How to contact the author

Bruce Powel Douglass, Ph.D.
Chief Evangelist
*i-Logix, Inc.*
1309 Tompkins Drive Apt F
Madison, WI 53716
(608) 222-1056
bpd@ilogix.com

see our web site
www.ilogix.com
About the Author

- Almost 20 years in safety-critical hard-real time systems
- Mentor, trainer, consultant in real-time and object-oriented systems
- Author of
  - *Doing Hard Time: Using Object Oriented Programming and Software Patterns in Real Time*
- Partner on the UML proposal
- Embedded Systems Conference Advisory Board
All the best lies are actually true!
Agenda

- Approach taken for this talk
- Quick Overview of Finite State Machines
- Quick Overview of Harel Statecharts
- Advanced Statechart features
- Other State Notations
Approach taken for this talk

- This is meant to be a gentle introduction to states and state machines

- This section will be
  - mostly on advanced features of statecharts
  - other state representations

- Ask questions if you don’t think your neighbor is understanding
Finite State Machine Review

- What’s a STATE?
- What’s a TRANSITION?
- What are the three classes of behavior?
- What kinds of things have state?
- Why model states?
Simple Example

- **Message Ready / Start Timer**
- **Sending**
- **Idle**
  - Valid ACK
  - \( \text{tm(Wait\_Time)} \) \[ \text{Transmit\_Count} \leq \text{Limit} \]
- **Waiting**
  - \( \text{tm(Wait\_Time)} \) \[ \text{Transmit\_Count} > \text{Limit} \]
  - Done / Transmit\_Count++
  - Invalid ACK
Advanced Statechart Features

- Conditional Transitions
- Orthogonal Components
- Concurrency
- Broadcast transitions
- Inherited state behavior
Conditional Transitions

- **Uploading_Data**
  - \([\text{CMDID}(msg) == \text{Upload}]\)

- **Processing_Command**
  - \([\text{CMDID}(msg) == \text{Update}]\)
  - \([\text{CMDID}(msg) == \text{Store}]\)

- **Updating_Parameters**

- **Error**
  - \([\text{else}]\)
  - \([\text{isValid}(msg)]\)

- **Message_Received**

- **Receiving**

- **Storing_Sense_Data**
Orthogonal Components

- Model state behavior for independent aspects of objects
- Can be used to model
  - concurrency
  - independent attributes
- Simplify state diagrams by reducing “state explosion”
## Orthogonal Components

### myInstance: myClass

<table>
<thead>
<tr>
<th>tColor</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>boolean</td>
<td>ErrorStatus</td>
</tr>
<tr>
<td>tMode</td>
<td>Mode</td>
</tr>
</tbody>
</table>

```java
enum tColor {eRed, eBlue, eGreen};
enum boolean {TRUE, FALSE}
enum tMode {eNormal, eStartup, eDemo}
```

**How do you draw the state of this object?**
### Approach 1: Enumerate all

<table>
<thead>
<tr>
<th>eRed</th>
<th>eBlue</th>
<th>eGreen</th>
</tr>
</thead>
<tbody>
<tr>
<td>FALSE, eDemo</td>
<td>FALSE, eDemo</td>
<td>FALSE, eDemo</td>
</tr>
<tr>
<td>TRUE, eDemo</td>
<td>TRUE, eDemo</td>
<td>TRUE, eDemo</td>
</tr>
<tr>
<td>FALSE, eNormal</td>
<td>FALSE, eNormal</td>
<td>FALSE, eNormal</td>
</tr>
<tr>
<td>TRUE, eNormal</td>
<td>TRUE, eNormal</td>
<td>TRUE, eNormal</td>
</tr>
<tr>
<td>FALSE, eStartup</td>
<td>FALSE, eStartup</td>
<td>FALSE, eStartup</td>
</tr>
<tr>
<td>TRUE, eStartup</td>
<td>TRUE, eStartup</td>
<td>TRUE, eStartup</td>
</tr>
<tr>
<td>TRUE, eStartUp</td>
<td>TRUE, eStartUp</td>
<td>TRUE, eStartUp</td>
</tr>
<tr>
<td>TRUE, eNormal</td>
<td>TRUE, eNormal</td>
<td>TRUE, eNormal</td>
</tr>
<tr>
<td>TRUE, eDemo</td>
<td>TRUE, eDemo</td>
<td>TRUE, eDemo</td>
</tr>
</tbody>
</table>
Approach 2
What is Concurrency?

- Concurrency is the simultaneous execution of program statements within a system
- Types:
  - Pseudo-concurrency (Single CPU)
  - True Concurrency (Multiple CPUs)
Pseudo-Concurrency

- **Heavy-weight (process)**
  Each process has its own data and code space

- **Light-weight (thread)**
  Each thread shares a common data and code space
Synchronization Models

- Sharing data
  - Shared variables
  - Message passing

- Types of synchronization
  - Synchronous
  - Asynchronous
  - Balking
  - Timeout
Synchronization Models

- Operations may be
  - Guarded
  - Synchronous
  - Simple (i.e. function calls)

- Events imply
  - Asychronicity
  - Event queues
UML Concurrency

- Each thread is based from a single “active” object
- All components of the active object inherit the composite’s thread
- Each thread must have its own event queue
Concurrent Statecharts

- Many embedded systems consist of multiple threads, each running an FSM
- State charts allow the modeling of these parallel threads
Concurrent State Charts

- States S and T are active at the same time as long as X is active.
  - Either S.A or S.B must be active when S is active
  - Either T.C, T.D, or T.E must be active when T is active
Concurrent State Charts

- When X exits, both S and T exit
  - If S exits first, the FSM containing X must wait until T exits
  - If the two FSMs are always independent, then they must be enclosed at the highest scope
Explicit Synchronization

Starting

Explicit control branching

Finishing

Explicit control resynchronization
Example Concurrent FSM
Communication in Concurrent FSMs

- **Broadcast events**
  - Events received by more than one concurrent FSM
  - Results in transitions of the same name in different FSMs

- **Propagated transitions**
  - Transitions which are generated *as a result* of transitions in other FSMs
Propagation and Broadcasts
Inherited State Behavior

- Two approaches to inheritance for generalization of reactive classes
  - Reuse (i.e. inherit) statecharts of parent
  - Use custom statecharts for each subclass
- Reuse of statecharts allows
  - specialization of existing behaviors
  - addition of new states and transitions
  - makes automatic code generation possible
Inherited State Behavior

- Assumes Liskov Substitution Principle for generalization:
  *A subclass must be freely substitutable for the superclass in any operation*

- You CAN
  - Add new states
  - Elaborate substates in inherited states
  - Add new transitions and actions

- You CANNOT
  - Delete inherited transitions or states
Inherited State Models

Blower

Dual Speed Blower

Dual Speed Multiheat Blower

Off

Switch On / \( f() \)

On

Switch Off

Switch On / \( g() \)

Off

Switch Off / \( h() \), \( k() \)

On

Low

High

Switch On

Off

Switch Off / \( k() \)

On

Low

High

Cool

Warm

Hot
FSM Example: VVI Pacemaker

- 2 key objects executing concurrently
  - Communications object
  - Pacing Engine object

- Each can be modeled as an FSM

- IT IS NOT APPROPRIATE NOT TO USE CONCURRENCY IN THIS APP
Pacemaker Object Model

- Programmer
- Communication
- Coil Driver
- Communication
- Gnome
- Ventricular Pacing Engine
  - Mode
  - Pacing Rate
  - Pulse Amplitude
  - Pulse Width
- Heart
Ventricular Pacing Engine States

Statechart of Ventricular Pacing Engine:
- **On**
  - tm(PulseWidth)
  - Disable Pace Electronics
- **Refractory**
  - tm(RefractoryTime) / EnableSensor()
- **Pacing**
  - tm(SenseTime) / Disconnect Sensor
  - Enable Pace Electronics
- **Waiting_for_Sense**
  - Set Parameters / Activate for next cycle
- **Off**
  - Pace Start Cmd
  - Pace Stop Cmd
- V Sense

Communication Gnome States

Enable Comm

Disabled

Enable Comm

Receiving

ByteReceived

Waiting_for_Body

Validating

Processing

Enabled

Idle

tm(MsgTime)

Transmitting

Waiting_for_Msg_Timeout

tm(ByteTime)

[isDone()]

Waiting_for_Body_Req

tm(ByteTime)

[else]

[isValid(msg)]
Communication Coil Driver States

- **Idle**
  - Transmit Byte Ready
  - [isDone( )]
  - [else] / get next bit
  - tm(transWait)

- **Receiving_Bit**
  - Pulse Transition /
  - time = 0
  - tm(byteTime)
  - tm(transBitTime)

- **Waiting_for_Bit**
  - Pulse Transition /
  - ++

- **Transmitting_Bit**
New Pacemaker Spec

- Both Atrial and Ventricular Pacing must be supported:
  - AAI, AAT, VVI, VVT, AVI
- Behavior for AAI is the same as VVI except it is a different object instance
- Behavior for AAT is the same as VVT except it is a different object instance
- Atrial behavior in AVI is different from ventricular behavior
Pacemaker Inherited States

- Communication Coil Driver
- Communication Gnome
- Pacing Engine
  - Mode
  - Pacing Rate
  - Pulse Amplitude
  - Pulse Width
- Ventricular Pacing Engine
- Atrial Pacing Engine
- "actor" Heart
- "actor" Programmer
Pacing Engine States

The diagram illustrates the states and transitions of a pacing engine. The states include:

- **Idle**
- **On**
- **Off**
- **Dual**
- **Refactory**
- **Waiting**
- **Pacing**

Transitions include:

- **ToIdle**
- **ToInhibited**
- **ToOn**
- **ToOff**
- **ToDual**
- **ToTriggered**

Events and timer functions associated with the transitions are indicated in the diagram.
Atrial AVI Mode State

Atrial Pacing Engine AVI Mode

- **Refractory**
  - **Atrial Pacing Done**
  - **V Refractory Done**

- **Pacing**
  - tm(V_Sense Time) ^ Atrial Pacing Start

- **Waiting for Sense**
  - V Sense
  - Set Parameters / Activate for Next Cycle
Ventricular AVI Mode State

Ventricular Pacing Engine AVI Mode

- Refractory
- Atrial Pacing Done
  - tm(re refractoryTime) ^
  - V_Refractory Done / Enable Sensor
- Waiting for A Pace
- Atrial Pacing Start
  - V Sense
- Waiting for Sense
  - Set Parameters / Activate for Next Cycle
What is shown in Statecharts?

- Complete state space
- Static structural view
- Supports
  - Nesting
  - Concurrency
  - Propagated transitions
  - Broadcast Transitions
Other State Notations

- State Transition Tables
- State Specifications
- Augmented Message Sequence Diagrams
- Timing Diagrams
- Petri Nets
State Transition Tables

- Arranged as
  - Source x Target state
  - Source State x Transition

- Statecharts are very good at showing the structure of the state space

- Tables are very good at identifying missing transitions

- Shlaer & Mellor say you should do both
# State Table for VVI Engine

## Transitions

<table>
<thead>
<tr>
<th>States</th>
<th>Stop</th>
<th>Start</th>
<th>Done</th>
<th>Timeout</th>
<th>V Sense</th>
<th>Set Param</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Off</td>
<td>-</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2 Refractory</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3 Pacing</td>
<td>1</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4 Waiting</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>
What’s shown in State Tables?

- Complete state space
- Good for seeing missing/erroneous transitions
- No concurrency (one thread per table)
- Propagated transitions
- Broadcast transitions
- No actions
Object (Module) State Specifications

- Work in conjunction with statecharts and state tables
- Textual specifications
State Specifications

- **State**
  - Name
  - Description
  - Activities
  - Transitions accepted

- **Transitions**
  - Name
  - Guards
  - Event List
  - Actions List
State Specifications

- Easy to define requirements which are
  - Testable
  - Traceable (good for TUV, FDA, DoD)
- Can fully describe and define the states and transitions
- Recommendation: *Put all three in a single object behavioral document*
  - Statecharts
  - State tables
  - State specifications
Augmented Sequence Diagrams

- Dynamic
  - Do not show full state space
- Show specific thread through the state space
  - "Scenario"
- Can be augmented with State indicators
- Good for "walking through" behavior
- Do not replace static structural views
Sequence Diagrams

- Vertical lines represent objects
- Horizontal arrows represent messages (incl. transitions)
- Time flow from the top of the page downwards
- Sequence only is shown normally
Augmented Sequence Diagrams
Adding Time Annotations

Pacing_Engine  Pacing_Timer  Ventricular_Sensor

Pacing_Rate_Time()  

Ventricular_Event()  

Ventricular_Event()  

Pulse_Width_Time()  

\{ b - a < 2 \text{ ms} \}  

\{ 800 \text{ ms} +/- 10 \text{ ms} \}
What’s shown in Augmented Sequence Diagrams?

- Dynamic scenarios
  - typically a single state chart will result in *many* ASDs
- Good place to add dynamic timing information
- Not all messages result in state transitions
Timing Diagrams

- Familiar
  - Used by electrical engineers

- Show state along vertical axis

- Show linear time along horizontal axis

- Depict particular scenarios

- For usage see
  - *Doing Hard Time: Using Object Oriented Programming and Software Patterns in Real Time Applications* (Addison-Wesley, Spring 1999)
Simple Timing Diagram

- **State**: Off, Refractory, Waiting for V Sense, Pacing
- **Time**: Pace Start Cmd, Ventricular Sense, Timeout, Done

Bruce Powel Douglass, Ph.D.
Complex Timing Diagram

- Initiation Time
- Rise Time
- Execution Time
- Dwell Time
- Fall Time
- Slack Time
- Leading Jitter
- Trailing Jitter
- Period
- Deadline
Example with jitter and rise times
Example with Dwell and Slack

<table>
<thead>
<tr>
<th>Time</th>
<th>Initiation</th>
<th>Execution</th>
<th>Dwell</th>
<th>Deadline</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Concurrency in Timing Diagrams

- Concurrency can be shown by creating horizontal “bands” of states
  - Usually one band per object
- Shows the timing relationships between concurrent threads
Concurrency in Timing Diagrams

- Acquiring
- Storing
- Idle
- Inserting
- Removing
- Off
- Acquiring
- Scaling
- Displaying

Waveform Parameter
Queue
Waveform Display

Bruce Powel Douglass, Ph.D.
Other Applications of Timing Diagrams

- Show timing relationships of functional call threads
- Show testable time budgets
- Assist in understanding RMA results
- Shows sequence of states and object reactions to events
What’s shown in Timing Diagrams?

- Good view of overall time
- Timing of interaction of concurrent states
- Timing details
  - Jitter
  - Execution time
  - Dwell time
  - Slack time
  - Rise and Fall time
Petri Nets

- Petri nets are a generic modeling tool
- FSMs are a special case of Petri nets
- Petri nets are defined as a set of
  - Places which hold tokens
  - Tokens small filled circles
  - Arcs directed lines
  - Transitions bars connecting arcs from places to places
- Petri nets can show concurrency by permitting multiple tokens
Petri Net Rules

- A Petri net is executed by moving tokens
- A transition can fire iff all of its input places contain tokens
- The firing of a transition
  - Removes a token from each input place
  - Puts a token in each output place
- The number of tokens a place can hold is called its capacity
Simple Petri Net

Place $P_1$, $P_2$, $P_3$, $P_4$, $P_5$

Transition $T_1$, $T_2$

Tokens

Arcs

Transition $T_1$ connects to $P_1$ and $P_2$.
Transition $T_2$ connects to $P_3$, $P_4$, and $P_5$.

Bruce Powel Douglass, Ph.D.

i-Logix
Standard Programming Constructs

Sequencing

Selection (or contention)

Explicit Control Branching

Explicit Control Synchronization

Looping

Concurrent threads
Pacemaker Petri Net

RSO  Reed Switch Opens
PSC  Pace Stop Command

Comm Off  Idle  Sending
Receiving  Checking

Set Parameter Cmd Received

Waiting for V Sense
Pacing Off

Pacing
Refractory

Bruce Powel Douglass, Ph.D.
Example above shows a queuing model between two asynchronous threads: ECG Waveform acquisition and display.
What’s Shown in Petri Nets?

- Generalized behavior (incl. state behavior)
- Concurrency
- Can be augmented with time
- Many different extensions are available
- Petri nets suffer from
  - lack of scalability because they are flat like Mealy-Moore state models
  - lack of tools
FSMs and Development Process

- FSMs apply to *OBJECTS*
  - Sensor object
  - Queue object
  - Pacemaker pacing engine object
  - Language parser object
Structured Process

- Identify behavioral functions that exhibit state behavior
- For each such function, design a FSM
  - For each state, define
    - Valid transitions
    - Actions
    - Activities
- Decide on an implementation strategy
Object Oriented Process

- Identify classes and objects
- Identify which classes have FSMs
- Define a single FSM for each relevant class
  - For each state, define
    - Valid transitions
    - Actions
    - Activities
- Decide on an implementation strategy
Implementation Strategies

- Case/Switch statements
- FSM Generator
- Centralized state machine
- Separate state machines for each FSM object
Case/ Switch Statements

Switch (stateVar) {
    case state1: ... break;
    case state2: ... break;
    case state3: ... break;
    case default: // invalid state
}
Case/ Switch Statements

Switch (stateVar) {
    case state1: switch(transition) {
        case T1: ...
            break;
        case T2: ...
            break;
        case default: // invalid transition
    };
    break;
}
Centralized State machine

- Object 1
- State Table
- Transition
- ProcessTransition(...)
- Action list
- New State
- State Central
Separate State machines

class myClass: public FSM {
    private:
        FSM myFSM;
};
Separate State Machines

Class FSM

<table>
<thead>
<tr>
<th>Current State</th>
</tr>
</thead>
<tbody>
<tr>
<td>AcceptTransition(t)</td>
</tr>
<tr>
<td>ApplyTActions(s)</td>
</tr>
<tr>
<td>ApplyEntryActions(s)</td>
</tr>
<tr>
<td>ApplyExitActions(s)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
</tr>
<tr>
<td>TransitionList</td>
</tr>
<tr>
<td>EntryActionList</td>
</tr>
<tr>
<td>ExitActionList</td>
</tr>
<tr>
<td>ActivityList</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
</tr>
<tr>
<td>Target State ActionList</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>F( )</td>
</tr>
</tbody>
</table>

Bruce Powel Douglass, Ph.D.
i-Logix
Summary

- Objects have behavior
  - Simple
  - Continuous
  - State-driven
- Modeling objects as Finite State Machines simplifies the behavior
- States apply to objects
- FSM Objects spend all their time in exactly 1 state (which may contain concurrent substates)
Summary

States are **disjoint ontological conditions that persist for a significant period of time**.

States are defined by one of the following:

- The values of all attributes of the object
- The values of specific attributes of the object
- Disjoint behaviors
  - Events accepted
  - Actions performed
Summary

- Transitions are the representation of responses to events within FSMs
- Transitions take an insignificant amount of time
- Actions are functions which may be associated with
  - Transitions
  - State Entry
  - State Exit
- Activities are processing that continues as long as a state is active
Summary

- Harel Statecharts provide
  - Nested States
  - Concurrency
  - Propagated and Broadcast Transitions
  - Orthogonal Components
  - Guards on transitions
  - Flexible action model
  - Activities within states
  - History
  - Inherited state behavior
Summary

- Statecharts show static structural view
- State tables show missing transitions
- State specifications are good for defining testable, traceable requirements
- Sequence diagrams show scenarios
- Timing diagrams show overall timing in scenarios
- Petri nets are more general and show static structural view