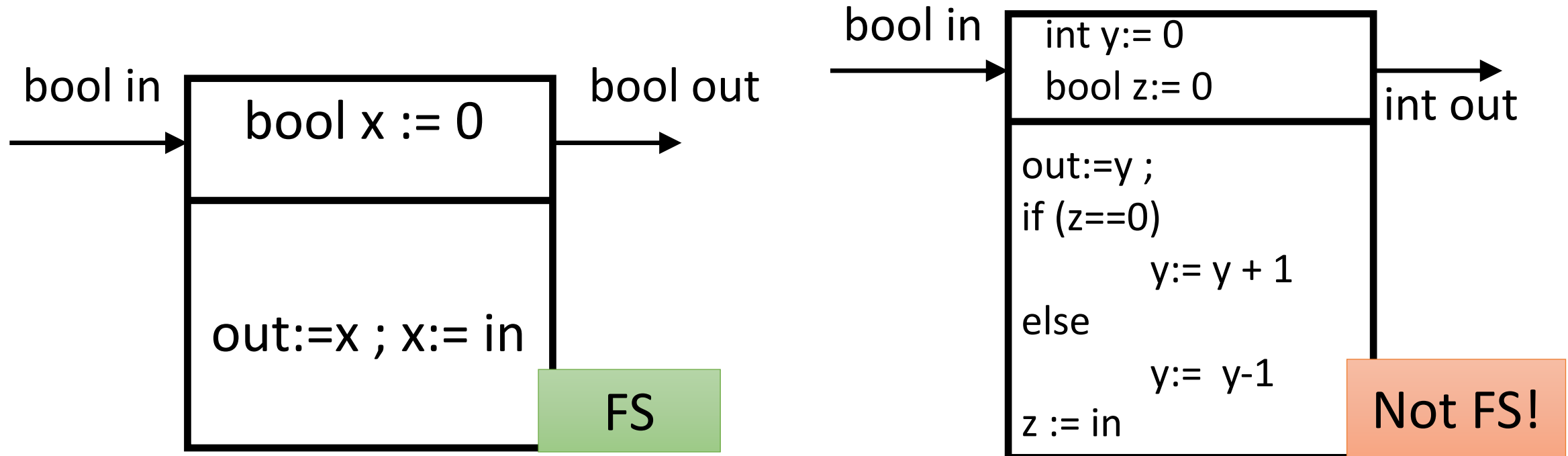
Cruise Controller Example
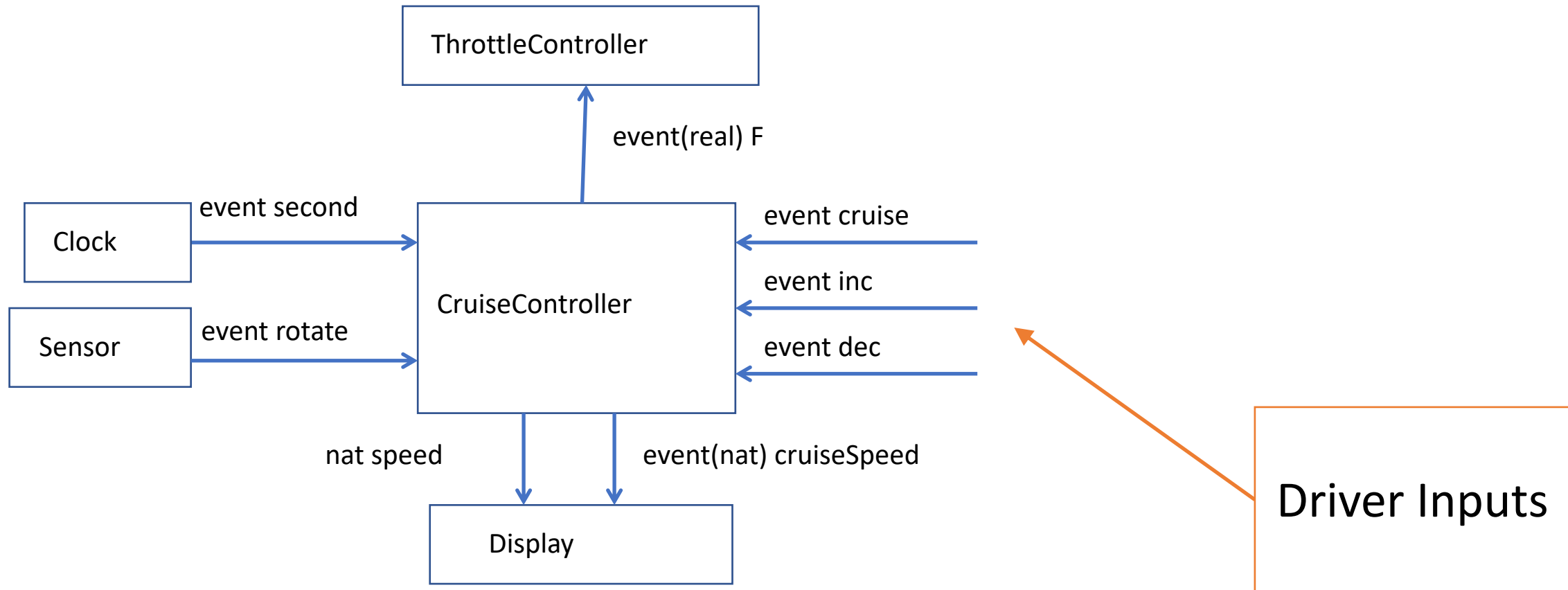
Sensors

- Rotation Sensor: Wheel speed sensor or vehicle speed sensor
- Type of a tachometer
- Counts number of rotations per second and as the wheel radius is known, can compute the linear speed of the car

AC current output

Induction coil
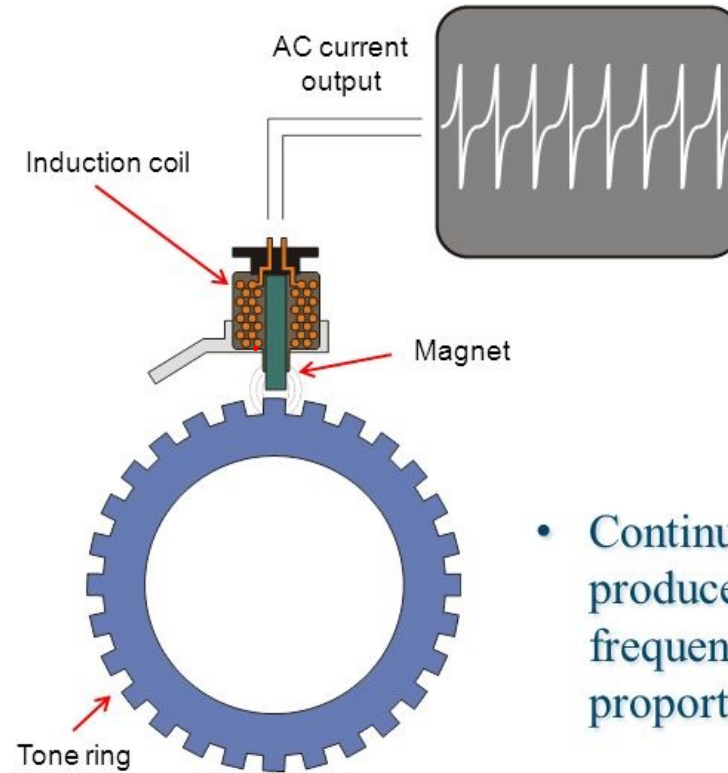
Magnet

Tone ring

- The ABS wheel speed sensor generates a small electrical pulse whenever a tooth on the tone ring moves through the magnetic field of the pick up coil

- Continuous rotation of the tone ring produces an AC current whose frequency – measured in Hertz – is proportional to wheel speed

(From Porter and Chester Institute slides on Google Image Search)

Actuator

ThrottleController

event(real) F

Clock — event second → CruiseController ← event cruise

Sensor — event rotate → ← event inc

← event dec

nat speed   event(nat) cruiseSpeed

Display
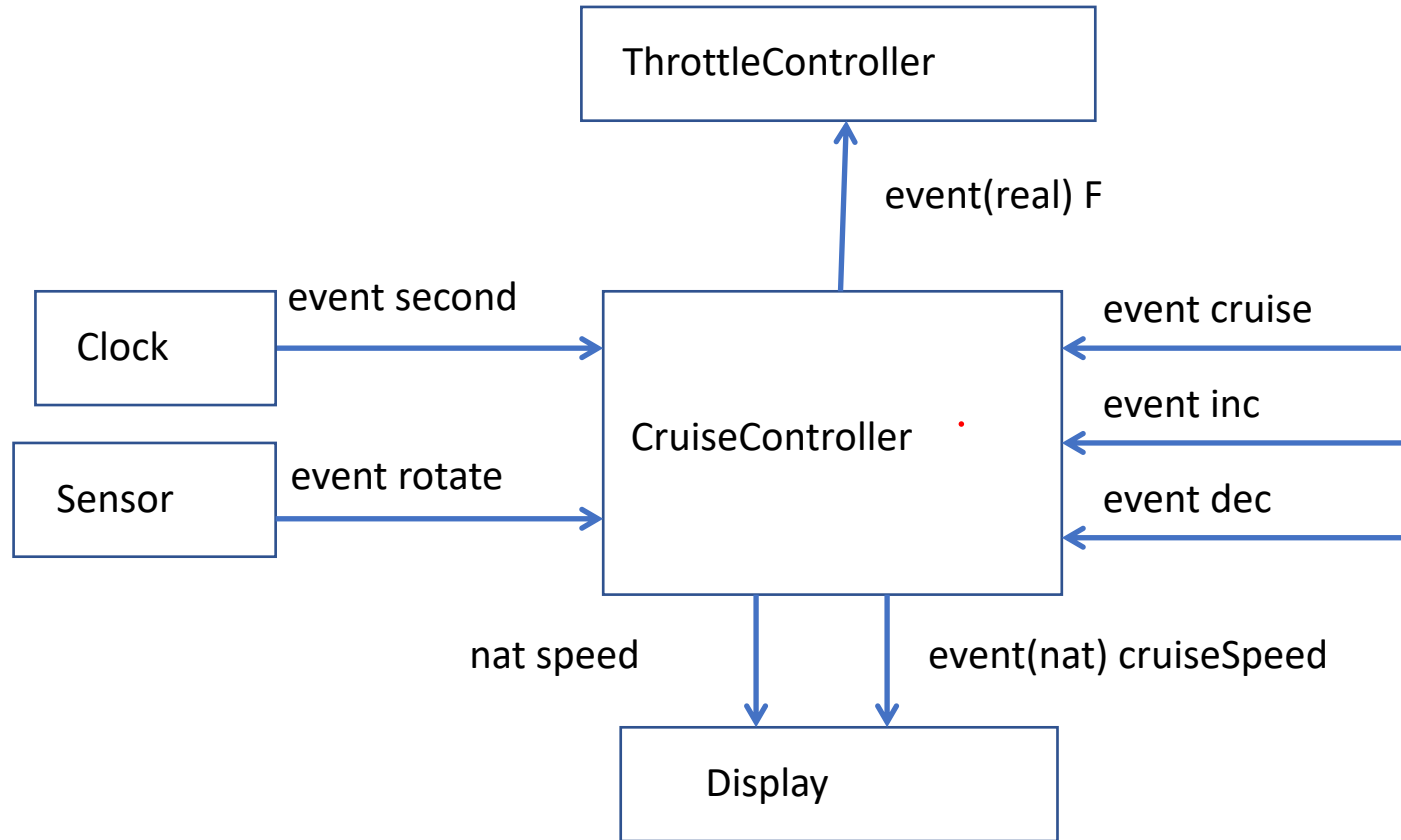
▶ **ThrottleController is an actuator that gets a force/torque required to adjust the throttle plate which leads to tracking the desired speed**

Decomposing CruiseController further

MeasureSpeed SRC

event rotate

event second

nat speed

```
nat count := 0, s:=0

if rotate?
    count:=count + 1;
if second?
    s:= round( K* count);
    count:=0;
speed:=s
```
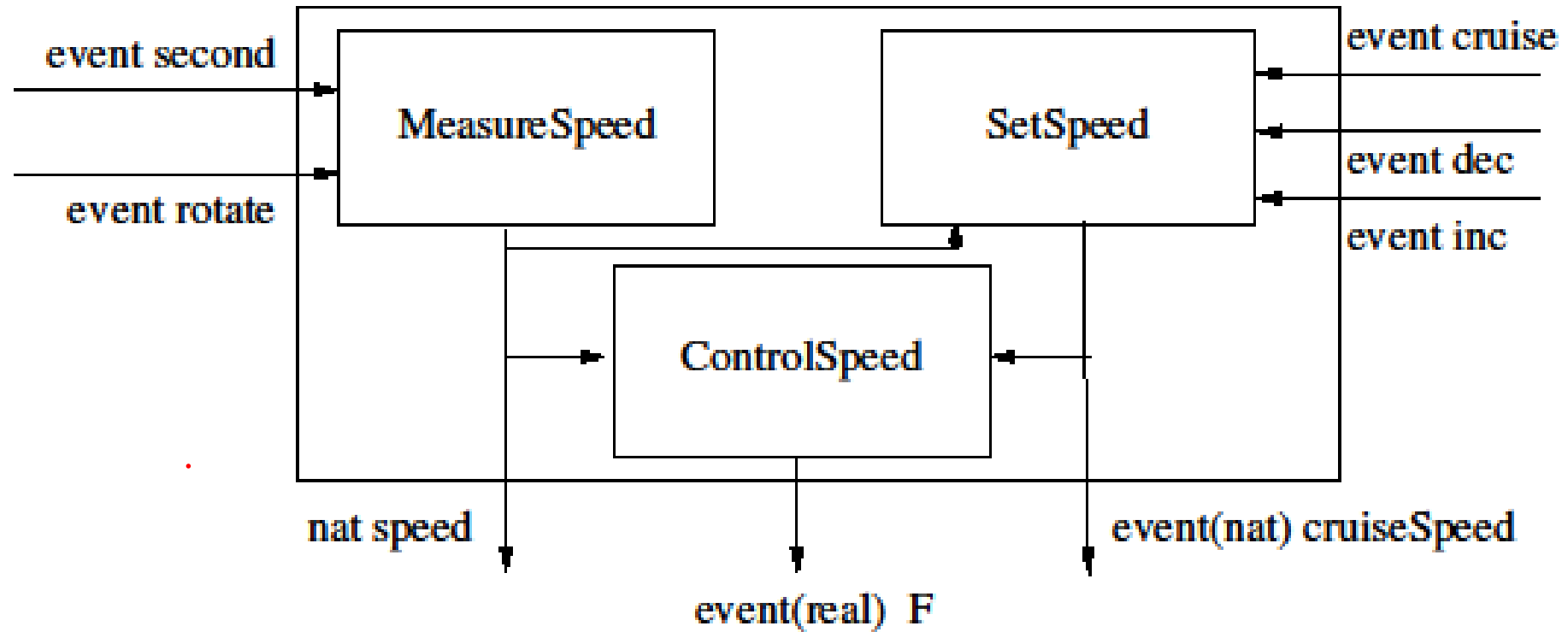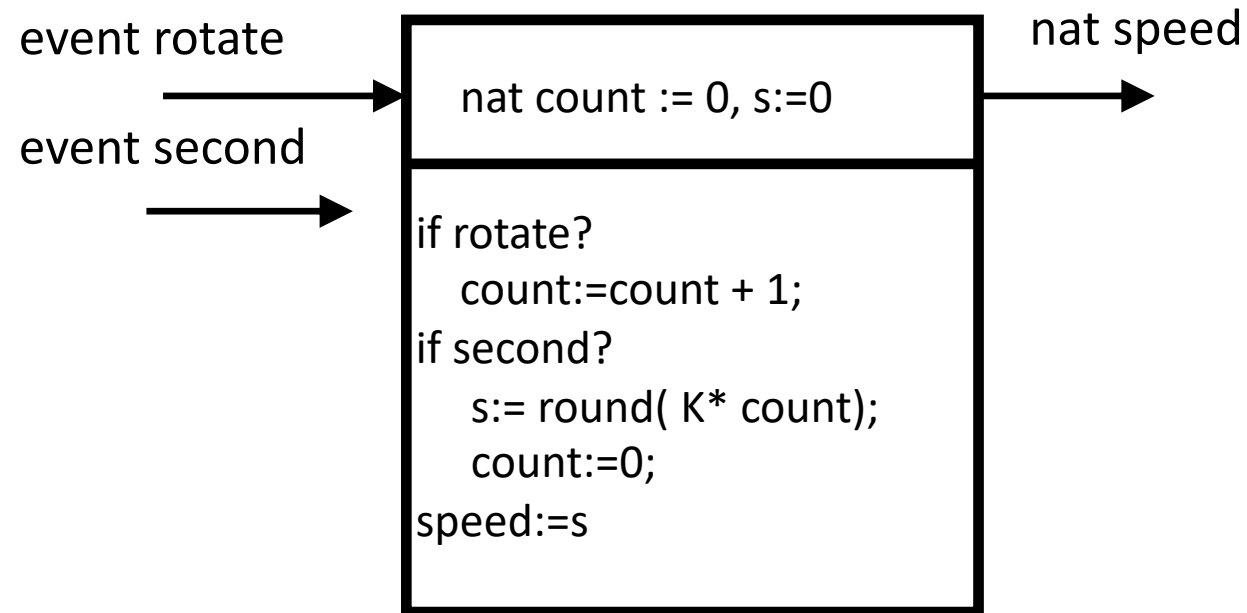
MeasureSpeed SRC

Asynchronous Components

Asynchrony

▶ Synchrony: All components execute in a sequence of rounds in lock-step

▶ Asynchrony: No lock-step computation!

▶ Natural model for networked, distributed communicating components executing independently and at possibly different speeds

▶ As there is no central, global clock, explicit coordination is required between components

▶ Examples:
  ▸ Processes in distributed computation, multiple threads in any modern OS
  ▸ Interrupt-driven processing

Asynchronous Reactive Component Example

bool in →

$bool_\emptyset$ x := $\emptyset$

bool out →

$bool_\emptyset = bool \cup \{\emptyset\}$

T_{in}: x := in

T_{out}:
x ≠ $\emptyset$ → { out := x;
                          x := $\emptyset$ }

Tasks: T_{in}, T_{out}

Guarded Update

Asynchronous Reactive Component

bool in

$bool_{\emptyset}$ $x := \emptyset$

bool out

$T_{in}: x := in$
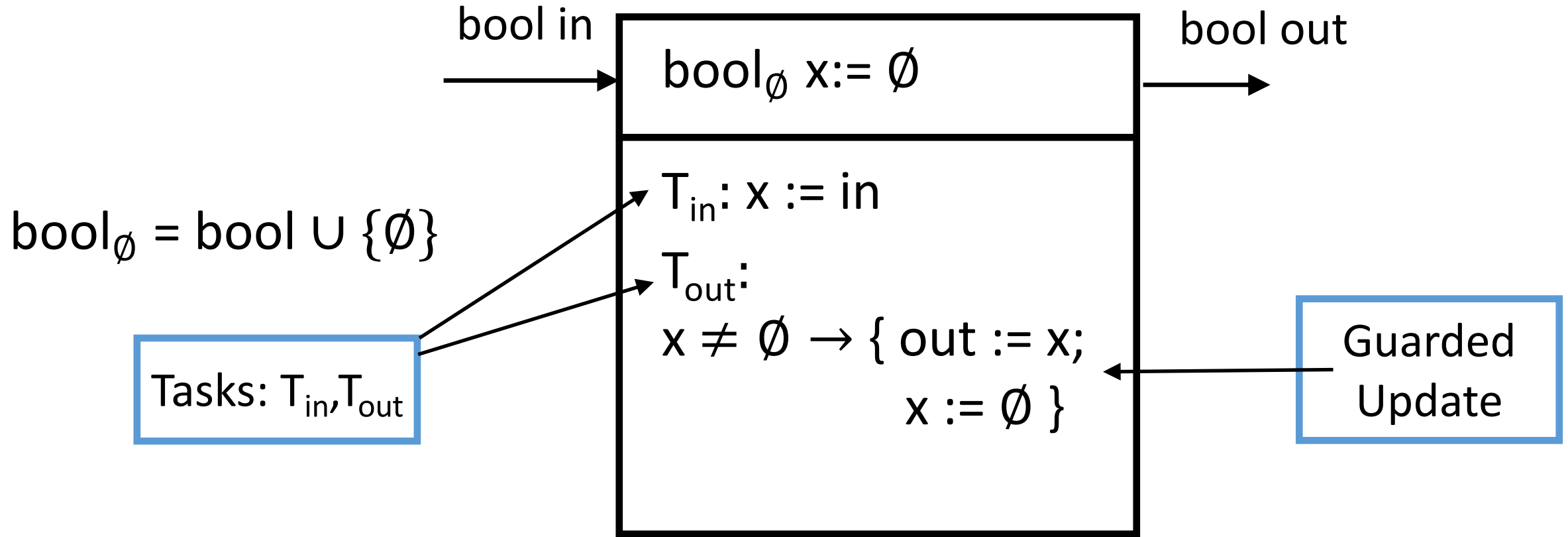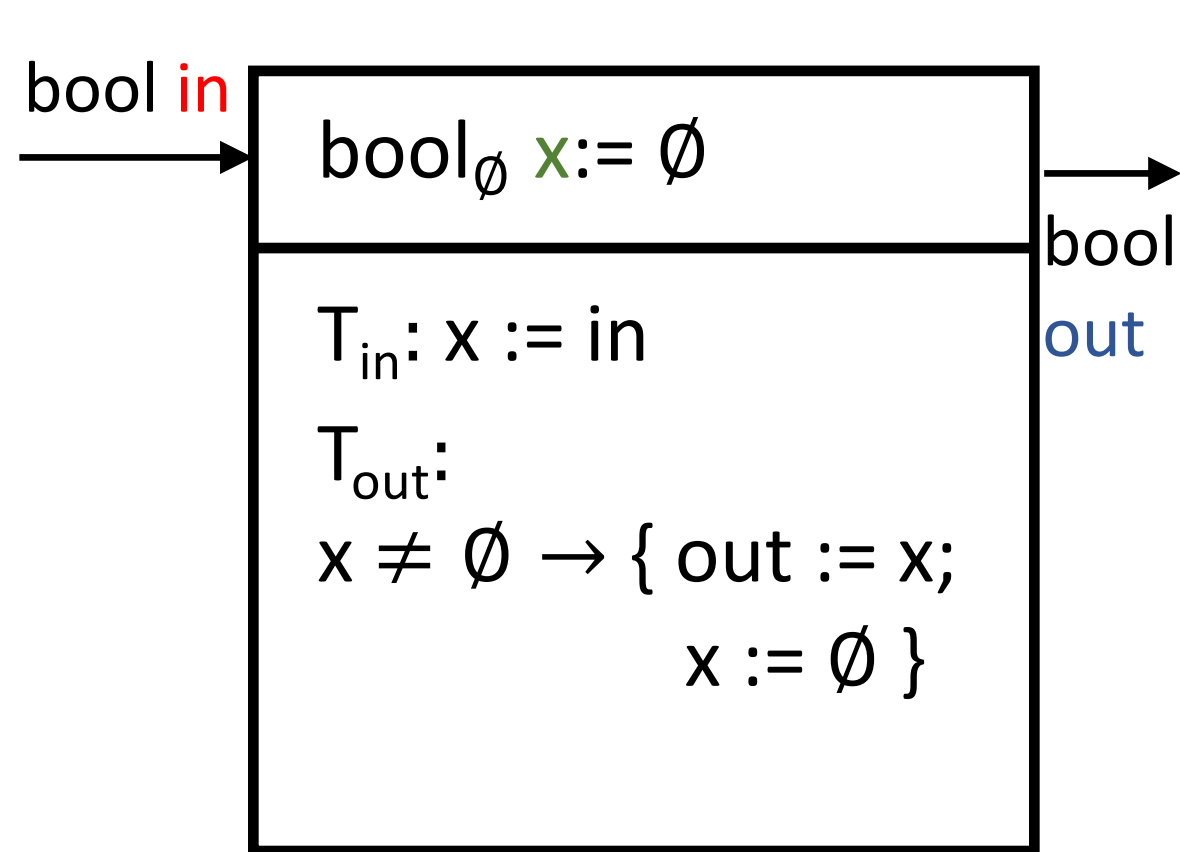
$T_{out}:$
$x \neq \emptyset \rightarrow \{ out := x;$
  $\qquad\qquad x := \emptyset \}$

▶ Input channel in of type bool

▶ Output channel out of type bool

▶ State variable x of type bool$+\emptyset$. The value $\emptyset$ indicates empty or null.

▶ x initialized to $\emptyset$

▶ Input task T_{in} reads input value into x

▶ Output task T_{out} produces output if x is not empty

Asynchronous Reactive Component Execution

▶ Execution Model: In each step only one task is executed

▶ Task can be executed only if it is enabled (i.e. if its guard condition is true)

▶ If multiple guard conditions are true, one task is nondeterministically executed

▶ Sample execution:

$$\emptyset \xrightarrow[\text{T}_{\text{in}}]{\text{in?0}} 0 \xrightarrow[\text{T}_{\text{out}}]{\text{out!0}} \emptyset \xrightarrow[\text{T}_{\text{in}}]{\text{in?1}} 1 \xrightarrow[\text{T}_{\text{in}}]{\text{in?0}} 0 \xrightarrow[\text{T}_{\text{out}}]{\text{out!0}} \emptyset$$

bool in

bool out

$$\text{bool}_\emptyset \quad x := \emptyset$$

$T_{\text{in}}: x := \text{in}$

$T_{\text{out}}:$

$x \neq \emptyset \rightarrow \{ \text{out} := x;$

$x := \emptyset \}$
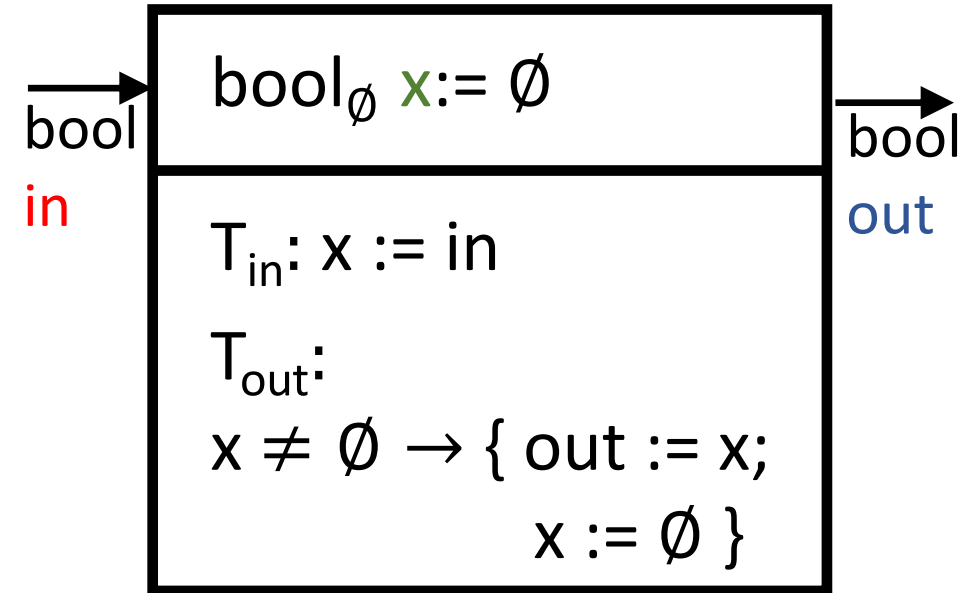
Buffer

Example: Asynchrony + Nondeterminism

int x:= 0, y:= 0
T_x: x := x+1 T_y: y:= y+1

- ARC may have no inputs or outputs, just internal tasks
  - Update may have no guards
- In each step, execute T_x or T_y
- Sample execution:

$$(0,0) \xrightarrow[T_y]{} (0,1) \xrightarrow[T_y]{} (0,2) \xrightarrow[T_x]{} (1,2) \xrightarrow[T_y]{} (1,3)$$

- Interleaved model of concurrency
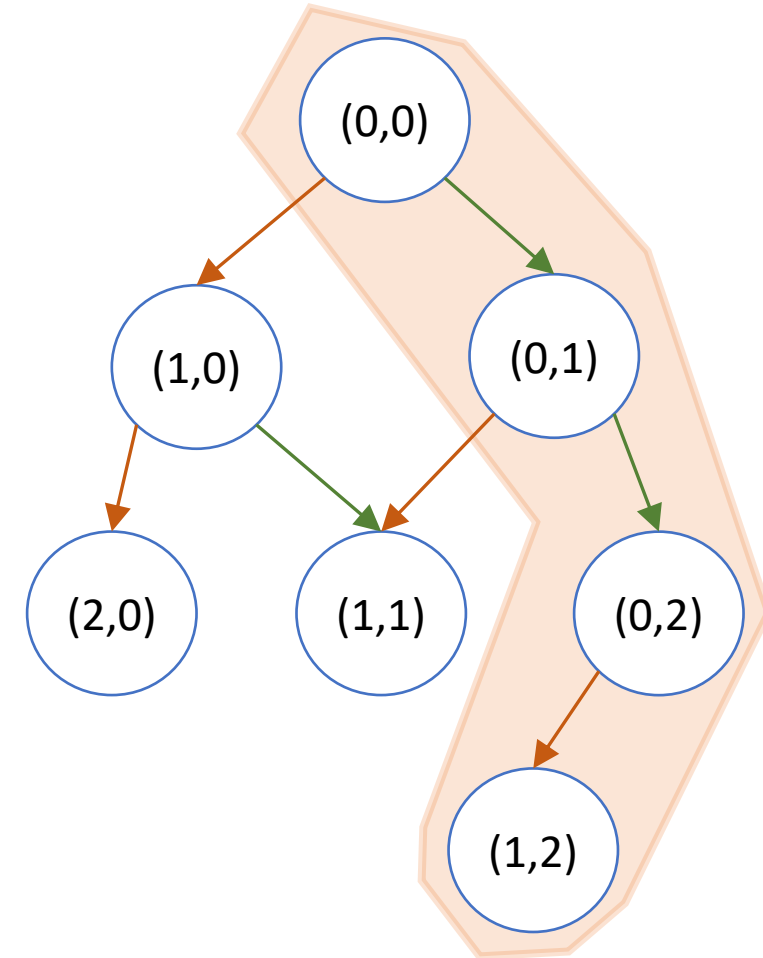
Asynchronous Process/Reactive Component

$bool_\emptyset$ x := $\emptyset$

bool
in

T_{in}: x := in

T_{out}:
x $\neq$ $\emptyset$ $\rightarrow$ { out := x;
                    x := $\emptyset$ }

bool
out
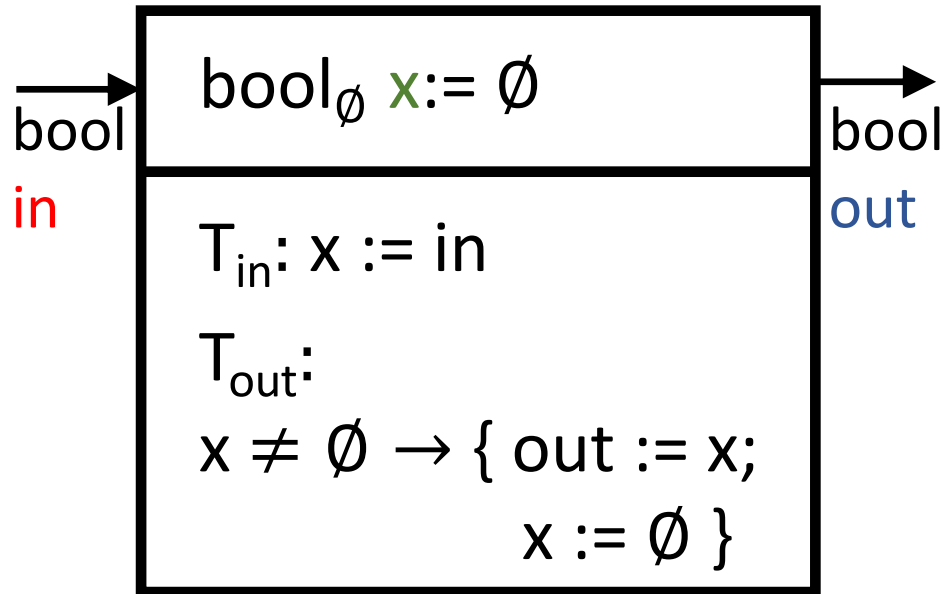
- ▶ Set of input channels: I
  - ▶ ESM representation: in?v, where v is the value to be received
- ▶ Set of output channels: O
  - ▶ ESM representation: out!v, where v is the value to be written
- ▶ Set of state variables X
- ▶ Initialization Init which maps state variables to initial values

Updates are different from SRCs!

Input Task defines updates of the form: **G → x:= E(X,in)**

▶ Guard condition G: some expression over *only* state variables X; input task can be executed only if G is true

▶ For each in in I, we associate a read-set (X ∪ {in}): variables that can appear in E for input task associated with in (rationale: can read value on in only if that task is enabled)

▶ Defines a set of input actions of the form: q $\xrightarrow{in?v}$ q'

  ▸ where q is value of state variables before update, and q satisfies G

  ▸ value of state variables after update is q' = E(X↦q, in↦v)

Updates are different from SRCs!

Output Task: defines updates of the form: **G → out := E(X)**

▶ Guard condition G: some expression over **only** variables in X; output task can be executed only if G is true

▶ Any expression containing only state variables can appear in E

▶ Defines an output action of the form $q \xrightarrow{out!v} q'$

  ▸ where q is value of state variables before update, and q satisfies G

  ▸ value of state variables after update is q'

  ▸ value v is output on channel out

Updates are different from SRCs!

Internal Task: defines updates of the form: **G → x := E(X)**

▶ Guard condition G: some expression over **only** variables in X; internal task can be executed only if G is true

▶ Any expression containing only state variables can appear in E, only state variables appear on LHS

▶ Defines an internal action of the form q$\xrightarrow{\varepsilon}$q'

  ▸ where q is value of state variables before update, and q satisfies G

  ▸ value of state variables after update is q'

  ▸ No input is read or output is produced!

Asynchronous Example

queue(bool) $x_1 := \emptyset$, $x_2 := \emptyset$

bool in_1

bool in_2

bool out

T_{in1}: $\neg$Full(x_1) $\rightarrow$ Enqueue(x_1,in_1)

T_{in2}: $\neg$Full(x_2) $\rightarrow$ Enqueue(x_2,in_2)

T_{out1}: $\neg$Empty(x_1) $\rightarrow$ out := Dequeue(x_1)

T_{out2}: $\neg$Empty(x_2) $\rightarrow$ out := Dequeue(x_2)
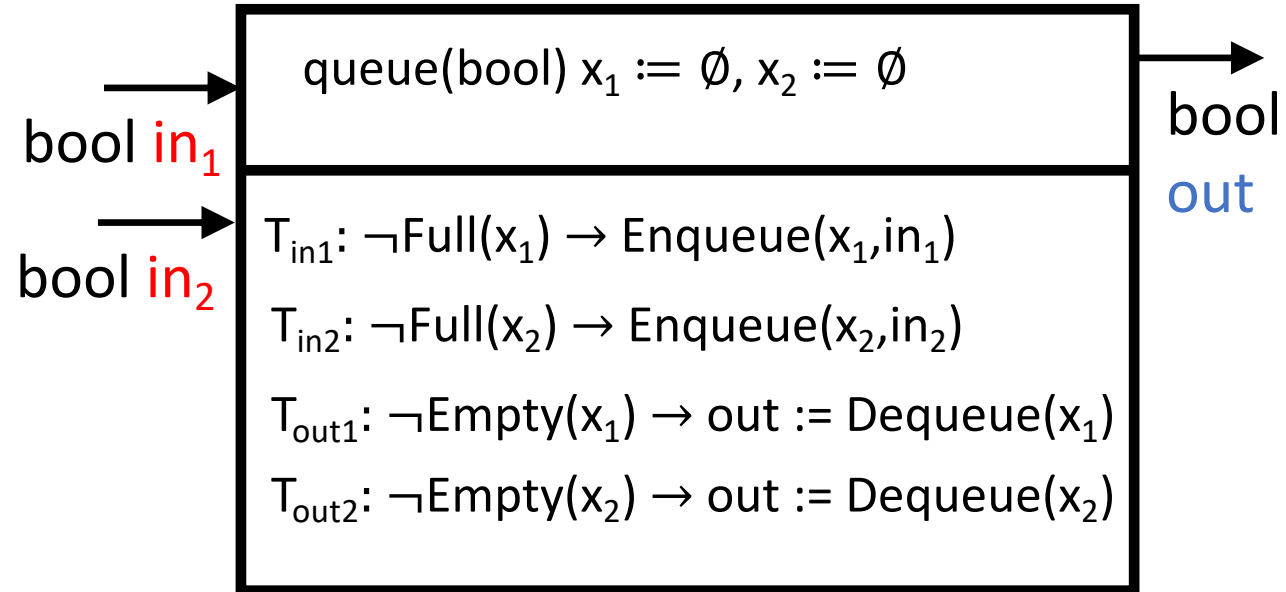
Asynchronous Processes can also be represented with extended state machines

Asynchronous Merge: Sequence of Actions

bool in_1

bool in_2

bool out

queue(bool) $x_1 := \emptyset$, $x_2 := \emptyset$

T_{in1}: $\neg$Full(x_1) $\rightarrow$ Enqueue(x_1, in_1)

T_{in2}: $\neg$Full(x_2) $\rightarrow$ Enqueue(x_2, in_2)

T_{out1}: $\neg$Empty(x_1) $\rightarrow$ out := Dequeue(x_1)

T_{out2}: $\neg$Empty(x_2) $\rightarrow$ out := Dequeue(x_2)

$(\emptyset, \emptyset)$

T_{in1} in1?1

$(<1>, \emptyset)$

out!1

T_{out2}

$(<1>, <1>)$

T_{in2} in2?0

T_{out2} out!0

$(<1>, <0>)$

T_{in2}

in2?1

$(<1>, <0,1>)$
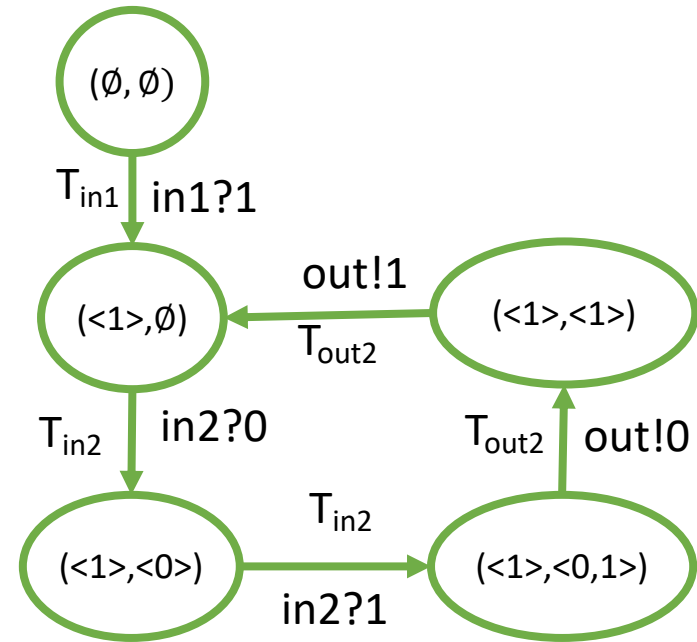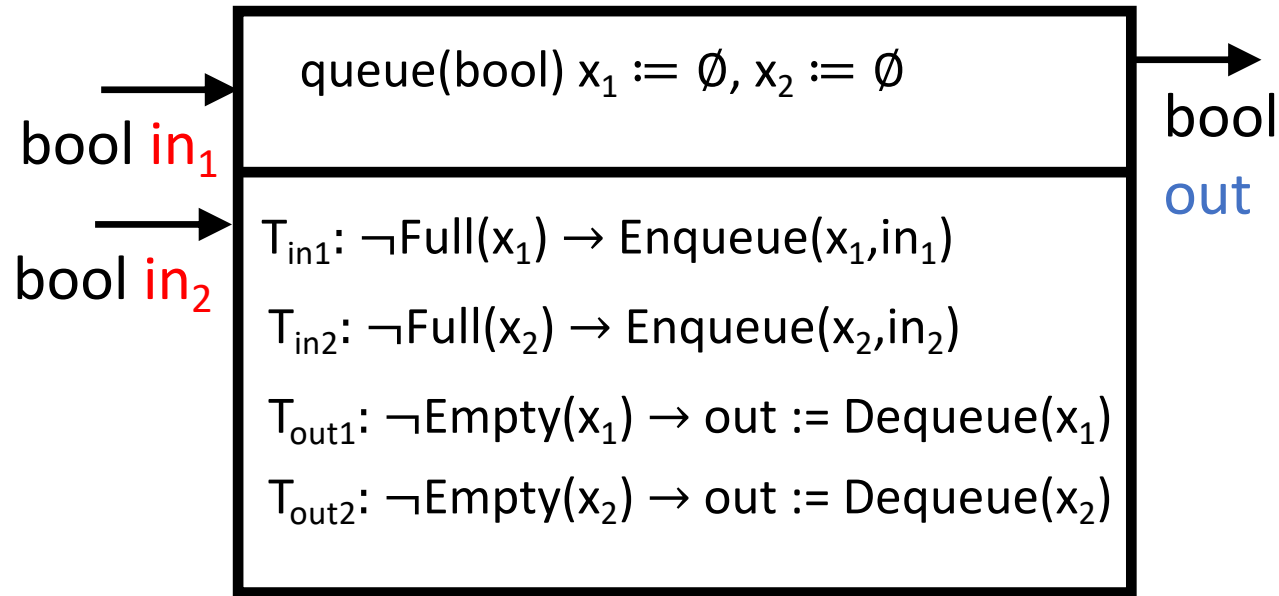
Asynchronous Processes can also be represented with extended state machines

Composing Asynchronous Processes

bool in

$bool_\emptyset\ x_1 := \emptyset$

$T_{in1}: x_1 := in$

$T_{out1}:$
$x_1 \neq \emptyset \rightarrow \{\ temp := x_1;$
$\qquad\qquad x := \emptyset\ \}$

Buffer

$bool_\emptyset x_2 := \emptyset$

bool out

$T_{in2}: x_2 := temp$

$T_{out2}:$
$x_2 \neq \emptyset \rightarrow \{\ out := x_2;$
$\qquad\qquad x_2 := \emptyset\ \}$
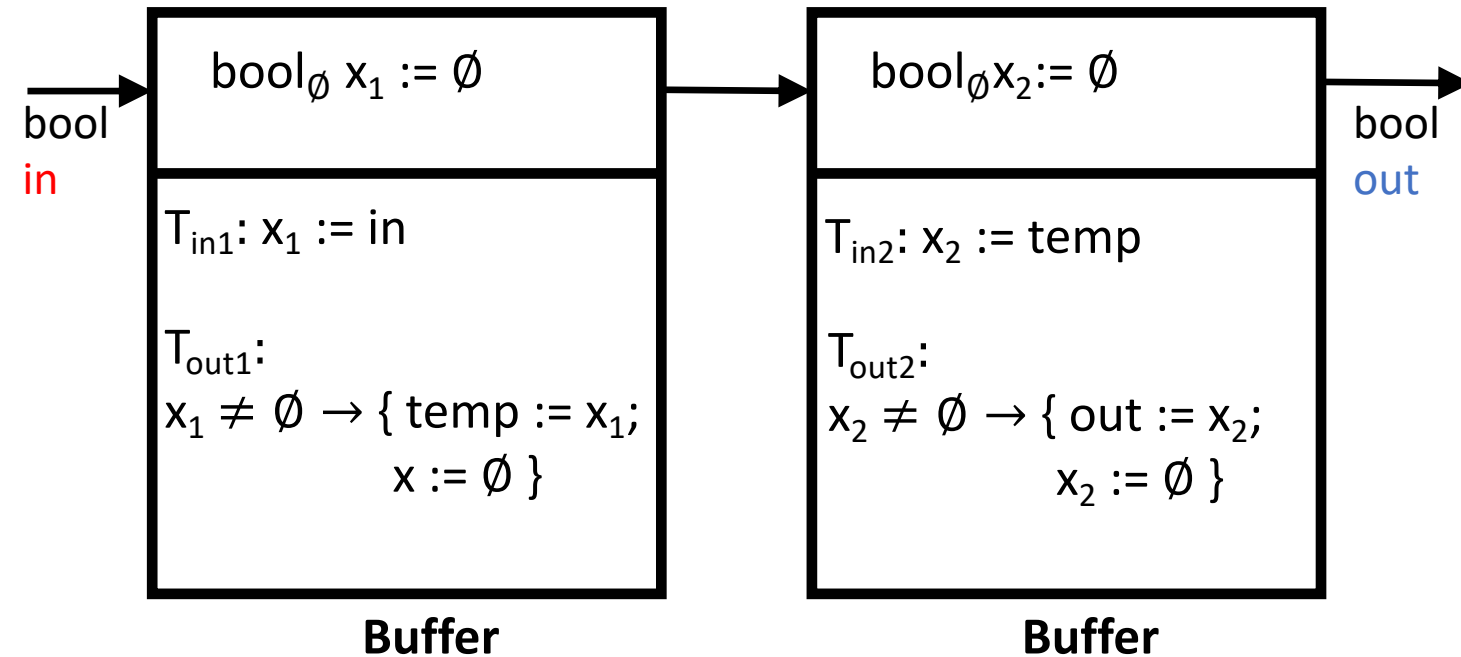
Buffer

▶ Parallel composition: Inputs, Outputs, States and Initialization similar to the synchronous case

▶ Input consumption needs to be synchronized with output production for the 'temp' variable

Composed DoubleBuffer

Buffer

$bool_\emptyset \ x_1 := \emptyset$

$T_{in1}: x_1 := in$

$T_{out1}:$

$x_1 \neq \emptyset \rightarrow \{ \ temp := x_1;$

$x_1 := \emptyset \ \}$

bool in

Buffer

$bool_\emptyset x_2 := \emptyset$

$T_{in2}: x_2 := temp$

$T_{out2}:$

$x_2 \neq \emptyset \rightarrow \{ \ out := x_2;$

$x_2 := \emptyset \ \}$

bool out

Double Buffer

$bool_\emptyset \ x_1 := \emptyset, \ x_2 := \emptyset$

$T_{in1}: x_1 := in$

$T_{out2}: x_2 \neq \emptyset \rightarrow \{ \ out := x_2;$

$x_2 := \emptyset \}$

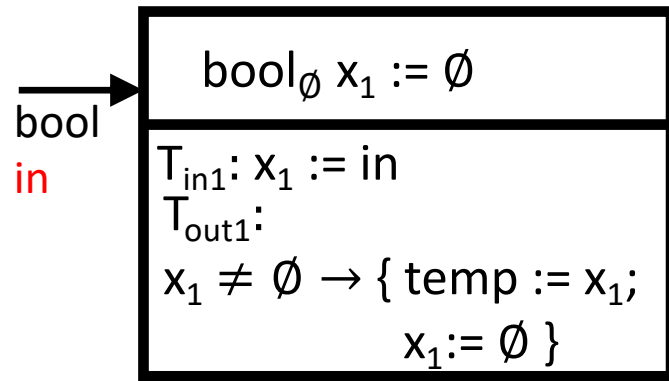$T_{out1in2}: x_1 \neq \emptyset \rightarrow \{ temp := x_1;$

$x_1 := \emptyset;$

$x_2 := temp \}$

bool in

bool out

bool temp
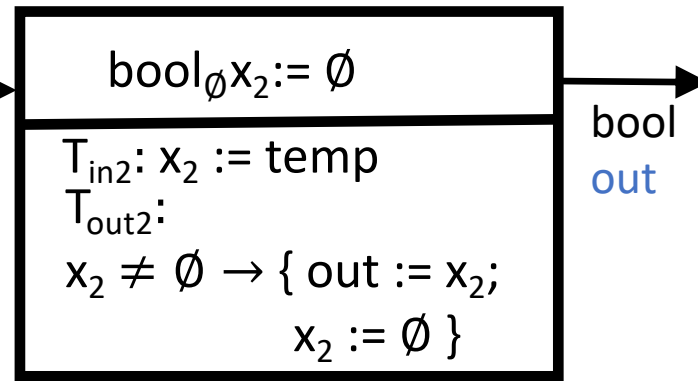
▶ Defining $P_1 \mid P_2$

▶ In each step only 1 task executes

▶ If y is an output channel of P_1 and input channel of P_2:

▶ Output task for $P_1: G_1 \rightarrow U_1$

▶ Input task for $P_2: G_2 \rightarrow U_2$

▶ Composition has output task for y with code: $G_1 \wedge G_2 \rightarrow U_1; U_2$

Output Hiding

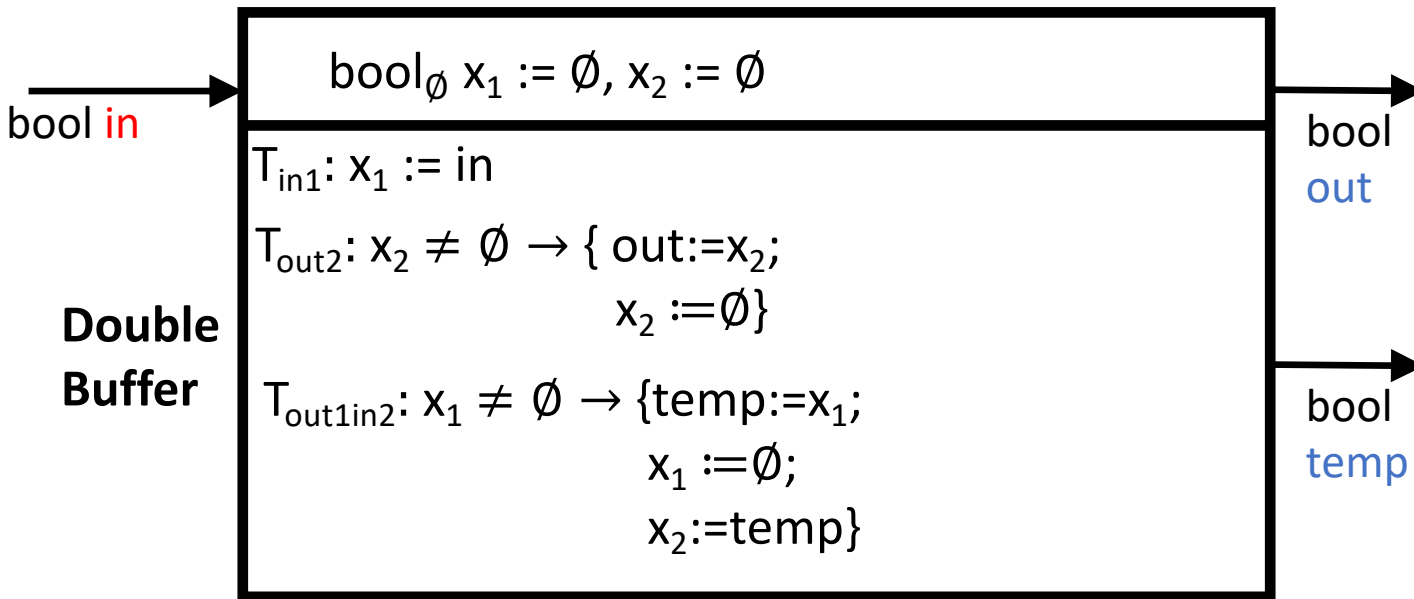Hiding ouput y: achieved by removing y from the set of output channels and turning each output task associated with the channel y into an internal task by declaring y to be a local variable

$bool_\emptyset$ $x_1 := \emptyset$, $x_2 := \emptyset$

bool in

bool out

Double Buffer

T_{in1}: $x_1 :=$ in

T_{out2}: $x_2 \neq \emptyset \rightarrow \{$ out:=x_2;
$x_2 := \emptyset \}$

$T_{out1in2}$: $x_1 \neq \emptyset \rightarrow \{$ local bool temp;
temp:=x_1;
$x_1 := \emptyset$;
x_2:=temp$\}$

bool temp

Blocking vs. Non-blocking Synchronization

int in

P1

T_{out}: tmp := in;

int tmp

int x := 0

T_{tmpe}: (x is even)→
x:= tmp

P2
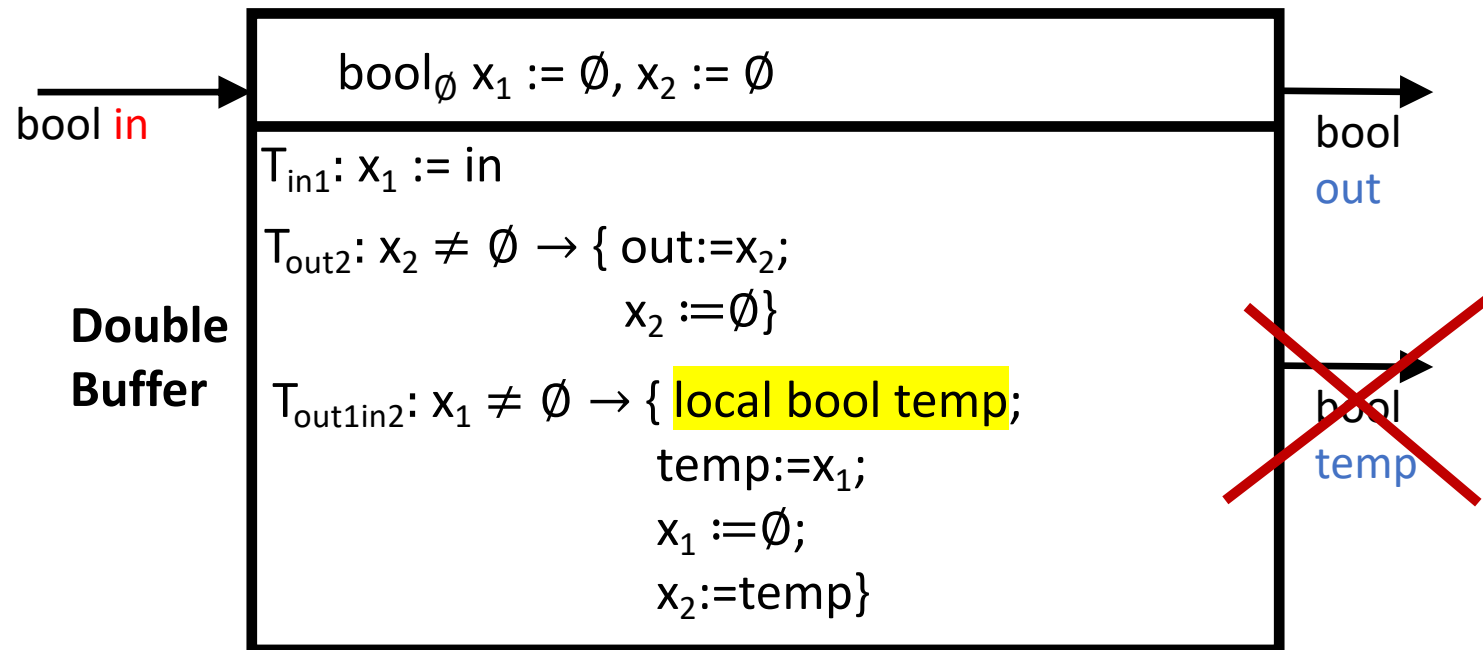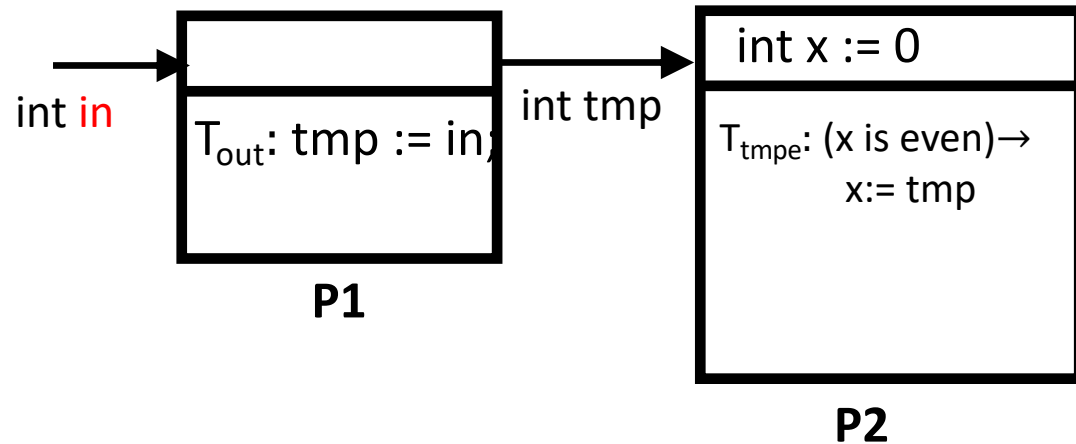
▶ Task T_{out} of P1 can *produce* a value on the output only if P2 has an input task that is enabled to *consume* the value with some input task

▶ In this example, once x becomes odd, P2 cannot consume (no enabled input task) and it **blocks** communication

▶ Process is **non-blocking** if for ∀ channel in and ∀ state s, at least one guarded update corresponding to input task for in is enabled

▶ Process is **non-blocking** if it is non-blocking on all channel in

Blocking vs. Non-blocking Synchronization in Buffer

Double Buffer

bool in →

→ bool out

$bool_\emptyset\ x_1 := \emptyset,\ x_2 := \emptyset$

T_{in1}: x_1 := in

T_{out2}: $x_2 \neq \emptyset \rightarrow$ { out:=x_2;
$\qquad\qquad\qquad\qquad x_2 :=\emptyset$}

$T_{out1in2}$: $x_1 \neq \emptyset \rightarrow$ { local bool temp;
$\qquad\qquad\qquad\qquad$ temp:=x_1;
$\qquad\qquad\qquad\qquad x_1 :=\emptyset$;
$\qquad\qquad\qquad\qquad x_2$:=temp}

Blocking vs. Non-blocking Synchronization in Merge

queue(bool) $x_1 := \emptyset$, $x_2 := \emptyset$

bool in_1

bool in_2

bool out

T_{in1}: $\neg Full(x_1) \rightarrow Enqueue(x_1,in_1)$

T_{in2}: $\neg Full(x_2) \rightarrow Enqueue(x_2,in_2)$

T_{out1}: $\neg Empty(x_1) \rightarrow out := Dequeue(x_1)$

T_{out2}: $\neg Empty(x_2) \rightarrow out := Dequeue(x_2)$
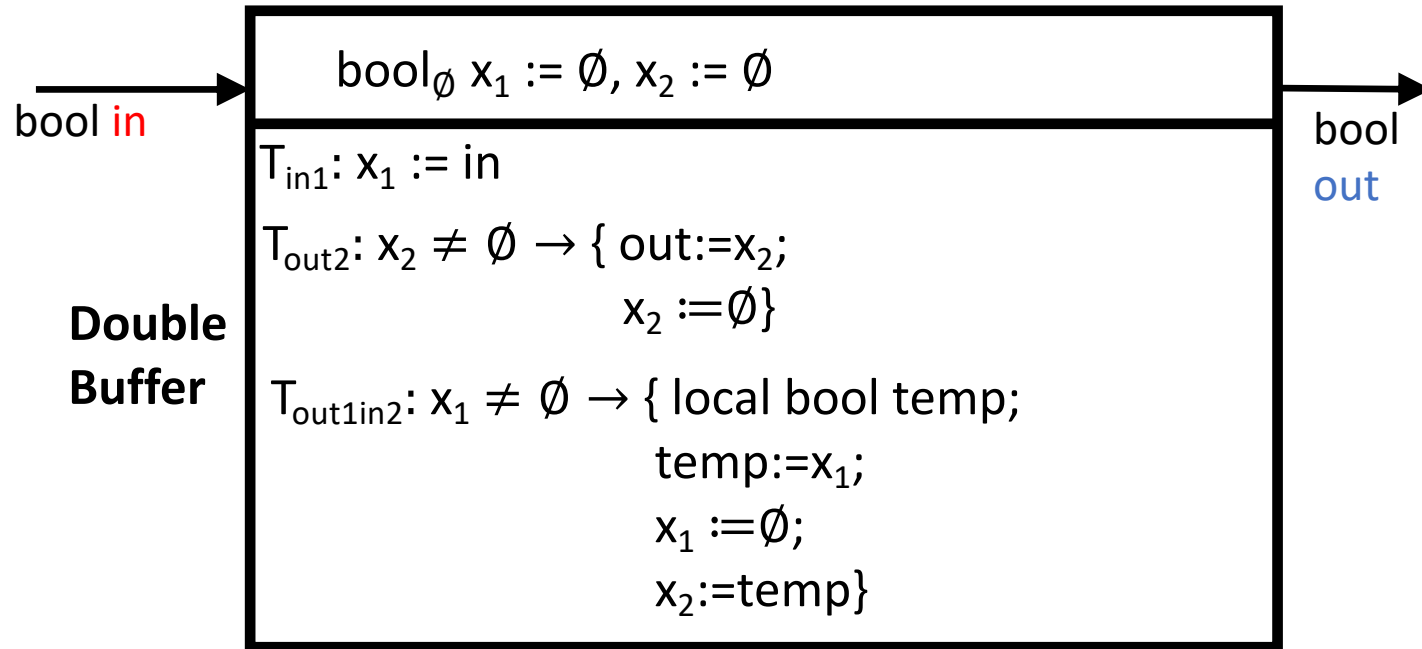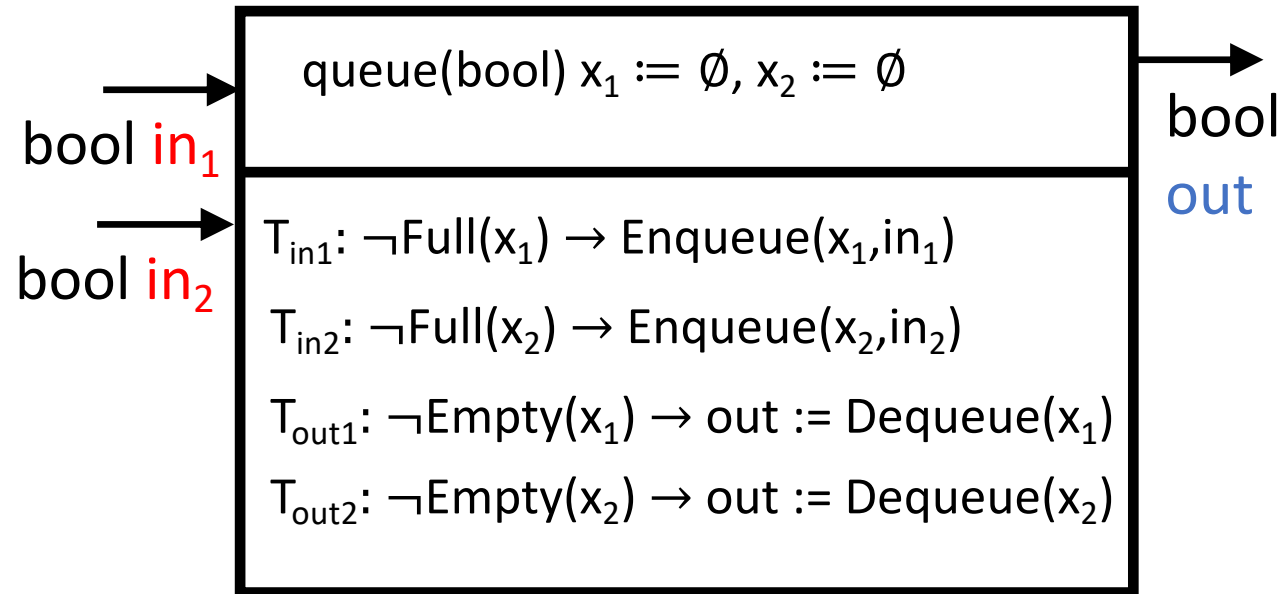
An input on the channel in_1 cannot be processed if the queue x_1 is full, and thus the producer of outputs on the channel in_1 has to wait until this queue becomes non-full

Deadlocks

- Common error in asynchronous designs
- Caused by each process waiting for another process to execute a task, but no task is enabled

bool $x_1 := 0, z_1 := 0$
$T_{11}: (x_1{==}0) \to x_1 := 1;$ $T_{12}: (x_1{==}1) \to z_1 := r_2$ $T_{13}: (z_1{==}1) \to r_1 := 1$

P1

r_1

r_2

bool $x_2 := 0, z_2 := 0$
$T_{21}: (x_2{==}0) \to x_2 := 1;$ $T_{22}: (x_2{==}1) \to z_2 := r_1$ $T_{23}: (z_2{==}1) \to r_2 := 1$

P2

$(0,0), (0,0)$

T_{11} ε

$(1,0), (0,0)$

T_{21} ε

$(1,0), (1,0)$