

# 4

# UML-Based Design

(with an emphasis on course project survival)

**Distributed Embedded Systems**

**Philip Koopman**

**January 26, 2009**

**Carnegie  
Mellon**

# Where Are We Now?

---

## ◆ Where we've been:

- Embedded system intro & foundations
- Requirements
- Elevator domain knowledge

## ◆ Where we're going today:

- UML overview & design process for course project

## ◆ Where we're going next:

- Pepsi vending machine example
- Reviews & Inspections
- Distributed + Embedded system concepts

# Preview

---

## ◆ Design process

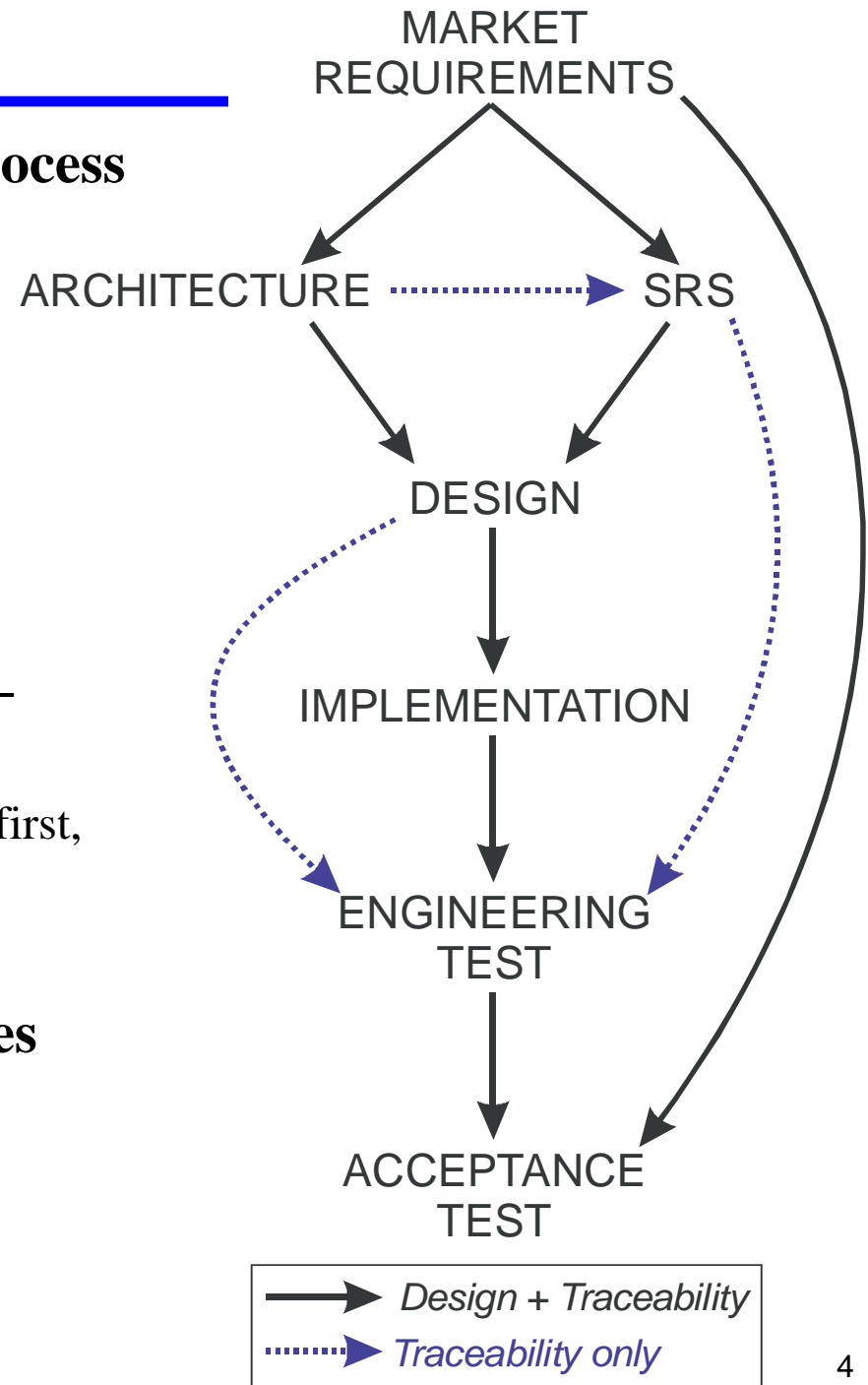
- A set of steps to get you from requirements to design
- Specifically, the design process we'll be using for the course project

## ◆ Intro to Unified Modeling Language

- A standard representation for designs and implementations
- It's not perfect, but it gets a lot of the job done
  - Note: we're not grading on nitty gritty language lawyer stuff, but this helps give a uniform representation for class work
- A complete end-to-end example in the next lecture!
  - This lecture has some informalities to simplify things; next lecture looks & feels like project notation
- *Important:* this course is about teaching survival skills, not being an all-encompassing tutorial on UML (or many other subjects)
- *Note:* you are going to see some things multiple times. These are the things some students struggled with in previous years – we are only repetitive where we have good reason to be!

# General Process Flow

- ◆ **We're going to assume a waterfall process**
  - Top-down refinement
  - Front-to-back flow
- ◆ **Real projects vary**
  - But the same representations are useful regardless of the sequencing
  - Usually architecture & requirements co-evolve
    - (Lecture flows better with architecture first, so that is today's discussion)
- ◆ **This lecture concentrates on the pieces**
  - What the pieces really are
  - How they fit together



# Why UML (Or Any Other Notation?)

---

## ◆ UML = “Unified Modeling Language”

- It isn't actually Unified; it's all the best known ideas tossed into the same sack
- And, it's more a set of graphical techniques than a textual language

## ◆ UML isn't novel; it's just a common representation

- Gives a way to exchange ideas via standardized set of diagrams
- Gives a standard way to document thoughts for later access
  
- UML is NOT a design methodology ...  
...there are many ways to use UML in a methodology and we're just now figuring out the better ways to do this.

## ◆ There is not (yet) any “best” process

- “Best” varies depending on size of team, complexity/novelty, and company culture
- But, it's better to have some process than no process
- And, the ability to follow an arbitrary, but specified, process is important

# UML-Based Process-“Lite” For Our Course

---

## ◆ System-level requirements

- Use cases
- High level text requirements

## ◆ Architecture – emphasis on “nouns”

- Class Diagrams & object descriptions – sensors, actuators, controllers
- Interfaces – network message dictionary

## ◆ Software Requirements – emphasis on “verbs”

- Text-Based Scenarios – different scenarios for each use case
- Sequence Diagrams – graphical scenarios with emphasis on interaction “messages”

## ◆ Design

- Textual software requirements specification – per-module behaviors
- State Charts – state transitions
- Test Design
- Failure analysis (covered later in semester)

## ◆ Verification & Validation

- Traceability
- Unit testing
- Integration testing
- Acceptance testing

# Why Not Just Write The Code?

---

- ◆ **That actually works for up to perhaps 100 lines of code**
  - Most embedded systems are a lot bigger
  - Most embedded systems have to be nearly perfect and on time
  - Problems tend to become exponentially worse with complexity/program size
  
- ◆ **The stakes are too high to get it wrong!**
  - But, there are *countless* projects that get it wrong
    - With resultant loss of money, jobs, lives, ....
  
- ◆ **Example:**

In July 1999, **General Motors had to recall 3.5 million vehicles because of an anti-lock braking software defect.** Stopping distances were extended by 15- 20 meters. Federal investigators received reports of 2,111 crashes and 293 injuries.

  - [http://autopedia.com/html/Recall\\_GM072199.html](http://autopedia.com/html/Recall_GM072199.html)

# “Marketing/Business” Context

---

- ◆ **Goal: “Build an elevator using distributed embedded system approach”**
  - Note: there is a lot of historical precedent for what it means to be “an elevator”
  - High level spec. is: “make it act like the HH primary elevator except better”
- ◆ **In our role as the “customer,” we require you to use:**
  - Our set of predefined components (buttons, lights, *etc.*)
  - Our embedded network message types (you can add some later)
  - Our simulation framework in Java as the implementation platform
  - Our design process
- ◆ **General guidance:**
  - If in doubt, make it act like the Hamerschlag Hall main elevator
  - You can add extra features later in project
    - You can add network messages with our permission only
    - In general, you can *NOT* add extra system objects until after mid-term...  
... because everyone in the past got themselves into trouble doing it!

# Top-Level Requirements

---

## ◆ Elevator Top-Level Requirements

- All passengers shall eventually be delivered to their intended destination floor.
- Any unsafe condition shall cause an emergency stop.
- An emergency stop should never occur.
- Performance shall be optimized to the extent possible, where performance is defined by the formula:
  - $(4 * \text{average\_passenger\_delivery\_time}) + \text{maximum\_passenger\_delivery\_time}$   
Performance is improved by reducing that value (short delivery times are better).
  - Delivery time is counted from the time a passenger arrives at a floor to begin a trip and ends when that passenger exits the elevator car. (Note: this is an arbitrary formula for this project, but the general idea holds true for real elevators.)

# What's an Architecture?

---

## ◆ Architecture definitions:

- **System:** The structure – in terms of components, connections, and constraints – of a product, process, or element. [Rechtin96]

## ◆ For our purposes, an architecture is:

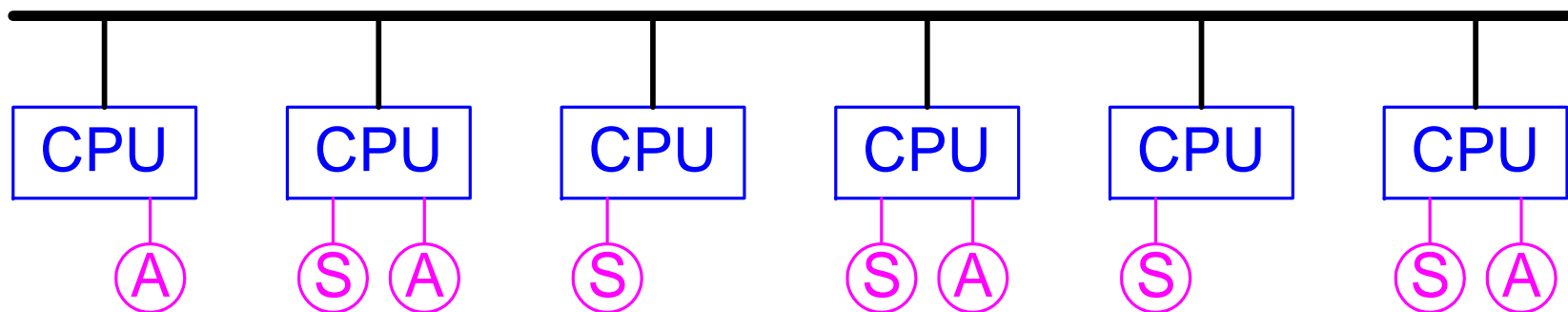
- A set of objects
  - Sensors
  - Actuators
  - Controllers
- The interfaces between those objects
  - Network messages
  - Analog interface pseudo-messages

# Hardware Architecture Pattern For This Project

---

## ◆ Highly Distributed Networked System

- Abstraction principle: One sensor, actuator, or servo pair per CPU, on a network
- Bus interconnect
  - Bus hierarchy may be needed to overcome bandwidth limits
- Pro: doesn't predispose system to any other architectures
- Con: bus can be a bottleneck

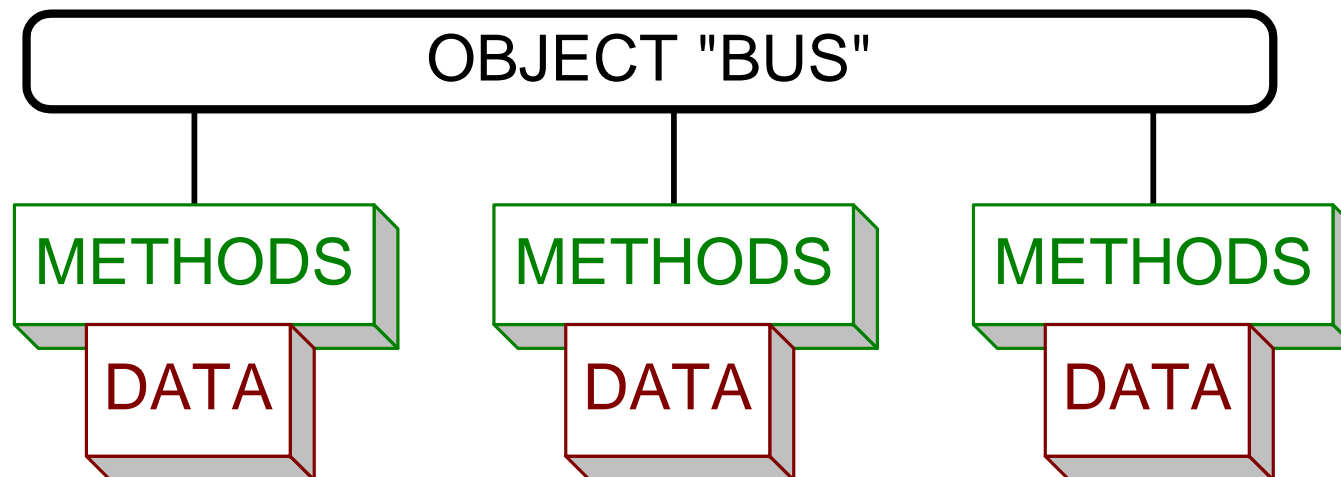


# Software Architecture Pattern For This Project

---

## ◆ Object oriented / Federated

- Abstraction principle: partition by data types, hide data behind methods
  - Note: flow of control is completely obscured
- Pro: helps with multi-vendor/mult-subsystem integration (compatible with CORBA)
- Con: can have high overhead to access data

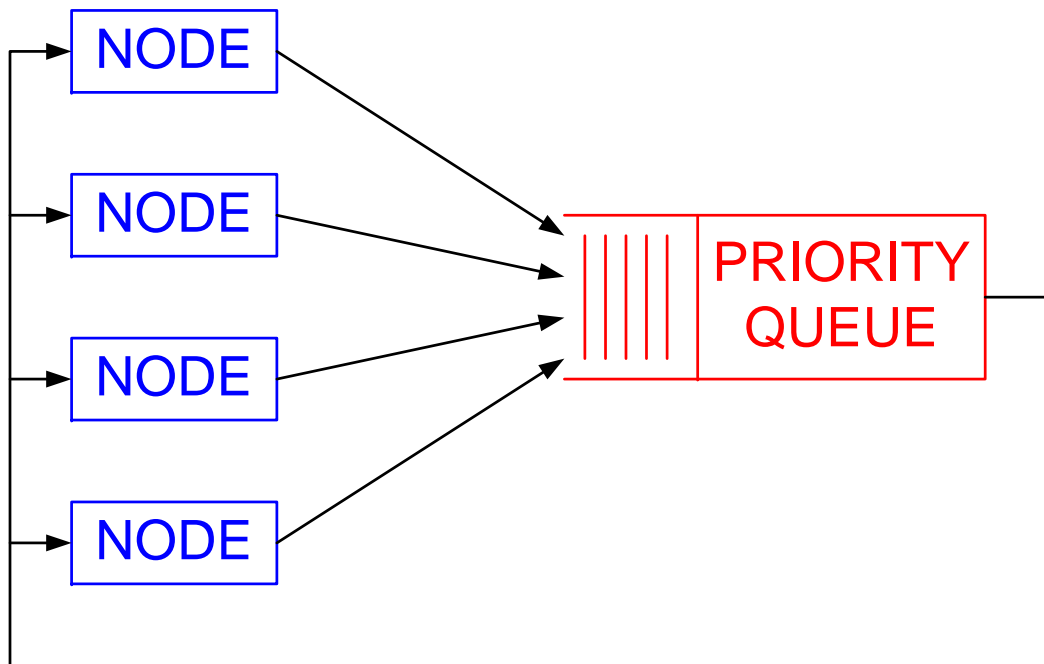


# Communication Architecture Pattern For This Project

---

## ◆ Global priority

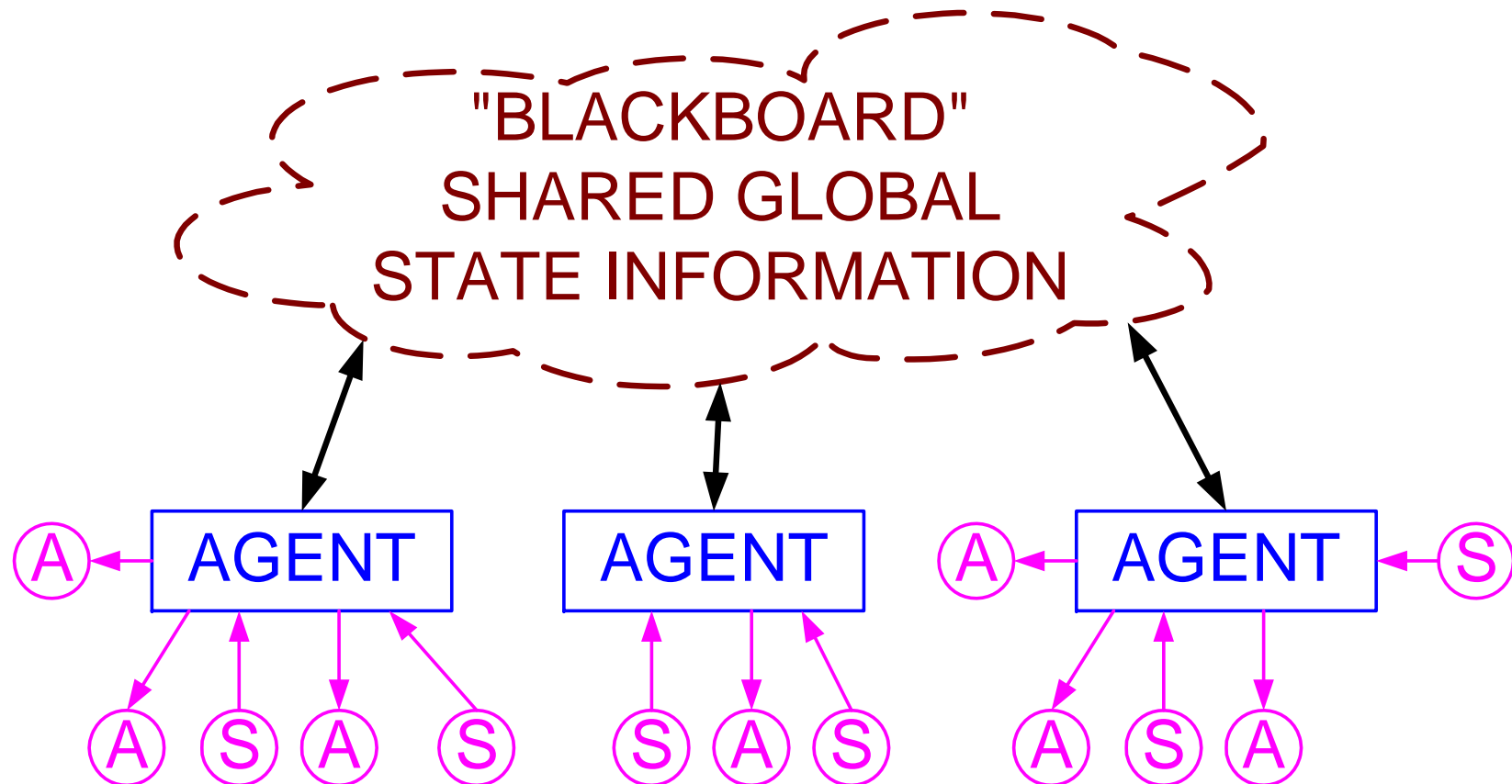
- Abstraction principle: highest priority message delivered first
  - Does ***NOT*** require a physical node to act as a queue – fully distributed implementations are commonly used!
  - Represents CAN protocol
- Pro: priority helps meet deadlines
- Con: priority interferes with fairness



# Control Architecture Pattern For This Project

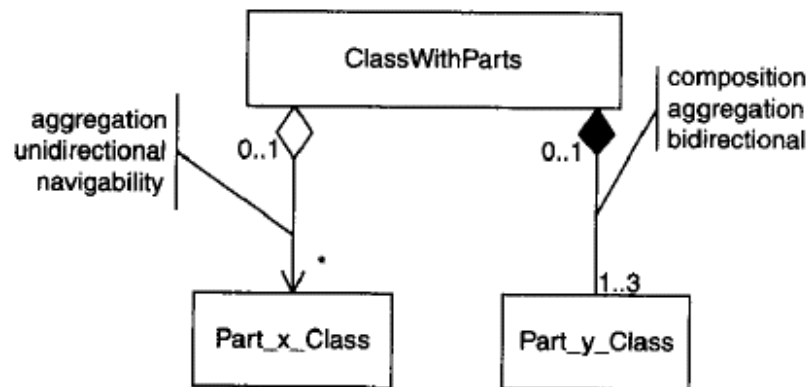
## ◆ Federated Agents/“Blackboard”

- Abstraction principle: each object has a control agent; agents monitor and transmit global state information for coordination
- “Blackboard” has shared state variables



# Software Architecture: UML Class Diagrams

- ◆ Used to show system in terms of objects, attributes, and relationships
  - Objects are “nouns” in the system
  - Attributes are local state data within an object
  - This is “sort of” an architectural diagram

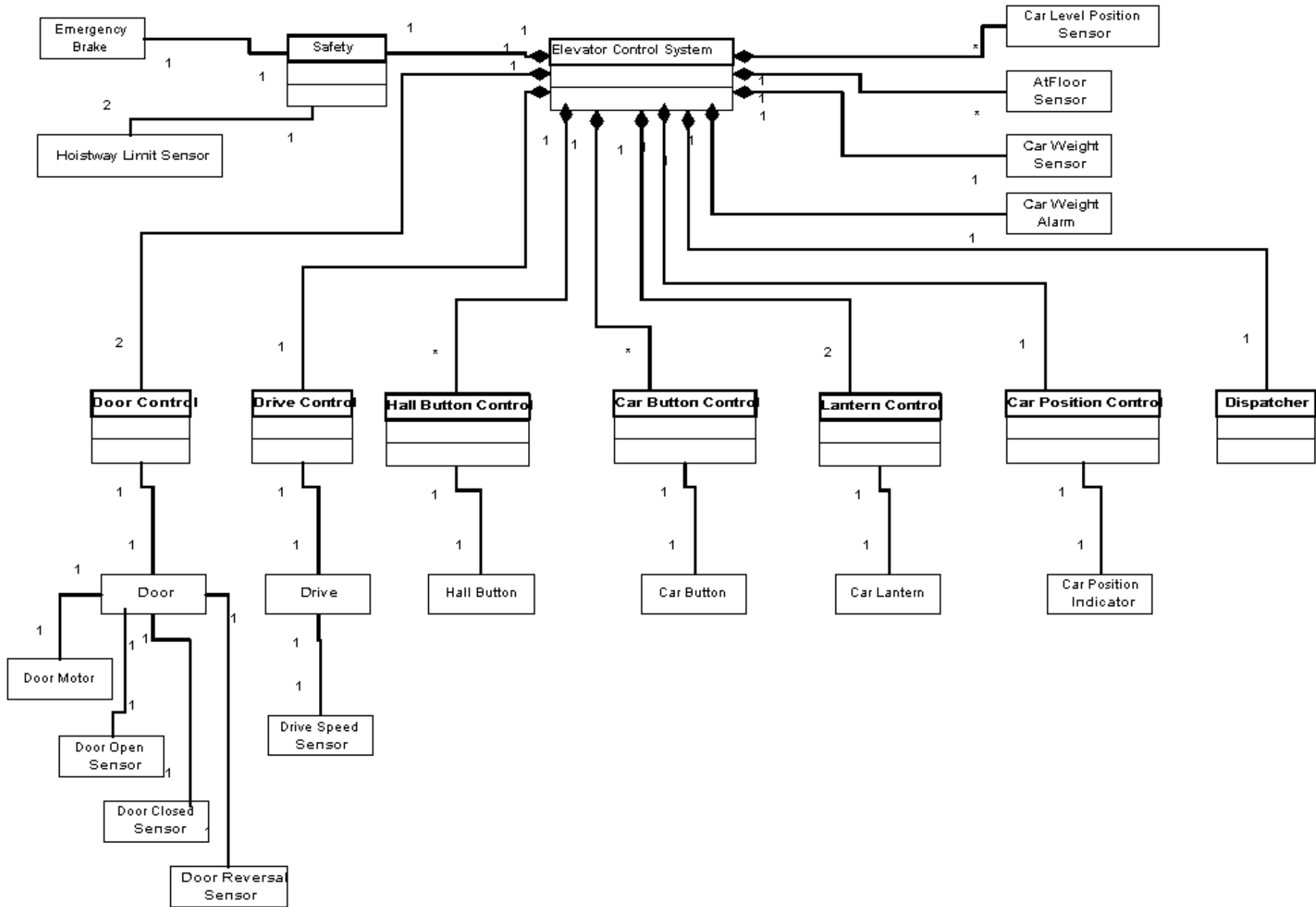


Multiplicity Symbol	Meaning
1	Exactly 1
0,1	Optionally 1
x..y	From x to y inclusive
a,b,c	Only specific values of a, b, and c
*	0 or more
1..*	1 or more

[Rational]

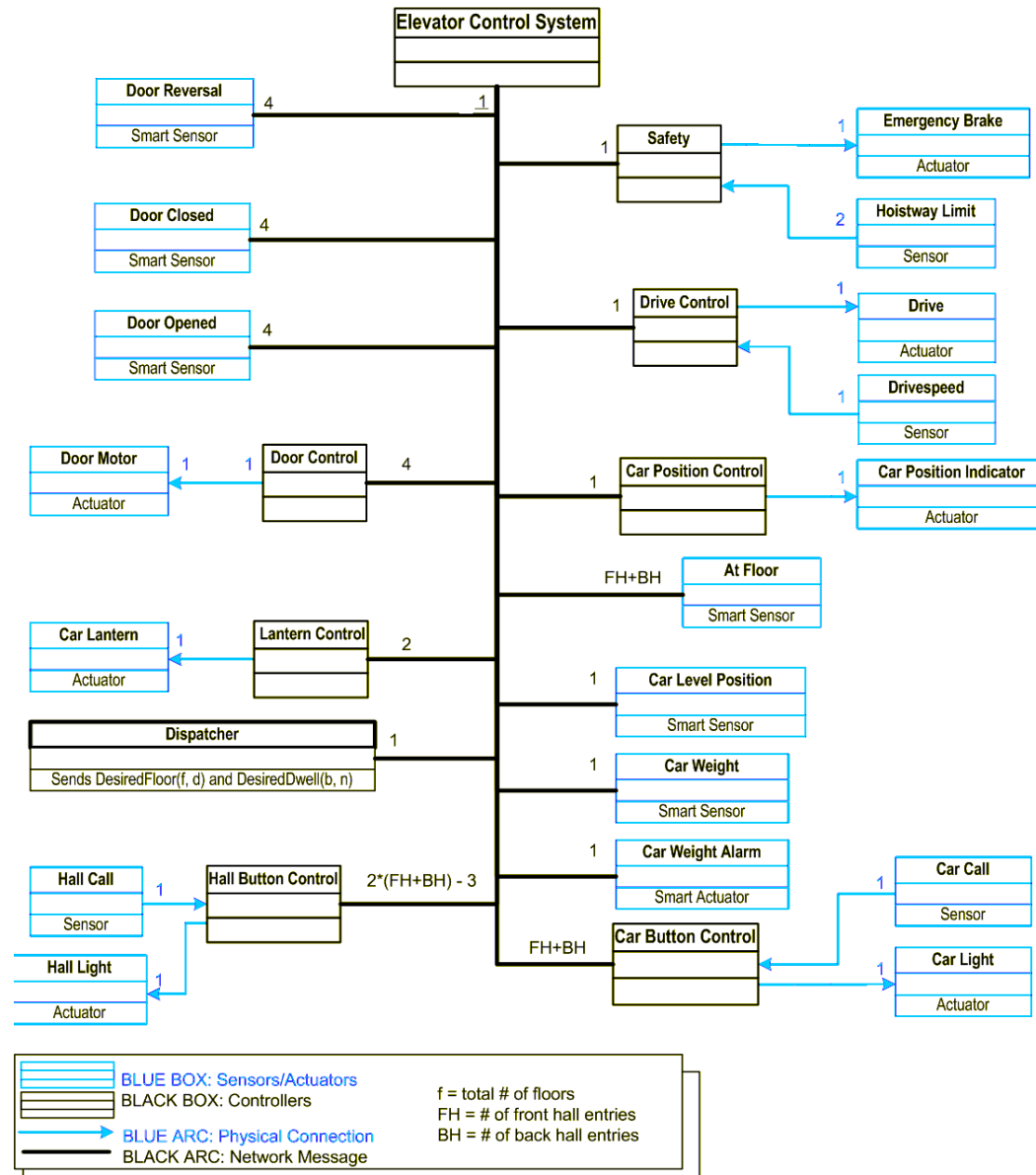
- For our purposes, composition & aggregation are the same thing

# Example Elevator Class Diagram



# Our “Architecture Diagram”

## Project 2: Elevator Architecture Diagram



# Detailed Object Descriptions (part of architecture)

---

## DoorMotor[j]

- Moves door [j]
- One per DoorControl
- Can be commanded to Close, Open, and Stop

...

# Message Dictionary (part of architecture)

---

## AtFloor[f]

- True if the elevator is at the floor f, false otherwise. There is one per floor.

## DriveSpeed

- Tells what speed the drive is commanded to – can be Fast, Slow, or Stop.

## DoorClosed[j]

- True if the door is completely closed. Otherwise false. One per door. They might be different!

## DoorOpen[j]

- True if the door is completely open. Otherwise false. One per door. They might be different!

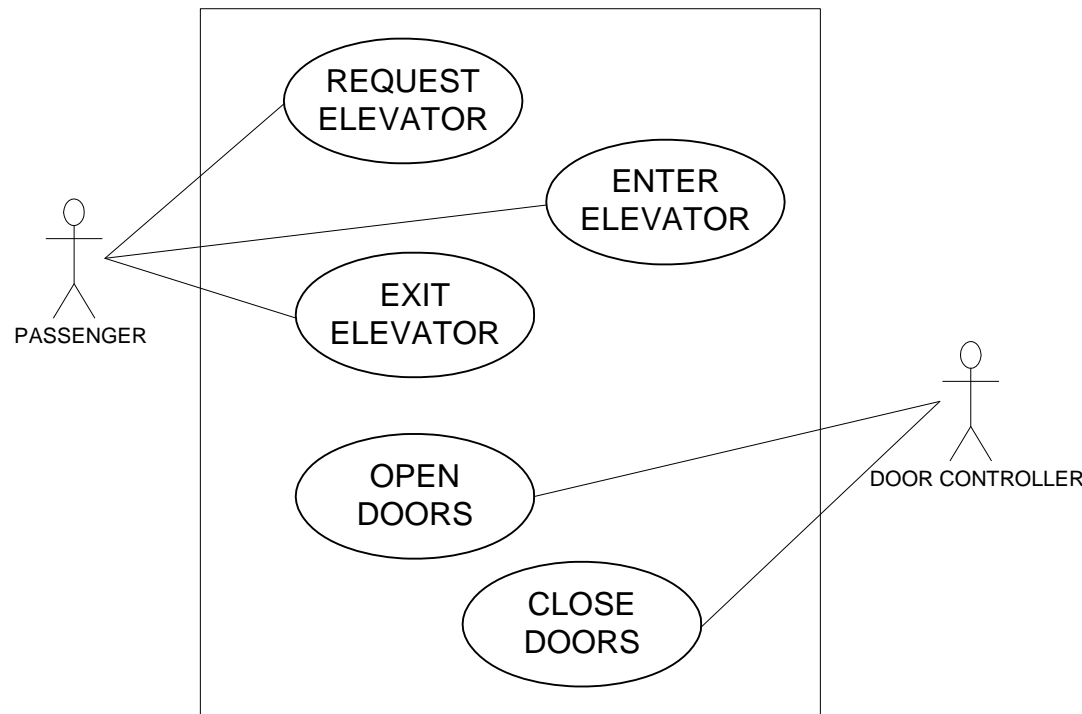
◆ ...

- ◆ **For our type of system, it is a list of *state variables* that describe state of objects**

# System-Level Requirements: Use Cases

## ◆ Useful for identifying different things system must do

- Actor initiates a Use Case
- Represents the system from the actor's point of view
- System can act on environment too

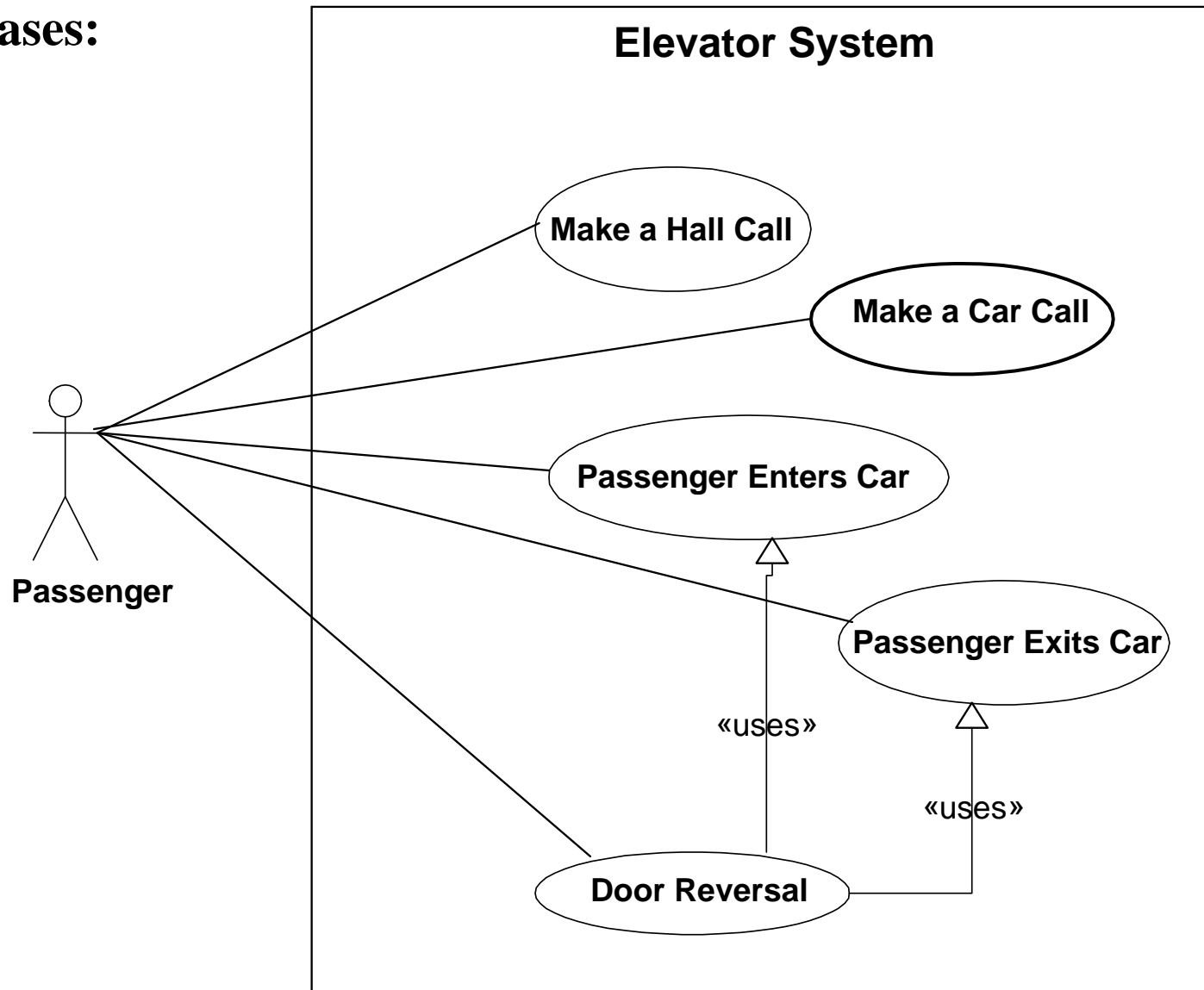


## ◆ Problems:

- Who are the actors? (In general must include machines as well as people)
- Usually end up assuming a single centralized system control actor

# An Example (but current project is different)

## ◆ Use Cases:



# How Big Should A Use Case Be?

---

- ◆ **There is some art to sizing the use cases**
  - End-to-end ride on elevator is too big
  - One line of code is too small
- ◆ **In general, use cases are intended to capture a “transaction”**
  - E.g., request a bank balance on an automated teller machine
  - Usually, a user session has multiple transactions (request balance; withdraw money; ...)
- ◆ **In elevator case, it should be a situation that is a nice building block**
  - For example, approach elevator and tell it you want to go up/down
    - Or, “make a hall call” for short
  - Names should be 2-4 words long and relatively descriptive, with emphasis on *VERBS / actions*
    - These are about how users want to use the system, not how the system is built
- ◆ **Let’s talk about scenarios so you can see how size affects the next step**

# Scenarios – what happens inside the use case

---

- ◆ **Nominal – ways in which user and system interact**
  - Often multiple *alternate* scenarios for each use case
  - Each scenario is the same “size” as a particular use case from end to end
- ◆ **Off-nominal – exceptional and failure situations**
- ◆ **Informal Example** (a scenario for Enter Elevator use case):
  - Initial condition: user is waiting for elevator to arrive in desired direction
    1. The car reaches the floor, stops, and opens its door
    2. The car illuminates appropriate direction lantern
    3. User enters
    4. The car clears the hall call that was just serviced
    5. The car closes doors and extinguishes direction lantern
- ◆ **Note that multiple scenarios are invoked for end-to-end service**
  - Commonly scenarios are independent in “toy” problems and bank ATMs
  - But, NOTE: standard UML does not have any notion of Use Case order

# A More Complete Example Scenario

---

## ◆ **Summary Description:**

- Open doors from within car

## ◆ **Pre-conditions:**

- Passenger is in the car.
- Elevator has arrived at the desired floor, but the passenger has not yet exited the car.
- Doors are fully open.
- The car call button for the current floor is not lit.

## ◆ **Scenario:**

1. Doors begin to close.
2. Passenger's brain turns back on and (s)he presses car call button for current floor before doors are fully closed.
3. Doors stop closing and reopens fully.

## ◆ **Post-conditions:**

- Passenger is still in the car.
- The doors are fully open.
- The car call button for the current floor is not lit.

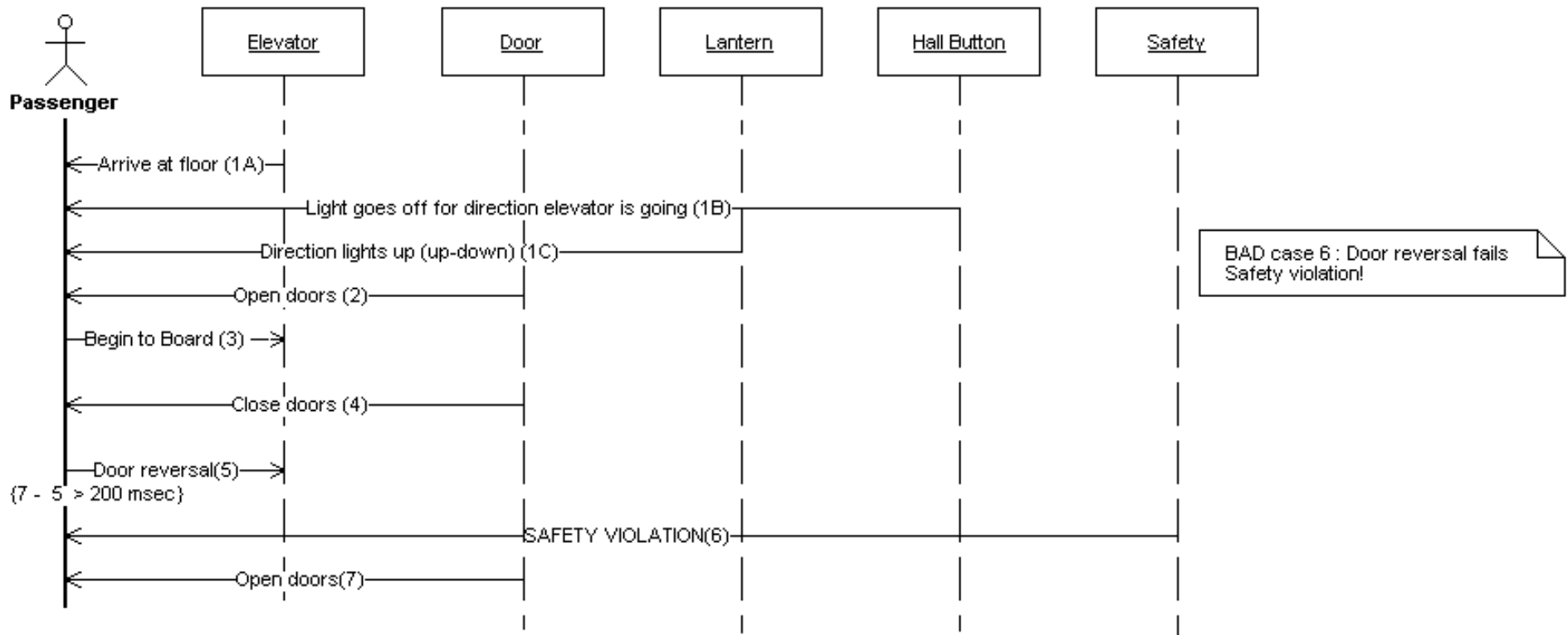
# How Big Is A Use Case? – Revisited

---

- ◆ **Using an elevator is a series of use cases**
  - Example: hall call, elevator moves to start floor, doors open, enter elevator, car call, doors close, elevator moves to destination floor, doors open, exit elevator, doors close
- ◆ **Each use case has multiple scenarios – almost always more than 1!**
  - Scenarios within use case must have compatible pre- & post-conditions
  - Post-conditions of one scenario need to match pre-conditions of next scenario
- ◆ **Thus, use cases should be sized to manage complexity**
  - Big enough use case to have a handful of reasonable scenarios
  - Split at natural breaking points to minimize # of pre- & post-conditions
- ◆ **Related question – how detailed is a scenario?**
  - Stay tuned for answer ... but first we have to talk about Sequence Diagrams

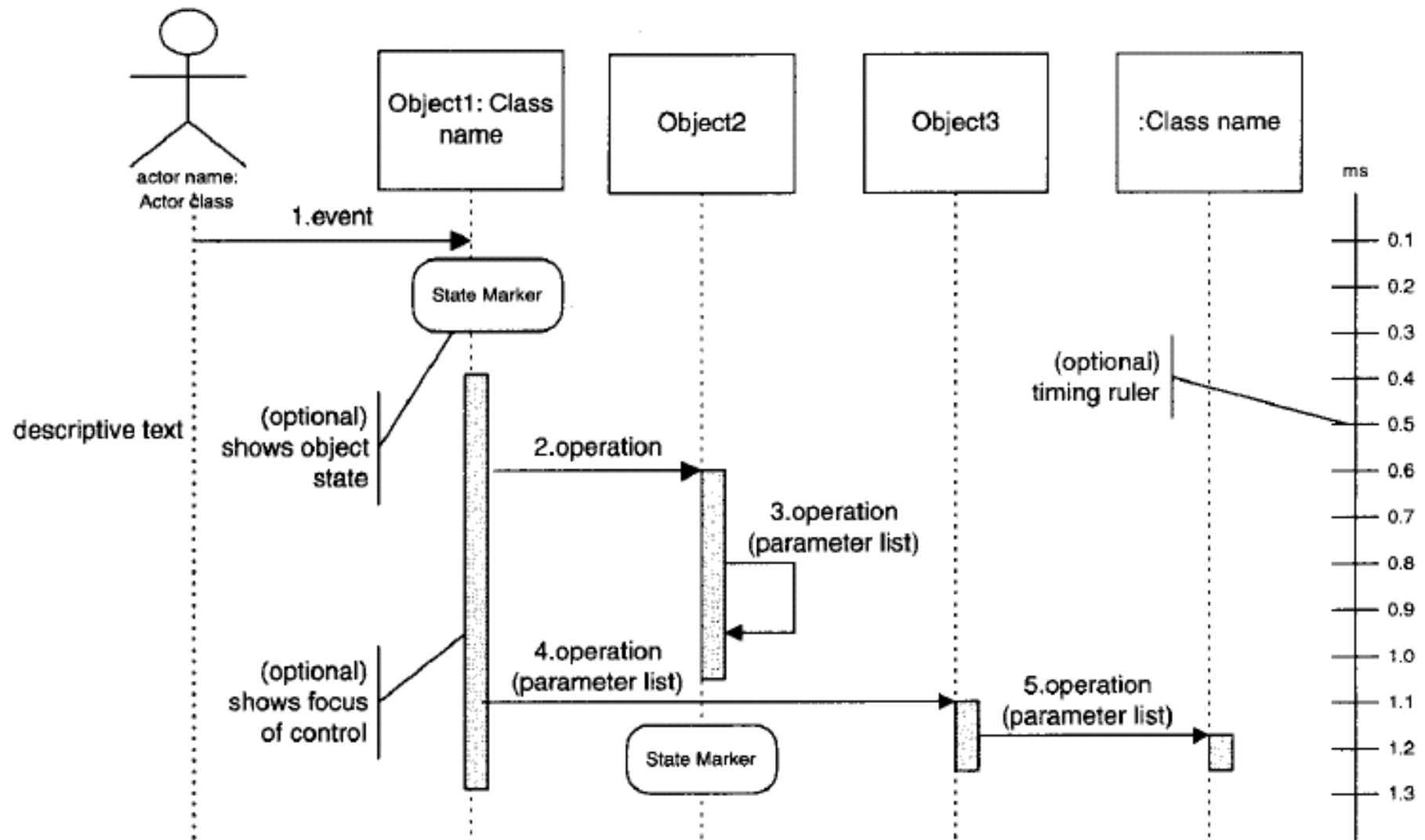
# Sequence Diagrams

- ◆ Shows which objects do what to implement a scenario
  - Emphasizes interaction/communication among components
    - “Feels” closer to a design at the system/interaction level
  - In our course, every arc is a “message” within the simulation framework



# Sequence Diagram

Shows a sequenced set of messages illustrating a specific example of object interaction.

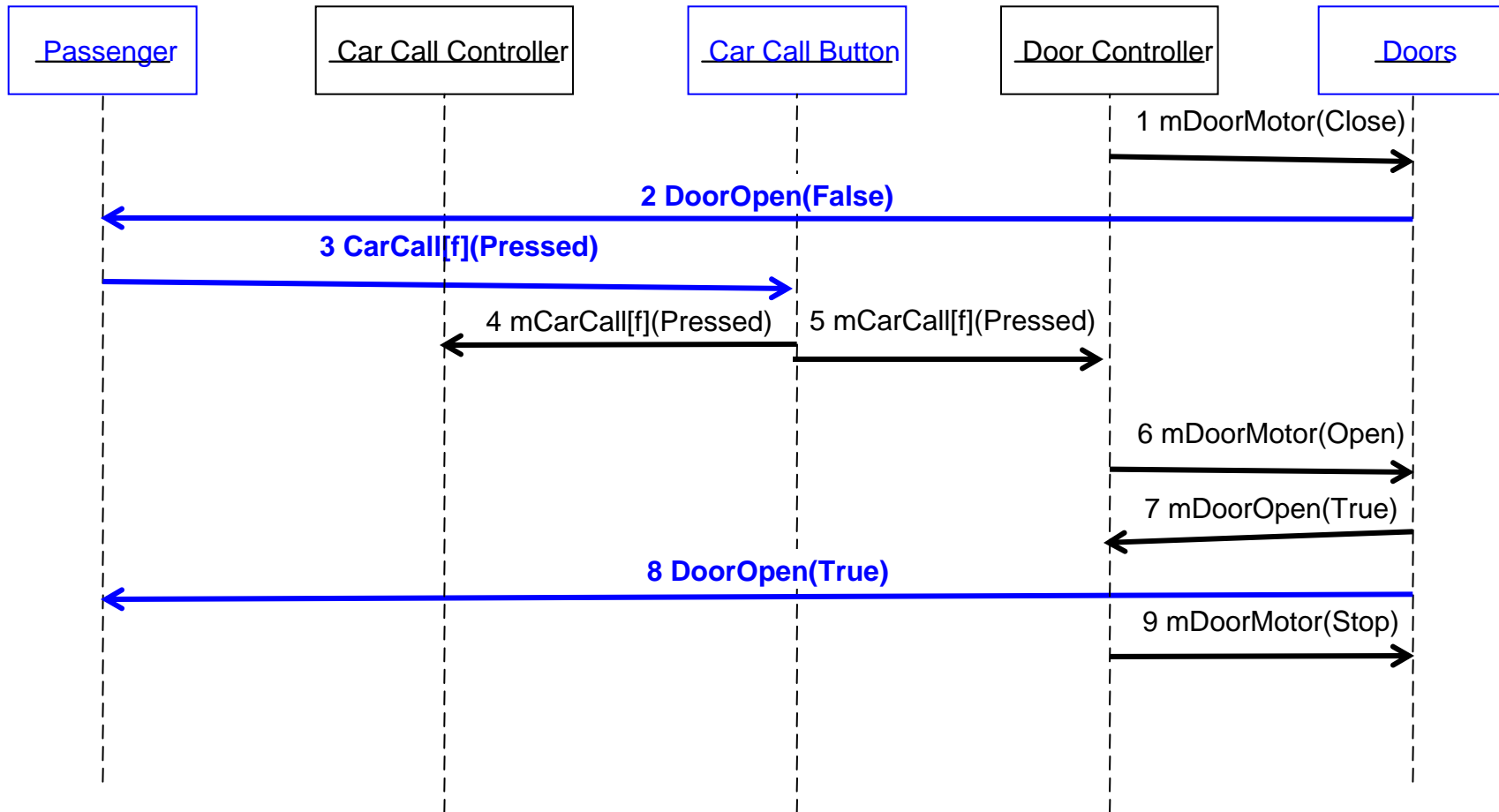


**Sequence diagrams** have two dimensions. The vertical dimension usually represents time, the horizontal represents different objects. (These may be reversed.)

[Rational]

# Sequence Diagram

- ◆ Constructing sequence diagram should just be a matter of connecting messages from your scenario in the right order:



# Messages Vs. Physical Actions

---

- ◆ **We use a discrete event simulator for the project**
  - Everything is an “event” at a specific time
  - Including simulated sensors and actuators
- ◆ **Some of the “messages” in the sequence diagram are not messages at all, but represent interaction between control system and environment**
  - When doors begin to close the DoorOpen sensor transitions from True to False. The passenger does not read this sensor, he/she simply sees the doors begin to close
  - When the passenger indicates a car call, he/she actually presses the physical button
  - We use an “m” prefix to keep track of things, with color-coding backup
    - “mDoorMotor(Close)” is a network message saying “DoorMotor ordered to close”
    - “DoorOpen(False)” is a physical action saying “passenger saw the door go to non-Opened”
    - In the project we use nearly identical mechanisms to represent both – keeps software environment simple

# How Detailed Is A Scenario?

---

- ◆ **You can have a scenario that is a text version of the SD**
  
- ◆ **Here is a very detailed scenario for the preceding SD:**
  1. Door controller commands doors to close. (mDoorMotor(Close) message)
  2. Doors begin to close. (DoorOpen sensor becomes False)
  3. Passenger presses car call button for current floor before doors are fully closed. (CarCall[f] button Pressed)
  4. Car call button sends sensor CarCall message to car call button controller. (mCarCall[f](Pressed) message)
  5. Car call button controller sends CarCall message to door controller. (mCarCall[f](Pressed) message)
  6. Door controller commands doors to open. (mDoorMotor(Open) message)
  7. Doors become fully open, triggering mDoorOpen(True) message.
  8. Passenger observes door fully open (DoorOpen(True))
  9. Door controller commands doors to stop. (mDoorMotor(Stop) message)

# High Level Vs. Low-Level Scenarios

---

- ◆ **You can use both high & low level scenarios if you want!**
- ◆ **High level scenarios are *mandatory* for project**
  - Each scenario step should have, perhaps 1 to 3 arcs in SD
  - Each scenario step typically involves a different actor or object initiating a set of related SD arcs
  - Scenario should be in terms of what is happening (use case) more than in terms of messages being sent
  - Scenario should be mostly in terms of everyday English, not “messages”
- ◆ **Detailed scenarios can be used if they help you get to a SD**
  - One line of text for each arc on SD
  - Probably most people will skip this and just draw the SDs from high level scenarios
  - In general this is too detailed to look at and understand in terms of how it fits to the use case

# Use Cases; Scenarios; SDs revisited

---

- ◆ **Use cases are general types of interactions**
  - Set of use cases covers all interactions
  - More than one use case often invoked in sequence
- ◆ **Scenario is a list of actions within a Use Case**
  - Generally each Use Case completely “owns” multiple Scenarios
  - Scenario is one way a Use Case is performed
  - Pre-conditions: which situations must be true for scenario to “execute”
    - Scenarios need mutually exclusive pre-conditions within a use case
  - Actions: list of things to do
  - Post-conditions: conditions summarizing situation after actions take place
- ◆ **Sequence Diagram is a picture of objects and messages**
  - Each Scenario has one Sequence Diagram
  - This is a more rigorous notation that shows how to make objects behave

# Textual Software Behaviors

---

- ◆ **Text-based specification, written per module of architecture**
  - English/pseudocode behaviors of each architectural component
  - Discussed in detail in the next lecture
  - Usually in terms of how module or actuator behaves given a sensor input
    - But, we can abstract this as saying behavior in response to input messages
- ◆ **Why this extra step? It's not a UML diagram**
  - Sequence diagrams look from the outside in
    - Often there is a simpler way to do implementation than a case statement that handles each different scenario/sequence diagram
  - Think of this as looking from the inside out
    - What software behaviors are required so that all the sequence diagrams work?
    - Sometimes simple behaviors suffice for complex interactions
  - But we need this bridging step before jumping to design to also catch:
    - Things that it is supposed to not do or guarantee never happen
    - Situations where order is unimportant or there are timing constraints
    - Assumptions made in design that other modules have to respect
  - Yes you can use ad hoc text boxes in UML diagrams, but that's a mess

# Example Elevator Behavioral Requirements – 1

---

## *LanternControl[d]*

### ◆ **Replication:**

- *(How many are there and where are they?)*
- Two controllers, one for each lantern {Up, Down} mounted in the Car by the Car Doors.

### ◆ **Instantiation:**

- *(What are settings at initialization; when are they created (default is permanent))*
- Lanterns are Off at initialization.

### ◆ **Assumptions:**

- *(What do you need to assume to meet constraints given listed behaviors?)*
- Rest of system never commands both lanterns on at the same time

### ◆ **Input Interface:**

- *(What inputs are available?)*
- mDoorClosed[j]
- mDesiredFloor(f,d)
- mAtFloor[f,d]

# Example Elevator Behavioral Requirements – 2

---

## *LanternControl[d] (continued)*

### ◆ **Output Interface:**

- *(What outputs are available?)*
- CarLantern[d](k) (physical interface to light bulbs!)

### ◆ **Internal State:**

- *(What private state variables are maintained? What notational macros are used?)*
- **DesiredDirection** = {Up, Down, Stop} computed desired direction based on comparing CurrentFloor with Floor desired by Dispatcher. This is implicitly computed and used as a macro in the behavior descriptions.
- **CurrentFloor**, is a shorthand notation for the value of whichever AtFloor[f,Stop] is True, if any. If CurrentFloor is invalid it has a mnemonic value of None.

### ◆ **Constraints:**

- *(What invariants must hold? – “passive” requirements.)*
- 7.1 Both CarLanterns[d] shall not be On at the same time.

# Example Elevator Behavioral Requirements – 3

---

## *LanternControl[d] (continued)*

### ◆ **Event-Triggered BEHAVIORS:**

- *(What active behaviors must be implemented?)*

7.2 Whenever any mDoorClosed[j] becomes False, CarLantern[DesiredDirection] shall be set to On.

7.2.1 If DesiredDirection is Stop, both lanterns shall be set to Off.

- » (Note: this is a more convenient way to write two parallel cases for DesiredDirection Stop and not Stop for 7.2)

7.3 Whenever any mDoorClosed[j] becomes True, CarLantern[d] shall be set to Off.

### ◆ **Philosophical notes:**

- These requirements are really half-way to implementation (but that's good)
- You need detailed object interfaces & message dictionary to do this

# Formula for Event-Driven Systems

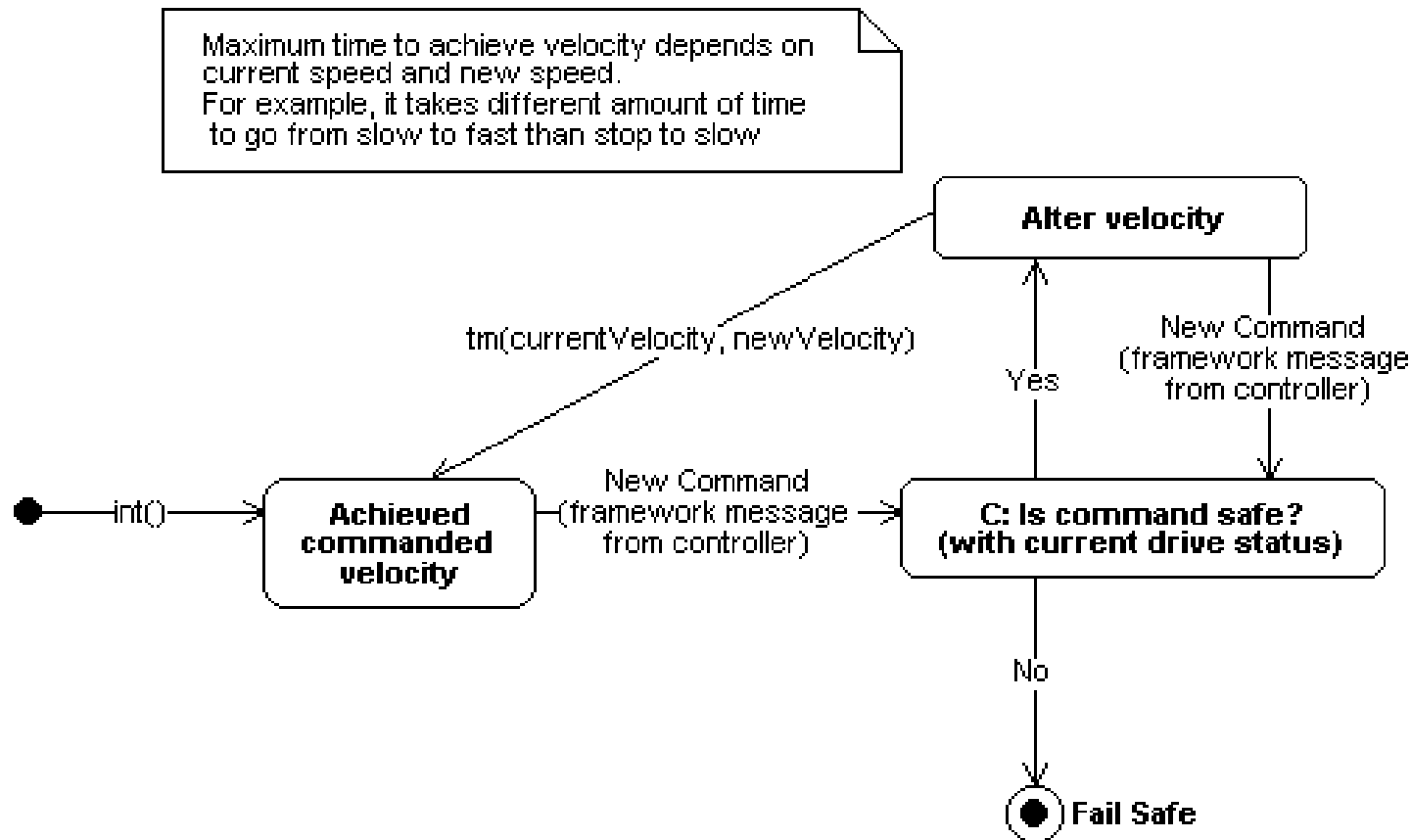
---

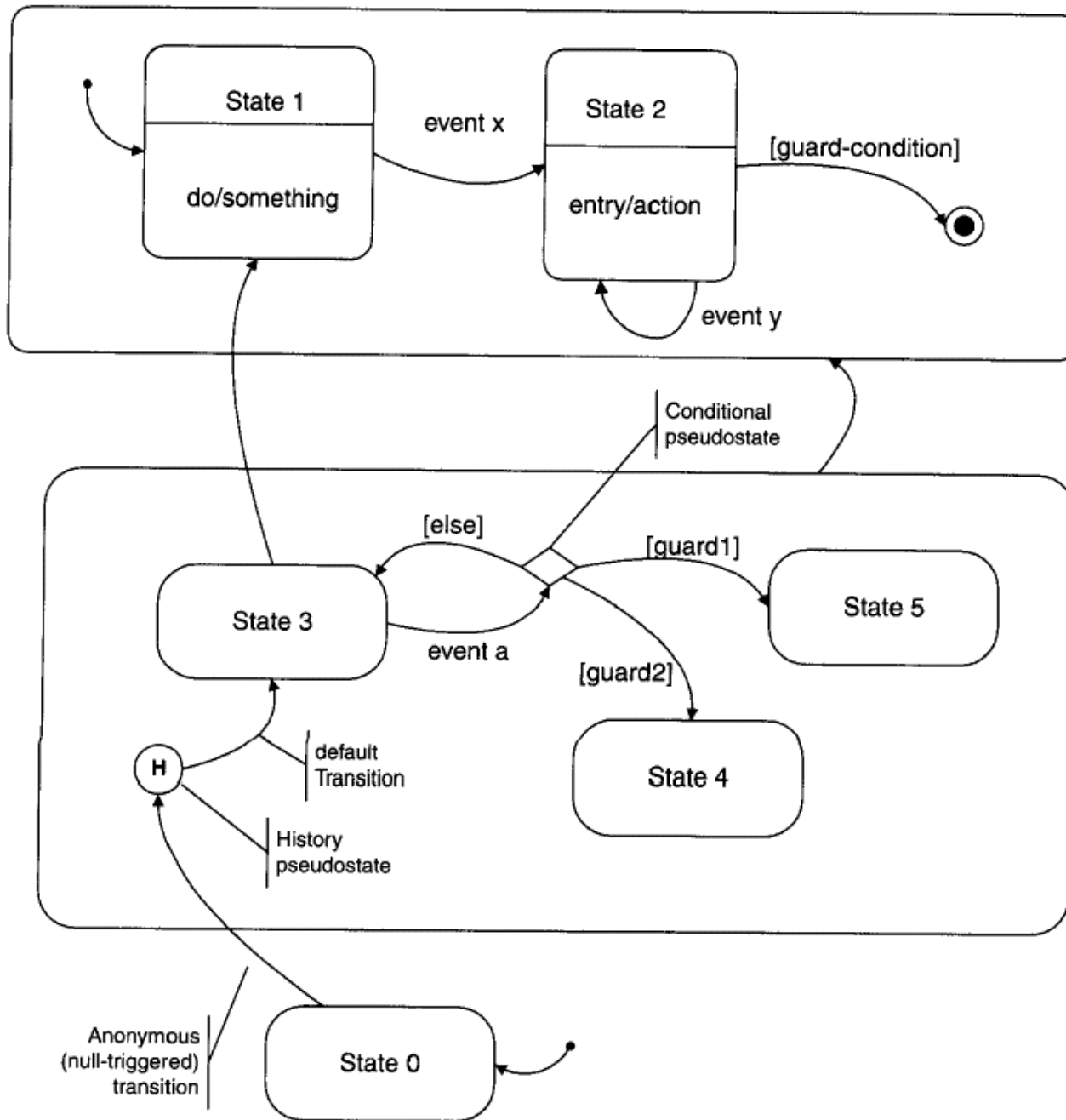
## ◆ Behavioral Requirements:

- *<message received>* shall result in *<message transmitted> ...*  
and/or *<variable value assigned> ...*
- *OR*
- *<message received>* and *<variable value test(s)>*  
shall result in *<message transmitted> ...*  
and/or *<variable value assigned> ...*
- Account for all possible messages received
- Account for all possible messages that need to be transmitted
- Make sure all variables are set as required
- **EXACTLY ONE received** message per requirement (network serializes messages; simultaneous reception of multiple messages is ***impossible***)
- **OK to have:** multiple messages transmitted; multiple variables assigned

# Design: State Charts

- ◆ **Describes finite state machine behaviors** (it's an “FSM transition diagram”) – emphasizes how object achieves its behaviors
  - Most statecharts “want” to be event-triggered
    - But many embedded control systems are time-triggered
  - Look a lot like finite state machine state transition diagrams





## Sequential substates

[Rational]

# Implementation: Java Code

---

- ◆ **Elevator implemented in Java with a course-supplied simulation framework**
  - We give you the software to implement the environmental objects (e.g., people)
  - We give you some example code based on last year's project
    - It is simpler, but it gives you a starting point
  - You create Java code to implement the Statecharts and any algorithms required

# Testing: Checking It Actually Works

---

## ◆ Test Cases are Scenarios in which a test will be performed

- Some possible types of testing:
  - Exercise all arcs of statecharts (is one way to do unit test)
  - Exercise each sequence diagram (is one way to do integration test)
  - Exercise concurrent use cases (is one way to do acceptance test)
    - » But, need to address things like performance as well for acceptance testing
- Short description of the “environment” of the test, includes:
  - What level (unit, subsystem, simulation)
  - What units included
  - What resources needed (simulation, input files, etc.)
  - What setup is to be done for the test
  - The test itself (description of inputs/actions in actual test)
  - Expected results
  - Requirements verified
- Can more or less use this approach at each level of abstraction, but no rigorous process available to do that

# Three Types of Testing We'll Use

---

## ◆ Unit Test

- Send messages at one object alone in simulation framework
- See if response messages match expectations based on **Statecharts**

## ◆ Integration Test

- Set initial conditions & send messages to whole elevator
- See if responses match expectations based on **Sequence Diagrams**

## ◆ Acceptance Test

- Run elevator with passenger workload
- See if responses match **Use Cases** & end-to-end passenger delivery

**Quick Check: What is the (indirect) relationship between Integration Tests and Use Cases?**

# How The Real World Differs From Classwork

---

## 1. You have to create your own requirements

- You aren't creating an "answer", you're solving an ill specified problem.
- Blaming the client for a defective problem statement is not an acceptable option.

## 2. The world is not a tidy place

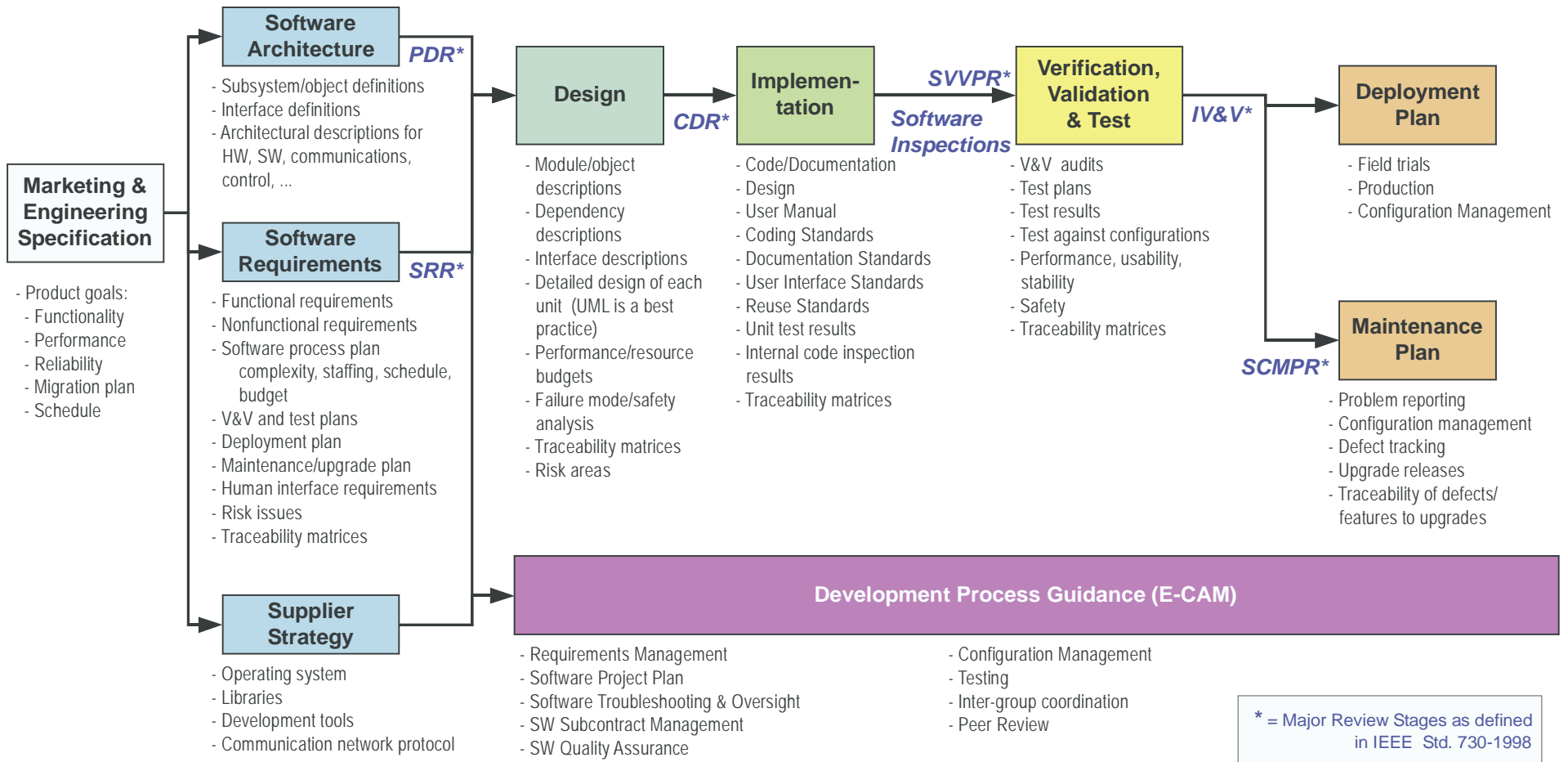
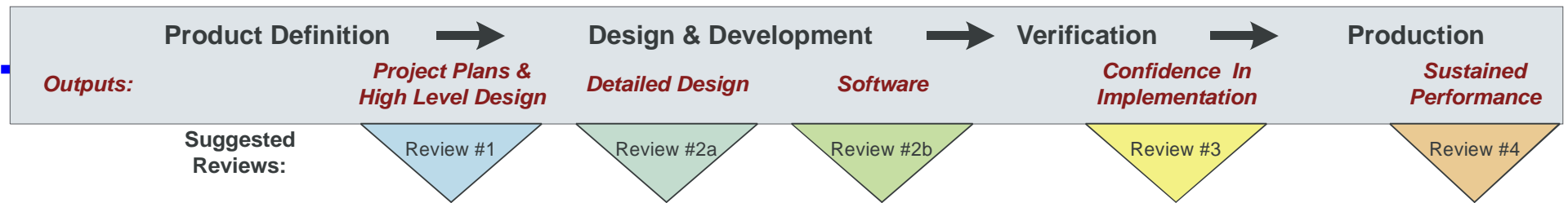
- Requirements are imperfect and not always understood.
- Once requirements are really understood, the client realizes they're wrong.
- Vendor-supplied components are imperfect. Get over it.

## 3. "Almost" doesn't cut it

- 90% right or just a little late can still get an "A" in school
  - 90% working means 10% not working, and any percent of not working means "broken"
- 10% wrong or missing a shipping date can mean losing your job in the real world

## ◆ For the course project you'll do some of #1 and #2

- You'll be using a process that is "lightweight", but not bad for industry
- 90% is still an "A" (so I guess we're just softies)



# Course Project Phases

---

- 1. Warm-up Exercise**
  - Take a small piece of design through to sequence diagram
- 2. Elevator event-triggered specification**
  - Use cases // scenarios // SDs // behavioral specs for event-triggered elevator
- 3. Elevator time-triggered design**
  - Convert elevator to time-triggered approach
  - Create statechart-based design
- 4. Network message design**
  - Define details of network operation
  - End-to-end scheduling
- 5. Test design**
  - Design tests to execute later using a capability of the simulation framework
- 6. Implementation**
  - Write the code & get it to run
  - Run unit tests & integration tests
- 7. Failure analysis & acceptance test**
  - Ask “what if component X breaks?” and predict outcome
  - Measure end-to-end passenger delivery

**Note: there is some iteration after mid-term to include fancier functionality**

# Review

---

## ◆ **Unified Modeling Language**

- A standardized set of graphical representations
- A convenient communication medium; we're not fussy about semantics

## ◆ **Important pieces of real projects represented in course**

- System-level requirements
- Architecture
- Software Requirements
- Design
- Verification & Validation
  - Engineering Test
  - Acceptance Test
  - Process monitoring (e.g., traceability)