Expressing structural temporal properties of safety critical hierarchical systems

Massimo Benerecetti, Ruggero Lanotte, Fabio Mogavero, Adriano Peron, and

Luigi Libero Lucio Starace
Università degli Studi di Napoli Federico II, Naples, Italy
luigiliberolucio.starace@unina.it

September 10, 2021

Safety Critical Systems

- A system is **Safety Critical** if its failure could lead to **unacceptable consequences**.
- Typical examples include:
  - medical care devices
  - Aircraft controllers
  - Railway traffic controllers
  - Nuclear plants
  - Many more

Safety Critical Systems

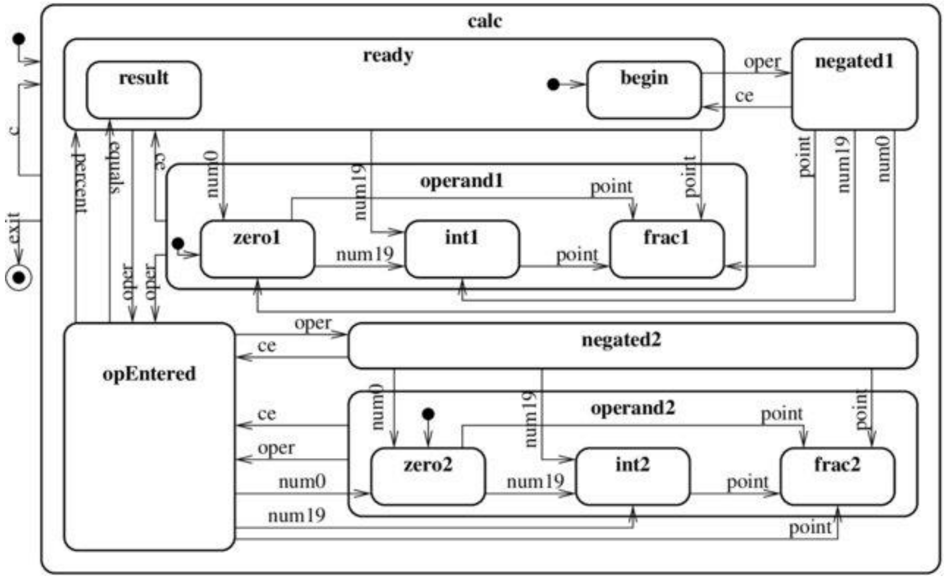
- A way broader class of systems has the potential for unacceptable consequences of failure
- A malfunction in telephone exchange system could have serious consequences as well!
- General trend towards **more complex**, interconnected, **software-intensive** safety critical systems
- It is **imperative** to guarantee high safety standards

Formal Methods

- A way to ensure high safety standards is using **formal methods**
  - *applied mathematics for modelling and analysing ICT systems*
- Key steps to apply formal methods include **specification** of
  - The System to be designed (via **modelling** languages)
  - The Properties that such system must satisfy

Hierarchical Models

- The notion of **hierarchy** arises naturally to deal with the increasing complexity of these systems
  - Popular hierarhical modelling languages include **Statechart**, **Simulink**
- System is described as a collection of **modules** in a tree-like hierarchy



Example of a Statechart, from [1]

[1] Pinter, Gergely, and Istvan Majzik. "Impact of statechart implementation techniques on the effectiveness of fault detection mechanisms." *Proceedings. 30th Euromicro Conference, 2004.*. IEEE, 2004.

Motivations

- A lot of work has been done on defining **hierarchical modelling** languages, and towards integration with model-driven development frameworks.
- Less work, on the other hand, has been directed towards languages to express relevant **behavioural properties** of hierarchical models

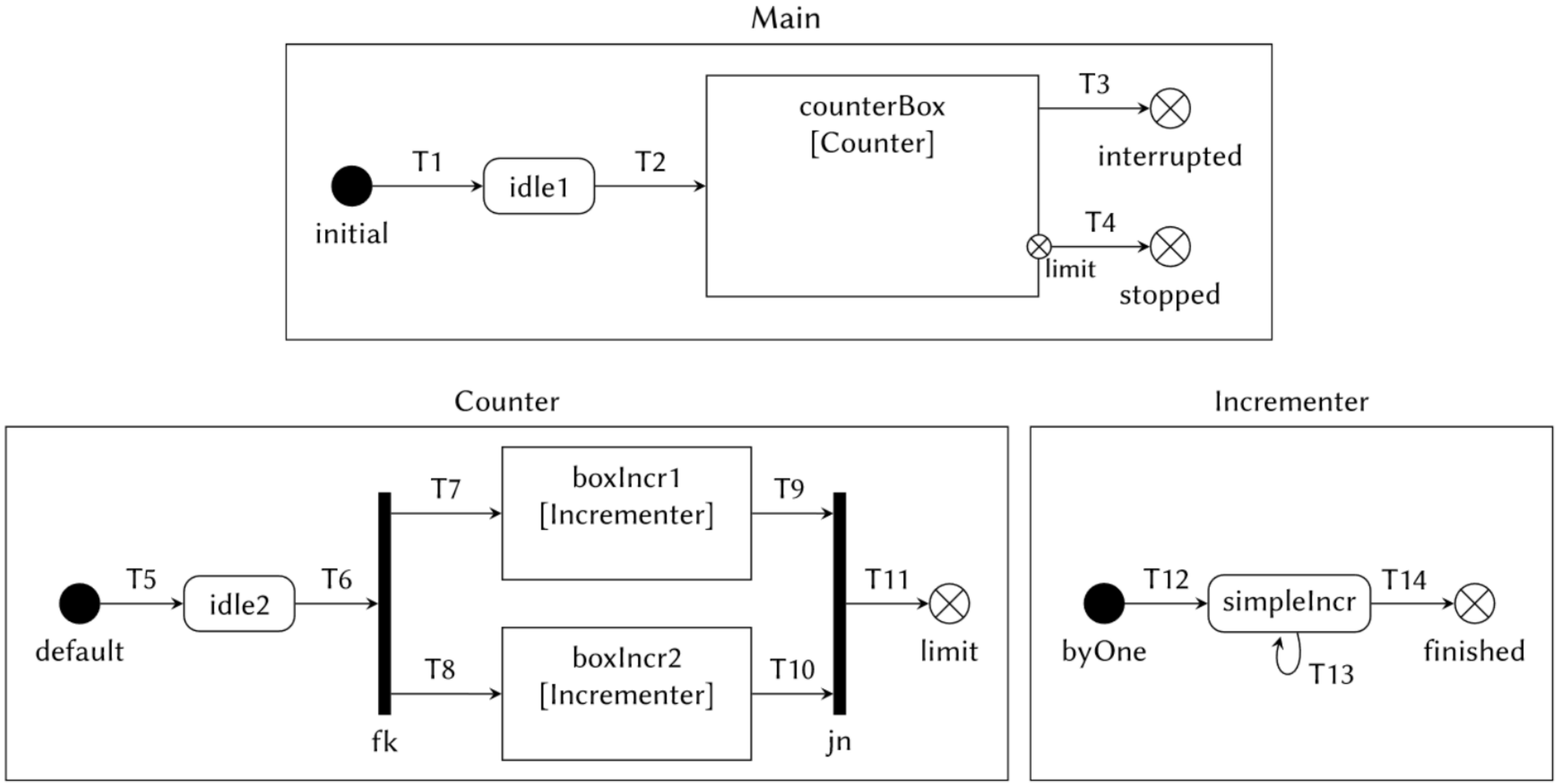
Goals

In this work, we propose HLTL, a logical formalism designed to express temporal structural properties of hierarchical models

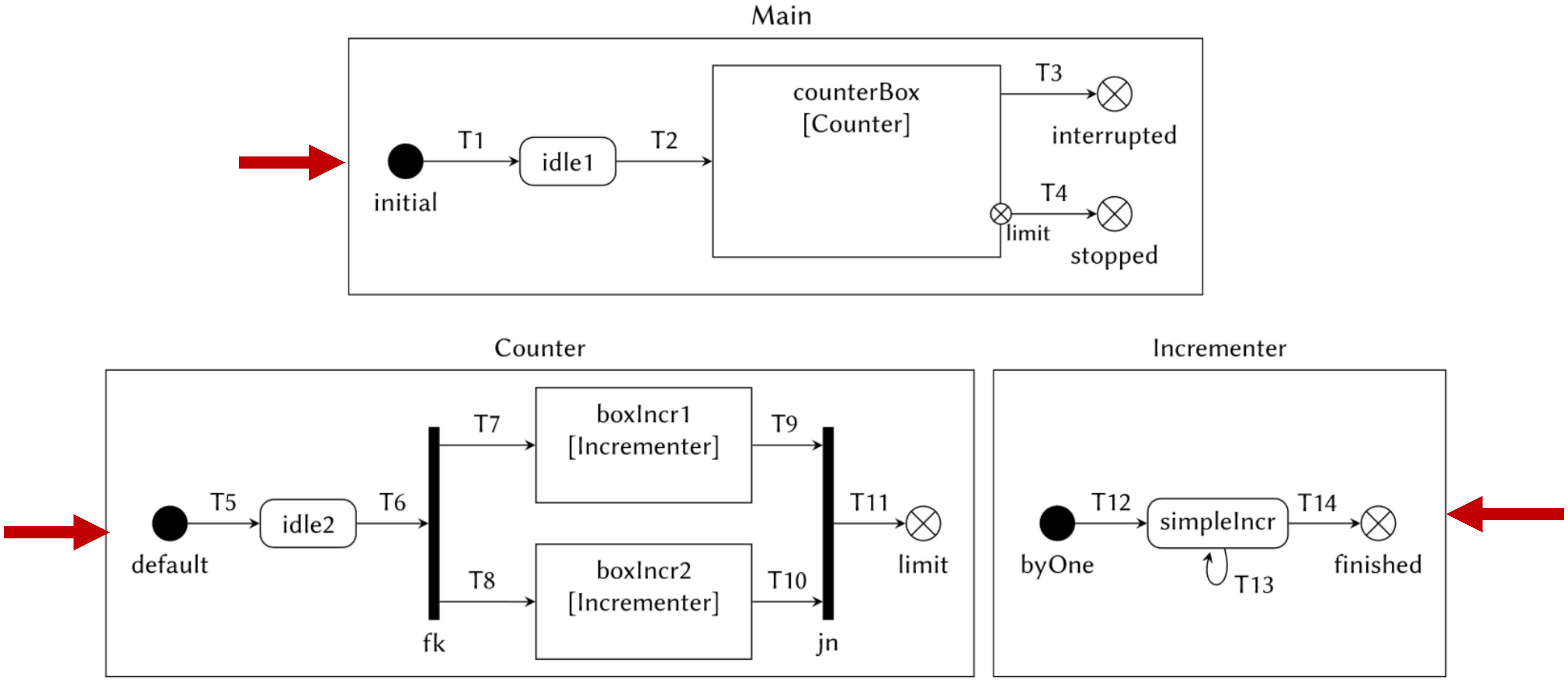
- Firstly we'll introduce Dynamic State Machines (DSTMs), a hierarchical modelling language
- Then, we'll introduce the formalism we propose

A hierarchical modelling language: Dynamic State Machines (DSTMs)

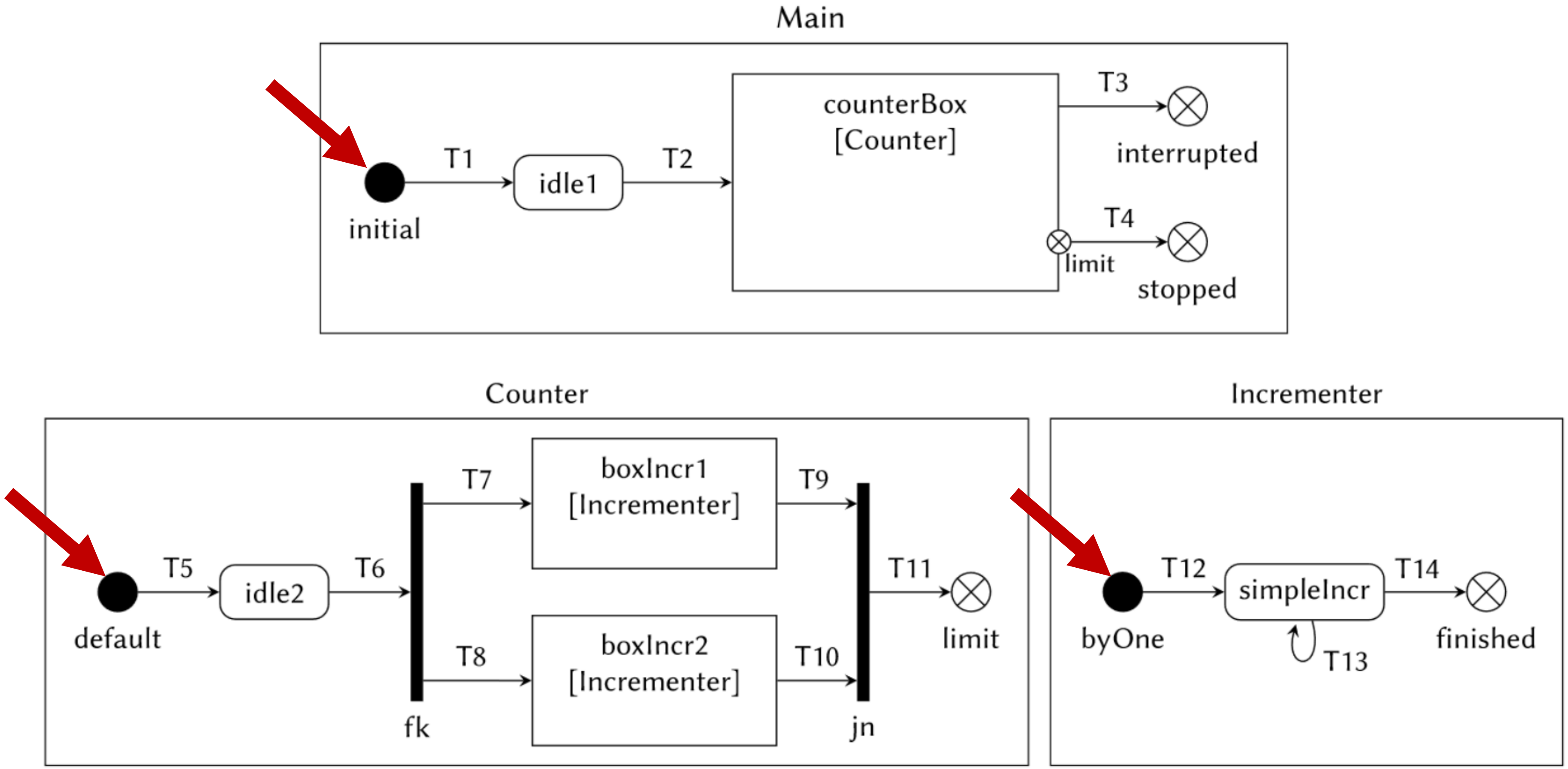
DSTM Syntax


Main
initial
T1
idle1
T2
counterBox
[Counter]
T3
interrupted
T4
limit
stopped
Counter
default
T5
idle2
T6
fk
T7
T8
boxIncr1
[Incrementer]
boxIncr2
[Incrementer]
T9
T10
jn
T11
limit
Incrementer
byOne
T12
simpleIncr
T13
T14
finished

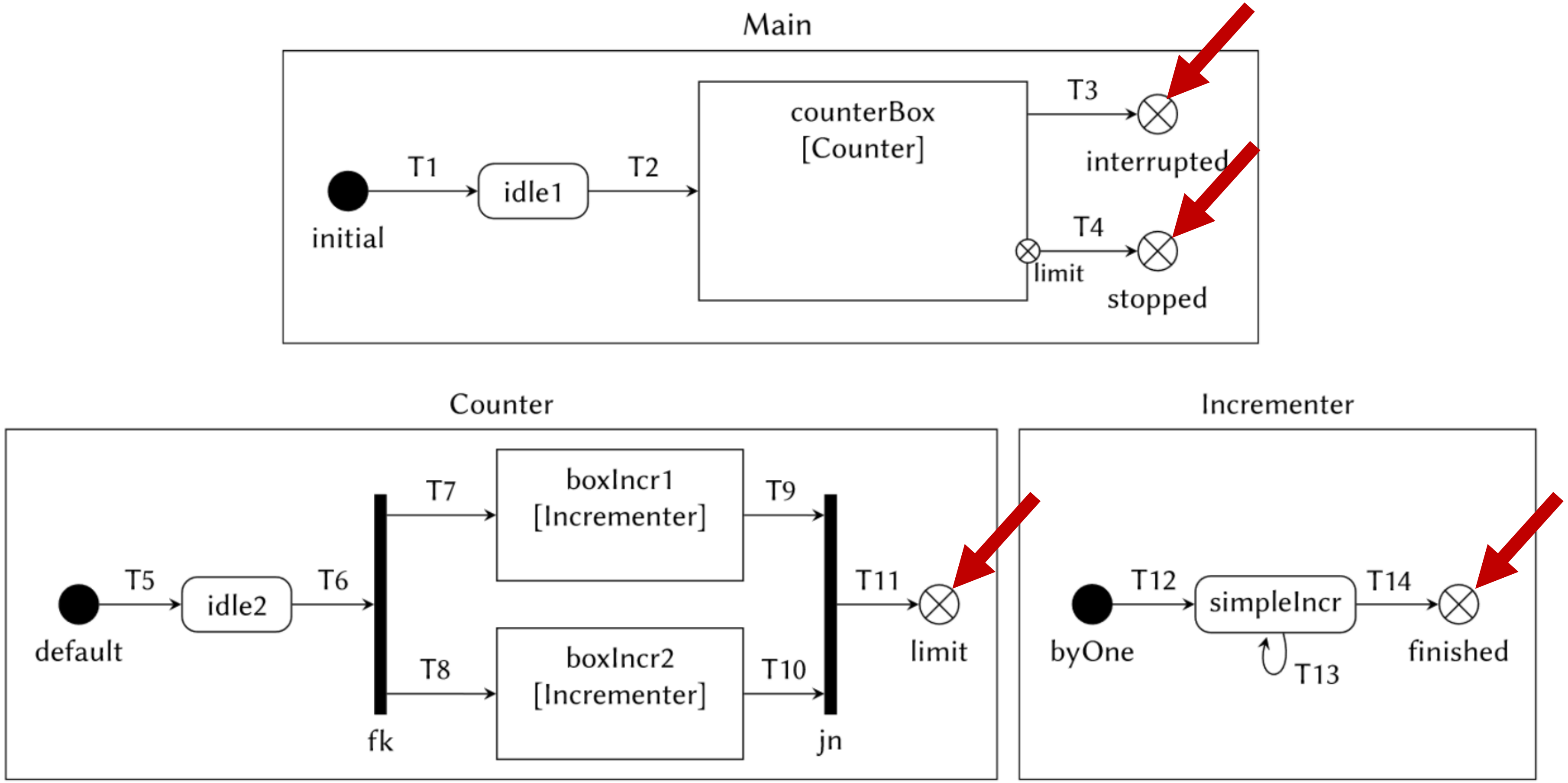
Machines or modules



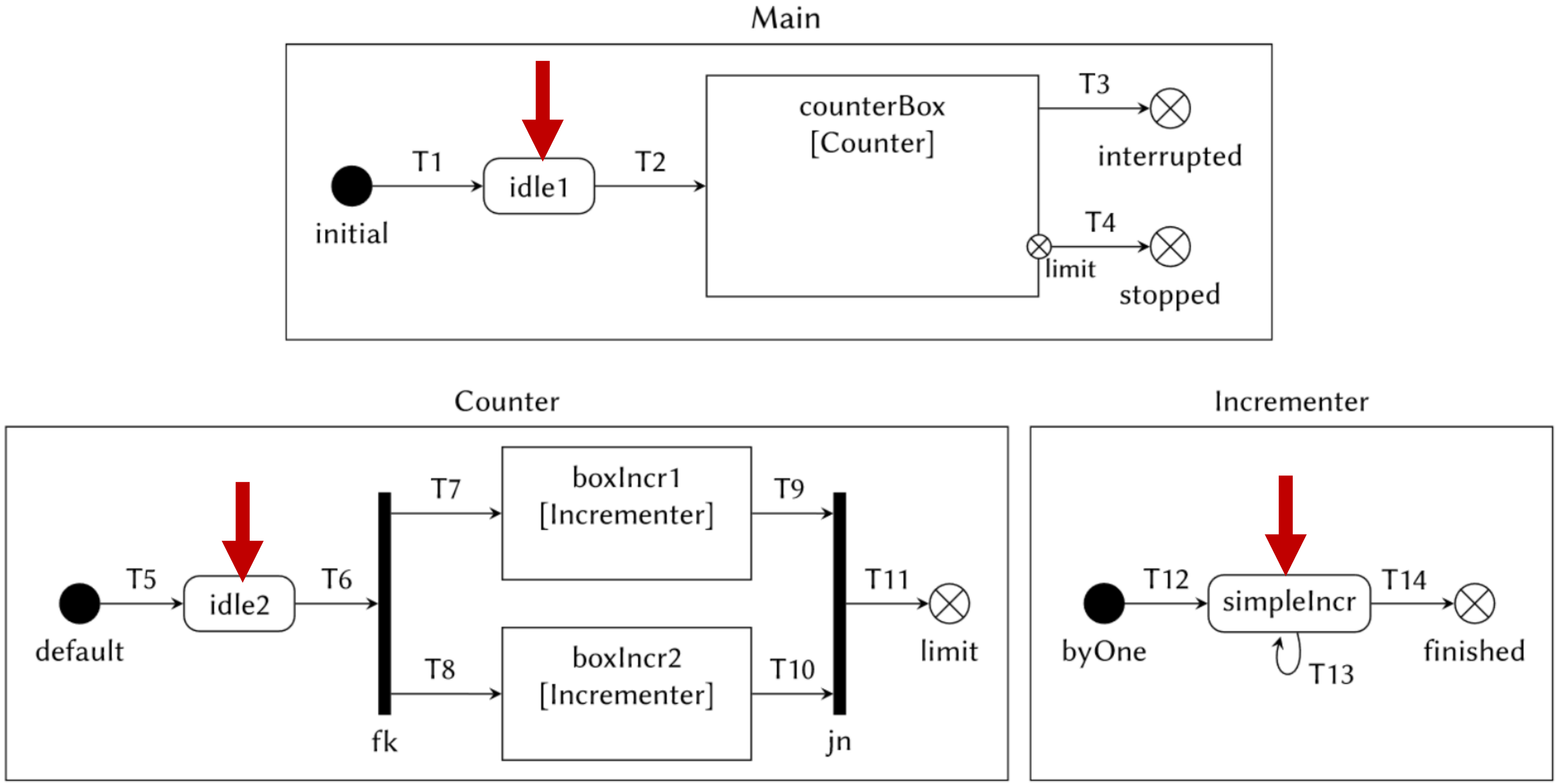
Entering nodes



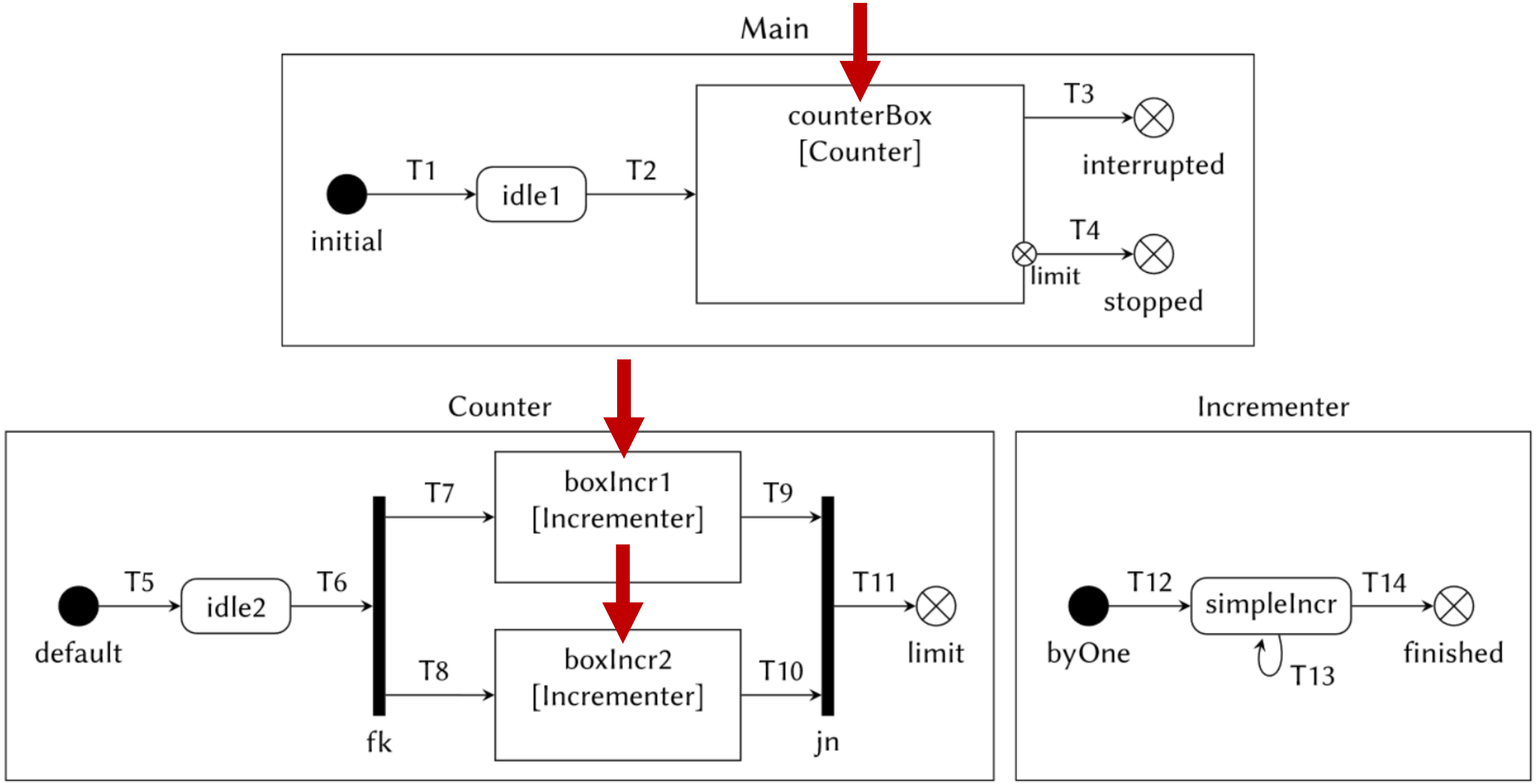
Exiting nodes



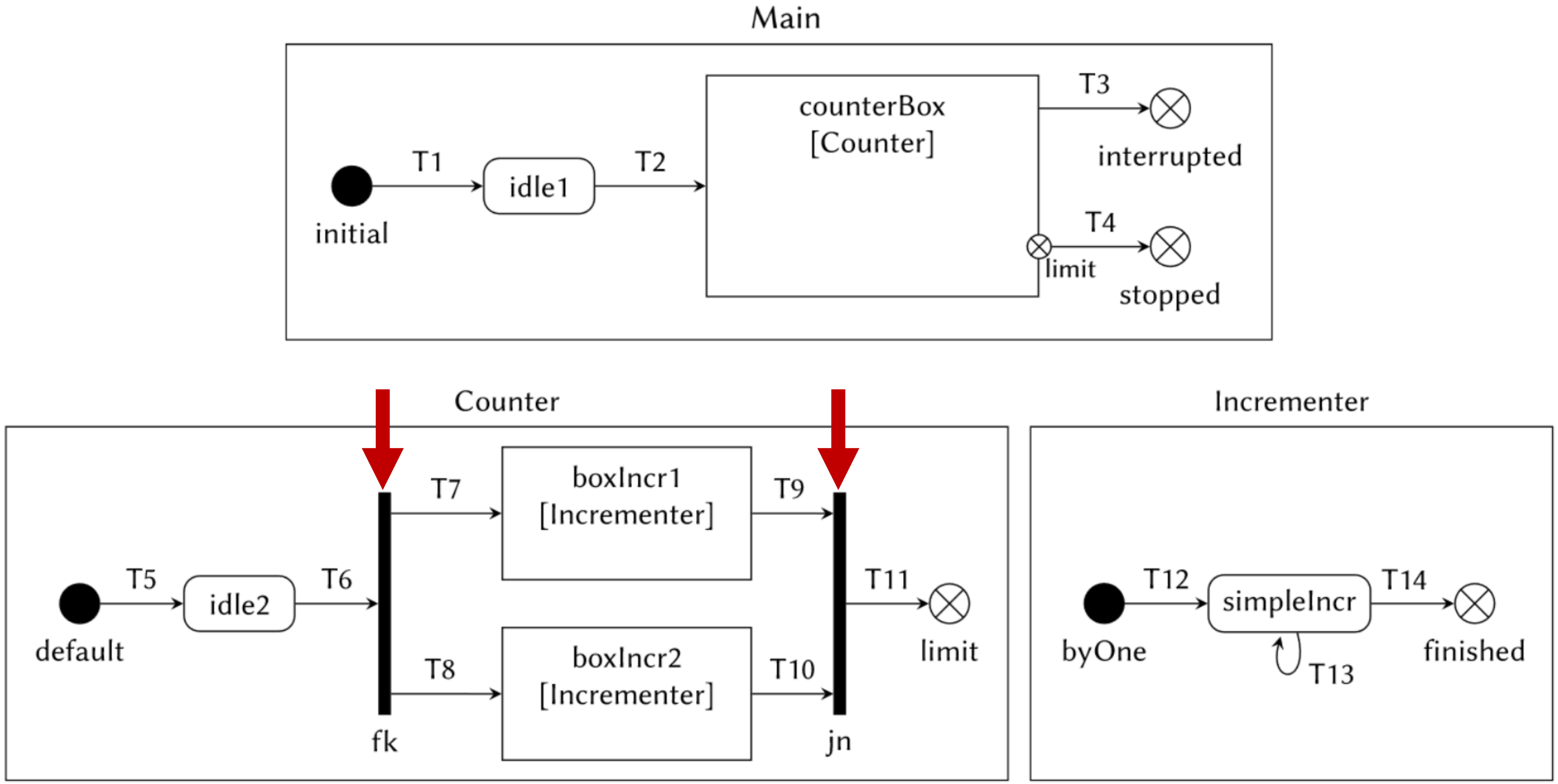
Simple states



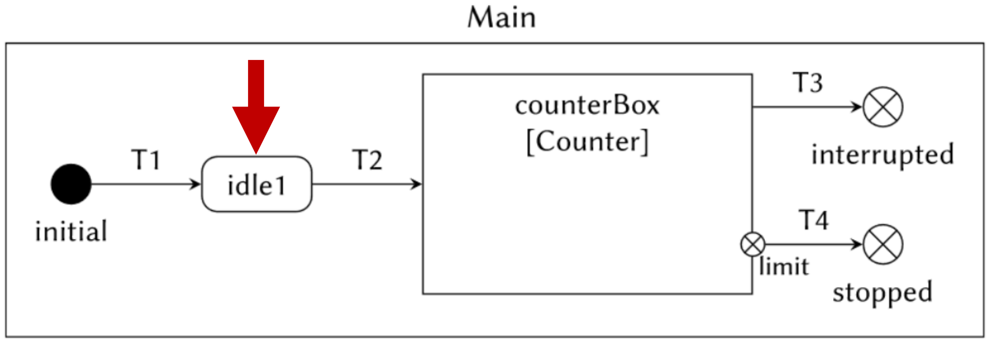
Boxes


Main
counterBox
[Counter]
T1
idle1
T2
T3
interrupted
T4
limit
stopped
initial
Counter
boxIncr1
[Incrementer]
boxIncr2
[Incrementer]
T5
idle2
T6
T7
T8
T9
T10
T11
default
fk
jn
limit
Incrementer
T12
simpleIncr
T14
byOne
T13
finished

Forks and Joins

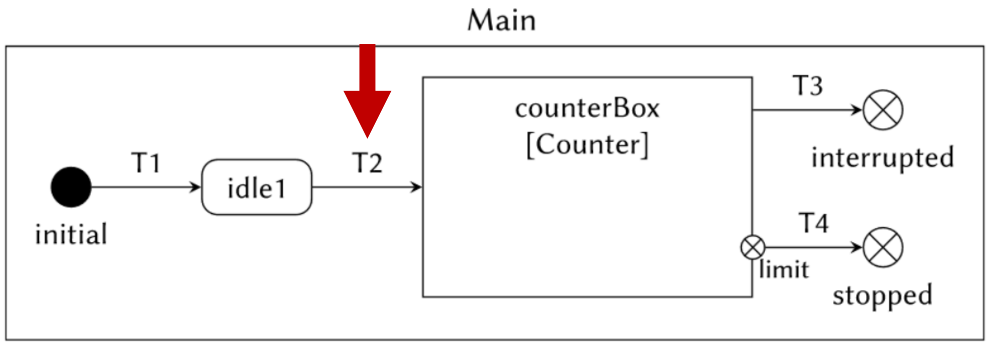


DSTM Semantics by Example



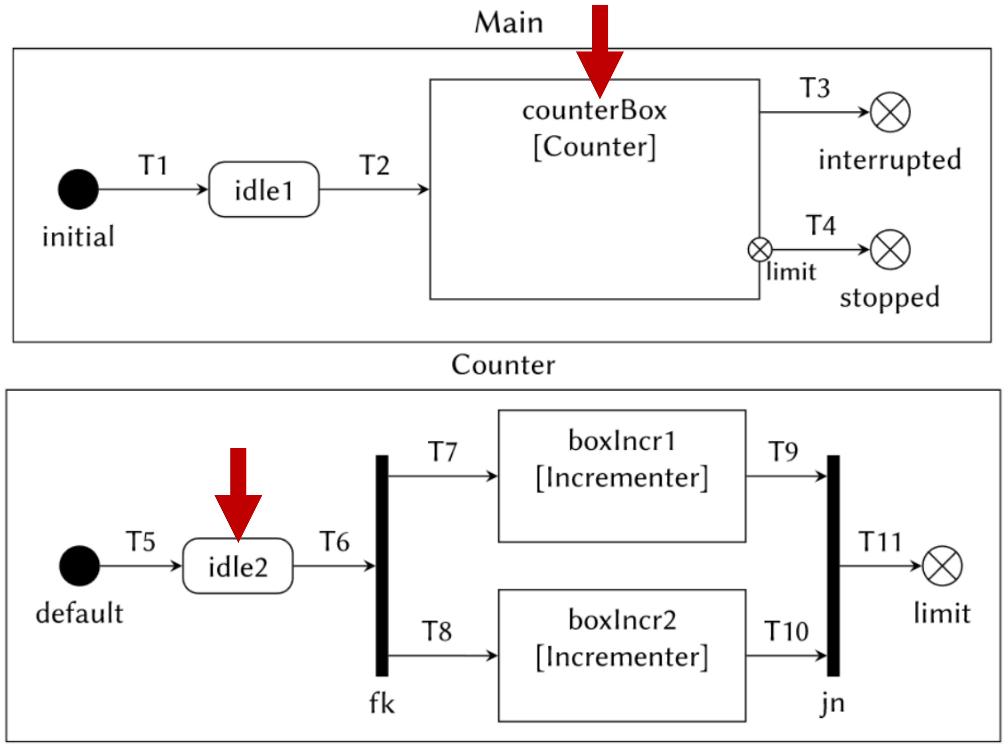
Main
State: idle1

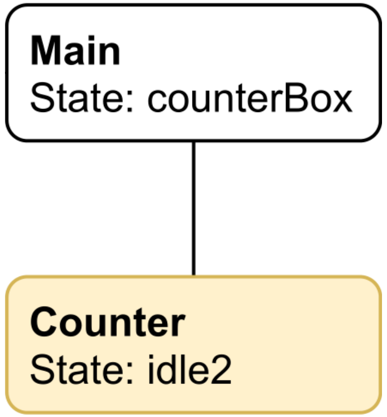
DSTM Semantics by Example



Main
State: idle1

DSTM Semantics by Example

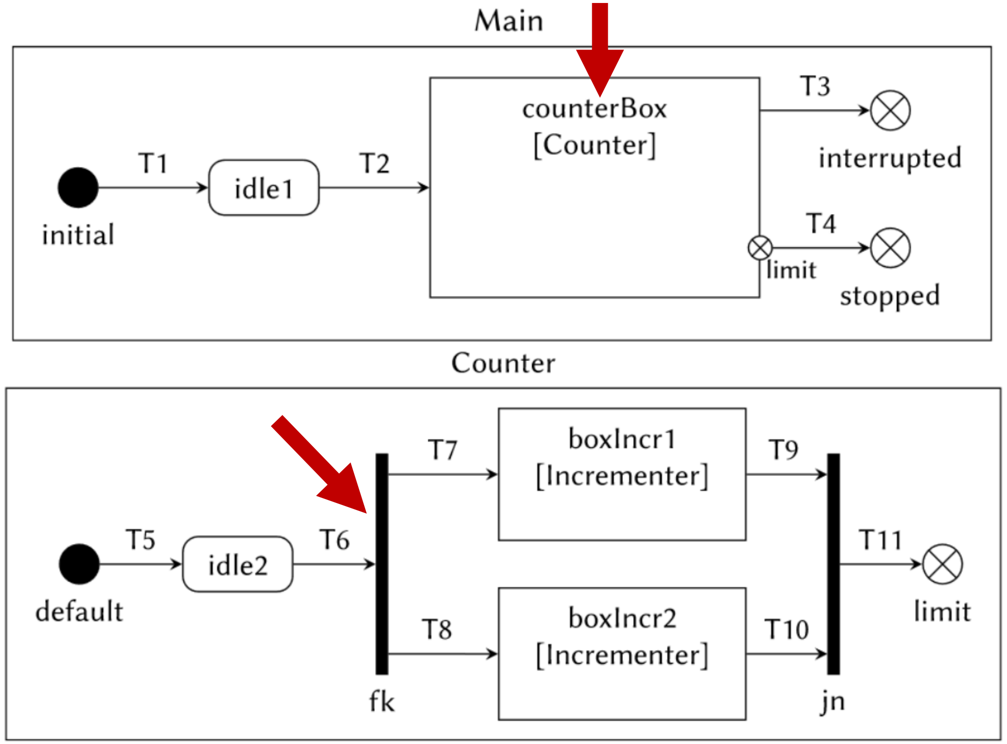


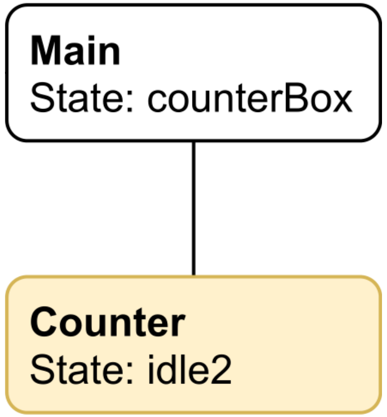


Main
State: counterBox

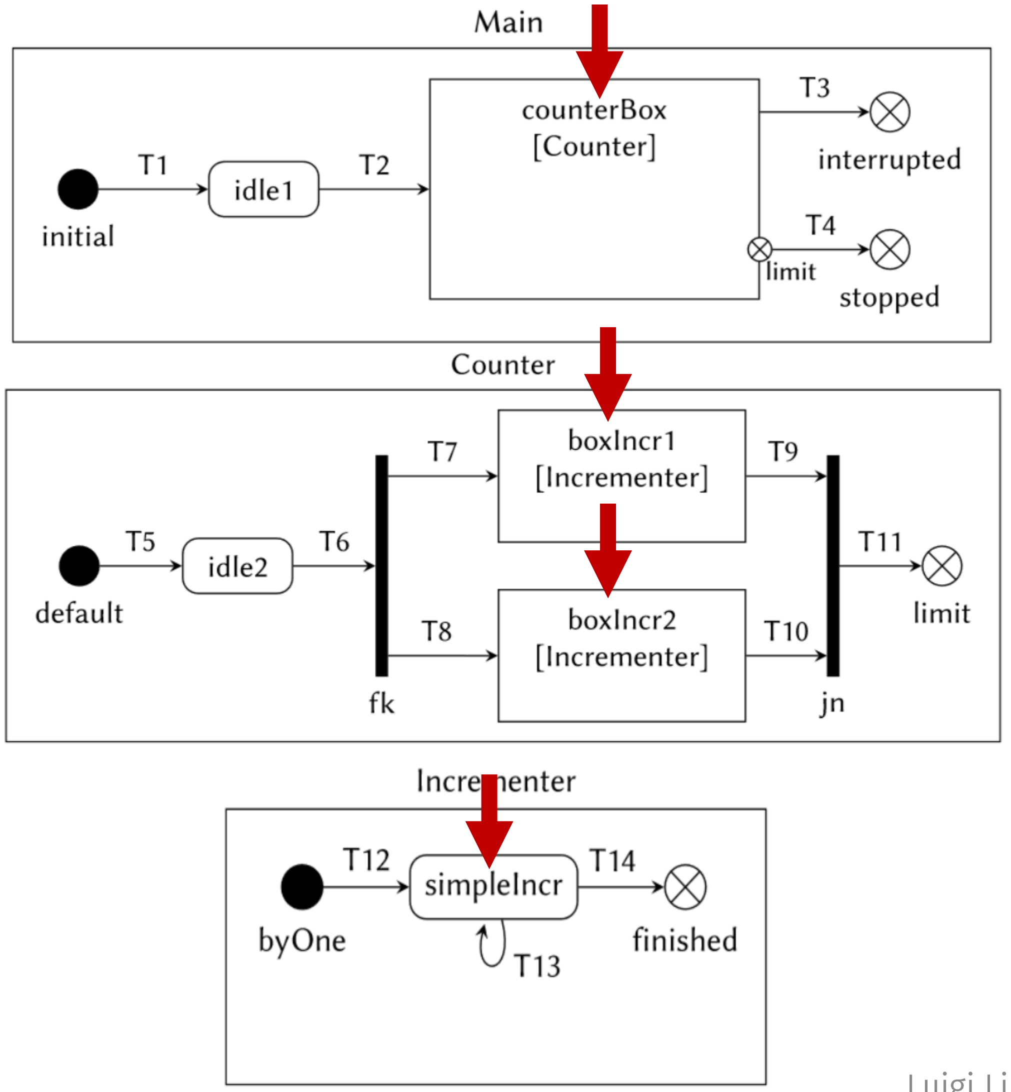
Counter
State: idle2

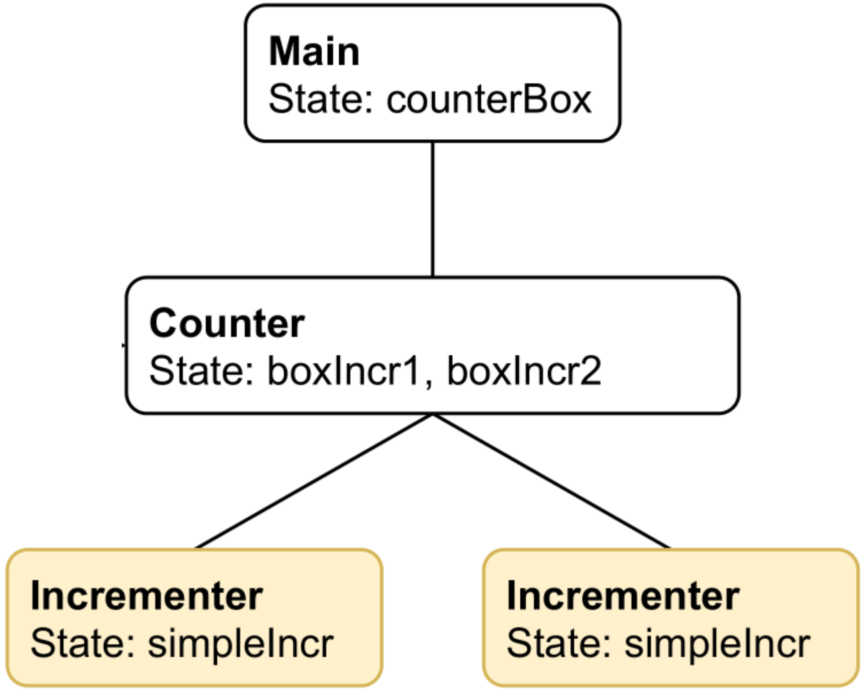
DSTM Semantics by Example





DSTM Semantics by Example





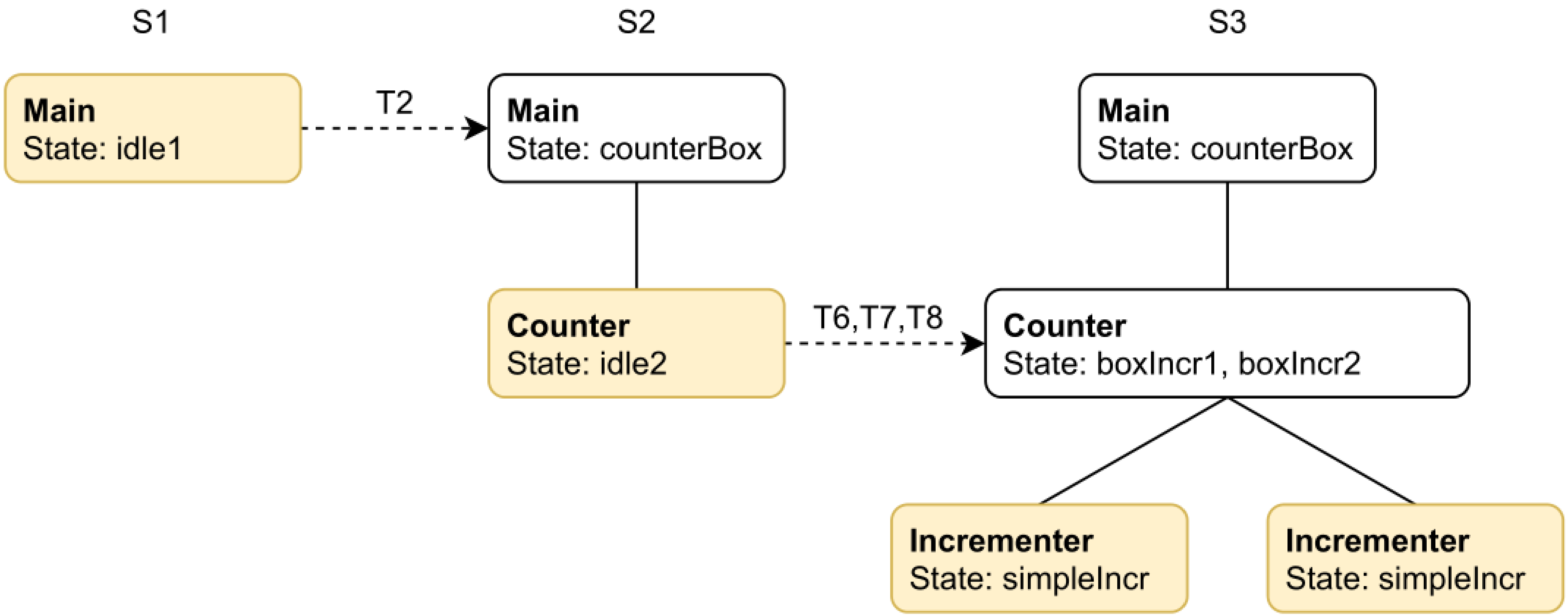
Main
State: counterBox

Counter
State: boxIncr1, boxIncr2

Incrementer
State: simpleIncr

Incrementer
State: simpleIncr

Hierarchical Computations



Reasoning about computations

- How can we **predicate** over such hierarchical computations?

Temporal Logics

- How can be **predicate** over such hierarchical computations?
- Formalisms to express properties of system behaviours (sequences of system states)
- Extensions of standard propositional logics with **temporal modalities**
- LTL is a widely-used temporal logic, and it is very effective when reasoning about sequences of flat, unstructured states

Dealing with Hierarchical Computations

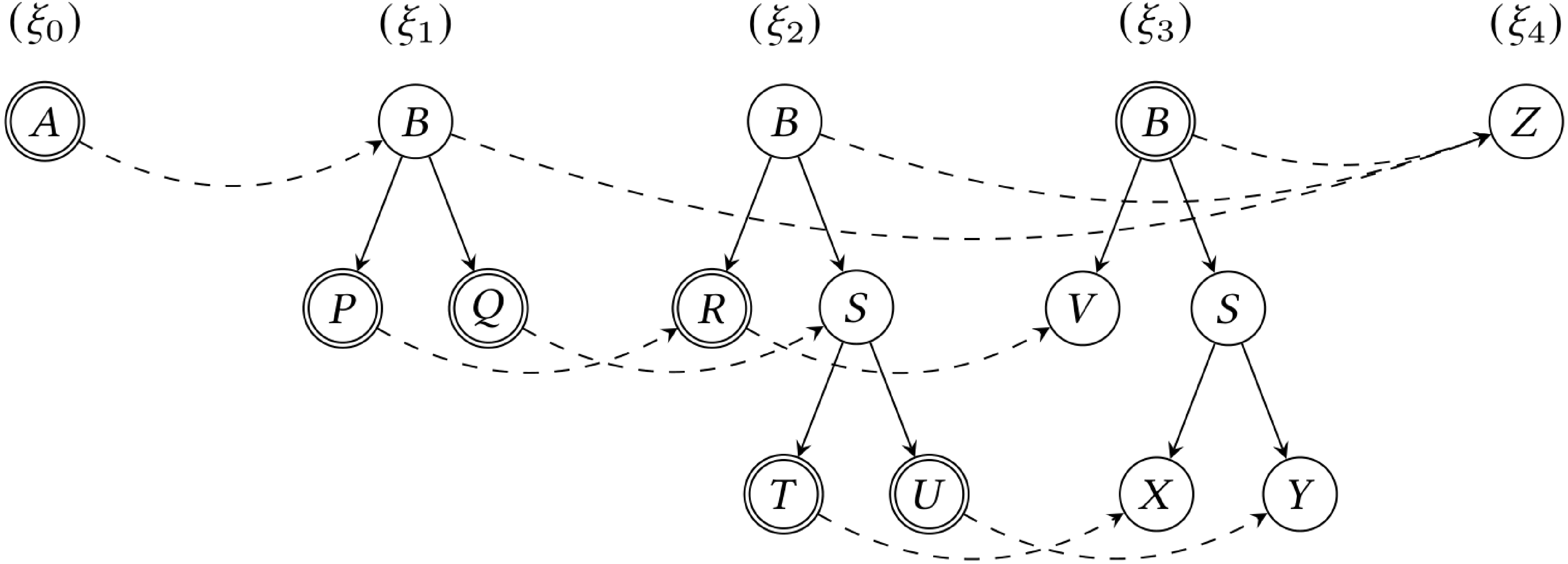
- In hierarchical computations, states are not flat, they have an intrinsic, tree-like hierarchical structure
- LTL cannot predicate naturally over this intrinsic structure
- We extended LTL with operators that allow to **contextualize formulae in the hierarchical structure** of states
- We called this extension Hierarchical LTL (**HLTL**)

Hierarchical Linear-time Temporal Logic

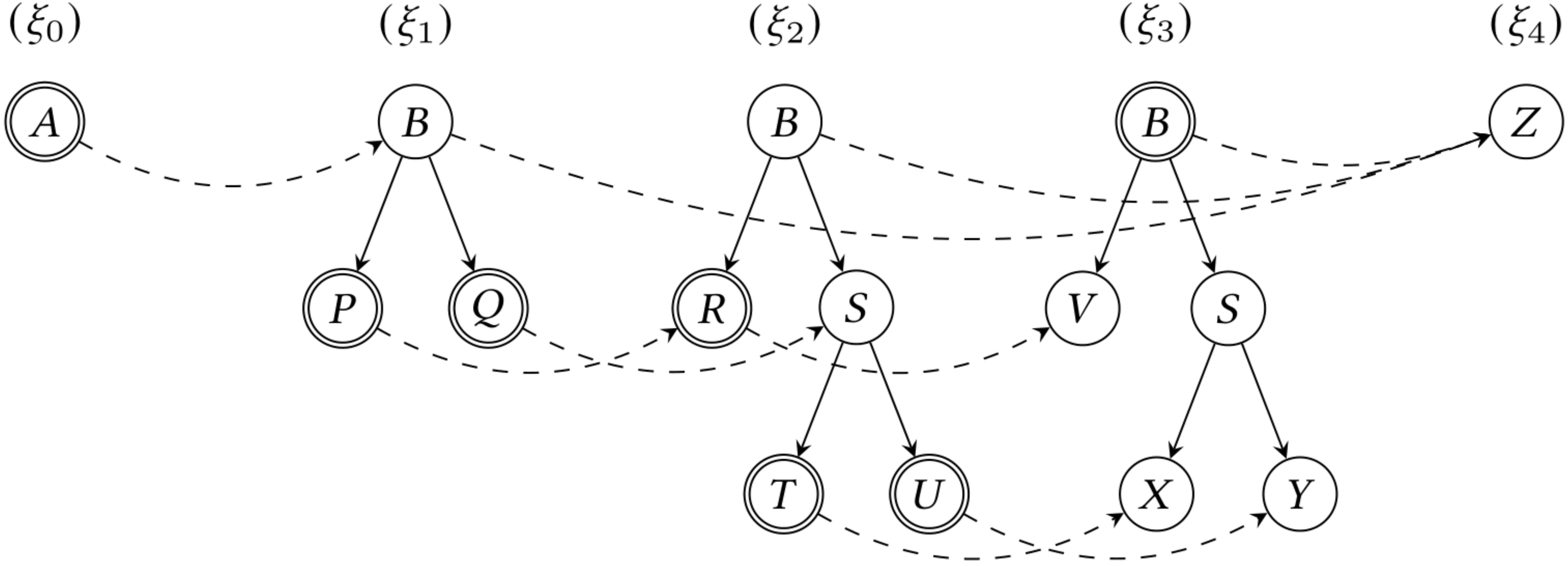
An **HLTL** formula is defined inductively as follows:

$\phi \coloneqq \top \mid p \in P \mid \neg\phi \mid \phi_1 \vee \phi_2 \mid \phi_1 \wedge \phi_2$	Standard Propositional Logic
$\mid X(\phi) \mid \phi_1 U \phi_2$	LTL operators
$\mid\leftarrow(\phi)\mid\rightarrow(\phi)\mid\downarrow_n(\phi)$	HLTL operators

HLTL by Example

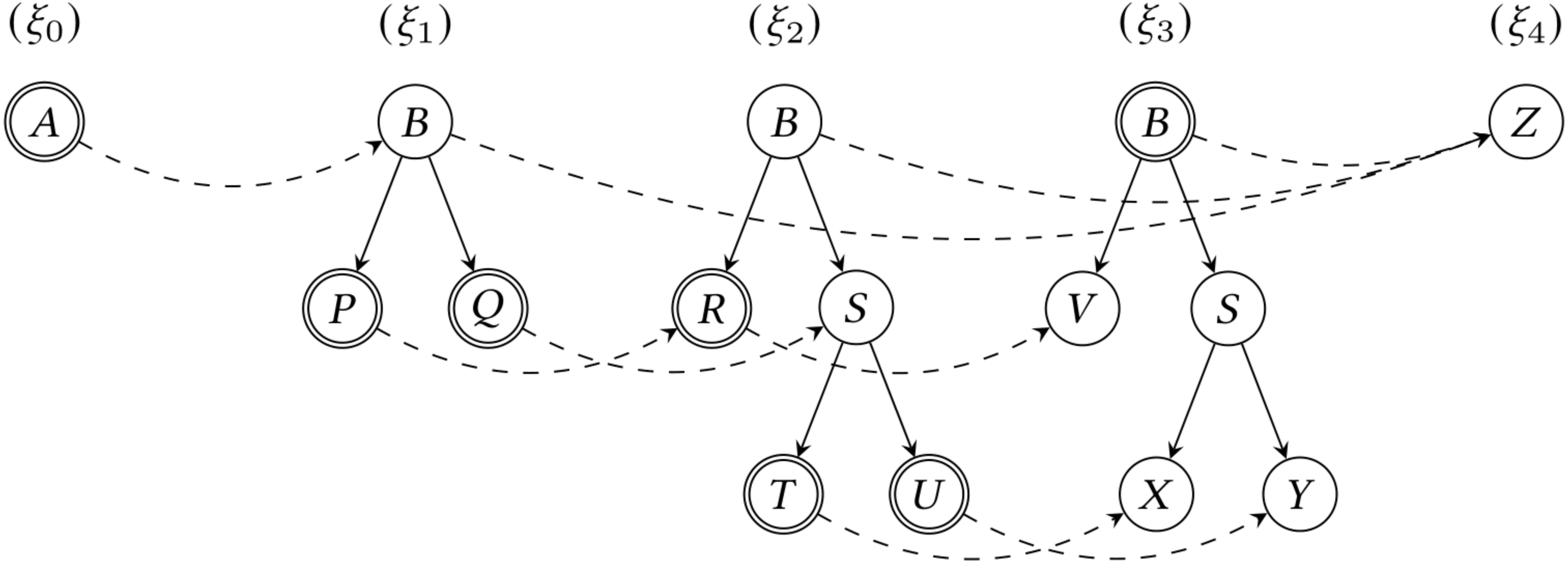


HLTL by Example



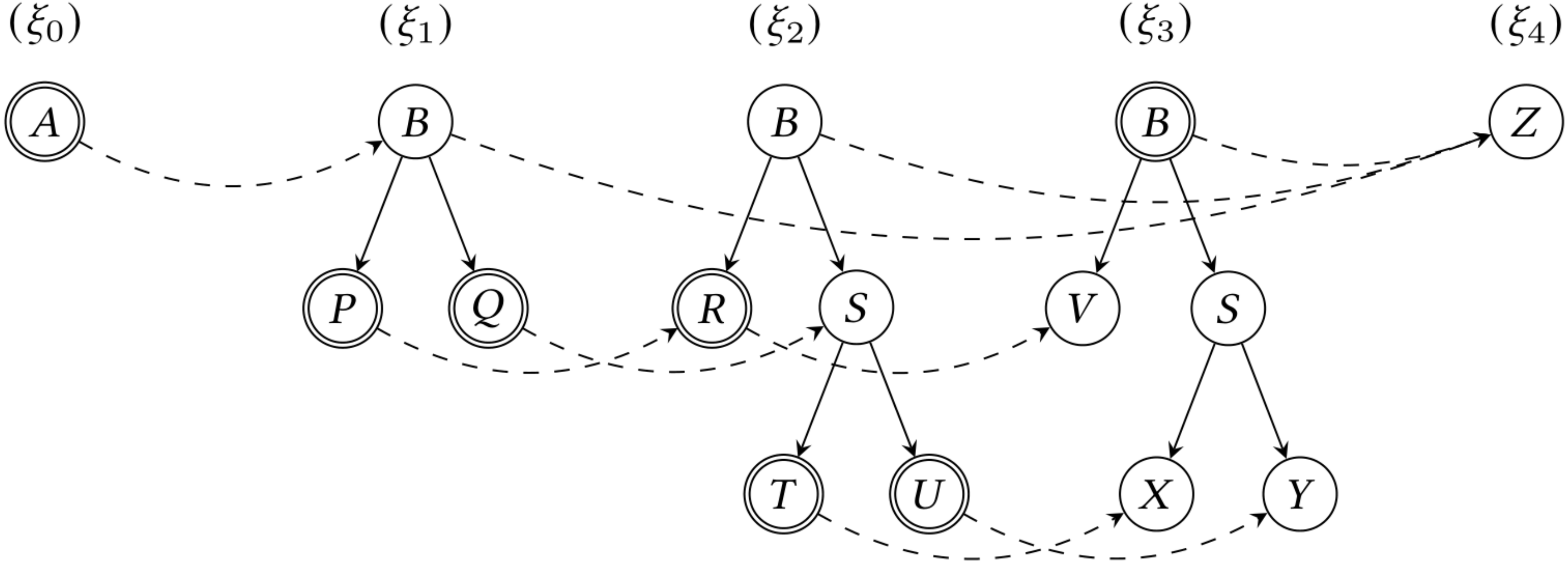
$$X(\downarrow_2 (Q))$$

HLTL by Example



$$X\left(\downarrow_1 \left(P \wedge \rightarrow (Q)\right)\right)$$

HLTL by Example



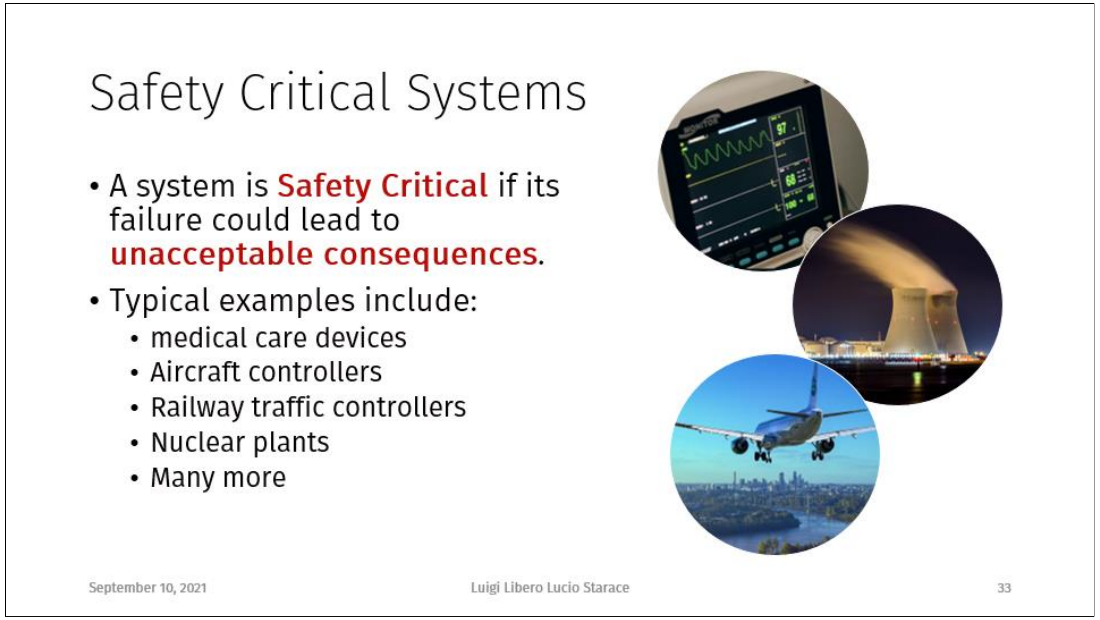
$$X\left(\downarrow_1 \left(P \wedge X(R)\right)\right)$$

Conclusions and Future Works

- We have presented and formalized **HLTL**
- In future works:
  - Devise a **model checking** procedure
  - Integrate HLTL within the modelling framework for Dynamic State Machines presented in [2]

[2] Benerecetti, M., Gentile, U., Marrone, S., Nardone, R., Peron, A., Starace, L.L.L., Vittorini, V.: From dynamic state machines to Promela. In: Model Checking Software. pp. 56–73. Springer International Publishing, Cham (2019)

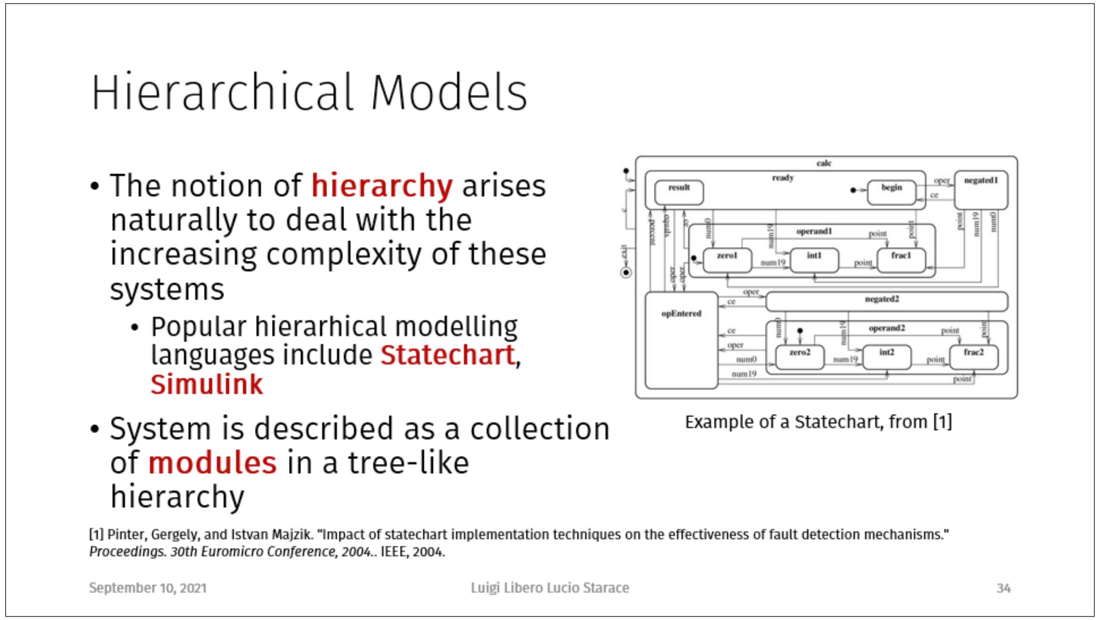
Expressing structural temporal properties of safety critical hierarchical systems



Safety Critical Systems

- A system is **Safety Critical** if its failure could lead to **unacceptable consequences**.
- Typical examples include:
  - medical care devices
  - Aircraft controllers
  - Railway traffic controllers
  - Nuclear plants
  - Many more

September 10, 2021 Luigi Libero Lucio Starace 33



Hierarchical Models

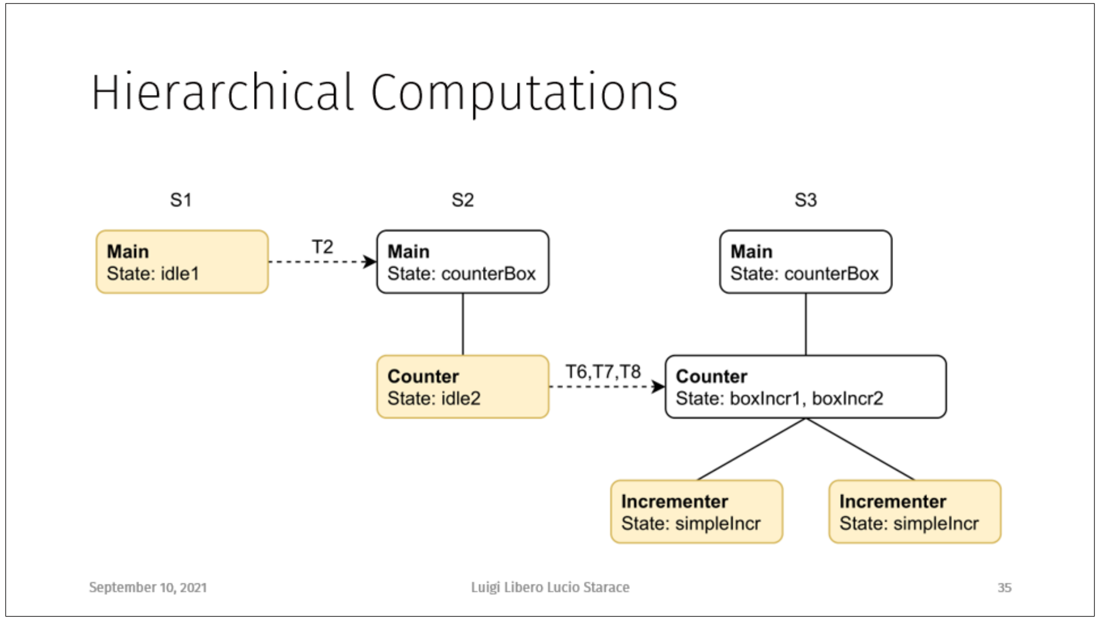
- The notion of **hierarchy** arises naturally to deal with the increasing complexity of these systems
  - Popular hierarhical modelling languages include **Statechart**, **Simulink**
- System is described as a collection of **modules** in a tree-like hierarchy

calc
ready
result
begin
negated1
operand1
zero1
int1
frac1
opEntered
negated2
operand2
zero2
int2
frac2
oper
ce
point
num0
num19
percent
equals
exit

Example of a Statechart, from [1]

[1] Pinter, Gergely, and Istvan Majzik. "Impact of statechart implementation techniques on the effectiveness of fault detection mechanisms." *Proceedings. 30th Euromicro Conference, 2004..* IEEE, 2004.

September 10, 2021 Luigi Libero Lucio Starace 34



Hierarchical Computations

S1

Main
State: idle1

T2

S2

Main
State: counterBox

Counter
State: idle2

T6,T7,T8

S3

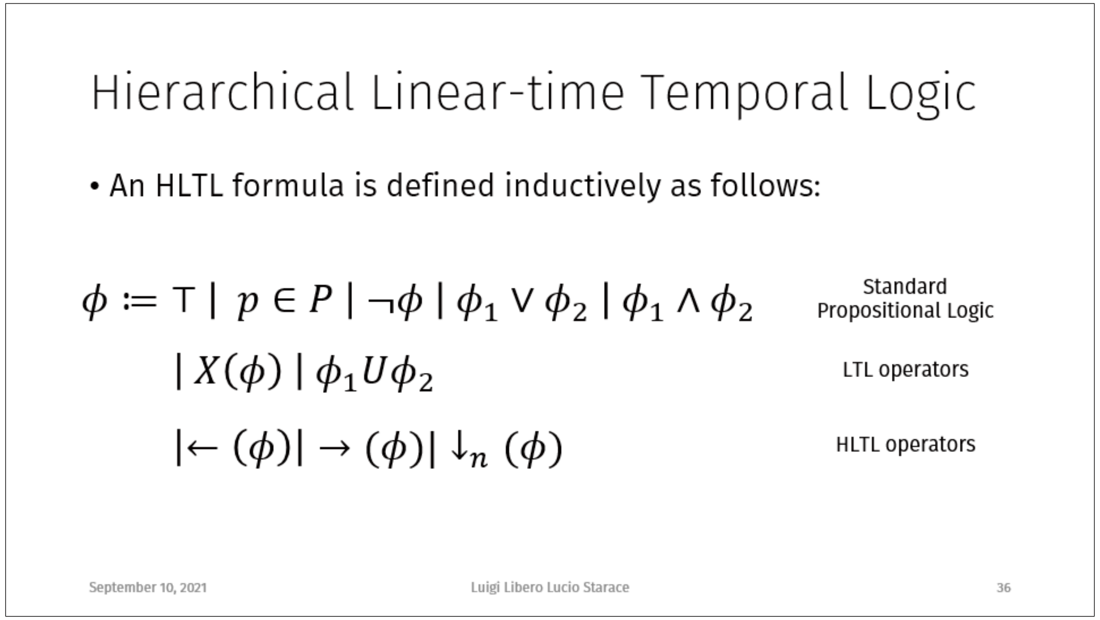
Main
State: counterBox

Counter
State: boxIncr1, boxIncr2

Incrementer
State: simpleIncr

Incrementer
State: simpleIncr

September 10, 2021 Luigi Libero Lucio Starace 35



Hierarchical Linear-time Temporal Logic

- An HLTL formula is defined inductively as follows:

$$\phi \coloneqq \top \mid p \in P \mid \neg\phi \mid \phi_1 \vee \phi_2 \mid \phi_1 \wedge \phi_2$$

Standard Propositional Logic

$$\mid X(\phi) \mid \phi_1 U \phi_2$$

LTL operators

$$\mid \leftarrow (\phi) \mid \rightarrow (\phi) \mid \downarrow_n (\phi)$$

HLTL operators

September 10, 2021 Luigi Libero Lucio Starace 36

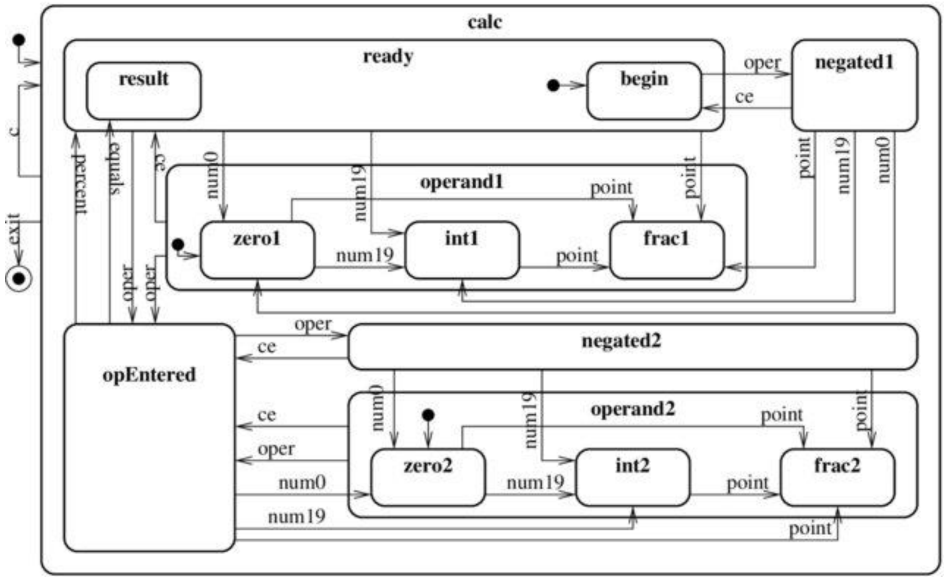
Luigi Libero Lucio Starace – luigiliberolucio.starace@unina.it

Safety Critical Systems

- A system is **Safety Critical** if its failure could lead to **unacceptable consequences**.
- Typical examples include:
  - medical care devices
  - Aircraft controllers
  - Railway traffic controllers
  - Nuclear plants
  - Many more

Hierarchical Models

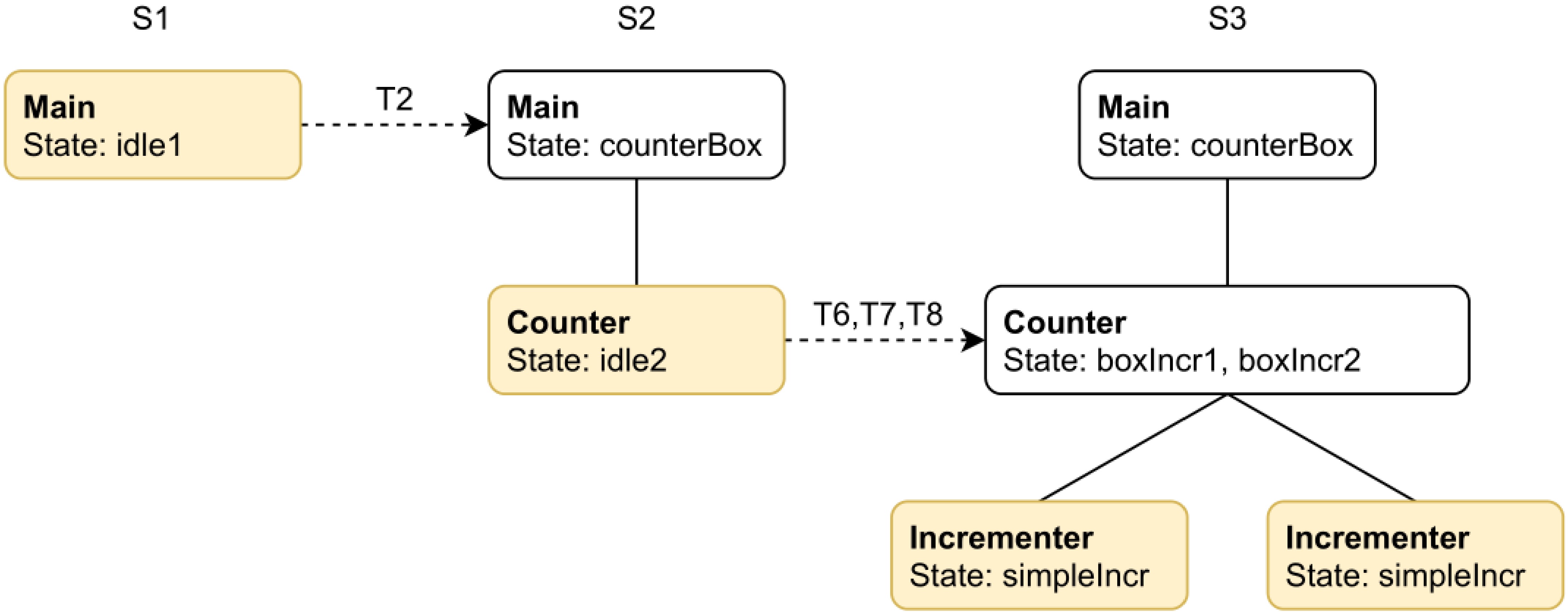
- The notion of **hierarchy** arises naturally to deal with the increasing complexity of these systems
  - Popular hierarhical modelling languages include **Statechart**, **Simulink**
- System is described as a collection of **modules** in a tree-like hierarchy



Example of a Statechart, from [1]

[1] Pinter, Gergely, and Istvan Majzik. "Impact of statechart implementation techniques on the effectiveness of fault detection mechanisms." *Proceedings. 30th Euromicro Conference, 2004.*. IEEE, 2004.

Hierarchical Computations



Hierarchical Linear-time Temporal Logic

- An HLTL formula is defined inductively as follows:

$$\phi \coloneqq \top \mid \; p \in P \mid \neg\phi \mid \phi_1 \vee \phi_2 \mid \phi_1 \wedge \phi_2$$

Standard
Propositional Logic

$$\mid X(\phi) \mid \phi_1 U \phi_2$$

LTL operators

$$\mid\leftarrow(\phi)\mid\rightarrow(\phi)\mid\downarrow_n(\phi)$$

HLTL operators