Part 6 Integrated Formal Modeling

Overview

- Object-Z Revisited
- Timed Communicating Object Z – TCOZ
- Active Objects and Network Topology
- Case Study: Lift System
- Sensor, Actuator and Control Systems
- Unified Modeling Language (UML)
- Linking TCOZ with UML
- Z family on the Web with their UML pictures

Object-Z

$Buffer[X]$

$max : \mathbb{N}$
$items : \mathrm{seq}\, X$
Δ
$size : \mathbb{N}$

$\#items = size \wedge size \leq max$

INIT

$items = \langle\ \rangle$

$Join$

$\Delta(items)$
$i? : X$

$items' = \langle i? \rangle \frown items$

$Leave$

$\Delta(items)$
$i! : X$

$size \neq 0 \wedge items = items' \frown \langle i! \rangle$

Exercise: For this *Buffer* class specify:

(a) an operation *count* which, given a message, outputs the number of times that message occurs in the buffer;

(b) an operation *duplicate* which appends to the buffer the message currently at the head of the buffer, provided the buffer is not empty or already full;

(c) an operation *titanic* whereby a sequence of messages is appended to the buffer except those messages for which there is no room are discarded (the buffer is like a life-boat on the Titanic: people queue to get on, but once the boat is full all the remaining people are left behind);

(d) an operation *penguin* whereby, like the operation *titanic*, a sequence of messages is input to the buffer, but this time the messages on the end of the sequence are accepted while those at the front are discarded if there is no room (the messages are acting like penguins, pushing out the messages already in the buffer once the buffer is full).

Solution

count

$$m? : X$$
$$count! : \mathbb{N}$$

$$count! = \#(items \rhd \{m?\})$$

duplicate

$$\Delta(items)$$

$$\#items \in 1 \mathinner{..} (max - 1)$$
$$items' = items \frown \langle \mathrm{head}\ items \rangle$$

titanic

$$\Delta(items)$$
$$s? : \mathrm{seq}\ X$$

$$items' = (1 \mathinner{..} max) \lhd (items \frown s?)$$

penguin

$$\Delta(items)$$
$$s? : \mathrm{seq}\ X$$

$$\exists\, s : \mathrm{seq}\ X \bullet$$
$$\quad s \frown items' = items \frown s?$$
$$\quad s \neq \langle\ \rangle \Rightarrow \#items' = max$$

Two Linked Buffers (single thread)

$TwoBuffers[X]$

$b_1, b_2 : Buffer[X]$

$b_1 \neq b_2$

$\textsc{Init}$

$b_1.\textsc{Init} \wedge b_2.\textsc{Init}$

$Join \mathrel{\widehat{=}} b_1.Join$

$Leave \mathrel{\widehat{=}} b_2.Leave$

$Transfer \mathrel{\widehat{=}} b_1.Leave \parallel b_2.Join$

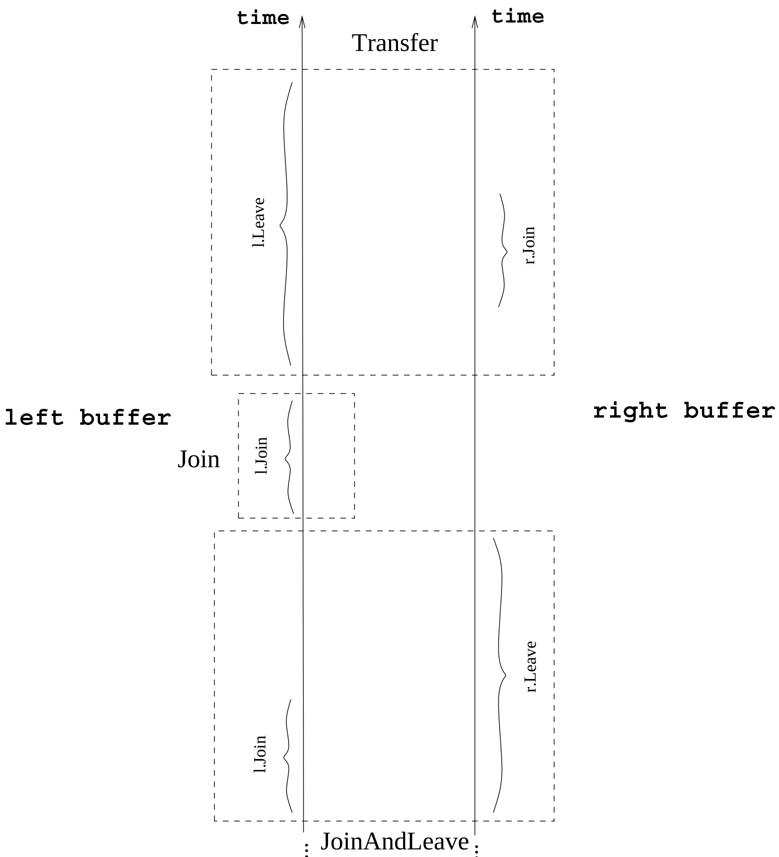


Figure 1: passive events

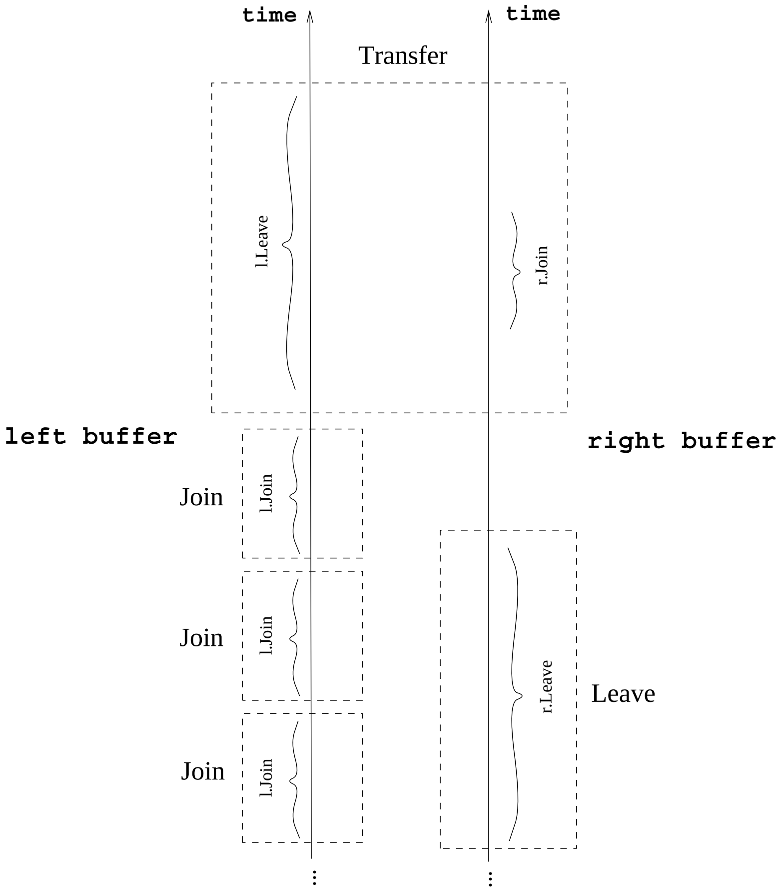


Figure 2: active events

Object-Z and Timed CSP

- Object-Z
  - ✓ an excellent tool for modeling data states
  - × but difficult for modelling real-time concurrent systems
- Timed CSP
  - ✓ Good for specifying the timed process and communication
  - × Like CSP, cumbersome to capture the data state of a complex system
- Timed Communicating Object Z: a blending of Object-Z and Timed CSP

Related Work

* Z/OZ with CSP: Fischer, Smith, Derick, Suhl, Bolton, Davies, Woodcock ...

* Z with CCS: Galloway, Stoddart, Taguchi, Araki ...

Timed Communicating Object Z (TCOZ)

$TimedBuffer[X]$

$$items : \mathrm{seq}\ X$$
$$left, right : \mathbf{chan}$$

INIT

$$items = \langle\ \rangle$$

Add

$$\Delta(items)$$
$$i? : X$$
$$items' = \langle i? \rangle \frown items$$

$Remove$

$$\Delta(items)$$
$$items' = items \rhd \{last(items)\}$$

$$Join \mathrel{\widehat{=}} [i : X] \bullet left?i \to Add;\ \mathrm{DEADLINE}\ tj$$

$$Leave \mathrel{\widehat{=}} [items \neq \langle\ \rangle] \bullet right!last(items) \to Remove;\ \mathrm{DEADLINE}\ tl$$

$$\mathrm{MAIN} \mathrel{\widehat{=}} \mu\, Q \bullet (Join \,\Box\, Leave);\ Q$$

Abstract syntax

$[ZS, ZE]$ [Z schemas and expressions]

$TZE ::=$ [TCOZ constructor expressions]

$ref\langle\langle NAME\rangle\rangle \mid \textsc{Stop} \mid \textsc{Skip} \mid \textsc{Wait}\langle\langle ZE\rangle\rangle \mid (\_ \bullet \_)\langle\langle ZS \times TZE\rangle\rangle \mid$

$(\_ \rightarrow \_)\langle\langle \Sigma \times TZE\rangle\rangle \mid (\_.\_ \rightarrow \_)\langle\langle \Sigma \times ZE \times TZE\rangle\rangle \mid$

$(\_ \Box \_)\langle\langle TZE \times TZE\rangle\rangle \mid \ldots \mid (\mu \_ \bullet \_)\langle\langle NAME \times TZE\rangle\rangle$

$$TZB == \{\mathcal{C} : NAME \twoheadrightarrow\!\!\!\!\!\!\!+\;\; TZE \mid \forall\, tze : \operatorname{ran}\mathcal{C};\ N : NAME \bullet N \in \operatorname{sig} tze \Rightarrow N \in \operatorname{dom}\mathcal{C}\}$$ [TCOZ class body]

$TZC_p == [init : ZS;\ \mathcal{C} : TZB]$ [passive classes]

$TZC_a ==$ [active classes]

$[init : ZS;\ \mathcal{C} : TZB;\ main : TZE \mid \operatorname{sig} main \subseteq \operatorname{dom} TZB]$

TCOZ Semantics

The support of timing primitives in TCOZ is made possible through the adoption of Reed's timed-failures semantics for Timed CSP. The timed-failures semantics models CSP processes in terms of timed event-traces and timed event-failures. This semantic model allows CSP to be extended with time related primitives such as delays, timeouts, and clock-interrupts. In order to support objects with encapsulated state this model is extended to include an initial state and state update events. Object-Z operations are modelled as terminating sequences of timed state-update events.

- B. Mahony and J.S. Dong. Overview of the Semantics of TCOZ. *Integrated Formal Methods (IFM'99)*, pages 66-85, Springer-Verlag, York, UK, June 1999.

Exercise: A generic timed-collection in TCOZ

The generic timed-collection denotes a collection of elements of type X with a time stamp. Operations are allowed to add elements to and delete elements from the collection. When deleting an element from the collection, the oldest element should be removed and output to the environment. The collection has the following timing properties. ...

Solution

TimedCollection[X]

$$tc : \mathbb{P}(\mathbb{T} \times X)$$
$$left, right : \textbf{chan}$$
$$\Delta$$
$$t : \mathbb{T};\ oldest : X$$
$$tc \neq \varnothing \Rightarrow (t, oldest) \in tc \wedge t = min\, \mathrm{dom}\, tc$$

INIT

$$tc = \varnothing$$

Add_0

$$\Delta(tc)$$
$$e? : X;\ t_i : \mathbb{T}$$
$$tc' = ps(t_i, tc) \cup \{(t_o, e?)\}$$

$Delete_0$

$$\Delta(tc)$$
$$t_i : \mathbb{T}$$
$$tc' = ps(t_i, tc \setminus \{(t, oldest)\})$$

$$Add \mathrel{\widehat{=}} [e : X;\ t_i : \mathbb{T}] \bullet left?e\,@t_i \rightarrow Add_0$$
$$Delete \mathrel{\widehat{=}} [t_i : \mathbb{T}] \bullet right!oldest\,@t_i \rightarrow Delete_0$$
$$\textsc{Main} \mathrel{\widehat{=}} \mu\, T \bullet [tc = \varnothing] \bullet Add;\ T\ \Box$$
$$[tc \neq \varnothing] \bullet ((Add\ \Box\ Delete) \triangleright\{t\}\ tc := ps(t, tc));\ T$$

The Notion of Active Object

- Active objects have their own thread of control.
- Passive objects are controlled by other objects in a system.
- A class for defining active objects is called an *active class*
- A class for defining passive objects is called a *passive class*.
- In TCOZ, MAIN, a non-terminating process definition, distinguishes the active and the passive classes.

Inheritance between active/passive classes

- When a new active class is derived from an existing active class, the MAIN process must always be redefined explicitly.
- A new active class can be derived from an existing passive class, in this case, a MAIN process definition needs to be added.
- A new passive class can also be derived from an existing active class, in this case, the MAIN process of the existing class is implicitly removed.
- A new passive class can be derived from an existing passive class following the same rules as the standard Object-Z.

Composition and interaction of active objects

A

$v : T;\ \ldots$

$c : \mathbf{chan};\ \ldots$

$OpA_1 \mathrel{\widehat{=}} \ldots$

$\ldots$

$\textsc{Main} \mathrel{\widehat{=}} \ldots$

B

$a : A$

$\ldots$

$\ldots$

$OpB_1 \mathrel{\widehat{=}} a.OpA_1$

$\ldots$

A

$\upharpoonright(v, \ldots, OpA_1, \ldots, OpA_n)$

$\ldots$

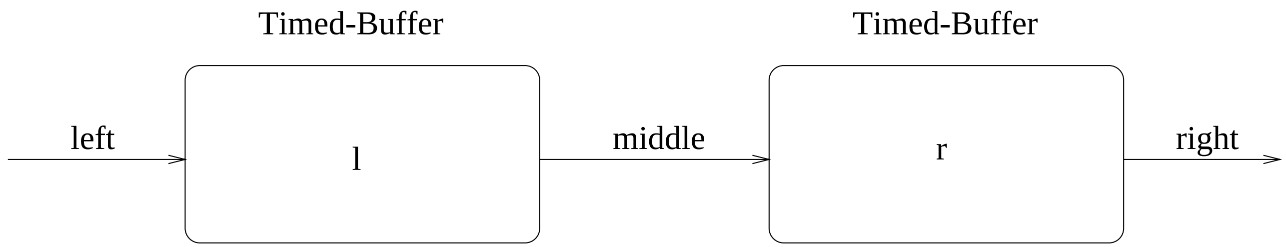
$OpA_1 \mathrel{\widehat{=}} \ldots$

$\ldots$

$\textsc{Main} \mathrel{\widehat{=}} \ldots$

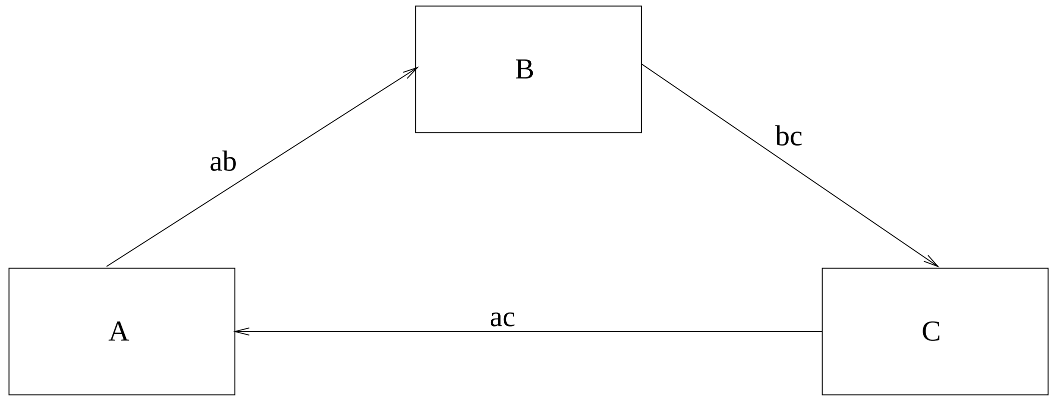
Identifying the object name with its MAIN process, e.g. if ob_1 and ob_2 are active object components, then $ob_1 \mid\mid\mid ob_2$ means $ob_1.\textsc{Main} \mid\mid\mid ob_2.\textsc{Main}$.

Two Communicating Timed Buffers



$$
\begin{array}{l}
\textit{TwoBuffers}[X] \\
\hline
l : \textit{TimedBuffer}[X][\textit{middle}/\textit{right}] \\
r : \textit{TimedBuffer}[X][\textit{middle}/\textit{left}] \\
\hline
\textsc{Main} \mathrel{\widehat{=}} (l \,|[\, \textit{middle} \,]|\, r \setminus \textit{middle})
\end{array}
$$

Complex network topologies



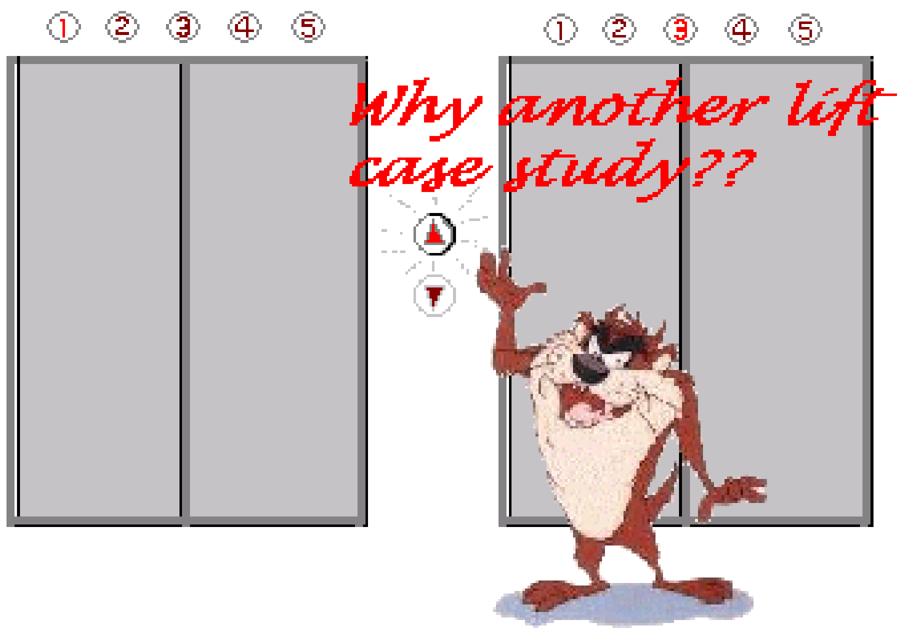
$$(A[bc'/bc] \,|[\, ab, ac \,]|\, (B[ac'/ac] \,|[\, bc \,]|\, C[ab'/ab]) \setminus ab, ac, bc)[ab, ac, bc/ab', ac', bc']$$

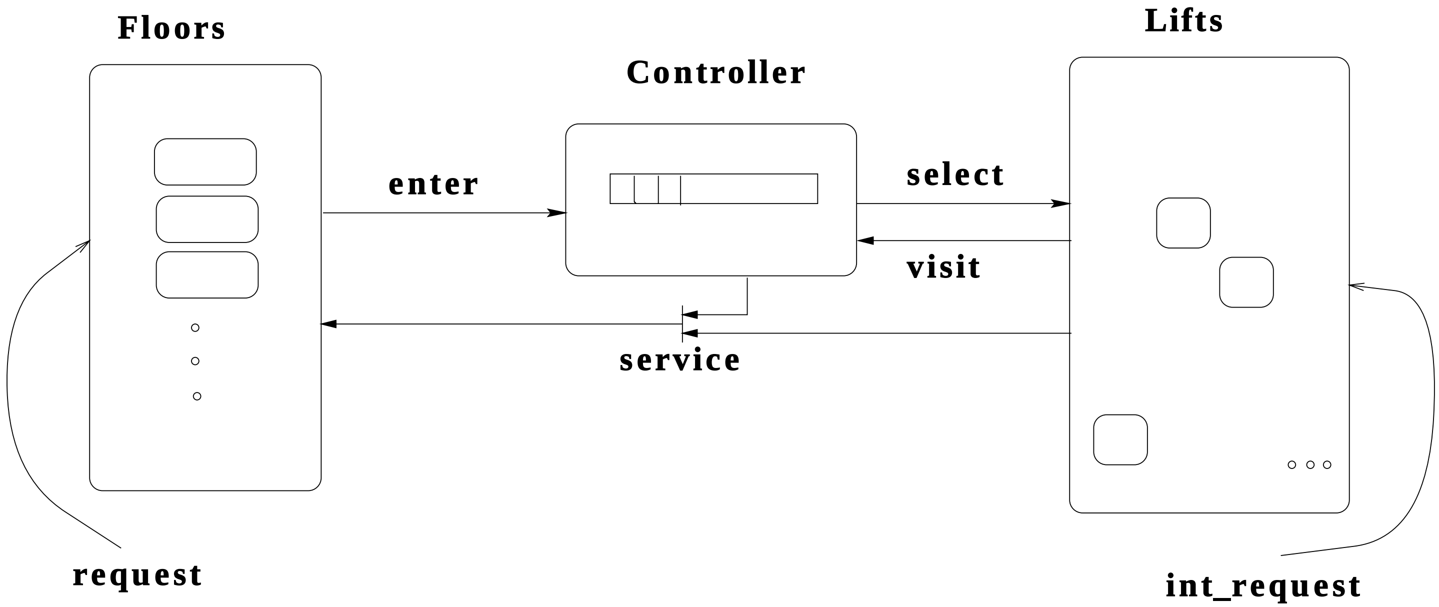
$$\left(\Big|\Big| \; v_1, v_2, v_3 \ldots \bullet \; v_1 \xleftrightarrow{ch_{12}} v_2, v_2 \xleftrightarrow{ch_{23}} v_3, v_3 \xleftrightarrow{ch_{13}} v_1, \ldots\right)(A, B, C)$$

$$\Big|\Big|(A \xleftrightarrow{ab} B, B \xleftrightarrow{bc} C, C \xleftrightarrow{ca} A) \quad or \quad \Big|\Big|(A \xleftrightarrow{ab} B \xleftrightarrow{bc} C \xleftrightarrow{ca} A)$$

The Lift Case Study

- Multi-floors with multi-elevators
- Non-trivial
- Commonly used example
- Both CSP and Object-Z have been applied (but no real-time issues)





Detailed model can be found at:

B. Mahony and J.S. Dong. Timed Communicating Object Z. IEEE Transactions on Software Engineering, 26(2):150-177, Feb 2000.

http://www.comp.nus.edu.sg/~dongjs/papers/tse00.ps

Button

$$state : On \mid Off$$

INIT

$$state = Off$$

TurnOn

$$\Delta(state)$$

$$state' = On$$

TurnOff

$$\Delta(state)$$

$$state' = Off$$

TopFloor

$$downbutton : Button_{©}$$

$$request, enter, service : \mathbf{chan}$$

INIT

$$downbutton.\textsc{Init}$$

$$PressDown \mathrel{\widehat=} [downbutton.state = Off] \bullet (request?Down \rightarrow downbutton.TurnOn);\ (enter!Down \rightarrow Skip)$$

$$DownOff \mathrel{\widehat=} service?Down \rightarrow downbutton.TurnOff$$

$$\textsc{Main} \mathrel{\widehat=} \mu\, T \bullet (PressDown \mathrel{\Box} DownOff);\ T$$

BottomFloor

$upbutton : Button_{©}$

INIT

$upbutton.\mathrm{INIT}$

...

MiddleFloor

$TopFloor, BottomFloor$

$\mathrm{MAIN} \mathrel{\widehat=} \mu\, M \bullet (PressDown \mathrel{\Box} DownOff \mathrel{\Box} PressUp \mathrel{\Box} UpOff);\ M$

$Floor \mathrel{\widehat=} TopFloor \cup BottomFloor \cup MiddleFloor$

Floors

$floors : \mathrm{seq}\, Floor_{©}$

...

$\mathrm{MAIN} \mathrel{\widehat=}\ ||| f : \mathrm{ran}\, floor$

Lift door control

Door

$$open, conf, close, servo, sensor : \mathbf{chan}$$

$$OpenDoor, CloseDoor \mathrel{\widehat=} \ldots$$

$$CycleDoor \mathrel{\widehat=} OpenDoor;\ conf \rightarrow$$

$$(\mu\, CD \bullet \textsc{Wait}\ t_o;\ CloseDoor \triangledown\{sensor?(self, Interrupt)\}\ OpenDoor;\ conf \rightarrow CD)$$

$$\textsc{Main} \mathrel{\widehat=} \mu\, D \bullet open \rightarrow CycleDoor;\ close \rightarrow D$$

Moving the lift

Shaft

$$move, arrive : \mathbf{chan}$$

$$\textsc{Main} \mathrel{\widehat=} \mu\, S \bullet move?n \rightarrow \textsc{Wait}\ |n| * \bar{t} + delay;\ arrive \rightarrow S$$

Internal_Q

$panel : \mathrm{seq}\ Button_{©}$
$int\_request, int\_sched, int\_serv : \mathbf{chan}$

$NextUp, NextDown, \textsc{Main} \mathrel{\widehat=} \ldots$

LiftControl

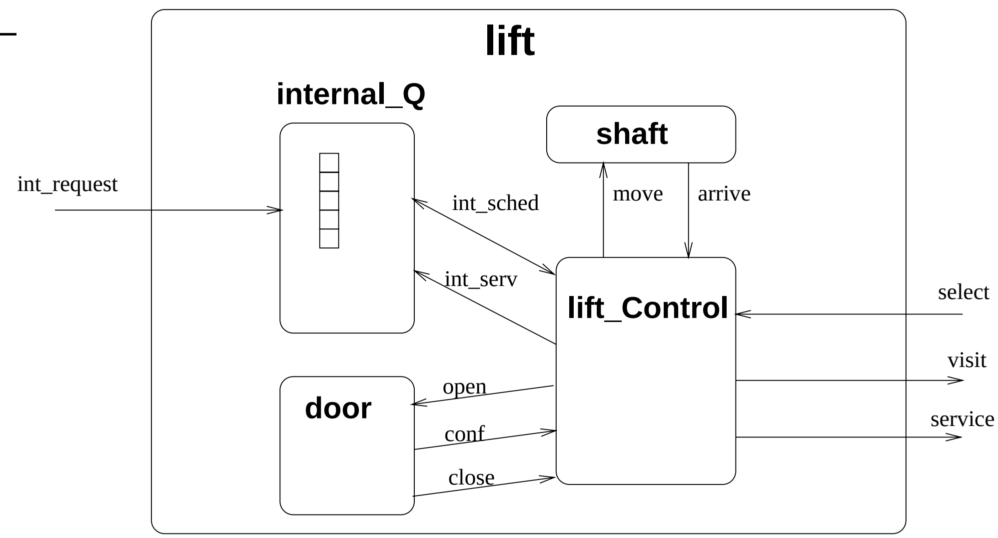
$fl : \mathbb{N}$
$md : MoveDirection$
$move, arrive : \mathbf{chan}$ [shaft]
$\ldots$

$\ldots$
$\textsc{Main} \mathrel{\widehat=} \mu\, LC \bullet$
$\quad \ldots \to Internal;\ LC\ \Box$
$\quad \ldots \to External;\ LC$

Lift

$iq : Internal\_Q_{©}$
$lc : LiftControl_{©}$
$s : Shaft_{©}$
$d : Door_{©}$

$\textsc{Main} \mathrel{\widehat{=}} \parallel ($
$\quad lc \overset{move, arrive}{\longleftrightarrow} s;$
$\quad lc \overset{open, close, conf}{\longleftrightarrow} d;$
$\quad lc \overset{int\_sched, int\_serv}{\longleftrightarrow} iq)$



Lifts

$lifts : \mathbb{P}\, Lift_{©}$

$\textsc{Main} \mathrel{\widehat{=}} \; ||| \; l : lifts$

Controller

$requests : \mathrm{seq}(\mathbb{N} \times MoveDirection)$

$enter, select, visit, service : \mathbf{chan}$

Join

...

Remove

...

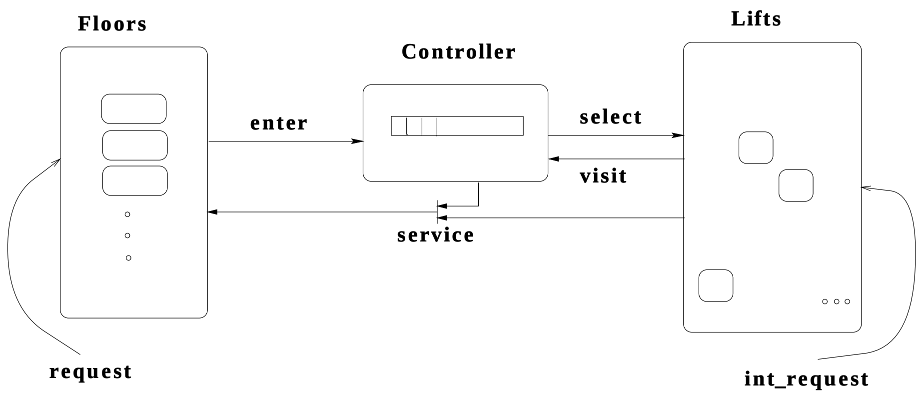
$Dispatch \mathrel{\widehat=} [...] \bullet select!item \rightarrow Remove$

$CheckServ \mathrel{\widehat=}$

$\quad [item : \mathbb{N} \times MoveDirection] \bullet visit?item \rightarrow ...$

$\textsc{Main} \mathrel{\widehat=} \mu\, C \bullet (Join \mathrel{\square} Dispatch \mathrel{\square} CheckServ);\ C$

The Lift System

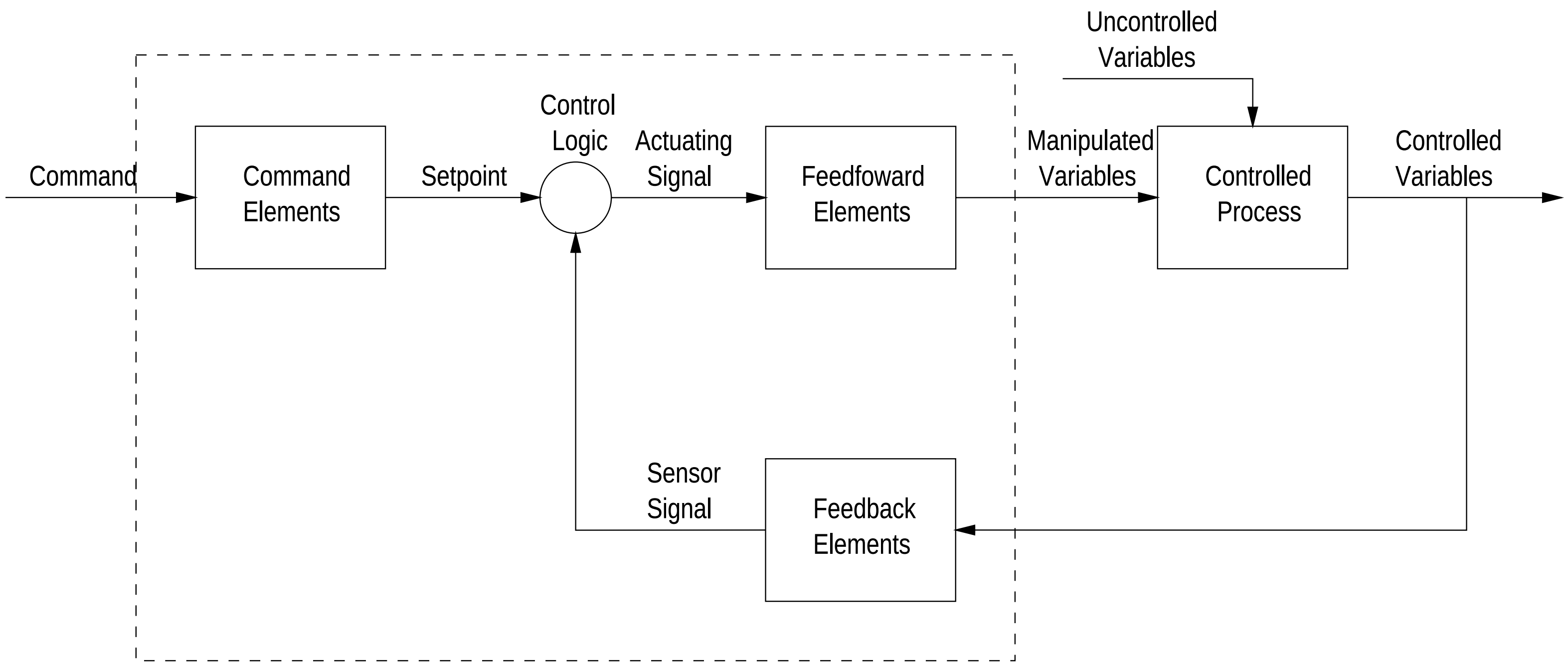


LiftSystem

$fs : Floors_{©}$
$ls : Lifts_{©}$
$contr : Controller_{©}$

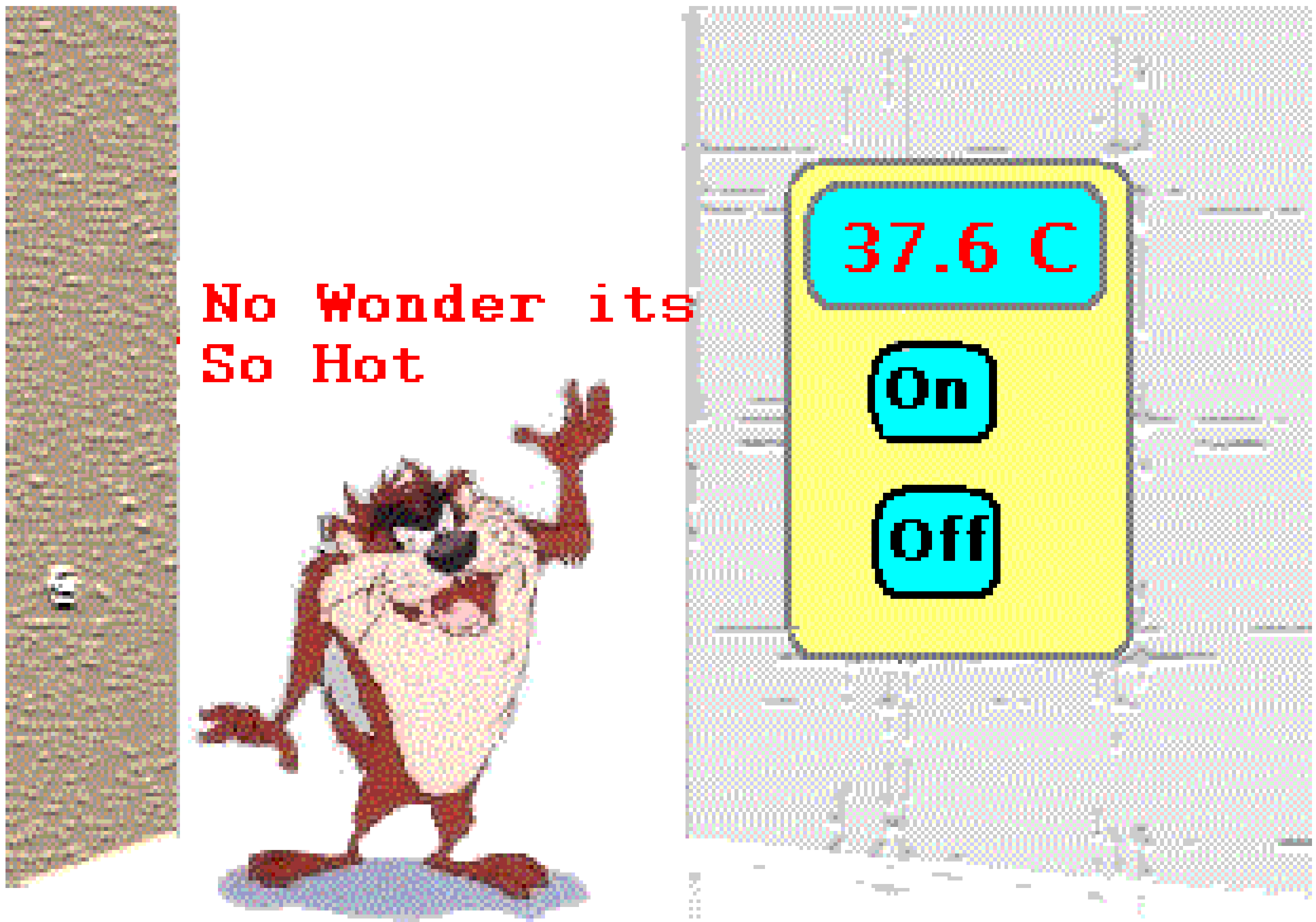
$$\textsc{Main} \mathrel{\widehat{=}} \|(fs \xleftrightarrow{enter} contr \xleftrightarrow{select,check} ls \xleftrightarrow{service} fs)$$

Sensors and Actuators — Control Systems



- CSP channel mechanism is discrete
- CSP channel mechanism is synchronous

Example: Digital Temperature Display



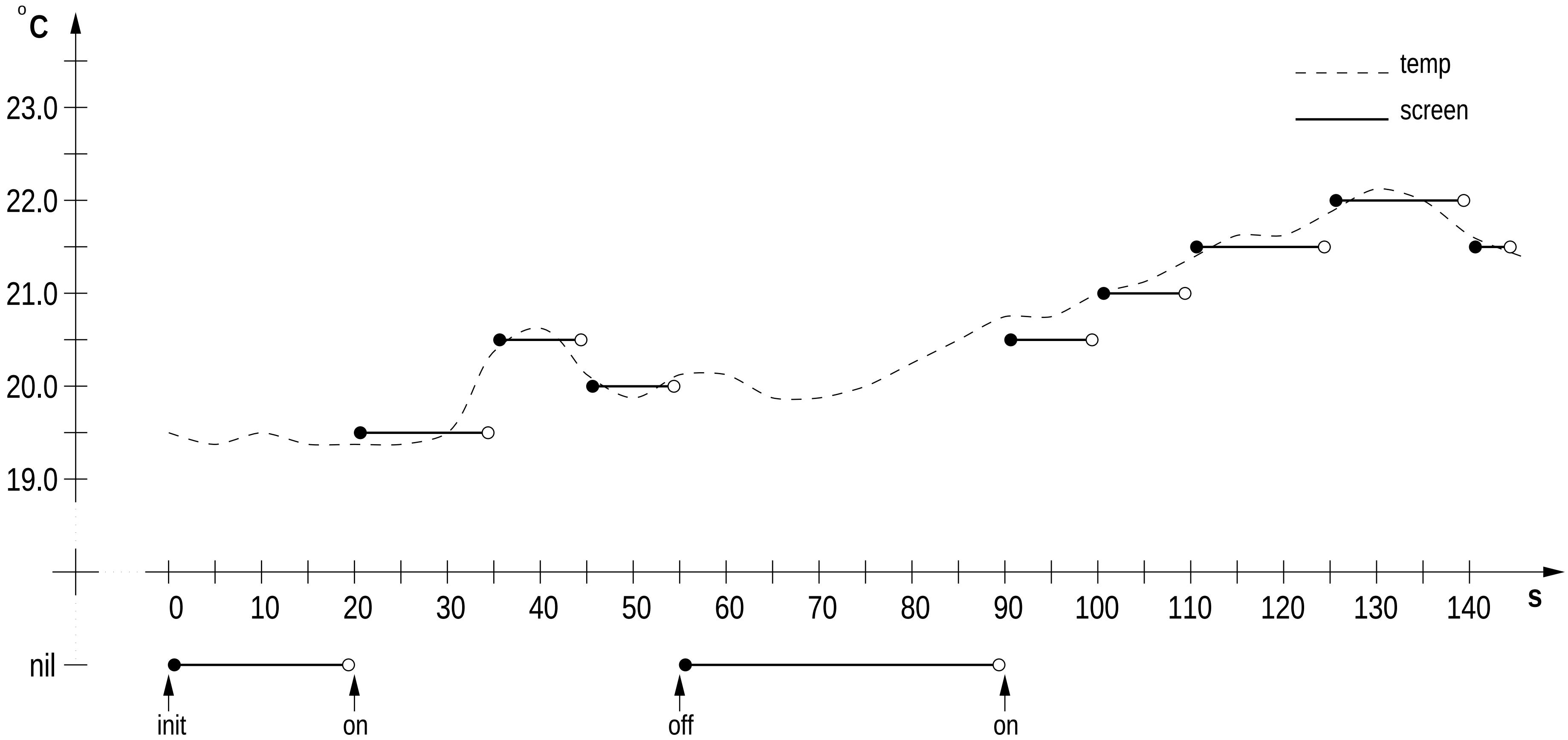


Figure 3: The office communication scenario.

$$temp : \mathbb{R}\,{}^\circ\mathsf{C}\,\mathbf{sensor}, \quad == \quad temp : \mathbb{R}\,\mathsf{s} \to \mathbb{R}\,{}^\circ\mathsf{C}\,.$$

Internally, *temp* takes the syntactic role of a CSP channel. Whenever a value v is communicated on the internal channel at a time t, $temp(t) = v$.

$$screen : Display\,\mathbf{actuator},$$

where

$$Display \ ::= \ Temp\langle\!\langle \mathbb{N} * 0.5\,{}^\circ\mathsf{C} \rangle\!\rangle \mid nil.$$

The internal role is that of the local state variable.

DTD

$$temp : \mathbb{R}\ \textbf{sensor}$$
$$screen : Display\ \textbf{actuator}$$
$$on, off : \textbf{chan}$$

SetScreen

$$\Delta(screen)$$
$$t? : \mathbb{R}^{\circ}\mathsf{C}$$

$$\exists\, dt : \mathbb{N} * 0.5^{\circ}\mathsf{C} \bullet$$
$$\quad dt = t \pm 0.5^{\circ}\mathsf{C} \wedge$$
$$\quad screen' = Temp(dt)$$

INIT

$$screen = nil$$

$$Show \mathrel{\widehat=} ([t : \mathbb{R}^{\circ}\mathsf{C}] \bullet temp?t \rightarrow SetScreen;\ \textsc{Deadline}\, 5\,\mathsf{s};\ \textsc{WaitUntil}\, 5\,\mathsf{s};\ Show)$$
$$\qquad \triangledown\ off \rightarrow NoShow$$

$$NoShow \mathrel{\widehat=} screen := nil;\ on \rightarrow Show$$

$$\textsc{Main} \mathrel{\widehat=} on \rightarrow Show$$

Asynchronous active object

Synchronous active objects

- have discrete interfaces, synchronous channels;
- are highly dependent.

Asynchronous active objects

- have analog interfaces, asynchronous sensor/actuators;
- are highly independent;
- can be further classified into *periodic* and non-periodic objects.

Exercise: a calendar clock

A typical periodic object: a calendar clock ticks every second ...

$$CalendarTime == \mathbb{N}\,\mathsf{yr} \times \mathbb{N}\,\mathsf{mn} \times \mathbb{N}\,\mathsf{dy} \times \mathbb{N}\,\mathsf{hr} \times \mathbb{N}\,\mathsf{min} \times \mathbb{N}\,\mathsf{s}\,.$$

$$Convert : \mathbb{N}\,\mathsf{s} \to CalendarTime$$

... [detail of function omitted]

Solution

Clock

$per == 1\,\mathsf{s}$

$gain == 50\,\mathsf{ms}$

$$total : \mathbb{N}\,\mathsf{s}$$
$$\Delta$$
$$display : CalendarTime\ \textbf{actuator}$$
$$\overline{}$$
$$display = Convert(total)$$

Inc

$$\Delta(total)$$
$$\overline{}$$
$$total' = total + 1$$

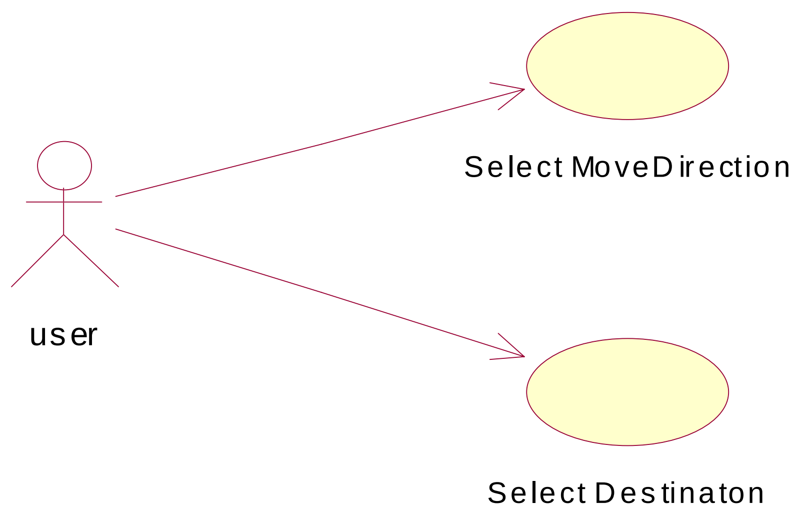
$\textsc{Main} \mathrel{\widehat=} \mu\, C \bullet Inc;\ \textsc{Deadline}\ gain;\ \textsc{WaitUntil}\ per;\ C$

UML – Revision

- UML stands for Unified (?) Modeling Language
- The UML combines/collects Data Modeling concepts (Entity Relationship Diagrams), Business Modeling (work flow), Object Modeling, and Component Modeling
- The UML is the OMG standard language for visualising, specifying, constructing, and documenting the artifacts of a software-intensive system
- UML consists of use case, class, statechart, collaboration diagrams ...

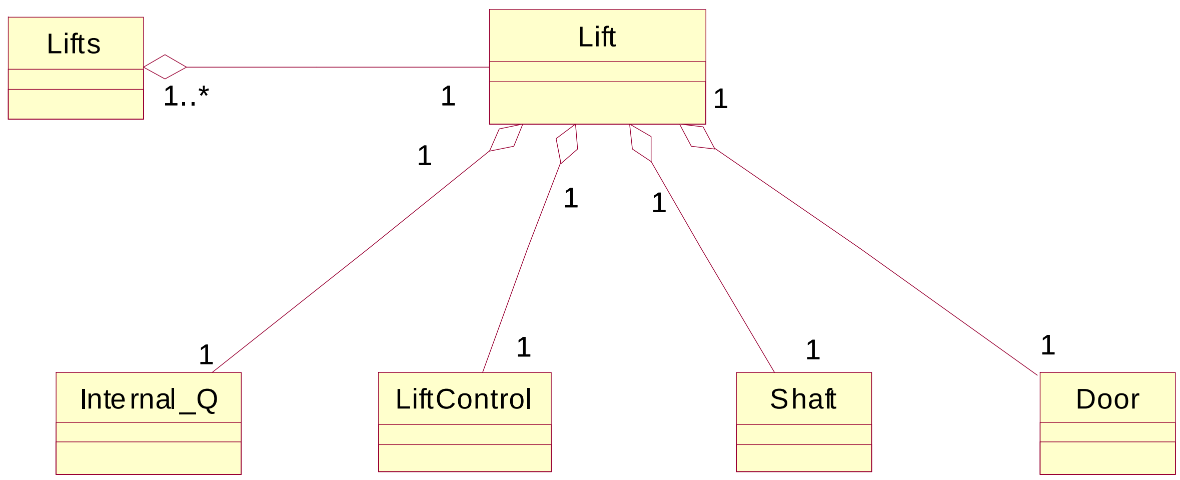
Use Case Diagram

- Use case is a pattern of behavior the system exhibits Each use case is a sequence of related transactions performed by an actor and the system in a dialogue. Actors are examined to determine their needs. Use case diagrams are created to visualise the relationships between actors and use cases



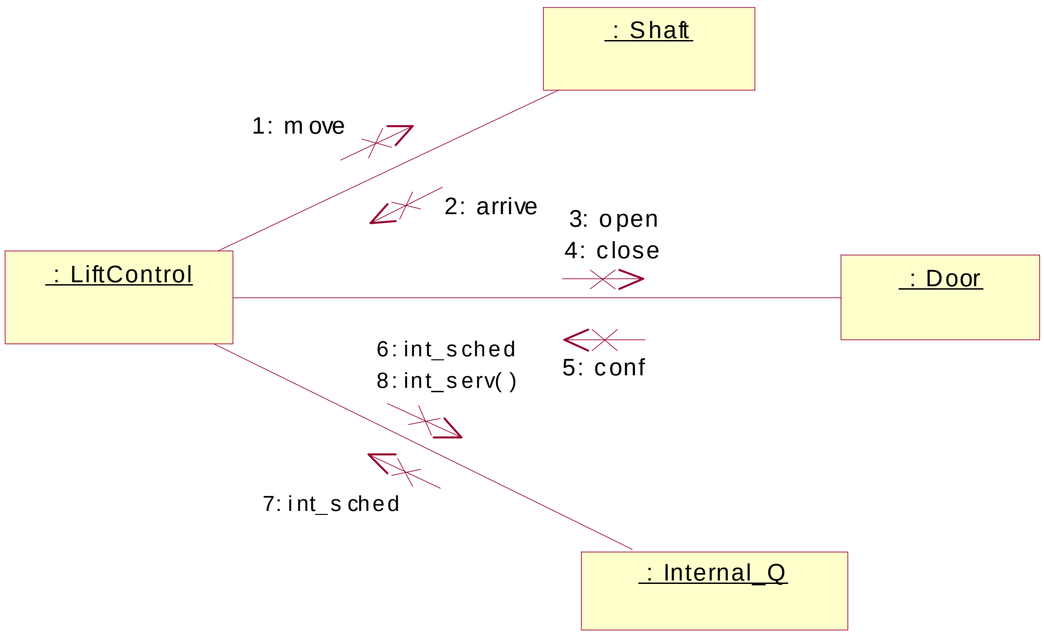
Class Diagram

- A class diagram shows the existence of classes and their relationships in the logical view of a system. It consists of classes and their structure and behavior, association, aggregation, dependency, and inheritance relationships, multiplicity and navigation indicators, and role names



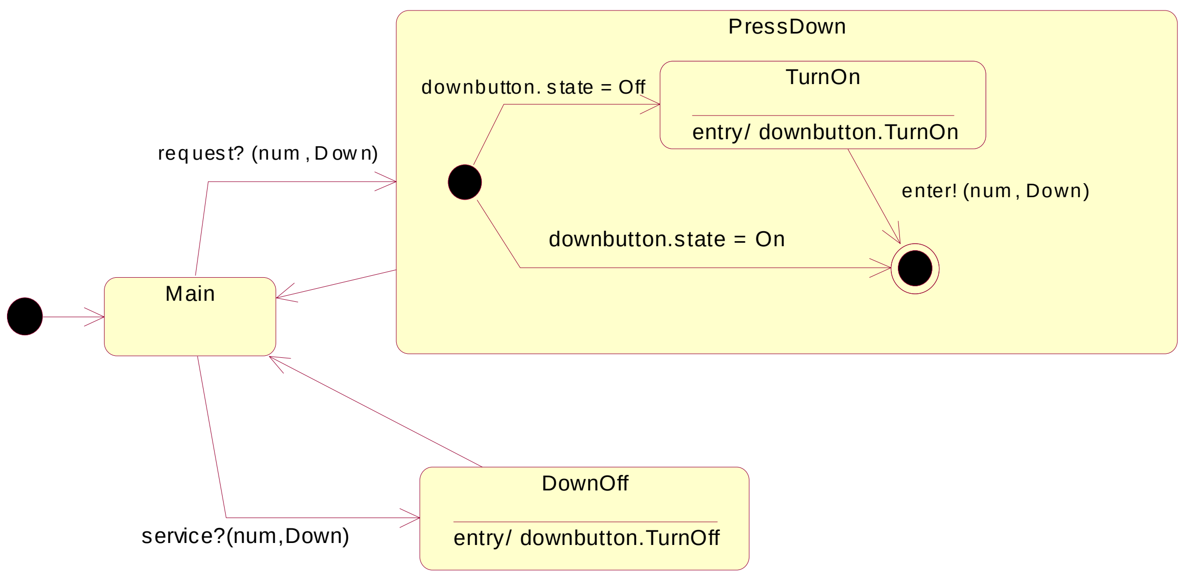
Collaboration Diagram – dynamic behavior, message-oriented

- A collaboration diagram displays object interactions organised around objects and their links to one another



Statechart Diagram – dynamic behavior, event-oriented

- A statechart diagram shows the life history of a given class, the events that cause a transition from one state to another, and the actions that result from a state change



Shortcomings of UML

- There is no unified formal semantics for all those diagrams. There are a few approaches to formalize a subset of UML, e.g. (Evans and Clark, 1998, Kim and Carrington, 1999) concentrated on class diagram semantics. Therefore, the consistency between diagrams is problematic; and

- There are limited capabilities for precisely modeling timed concurrency. For example, (in a new feature that has been added to the UML 1.3) synchronisation between concurrent substates of a single statechart diagram can be captured using a synch state link. However there is no facility to precisely model synchronous interactions between states in two different statechart diagrams.

Linking TCOZ and UML

- Syntactically, UML/OCL (Object Constraint Language) is extended with TCOZ communication interface types — chan, sensor and actuator. Upon that, TCOZ sub-expressions can be used (in the same role as OCL) in the statechart diagrams and collaboration diagrams.
- Semantically, UML class diagrams are identified with the signatures of the TCOZ classes. The states of the UML statechart are identified with the TCOZ processes (operations) and the state transition links are identified with TCOZ events/guards.
- Effectively, UML diagrams can be seen as the viewpoint visual projections from a formal TCOZ model.

Combination Process of TCOZ and UML

1. Firstly, the UML use-case models (user-case and collaboration diagrams) are used to analyse system requirements so that main classes and operations will be identified (e.g. classification of the boundary and control classes). Communication links of the collaboration diagrams guide the design of communication interfaces of the TCOZ model (synchronisation — channel, synchronisation — sensor/actuator).
2. Then, the UML class diagrams are used to capture the static structure of the system, in which class/object relationships can be captured.
3. Based on UML class diagrams, detailed TCOZ formal models are constructed in a bottom-up style. The states, timing and concurrent interactions of the system objects are captured precisely in the TCOZ models.
4. Finally, UML state diagrams are used to visualize the behaviors (process states and events) of essential components of the system, which are closely associated with the behavior parts of the TCOZ model.

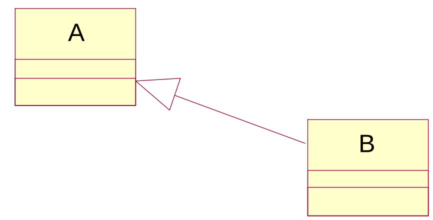
Class

B

A

......

......

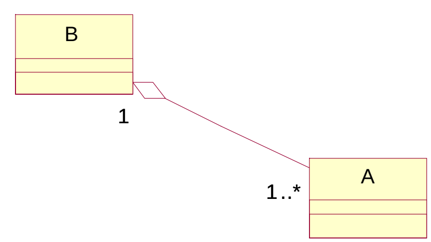


B

$a1, a2 : A$

......

......



Synchronisation

A

c : **chan**
......

$Main \mathrel{\widehat=} ...c!...$

B

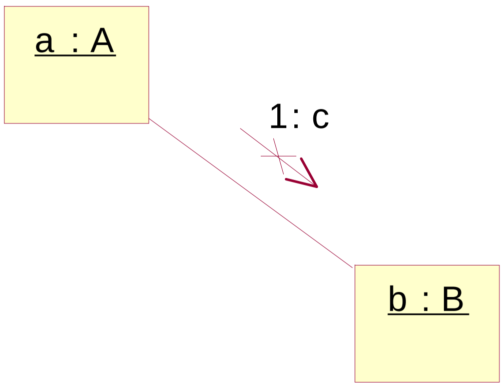
c : **chan**
......

$Main \mathrel{\widehat=} ...c?...$

AB

$a : A$
$b : B$
......

$Main \mathrel{\widehat=} ...a \overset{c}{\longleftrightarrow} b...$



Asynchronisation

A

$c : \mathbb{N}$ **actuator**
......

......

B

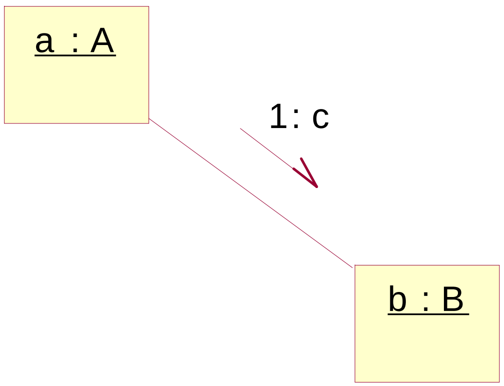
$c : \mathbb{N}$ **sensor**
......

......

AB

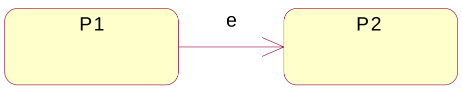
$a : A$
$b : B$
......

$Main \mathrel{\widehat{=}} ...a \xleftrightarrow{c} b...$

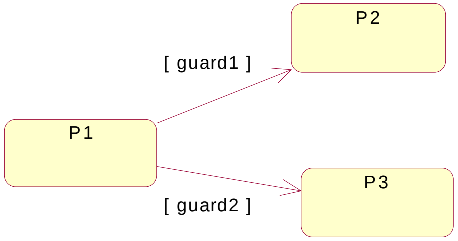


Dynamic Behavior

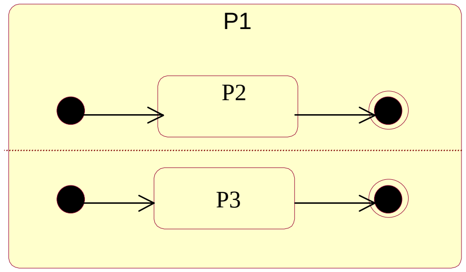
$P1;\ e \rightarrow P2$



$$P1;\ ([guard1] \bullet P2 \,\Box\, [guard2] \bullet P3)$$

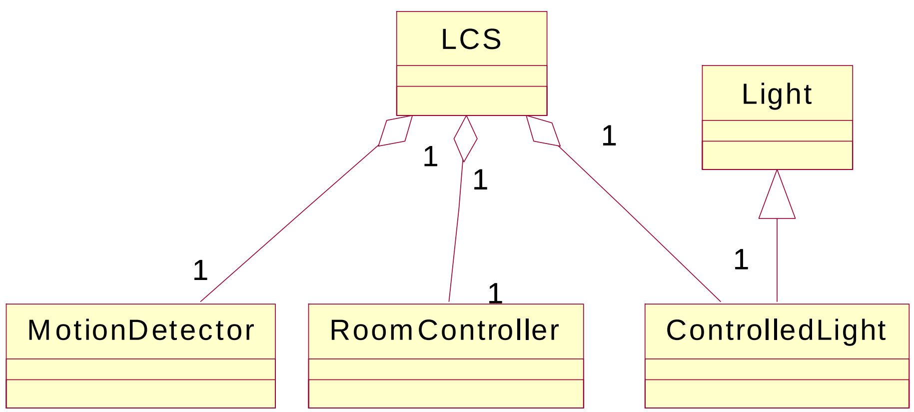


$P1 \mathrel{\widehat{=}} P2 \mid\mid\mid P3$



Light Control System (LCS)

In most existing light control systems, all lights are controlled manually. Electrical energy is wasted by lighting rooms that are not occupied and by not adjusting light levels relative to need and daylight. LCS is an intelligent control system. It can detect the occupation of the building, then turn on or turn off the lights automatically. It is able to tune illumination in the building according to the outside light level. It gains input from sensors and actuators.



$Illumination == 1..10000\,\mathsf{lux}$

$Percent == \{0\} \cup 10..100$

MotionDetector

$motion : \mathbf{chan}$

$md : (Move \mid NoMove)\ \mathbf{sensor}$ [motion sensor]

$NoUser \mathrel{\widehat{=}} md?Move \rightarrow motion!1 \rightarrow User \;\Box$

$\quad md?NoMove \rightarrow \textsc{Wait}\ 1\,\mathsf{s};\ NoUser$

$User \mathrel{\widehat{=}} md?NoMove \rightarrow motion!0 \rightarrow NoUser \;\Box$

$\quad md?Move \rightarrow \textsc{Wait}\ 1\,\mathsf{s};\ User$

$\textsc{Main} \mathrel{\widehat{=}} NoUser$

Light

$dim : Percent$ **actuator** [dim value]
$on : \mathbb{B}$

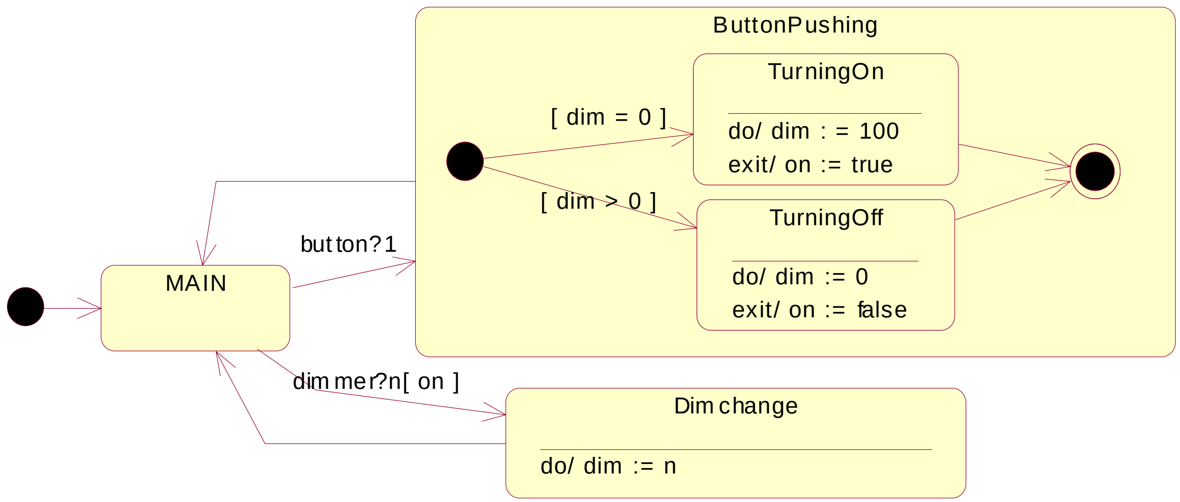
$TurningOn \mathrel{\widehat=} dim := 100;\ on := true$
$TurningOff \mathrel{\widehat=} dim := 0;\ on := false$

ControlledLight

Light

$button, dimmer :$ **chan** [control channels]

$ButtonPushing \mathrel{\widehat=} button?1 \rightarrow$
$\quad ([dim > 0] \bullet TurningOff \mathrel{\square} [dim = 0] \bullet TurningOn)$
$DimChange \mathrel{\widehat=} [n : Percent] \bullet dimmer?n \rightarrow$
$\quad ([on] \bullet dim := n \mathrel{\square} [\neg\ on] \bullet \textsc{Skip})$
$\textsc{Main} \mathrel{\widehat=} \mu\, N \bullet (ButtonPushing \mathrel{\square} DimChange);\ N$


ButtonPushing
TurningOn
do/ dim : = 100
exit/ on := true
[dim = 0]
[dim > 0]
TurningOff
do/ dim := 0
exit/ on := false
button?1
MAIN
dimmer?n[on]
Dim change
do/ dim := n

$$satisfy : Percent \leftrightarrow Illumination$$

RoomController

$$dimmer, motion : \mathbf{chan}$$
$$odsensor : Illumination\ \mathbf{sensor}$$
$$absenT : \mathbb{T}$$
$$olight : Illumination$$

Adjust

$$dim! : Percent\ \mathbf{on}\ dimmer$$

$$dim!\ \underline{satisfy}\ olight$$

$$Ready \mathrel{\widehat=} motion?1 \rightarrow On$$

$$Regular \mathrel{\widehat=} \mu R \bullet [n : Illumination] \bullet$$
$$\quad odsensor?n \rightarrow olight := n;\ Adjust;\ dimmer!dim \rightarrow R$$

$$On \mathrel{\widehat=} Regular \triangledown motion?0 \rightarrow OnAgain$$

$$OnAgain \mathrel{\widehat=} (motion?1 \rightarrow On) \triangleright\{absenT\}\ Off$$

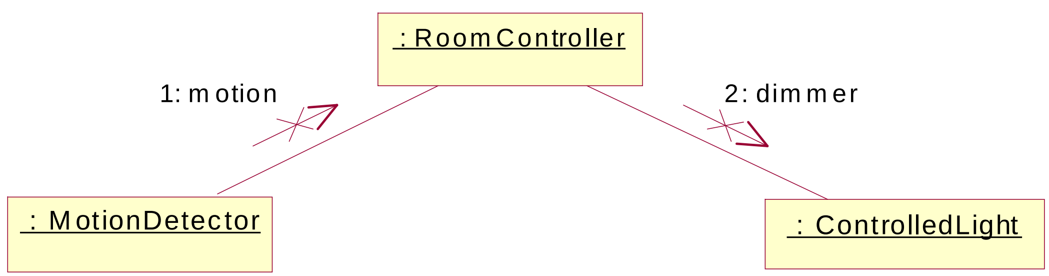
$$Off \mathrel{\widehat=} dimmer!0 \rightarrow Ready$$

$$\textsc{Main} \mathrel{\widehat=} Off$$

LCS

$m : MotionDetector$
$l : ControlledLight$
$r : RoomCtrller$

$$\textsc{Main} \mathrel{\widehat{=}} \|(m \xleftrightarrow{motion} r \xleftrightarrow{dimmer} l)$$

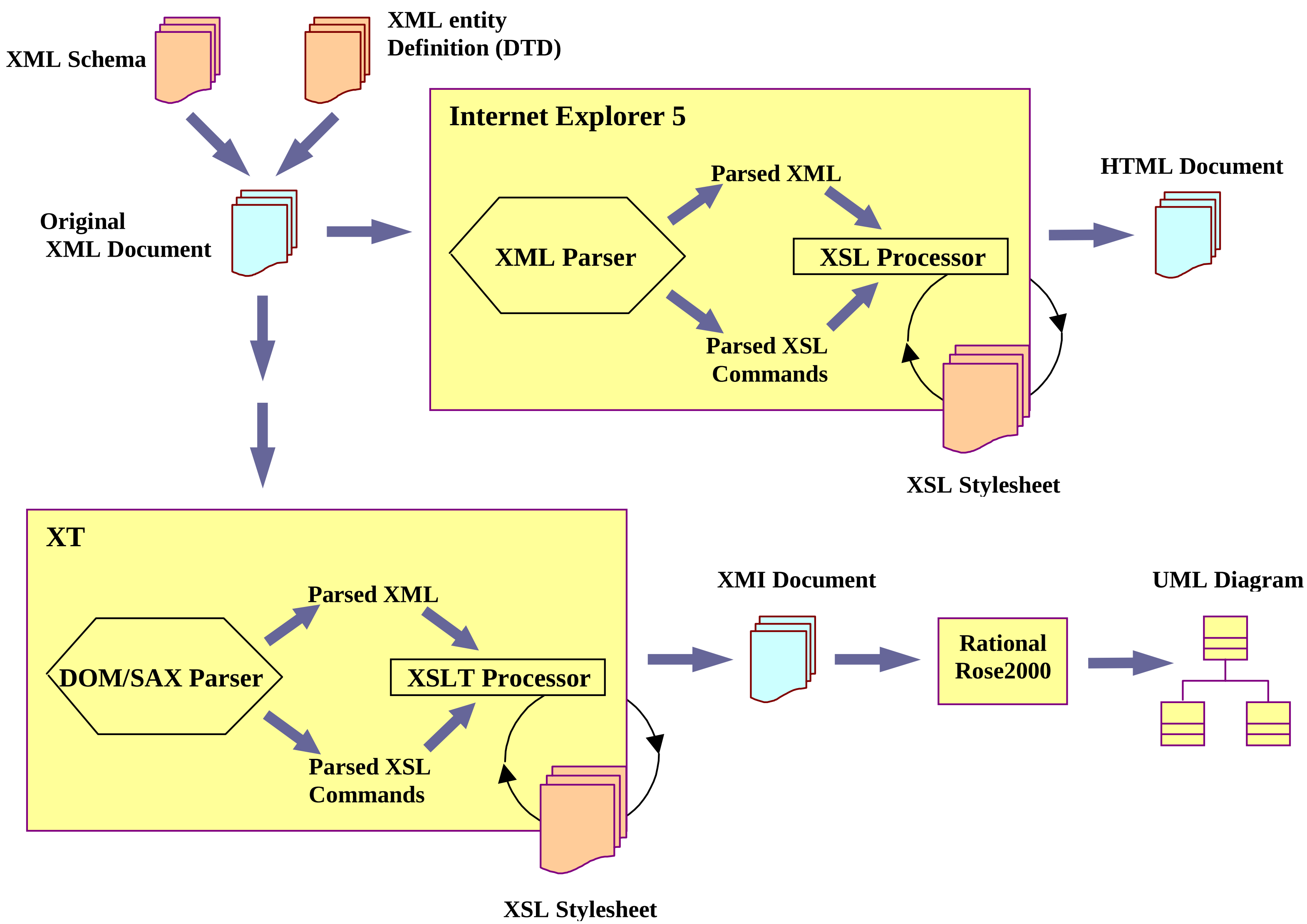


Z Family on the Web with their UML Photos

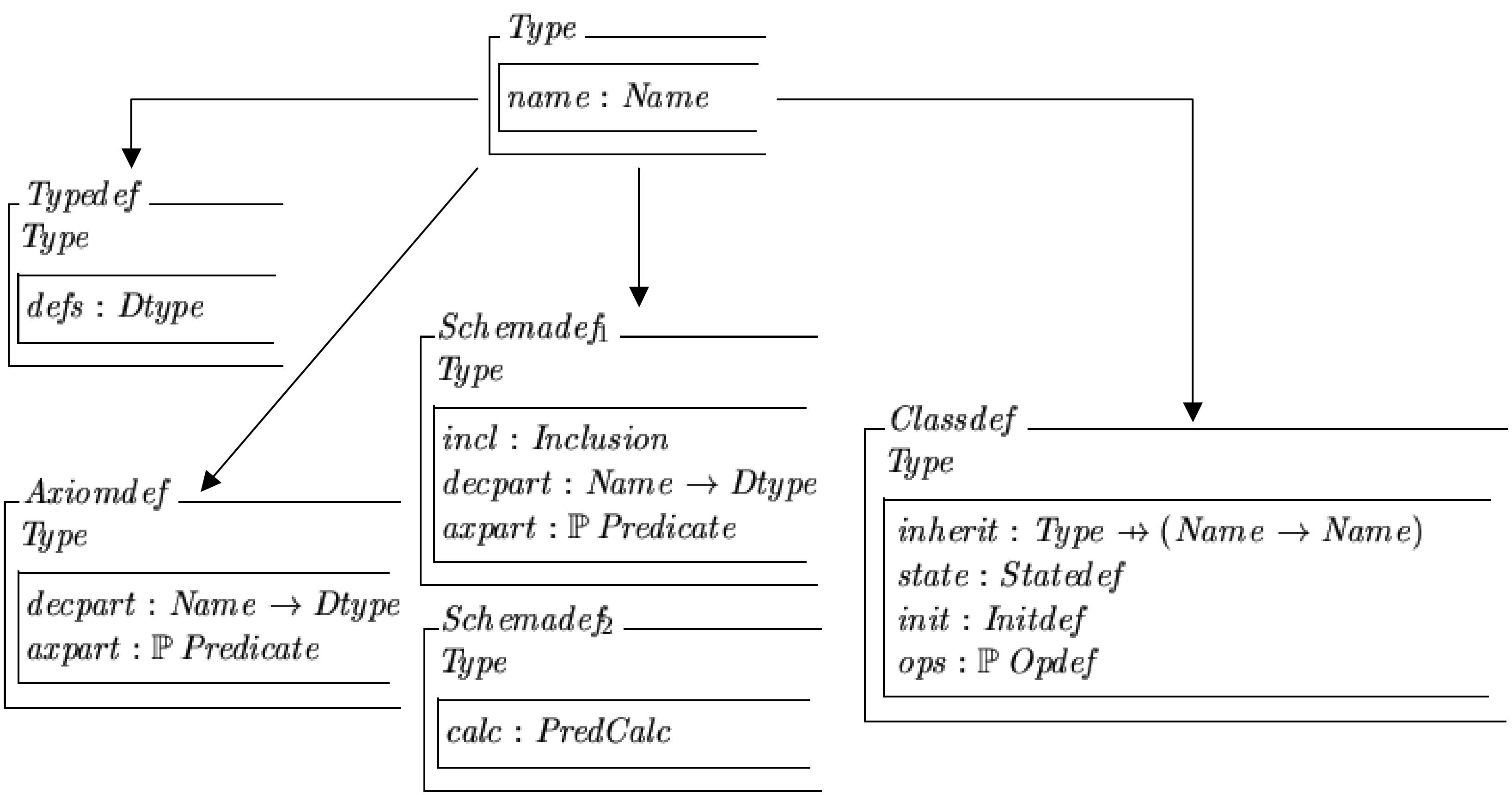
- Use eXtensible Markup Language (XML) to develop web environment for Z family languages
  - share design models
  - hyperlinks among models
  - advance browsing facilities

  `http://nt-appn.comp.nus.edu.sg/fm/zml/`

- Develop techniques for projecting (object-oriented) Z models to UML diagrams, based on XML Metadata Interchange (XMI).
- Use Object-Z to specify and design the essential functionalities of the ZML environment


XML Schema
XML entity
Definition (DTD)
Original
XML Document
Internet Explorer 5
XML Parser
Parsed XML
XSL Processor
Parsed XSL
Commands
HTML Document
XSL Stylesheet
XT
DOM/SAX Parser
Parsed XML
XSLT Processor
Parsed XSL
Commands
XSL Stylesheet
XMI Document
Rational
Rose2000
UML Diagram

Formal Object Design of ZML



$$
\begin{array}{l}
\textbf{UMLClass} \\
\hline
name : String \\
attris : String \rightarrow Dtype \\
ops : \mathbb{P}\, String \\
\hline
\end{array}
$$

$$
\begin{array}{l}
\textbf{UMLDiagram} \\
\hline
classes : \mathbb{P}\, UMLClass \\
inh, agg : UMLClass \leftrightarrow UMLClass \\
\hline
\mathrm{dom}(inh \cup agg) \cup \mathrm{ran}(inh \cup agg) \subseteq classes \\
\forall h : classes \bullet (h, h) \notin inh^{+} \\
\hline
\end{array}
$$

$$
\begin{array}{l}
project : \mathbb{P}\, Classdef \rightarrow UMLDiagram \\
\hline
\forall (oz, uml) : project \bullet \\
\quad \{c : oz \bullet c.name\} = \{c : uml.classes \bullet c.name\} \bullet \\
\quad \forall c_1, c_2 : oz \bullet \\
\qquad \exists_1\, c' : uml.classes \bullet \\
\qquad\quad c'.name = c_1.name \\
\qquad\quad c'.attris = \{cls : oz \bullet cls.name\} \lhd c_1.state.decpart \\
\qquad\quad c'.ops = \{o : Opdef \mid o \in c_1.ops \bullet o.name\} \\
\qquad c_2.name \in \{t : \mathrm{ran}\, c_1.state.decpart \bullet t.name\} \Rightarrow \\
\qquad\quad \exists_1 (c_1', c_2') : uml.agg \bullet c_1'.name = c_1.name \land c_2'.name = c_2.name \\
\qquad c_2.name \in \{inh : \mathrm{dom}\, c_1.inherit \bullet inh.name\} \Rightarrow \\
\qquad\quad \exists_1 (c_1', c_2') : uml.inh \bullet c_1'.name = c_1.name \land c_2'.name = c_2.name
\end{array}
$$

Basic Implementation Ideas

- ZML: Define a customized XML for Z family languages for web-browsing purpose
- UML tool: Rational Rose 2000 supports XMI import/export according to UML.DTD
- Translation rules are applied using XSLT techniques to automatically translate Object-Z/TCOZ model(XML) to UML diagrams(XMI) and vice versa

Syntax definition

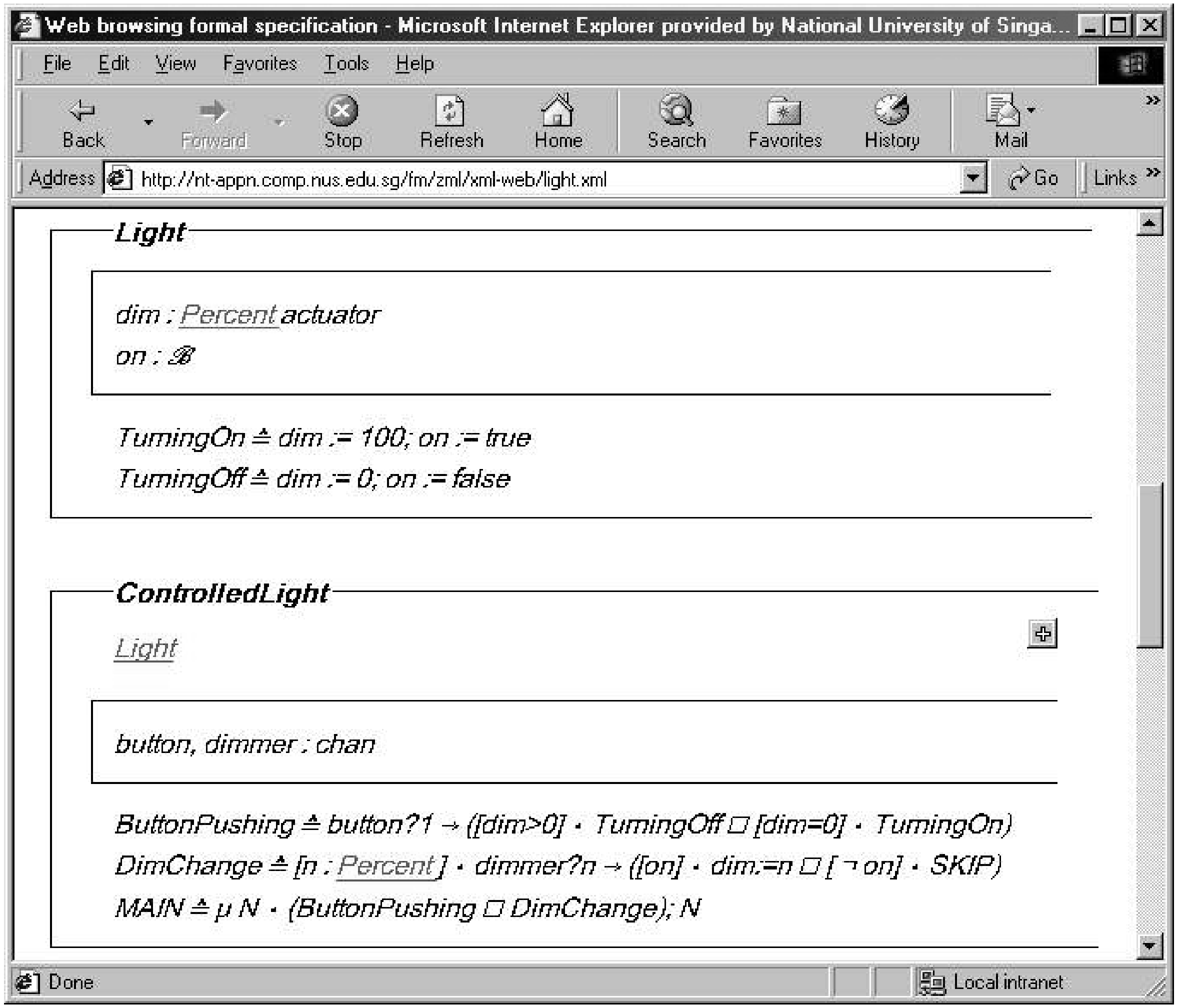
```
<ElementType name="op" content="eltOnly" order="seq">
  <element type="name" minOccurs="1" maxOccurs="1"/>
  <element type="delta" minOccurs="0" maxOccurs="1"/>
  <element type="decl" minOccurs="0" maxOccurs="*"/>
 <element type="predicate" minOccurs="0" maxOccurs="*"/>
  ...
</ElementType>
<ElementType name="classdef" content="eltOnly">
  <element type=state" minOccurs=1" maxOccurs=1"/>
  <element type=init" minOccurs="0" maxOccurs=1"/>
  <element type="op" minOccurs="0" maxOccurs="*"/>
  ...
</ElementType>
```

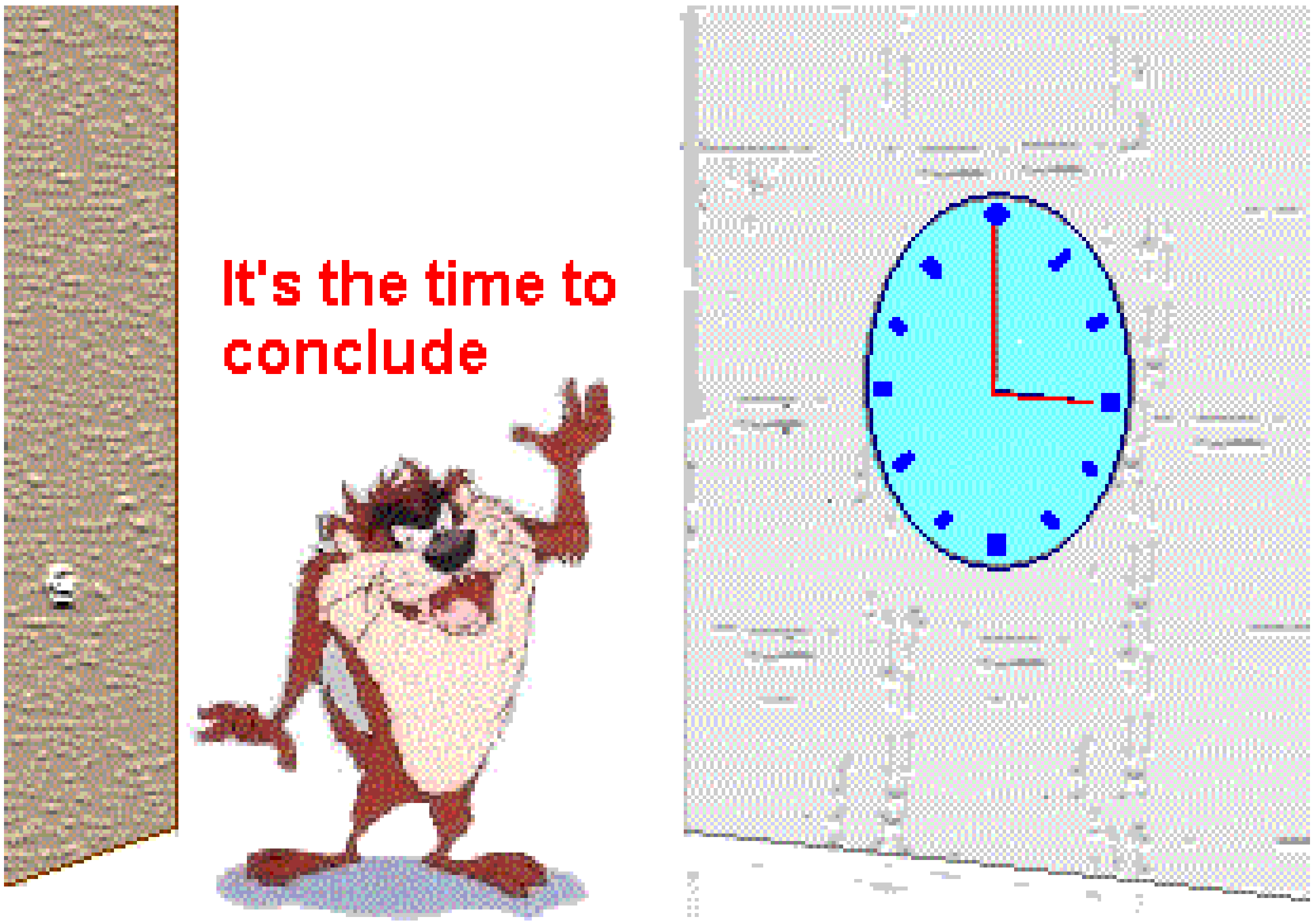
XSL Transformation

```
<xsl:template match="classdef[@layout='simpl'] classdef[@layout='gen']">
<html>
 ...
 <a><xsl:attribute name="name"><xsl:value-of select="name"/></xsl:attribute></a>
 ...
 <xsl:apply-templates select="state"/>
 <xsl:apply-templates select="init"/>
 <xsl:apply-templates select="op"/>
 ...
</html>
</xsl:template>
```

Light example

```
<classdef layout="simpl" align="left">
  <name>Light</name>
  <state>
      <decl>
          <name>dim</name>
          <dtype><type>Percent</type><type>&actuator;</type></dtype></decl>
      <decl>
         <name>on</name>
         <dtype><type>&bool;</type></dtype></decl>
  </state>
  <op layout="calc">
      <name>TurningOn</name>
      <predicate>dim := 100; on := true</predicate> </op>
      ...
</classdef>
```


Web browsing formal specification - Microsoft Internet Explorer provided by National University of Singa...
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail
Address http://nt-appn.comp.nus.edu.sg/fm/zml/xml-web/light.xml
Go Links
Light
dim : Percent actuator
on : 𝔹
TurningOn ≙ dim := 100; on := true
TurningOff ≙ dim := 0; on := false
ControlledLight
Light
button, dimmer : chan
ButtonPushing ≙ button?1 → ([dim>0] • TurningOff □ [dim=0] • TurningOn)
DimChange ≙ [n : Percent] • dimmer?n → ([on] • dim:=n □ [¬ on] • SKIP)
MAIN ≙ μ N • (ButtonPushing □ DimChange); N
Done
Local intranet


It's the time to conclude

Conclusion and Further Work

- State-based (Object-Z), Event-based (Timed CSP), Graph-based (UML)
- TCOZ
  - combines the modelling powers from Object-Z and Timed CSP
  - distinguishes the notion of *active* and *passive* objects
- Further research
  - applications to the specification of
    * software architectures
    * parallel distributed systems
  - tools support
  - Hoare and He's UTP to TCOZ semantics
  - TCOZ refinement rules

TCOZ papers

* J. Sun, J.S. Dong, J. Liu and H. Wang. Object-Z Web Environment and Projections to UML. *WWW-10: 10th International World Wide Web Conference*, ACM Press, May 2001.
* J. Liu, J.S. Dong and J. Sun. TRMCS in TCOZ, *10th International Workshop on S/W Specification and Design (ISSWD'00)*, San Diego, USA, IEEE Press, Nov, 2000.
* J. Liu, J.S. Dong, B. Mahony and K. Shi. Linking UML with Integrated Formal Techniques, *UML: Systems Analysis, Design, and Development Issues*, 2000.
* B. Mahony and J.S. Dong. Timed Communicating Object Z.*IEEE Transactions on Software Engineering*, 26(2):150-177, Feb 2000.
* J.S. Dong, B. Mahony and N. Fulton, Capturing Concurrent Interactions of Mission Computer Tasks, *The 6th Asia-Pacific S/E Conference (APSEC'99)*, IEEE Press, Dec, 1999.
* B. Mahony and J.S. Dong. Sensors and Actuators in TCOZ. *World Congress on Formal Methods (FM'99)*, Lecture Notes in Computer Science, Springer-Verlag, Toulouse, France, Sep 1999.
* B. Mahony and J.S. Dong. Overview of the Semantics of TCOZ. *Integrated Formal Methods (IFM'99)*, Springer-Verlag, York, UK, June 1999.
* J.S. Dong and B. Mahony. Active Object in TCOZ. *the IEEE International Conference on Formal Engineering Methods (ICFEM'98)*, pages 16-25, IEEE Press, Brisbane, Dec 1998.
* B. Mahony and J.S. Dong. Network Topology and a Case Study in TCOZ. *the 11th International Conference of Z Users (ZUM'98)*, LNCS, pp 308-327, Springer-Verlag, Berlin, Sep 1998.
* B. Mahony and J.S. Dong. Blending Object-Z and Timed CSP: An introduction to TCOZ. *the 20th International Conference on S/E (ICSE'98),* pages 95-104, IEEE Press, Kyoto, April 1998.

`Most online versions can be found at: http://www.comp.nus.edu.sg/~dongjs`

Other integrated approaches (partial collection)

- G. Smith and J. Derrick. Specification, refinement and verification of concurrent systems - an integration of Object-Z and CSP, Formal Methods in System Design, 2001. (To appear.)
- H. Treharne and S. Schneider. How to Drive a B Machine, ZB 2000 , Lecture Notes in Computer Science. Springer-Verlag, 2000.
- C. Fischer. Combination and implementation of processes and data: from CSP-OZ to Java. PhD thesis. University of Oldenburg, 2000.
- H. Wehrheim. Data Abstraction for CSP-OZ. In FM'99: World Congress on Formal Methods, Lecture Notes in Computer Science. Springer-Verlag, 1999.
- M. Butler. csp2B: A Practical Approach to Combining CSP and B. In FM'99: World Congress on Formal Methods, Lecture Notes in Computer Science. Springer-Verlag, 1999.
- C. Bolton, J. Davies and J. Woodcock. On the Refinement and Simulation of Data Types and Processes. In Integrated Formal Methods (IFM'99). Springer-Verlag, 1999.
- C. Suhl. RT-Z: An Integration o Z and timed CSP. In Integrated Formal Methods (IFM'99). Springer-Verlag, 1999.
- K. Taguchi and K. Araki. The State-Based CCS Semantics for Concurrent Z Specification ICFEM'97. IEEE Press, 1997
- A. Galloway and W. Stoddart. An operational semantics for ZCCS. ICFEM'97. IEEE Press, 1997