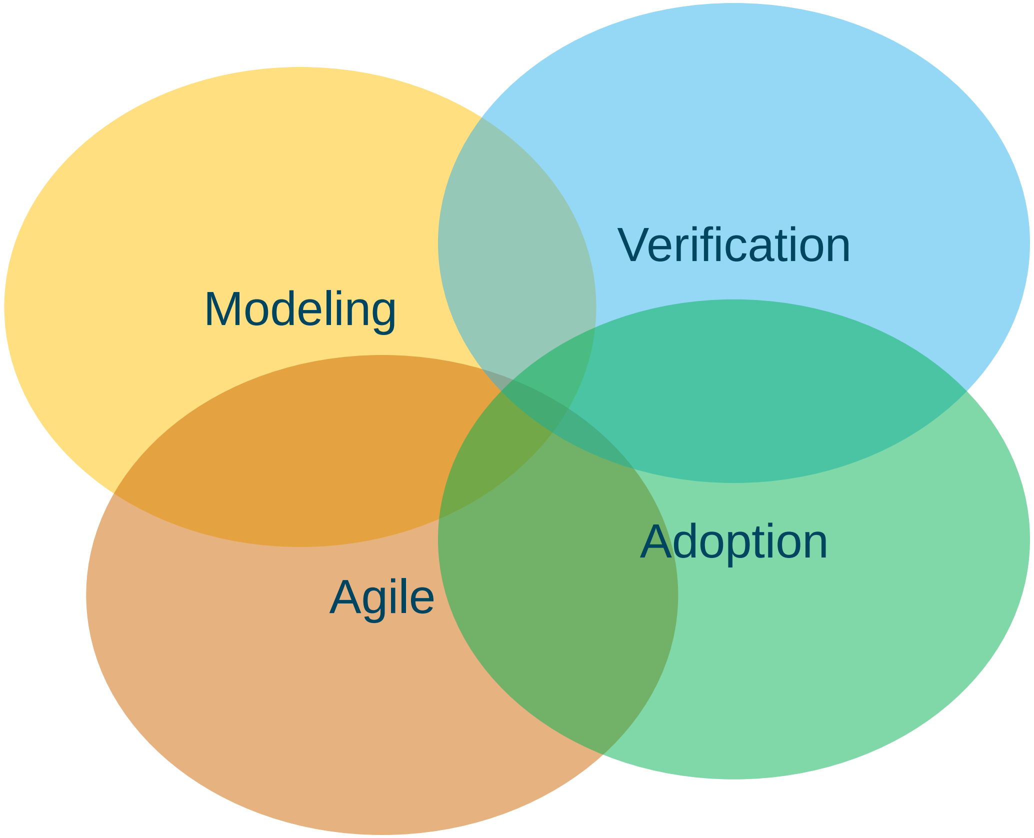
Effective Embedded Model-Based Development

Bruce Powel Douglass, Ph.D.
Chief Evangelist, Global Technology Ambassador
IBM Internet of Things (IoT)
bruce.douglass@us.ibm.com
Twitter: @IronmanBruce
Website: : www-01.ibm.com/software/rational/leadership/thought/brucedouglass.html

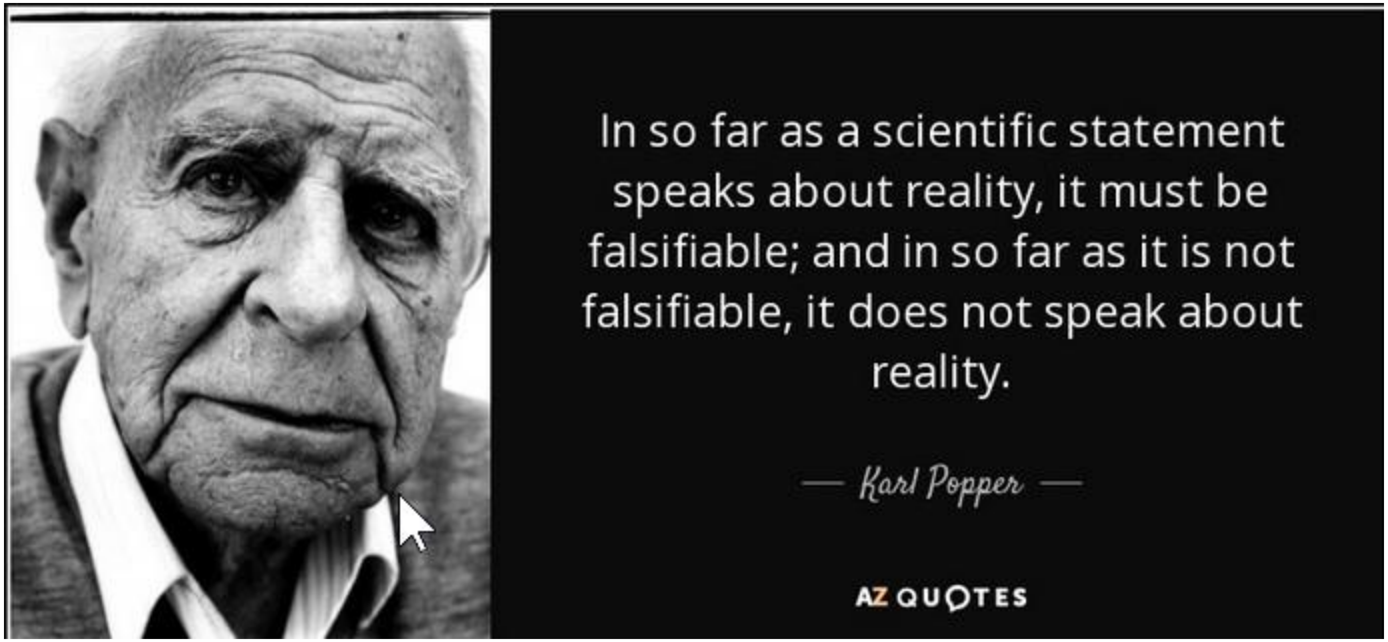
"Dance like nobody is watching,
Sing like you're alone in the shower,
Engineer like you're a passenger hurtling though space in a speeding tube of death that you designed."

Law of Douglass # 135

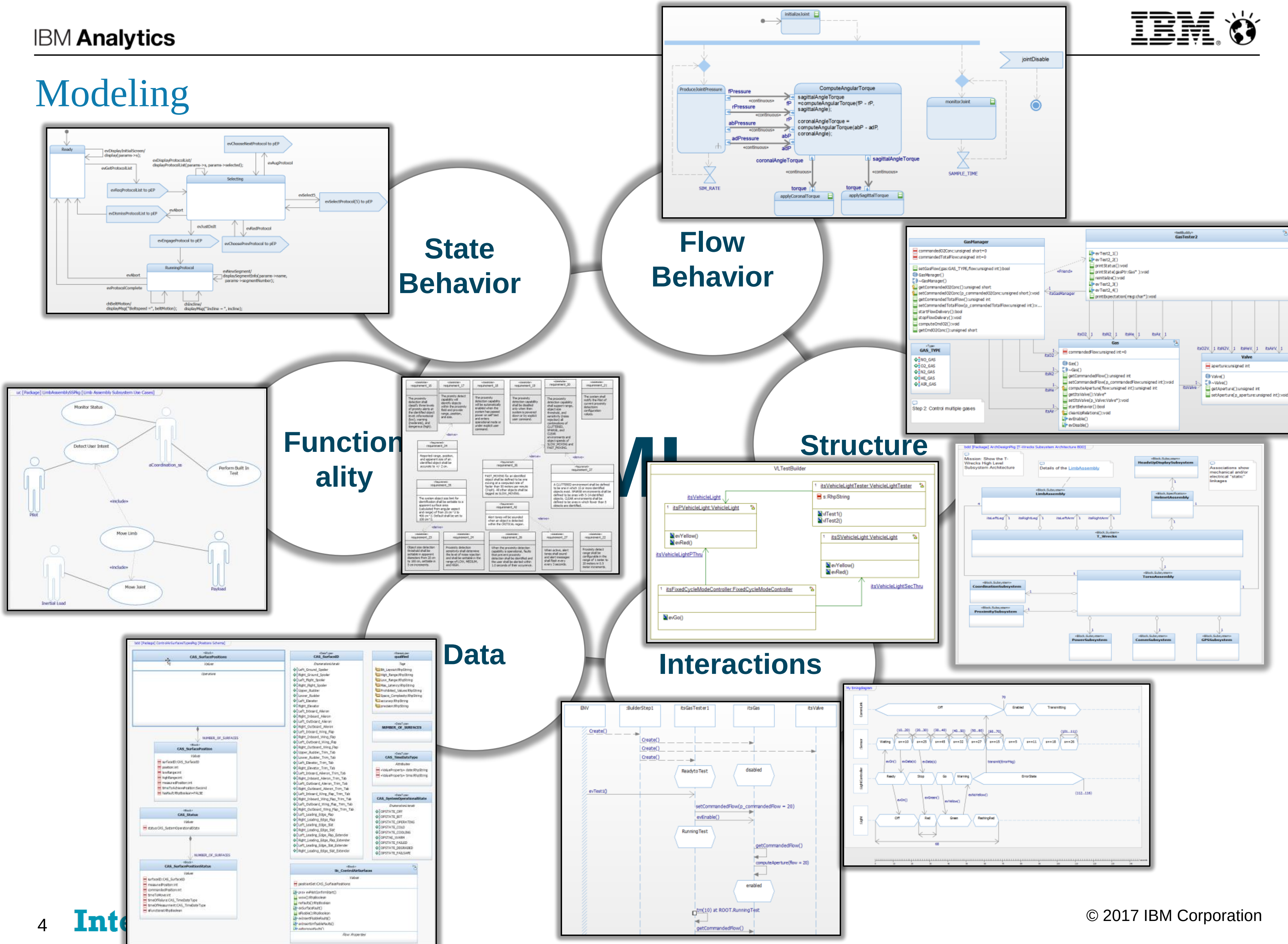
Key Topics



All Good Models are Falsifiable



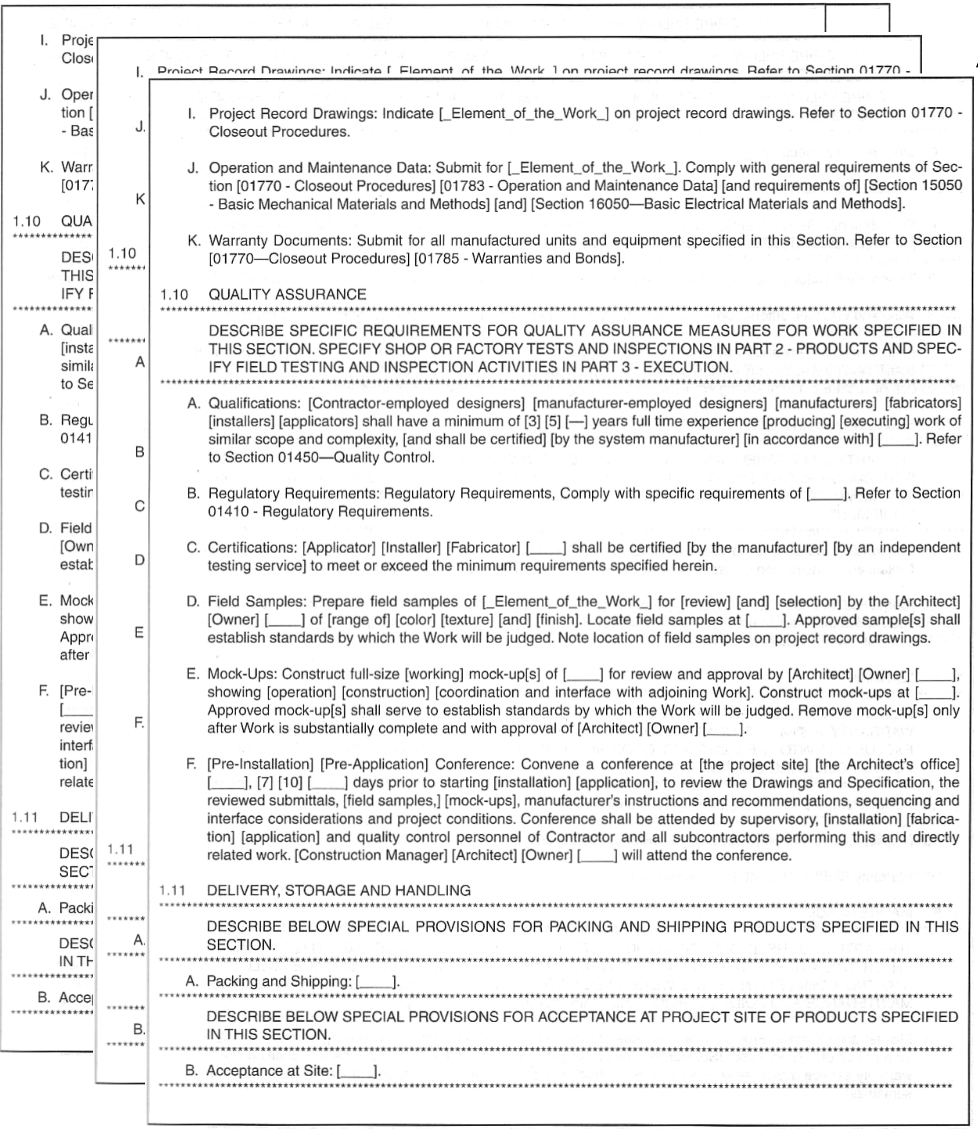
Modeling


State Behavior
Flow Behavior
Function ality
Structure
Data
Interactions

Why Model?
Let's compare Modeling versus Textual Specification

You meet with an architect to design your dream home.

2 months later …. he comes up with …



I. Project Record Drawings: Indicate [_Element_of_the_Work_] on project record drawings. Refer to Section 01770 - Closeout Procedures.

J. Operation and Maintenance Data: Submit for [_Element_of_the_Work_]. Comply with general requirements of Section [01770 - Closeout Procedures] [01783 - Operation and Maintenance Data] [and requirements of] [Section 15050 - Basic Mechanical Materials and Methods] [and] [Section 16050—Basic Electrical Materials and Methods].

K. Warranty Documents: Submit for all manufactured units and equipment specified in this Section. Refer to Section [01770—Closeout Procedures] [01785 - Warranties and Bonds].

1.10 QUALITY ASSURANCE

DESCRIBE SPECIFIC REQUIREMENTS FOR QUALITY ASSURANCE MEASURES FOR WORK SPECIFIED IN THIS SECTION. SPECIFY SHOP OR FACTORY TESTS AND INSPECTIONS IN PART 2 - PRODUCTS AND SPECIFY FIELD TESTING AND INSPECTION ACTIVITIES IN PART 3 - EXECUTION.

A. Qualifications: [Contractor-employed designers] [manufacturer-employed designers] [manufacturers] [fabricators] [installers] [applicators] shall have a minimum of [3] [5] [—] years full time experience [producing] [executing] work of similar scope and complexity, [and shall be certified] [by the system manufacturer] [in accordance with] [____]. Refer to Section 01450—Quality Control.

B. Regulatory Requirements: Regulatory Requirements, Comply with specific requirements of [____]. Refer to Section 01410 - Regulatory Requirements.

C. Certifications: [Applicator] [Installer] [Fabricator] [____] shall be certified [by the manufacturer] [by an independent testing service] to meet or exceed the minimum requirements specified herein.

D. Field Samples: Prepare field samples of [_Element_of_the_Work_] for [review] [and] [selection] by the [Architect] [Owner] [____] of [range of] [color] [texture] [and] [finish]. Locate field samples at [____]. Approved sample[s] shall establish standards by which the Work will be judged. Note location of field samples on project record drawings.

E. Mock-Ups: Construct full-size [working] mock-up[s] of [____] for review and approval by [Architect] [Owner] [____], showing [operation] [construction] [coordination and interface with adjoining Work]. Construct mock-ups at [____]. Approved mock-up[s] shall serve to establish standards by which the Work will be judged. Remove mock-up[s] only after Work is substantially complete and with approval of [Architect] [Owner] [____].

F. [Pre-Installation] [Pre-Application] Conference: Convene a conference at [the project site] [the Architect's office] [____], [7] [10] [____] days prior to starting [installation] [application], to review the Drawings and Specification, the reviewed submittals, [field samples,] [mock-ups], manufacturer's instructions and recommendations, sequencing and interface considerations and project conditions. Conference shall be attended by supervisory, [installation] [fabrication] [application] and quality control personnel of Contractor and all subcontractors performing this and directly related work. [Construction Manager] [Architect] [Owner] [____] will attend the conference.

1.11 DELIVERY, STORAGE AND HANDLING

DESCRIBE BELOW SPECIAL PROVISIONS FOR PACKING AND SHIPPING PRODUCTS SPECIFIED IN THIS SECTION.

A. Packing and Shipping: [____].

DESCRIBE BELOW SPECIAL PROVISIONS FOR ACCEPTANCE AT PROJECT SITE OF PRODUCTS SPECIFIED IN THIS SECTION.

B. Acceptance at Site: [____].

A 650 page specification document with 10,000 requirements:

… indented by 7 meters from the west border of the premises, there is a left corner of the house

… The entrance door is indented by another 3.57 meters

… 2.30 meters wide and 2.20 meters high, left-hand hinge, opening to the inside

… If you come in, there are two light switches and a socket on your right, at a height of 1.30 meters

…

Is this the house you want?

- Are the requirements correct?
- Accurate?
- Consistent?
- How can you tell?

Modeling versus Textual Specification

- Then you call another architect… And two weeks later he comes with this:

Main Level

Upper Level

- The second architect used ***Modeling*** to show different ***Views*** of the house based on an underlying collection of semantically-complete interconnected engineering data
  - Structural
  - Floor layout
  - Electrical
  - Plumbing and water flow
  - Heating capacity and flows

So What IS a Model then?

Modeling is the development of a semantically correct set of engineering data of relevant systems and their properties

Models have views (e.g. diagrams)

Diagrams show subsets of eng. data

Diagrams have singular purpose

Diagrams answer questions

Diagrams support specific reasoning

Models have scope

Models have purpose

Models have accuracy

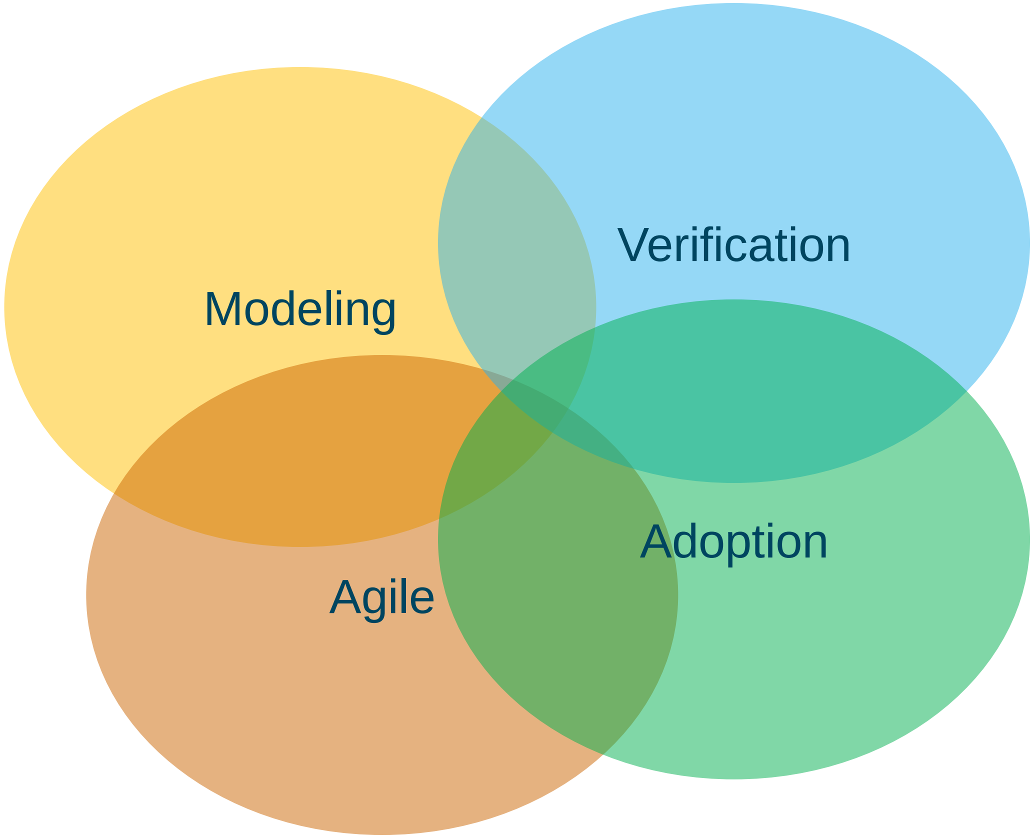
Models have fidelity

Models are falsifiable

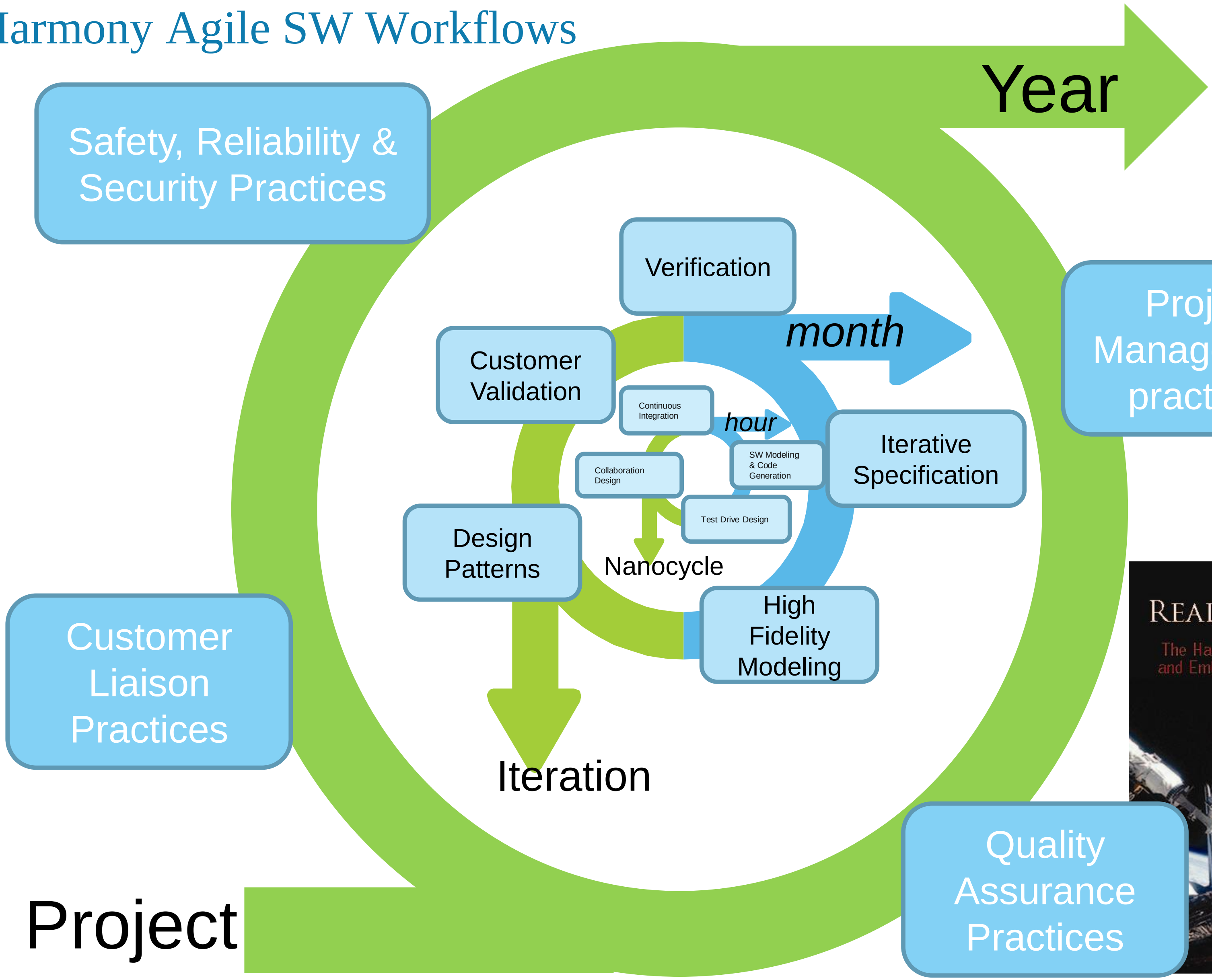
Models are verifiable

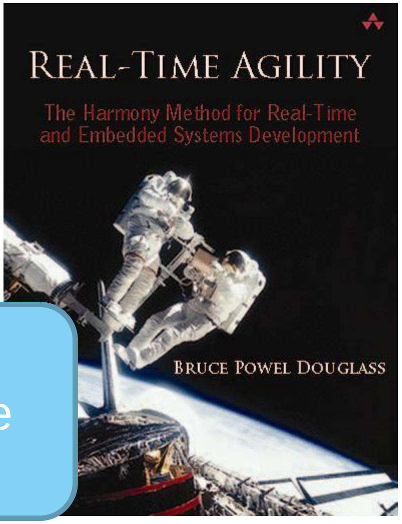
Models *are interconnected data!*

Key Topics



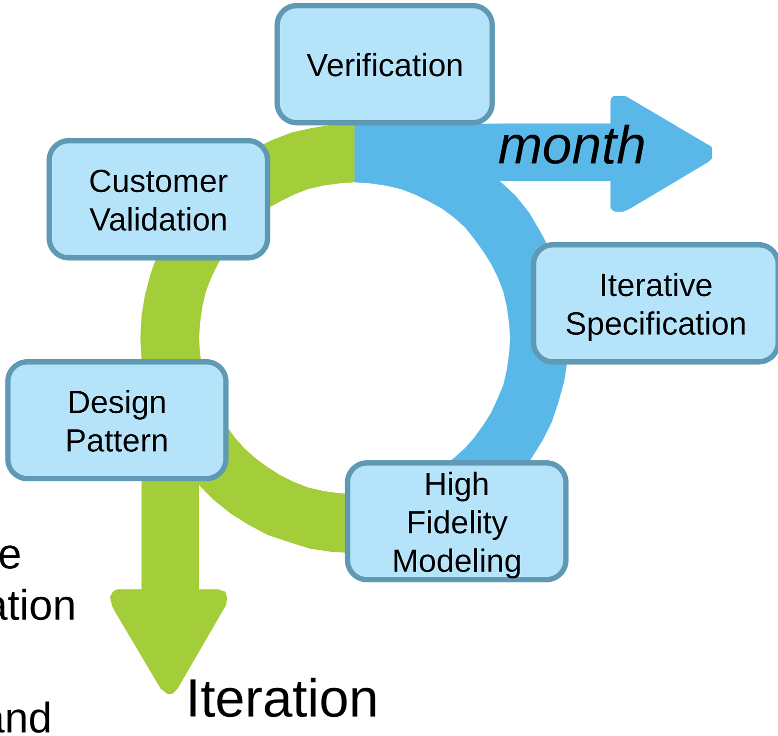
Harmony Agile SW Workflows



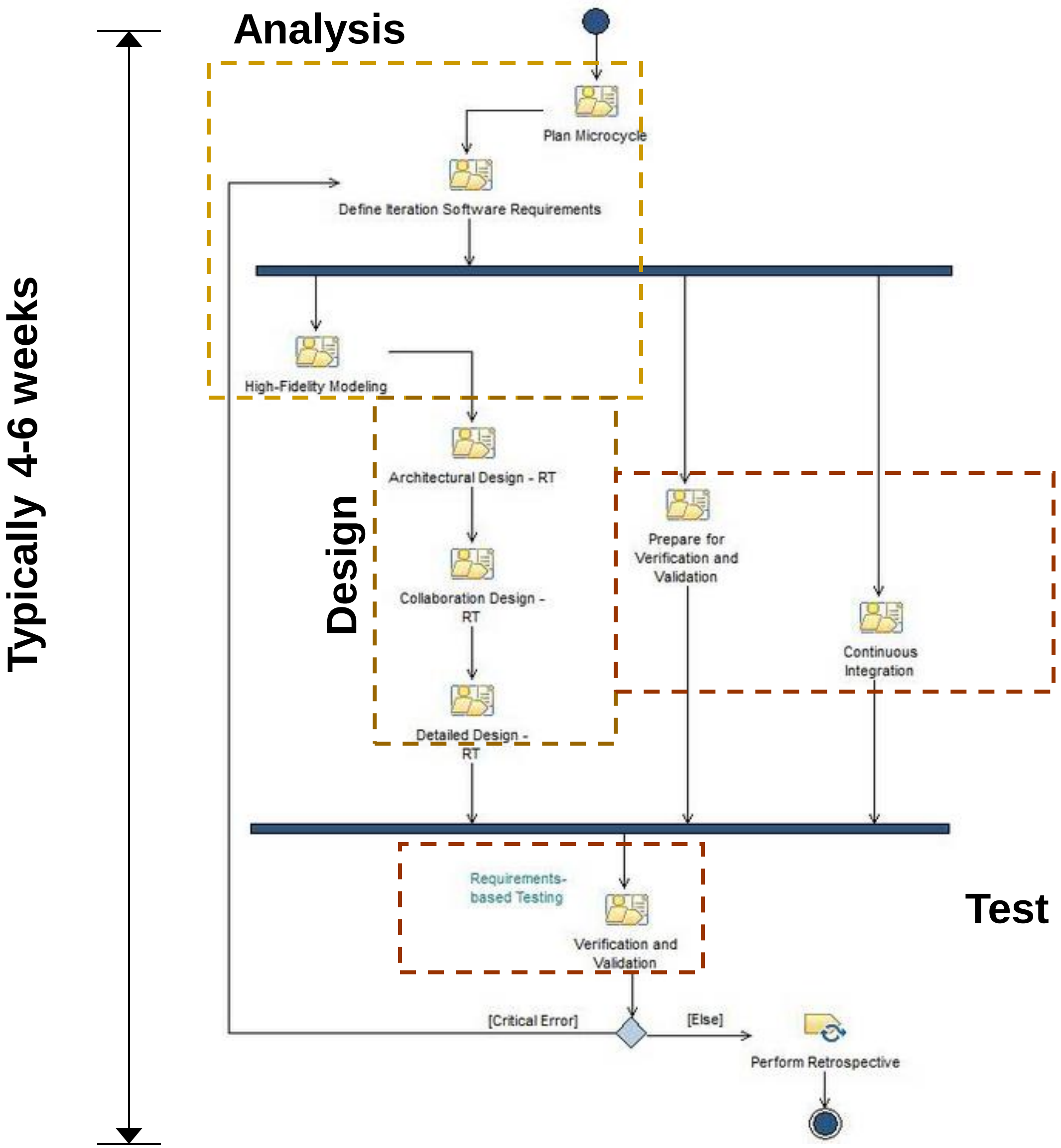


Incremental Development

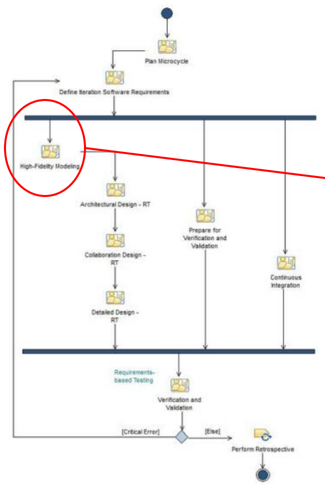
- Incremental (aka Spiral or Iterative) takes a hard problem and divides it up into a series of increments, each of which
  - Identifies a mission:
    - Implement a coherent set of requirements
    - Remove a set of identified defects
    - Reduce a set of identifies risks
    - Targets one or more platforms
    - Implements one or more architectural aspects
    - Plans a schedule with workers performing the work (usually in 4-6 weeks)
  - Creates a functional, executing model and code base of the solution to the mission (along with implementation code, test cases, test outcomes and other stuff)
  - Refines the model to optimize it against the design and quality-of-service constraints (qualities of service)
  - Tests the resulting increment against new and existing requirements

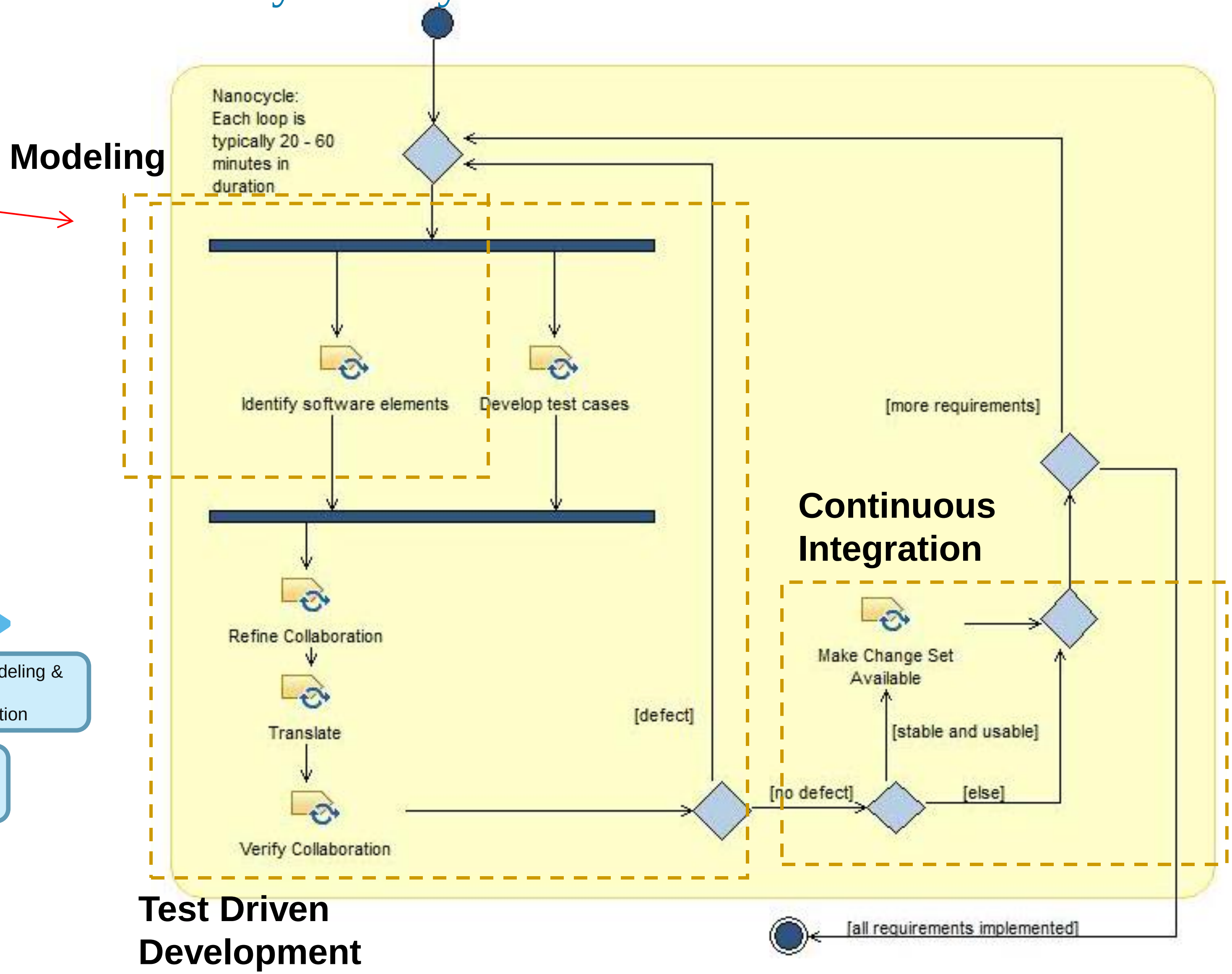


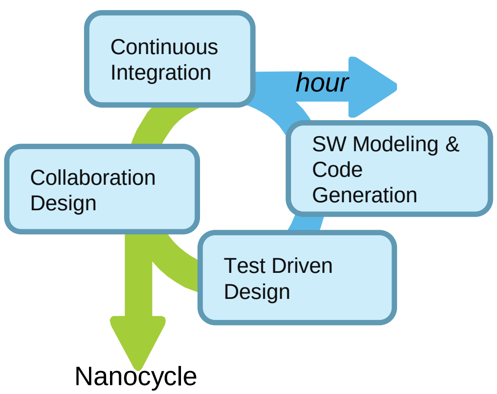
Incremental Development with Harmony®



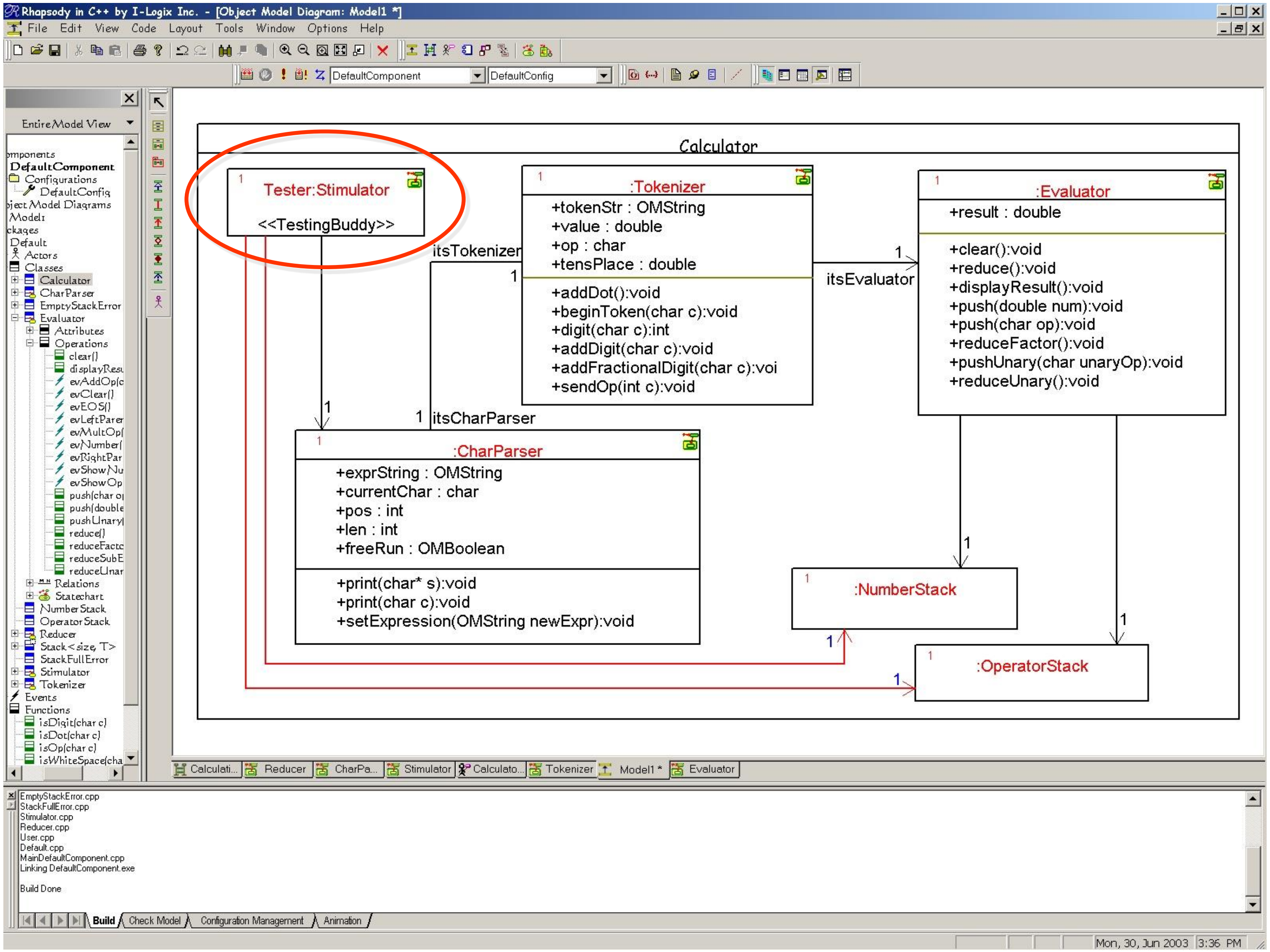
Agile Practices of the Harmony Nanocycle



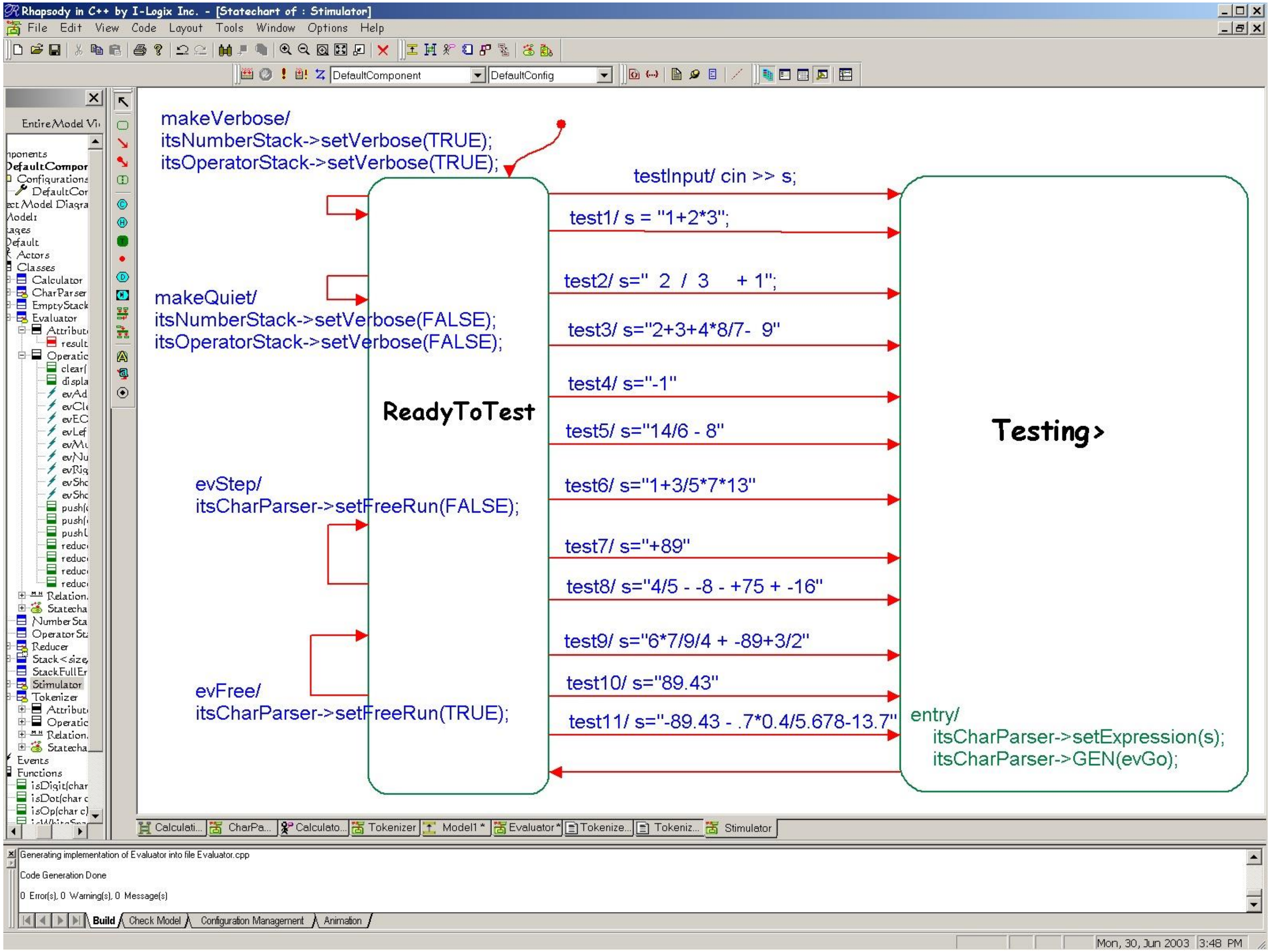




Test Driven Development



Test Driven Development



Defensive Design

- Quality cannot be effectively added later into developed software
- Defensive design is a practice that improves software robustness
  - Constant execution
    - Execute after small incremental changes, typically *at minimum* several times per day
  - Explicitly state pre- and post-conditions and class invariants
    - State assumptions for correct execution (e.g. memory needs, parameter value ranges, etc)
    - Explicitly *verify at run-time* the expectations and invariants and take corrective action as appropriate
    - NEVER ignore error indications
  - Use Test-Driven Development
    - Develop your tests prior to, or in conjunction with, the design of the software elements

Dynamic Planning

- Harmony® addresses dynamic planning with
  - 2 Level scheduling / planning
    - Overall project (e.g. initial planning + the set of iterations + deployment
    - Detailed just-in-time microcycle planning
      - Each iteration is planned around a *mission statement*, including
        - Use case/user stories to be implemented
        - Defects to be removed
        - Architectural concepts to be realized
        - Target platform to be supported (incl. hardware drivers as needed for hw integration and test)
        - Risks to be reduced via spikes (risk mitigation activities)
    - That your plans are wrong (to some degree) is expected, and results in plan updates
  - Actual progress ("truth on the ground") is monitored via metrics such as
    - Actual time (effort) vs estimated time (effort)
    - Defect density
    - Project velocity
  - Plans are updated *at least every microcycle* in the Increment Review ("Party Phase") task

Risk Management

- Projects don't fail at an instant in time - they fail gradually over months or years
- Most projects go awry because of predictable problems that were never addressed
- **Practice: The best way to reduce risk is to manage it:**
  - Identify the risks
  - Define spikes (risk mitigation activities)
  - Plan spikes execution in schedule
  - Heed the spike outcomes
  - Frequently look for new risks

Risk Management

Task: Plan For Risk Reduction

This task plans for the management of risks during the project.

Expand All Sections   Collapse All Sections

Purpose

The purpose of this task is to identify and prioritize project risks and how they will be handled, and capture this information in the risk management plan.

Back to top

Relationships

Roles	Main: • Project Manager	Additional:	Assisting:
Outputs	• Risk Management Plan		

Back to top

Steps

Expand All Steps   Collapse All Steps

- Identify key project hazards
- Determine likelihood of key project hazards
- Compute key project risks
- Rank project risks
- Specify risk mitigation activities for key project risks
- Write risk management plan

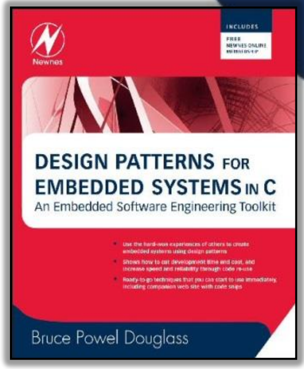
Risk Management

Project Risk List

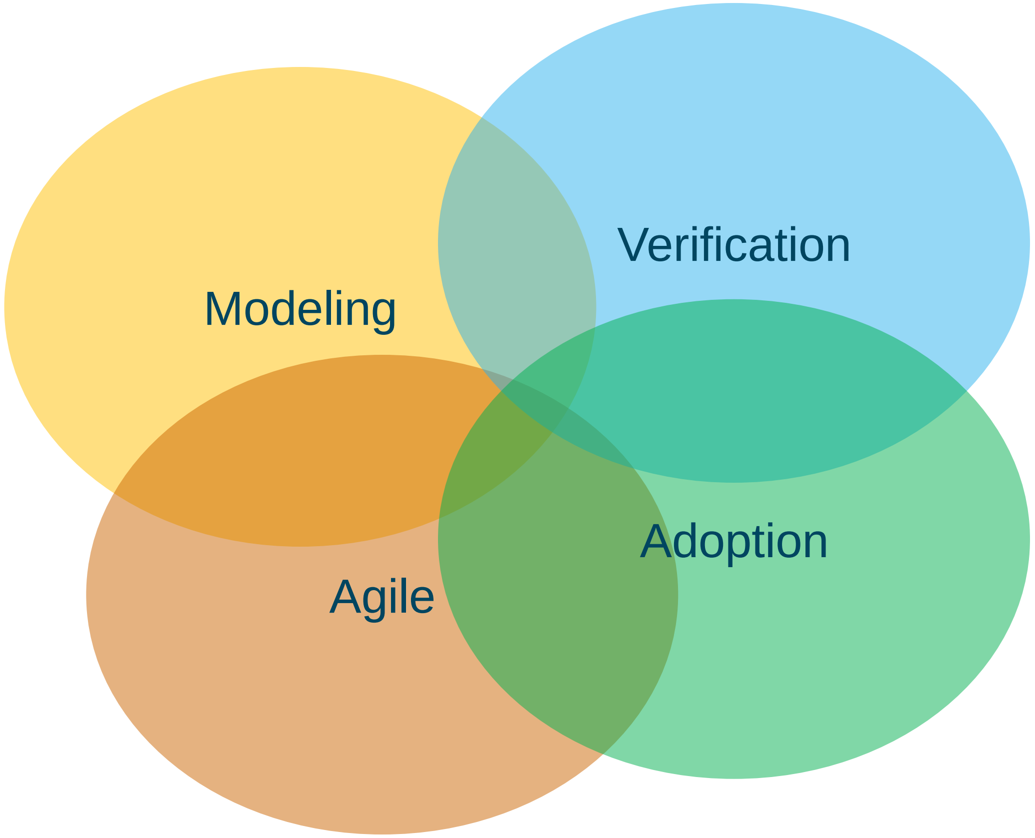
ID	Date	Name	Description	Impact	Probability	Magnitude	Owner	Mitigation Strategy
1	1/1/2011	CORBA Performance	The distributed PID control loop must have response times in < 2 ms for stability. Since elements are distributed using CORBA, this may lead to loss of the aircraft if performance is too low	4	60%	2.4	Sam	In microcycle 2, implement the effector smoothing loop over CORBA and measure the delay added
2	1/3/2011	UML Experience	The team is using UML for the first time on this project and if it doesn't work well, this could add significantly to the project time	3	90%	2.7	Joe	In prepsiral planning, engage IBM for Rhapsody and UML training with a Rapid Deployment Package to kick start the project
3	2/4/2011	Chips going end of life	Chip vendor has indicated that the 1753 bus chip used in the design will go end of life in 2014. We have to maintain the system for 20 years. We either need to stockpile enough chips or engineer a replacement design.	2	70%	1.4	Susan	In microcycle 4, evaluate alternatives and select one for going forward.
4	2/5/2011	Customer schedule is aggressive	Customer schedule is optimistic. We need to address this either by changing the expectations or figuring out how to satisfy the schedule.	4	80%	3.2	Maggy	In prespiral planning, work with the customer to see if the projet can be delivered in phases, or if ambitious features can be cut.
5	2/5/2011	Aerlion actuator has slow response time	The airfoil design is unstable and requires fast responses to maintain aircraft stability. The current actuator design may not be able to support the required QoS	5	30%	1.5	Sam	In microcycle 3, talk with control people to determine required response rate and airfoil engineers to determine alternative actuator design if necessary

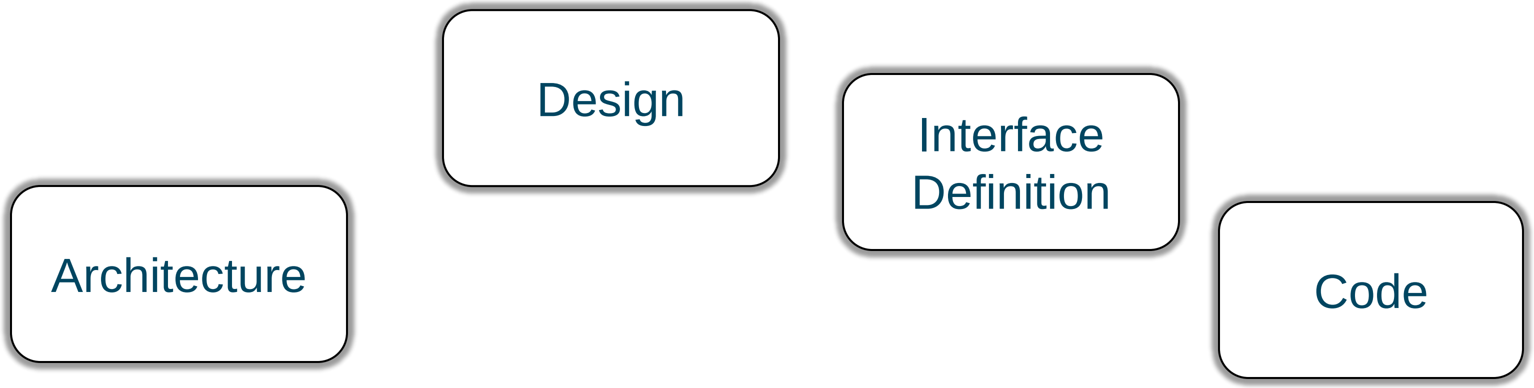
Architecture Through Design Patterns

- Harmony identifies 3 levels of design optimization
  - Architectural
  - Mechanistic
  - Detailed
- Architecture is divided into 5 primary views
  - Each view is characterized by its own set of design patterns, approaches, and technologies
  - Secondary architecture views include
    - Information Assurance & Security
    - Data Management
    - Quality of Service Management
    - Error and exception Management
- Each view has its own design patterns and technologies

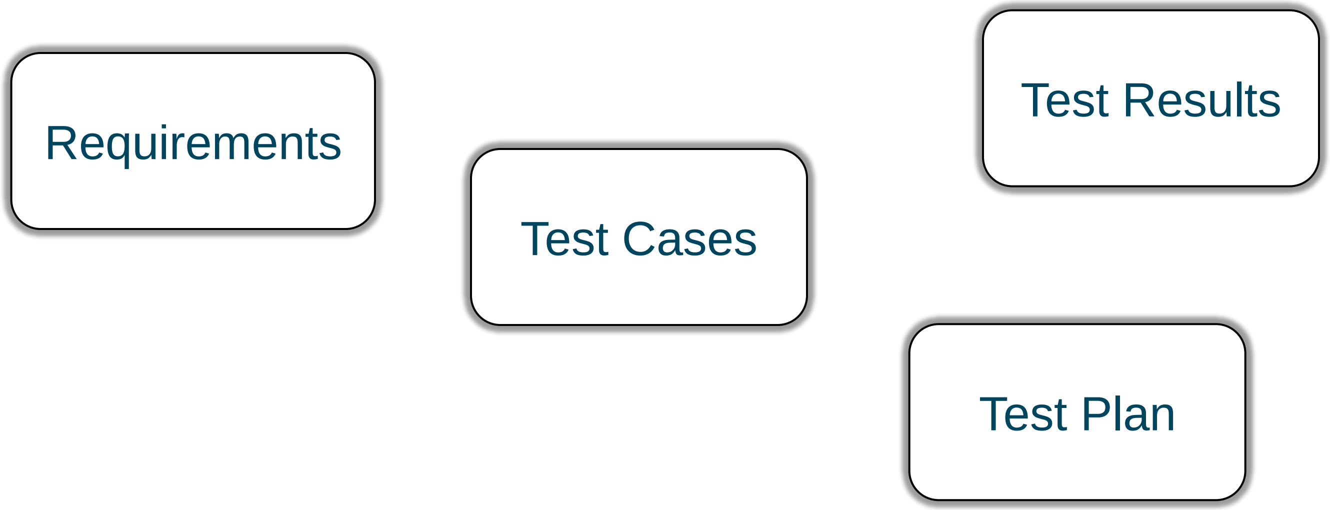


Key Topics





Code is not the only work product that needs verification and validation

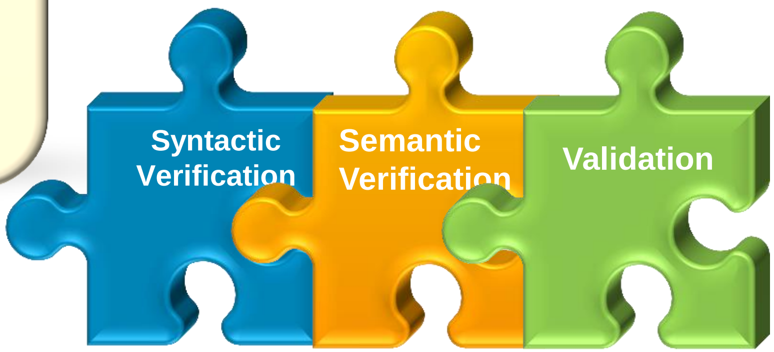


What do we mean by “verification & validation” of work products?

Semantic Verification

- “correct” (*compliance in meaning*)
  Performed by engineering personnel

Three basic techniques
- **Semantic review** (subject matter expert & peer) – most common, weakest means
- **Testing** – requires executability of work products, impossible to fully verify
- **Formal methods** – strongest but hard to do and subject to invariant violation



Syntactic Verification

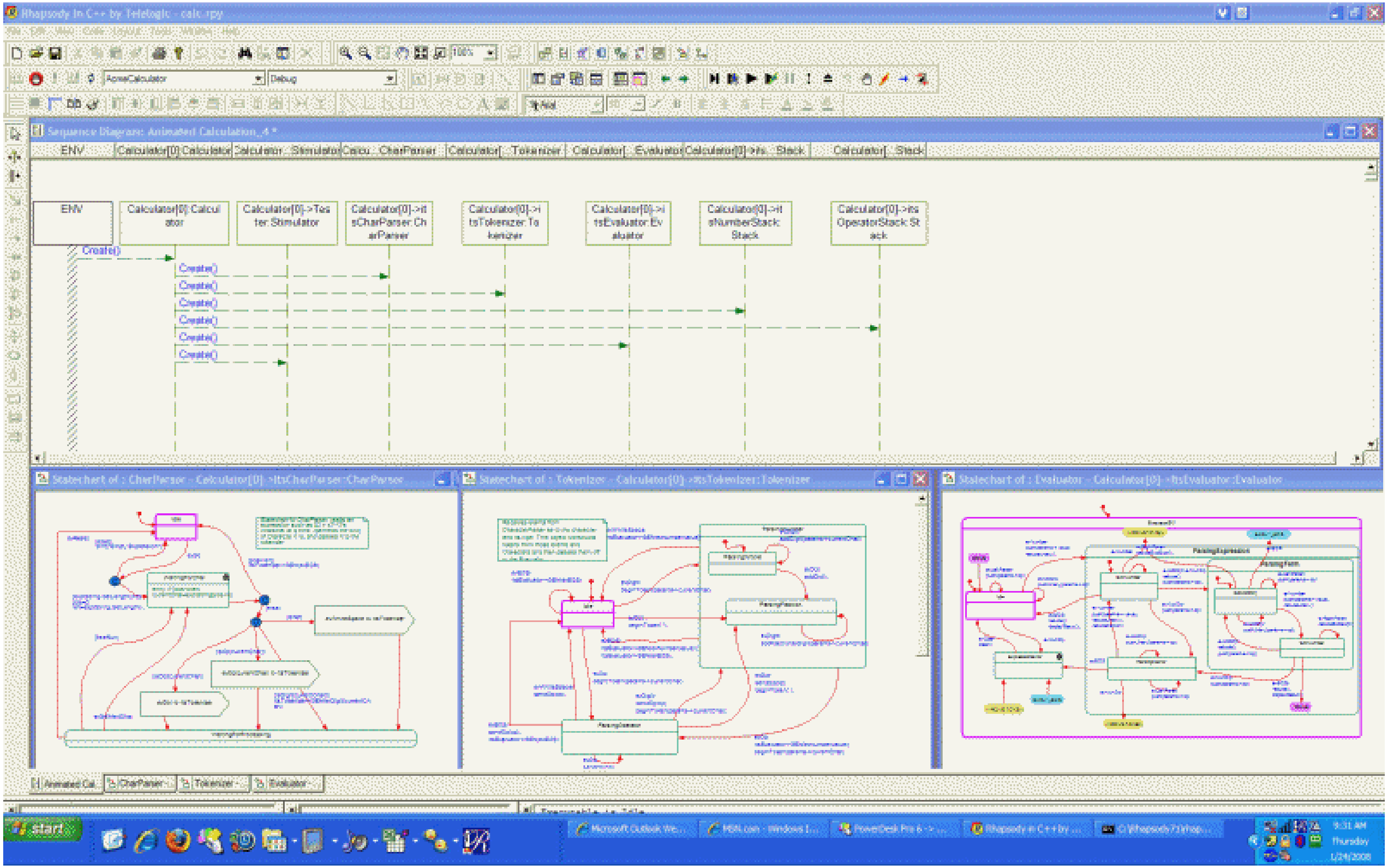
– “well-formed” (*compliance in form*)
  Performed by quality assurance personnel
- **Audits** – work tasks are performed as per plan and guidelines
- **Syntactic review** – work products conform to standard for organization, structure and format

Validation

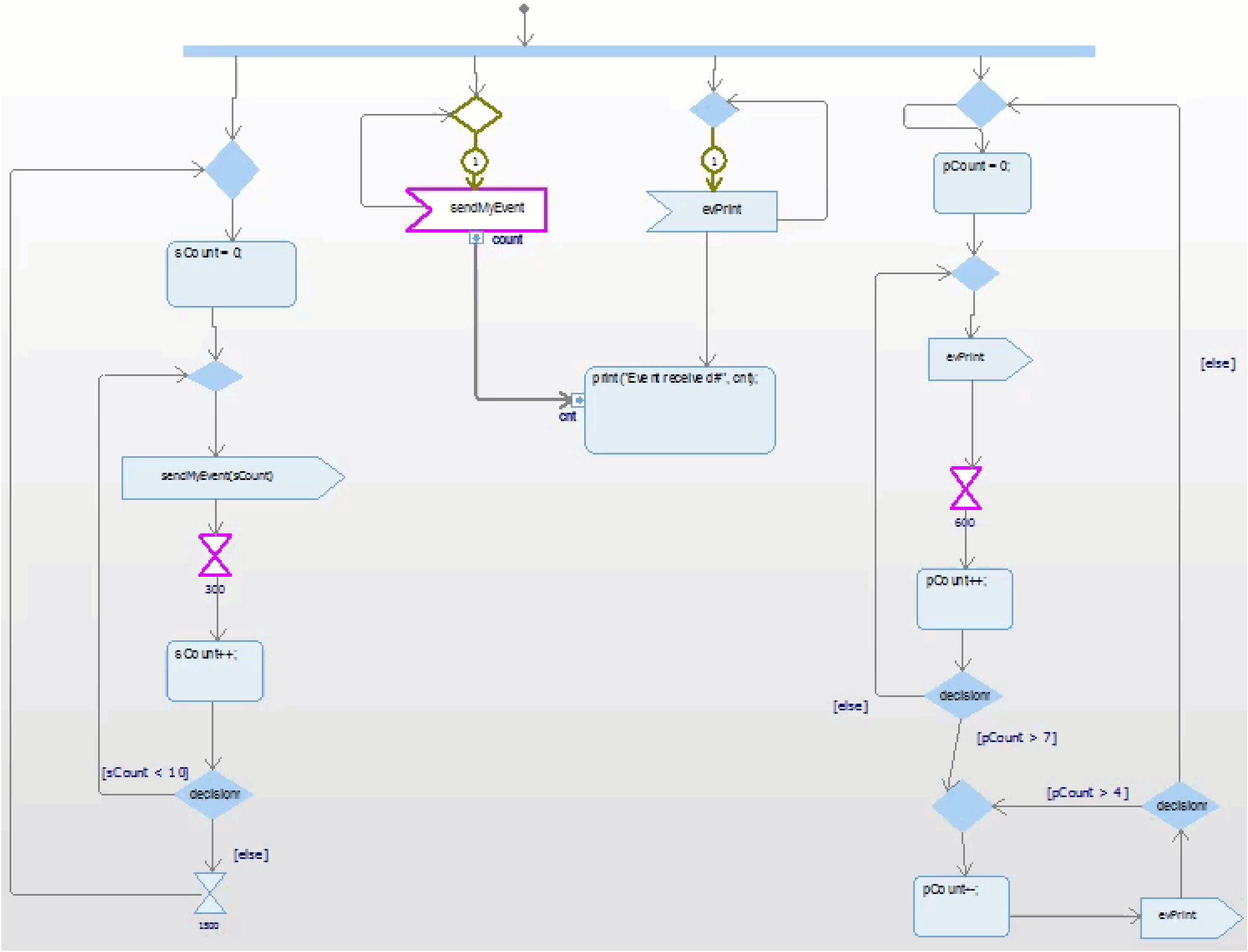
- “meets the stakeholder need”
  Performed by customer + engineering

Some common techniques
- **Review** – (subject matter expert & customer) – most common, weakest
- **Simulation** – show simulated input → outputs
- **Sandbox** – exploratory usage in constrained environment
- **Flight test** – demonstration of system capabilities
- **Deployment –** early usage of system of partial capability

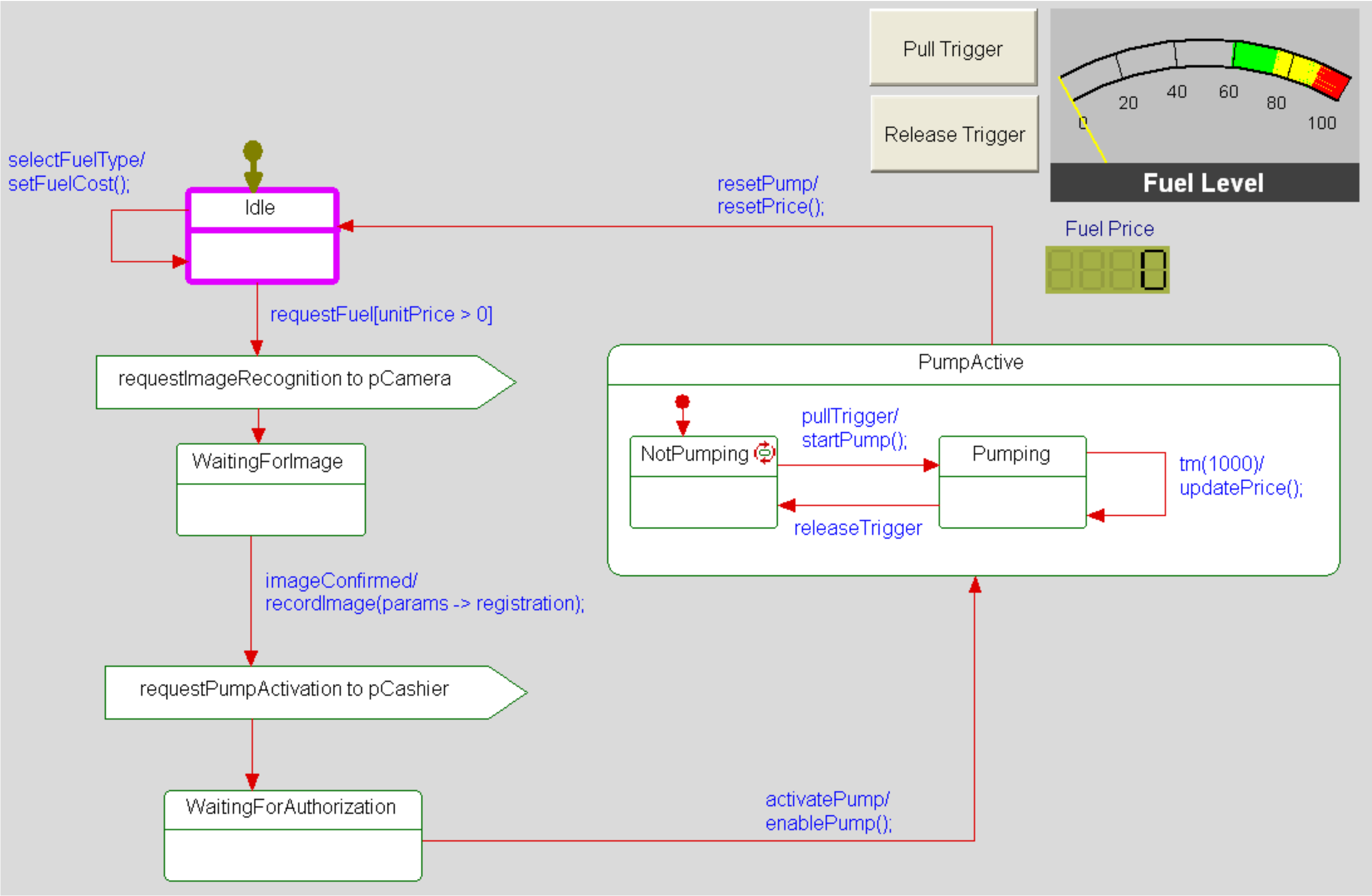
Executable Models are an important subset of Computable Models



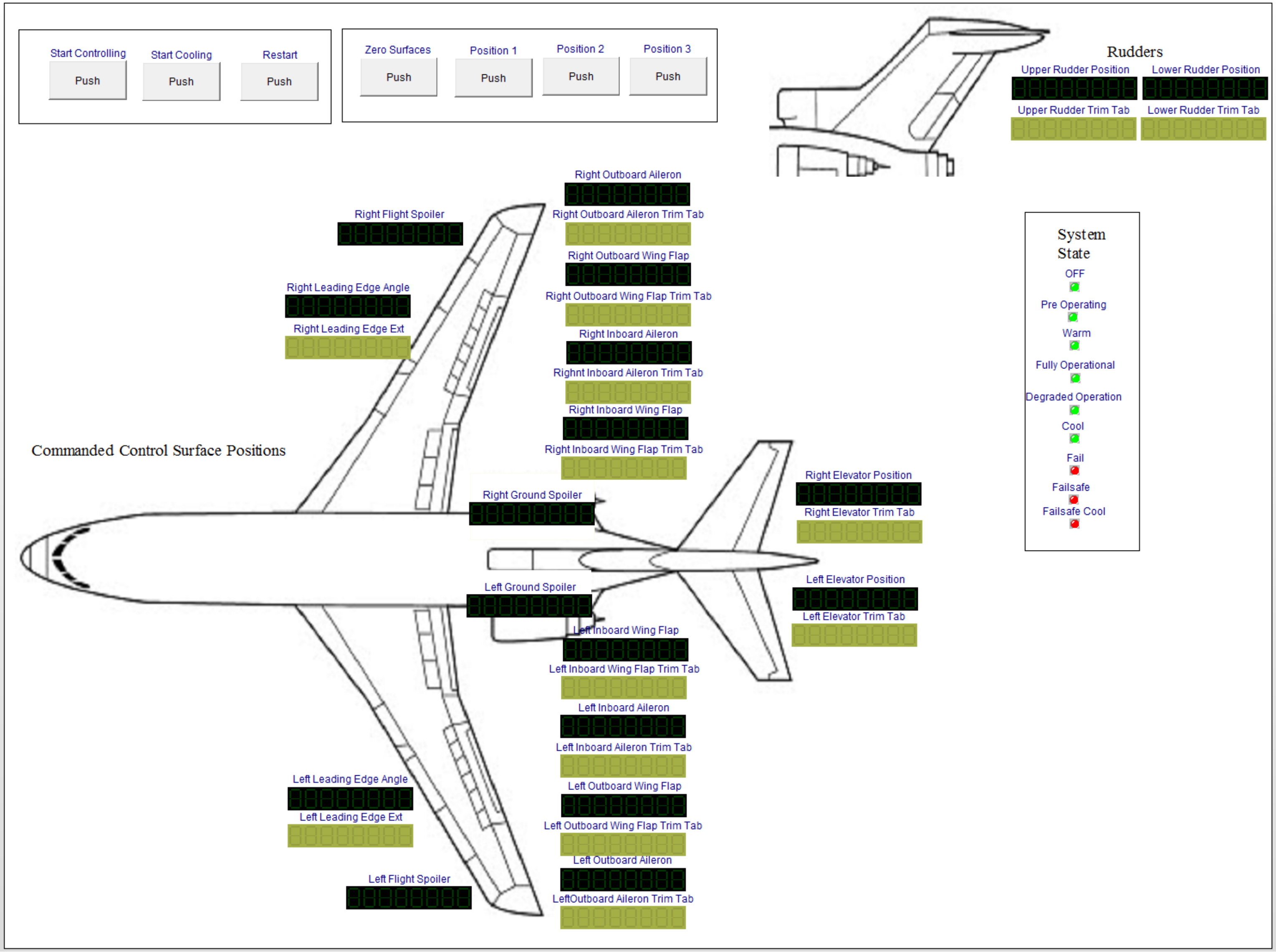
Executable Models



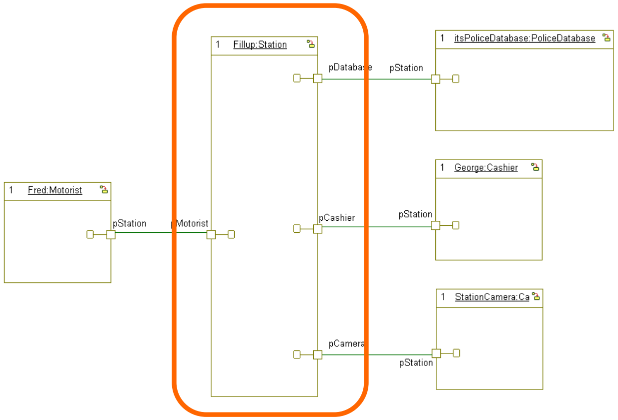
Executable Models



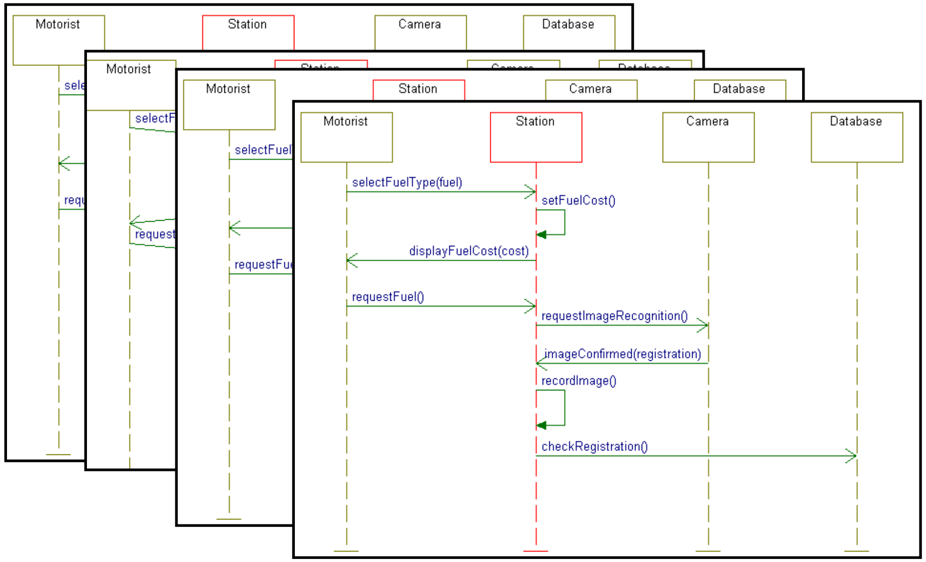
Control Surfaces System Simulation Control Panel Diagram



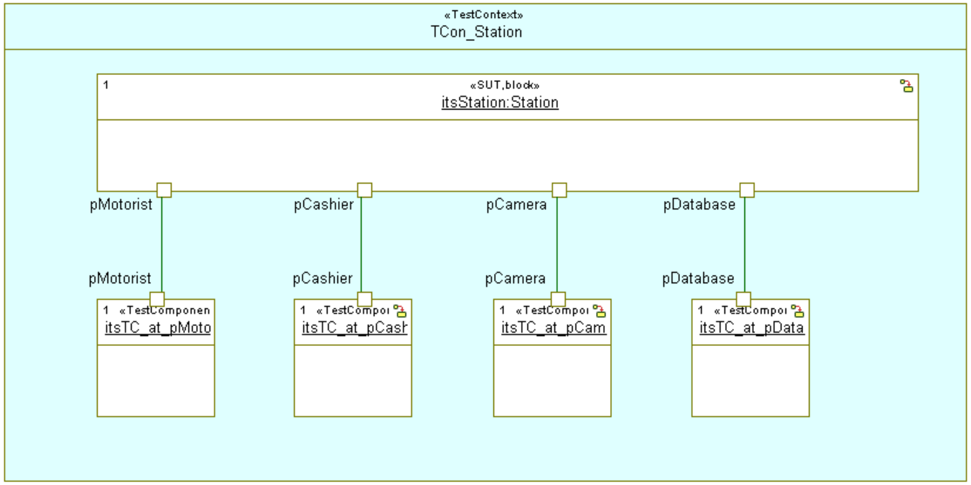
Model-Based Testing



System Under Test (SUT)



Test Cases



Test Architecture (Auto-generated)

Test Case Result

Test Case: SunnyDayTestCase

17:28:53, Tuesday, March 09, 2010

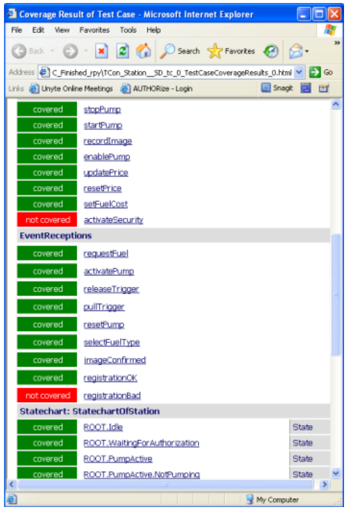
Environment Info	
Test executed on machine:	VIRTUALXP
Test executed by user:	andyl
Used OS version:	Windows 2000 / Windows XP
Used Rhapsody version:	7.5, build 1164537
Used TestConductor version:	2.4, build 1434

Tested Project	
Project:	TCTemp
Active Component:	TPkg_Station_Comp
Active Configuration:	DefaultConfig

SDs used in test
TPkg_Station::SD Motorist Arrives Sunny Day

Summary Info	Summary: passed
Total number of SDs used:	1
Total number of SD instances in test:	1
Total number of executed SD instances:	1
Total number of PASSED SD instances:	1 (100%)
Total number of FAILED SD instances:	0 (0%)
Total number of ACTIVE SD instances:	0 (0%)
Total number of NOT ACTIVE SD instances:	0 (0%)

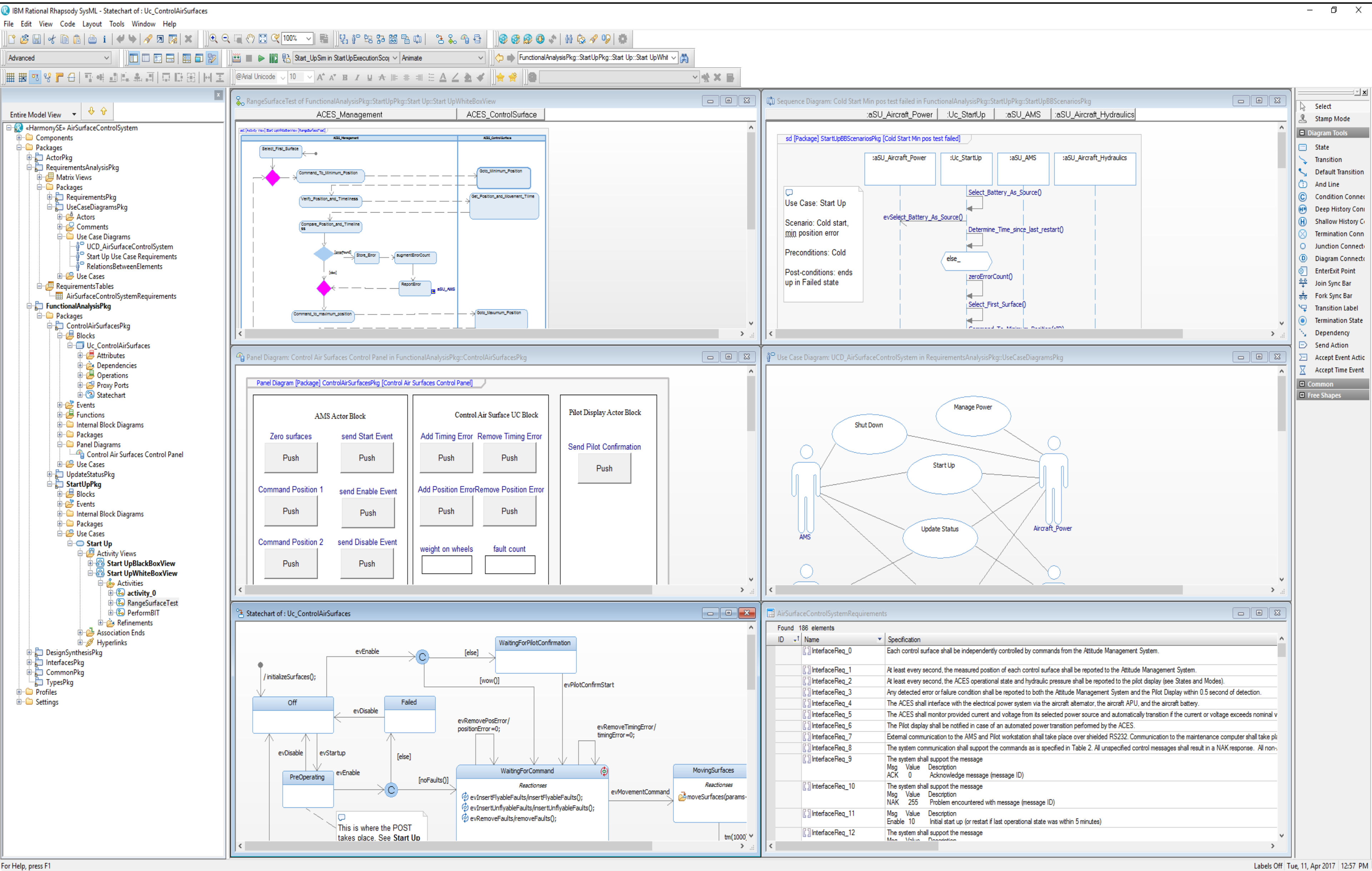
Test Coverage



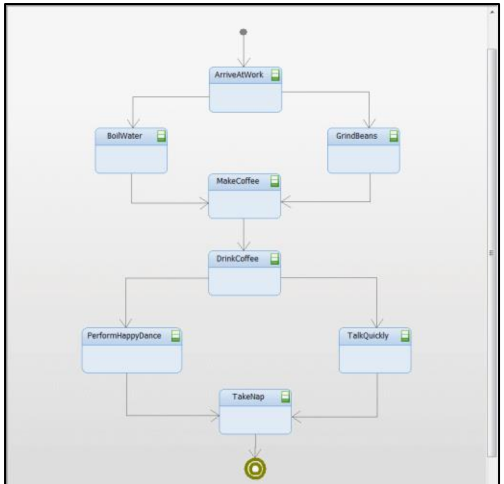
Test Outcomes

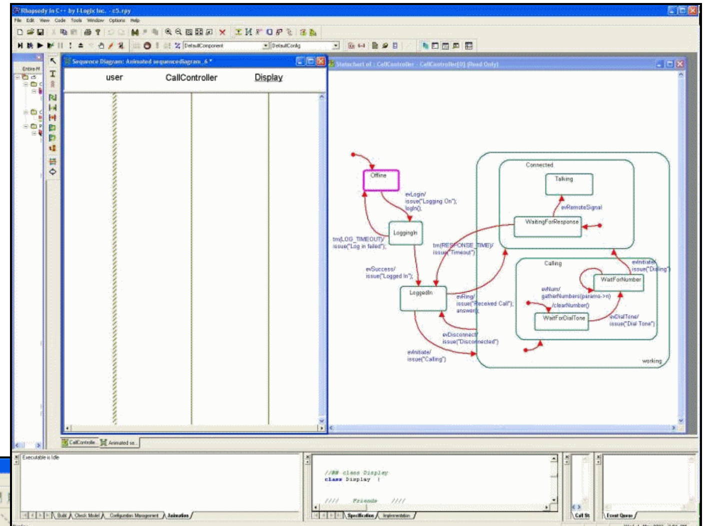
 Internet of Things

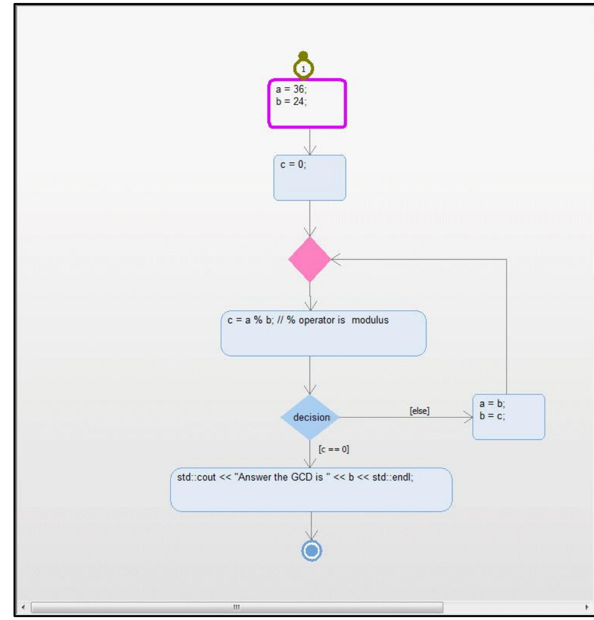
Tooling Couples **Views** with **Model Repository**

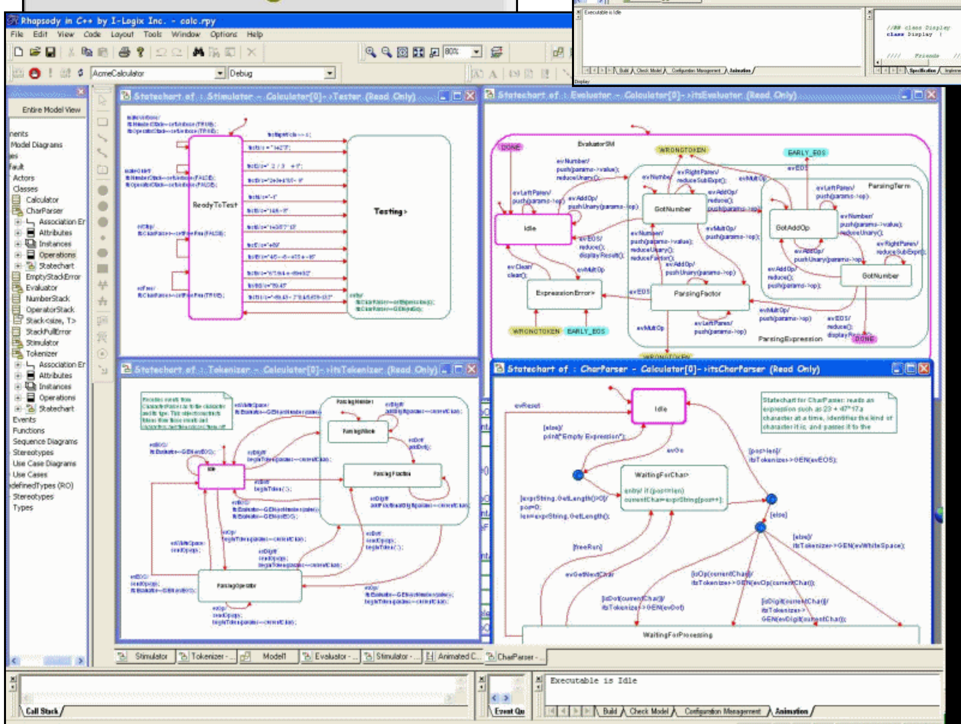


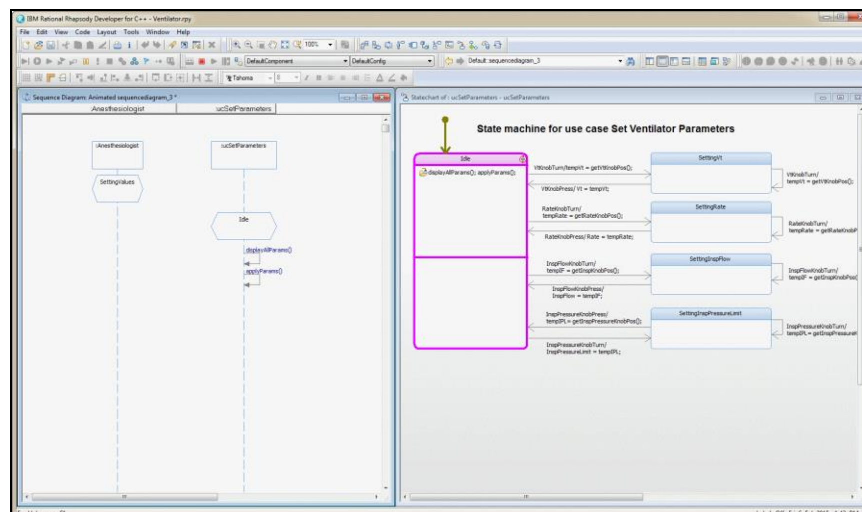
Computable Models



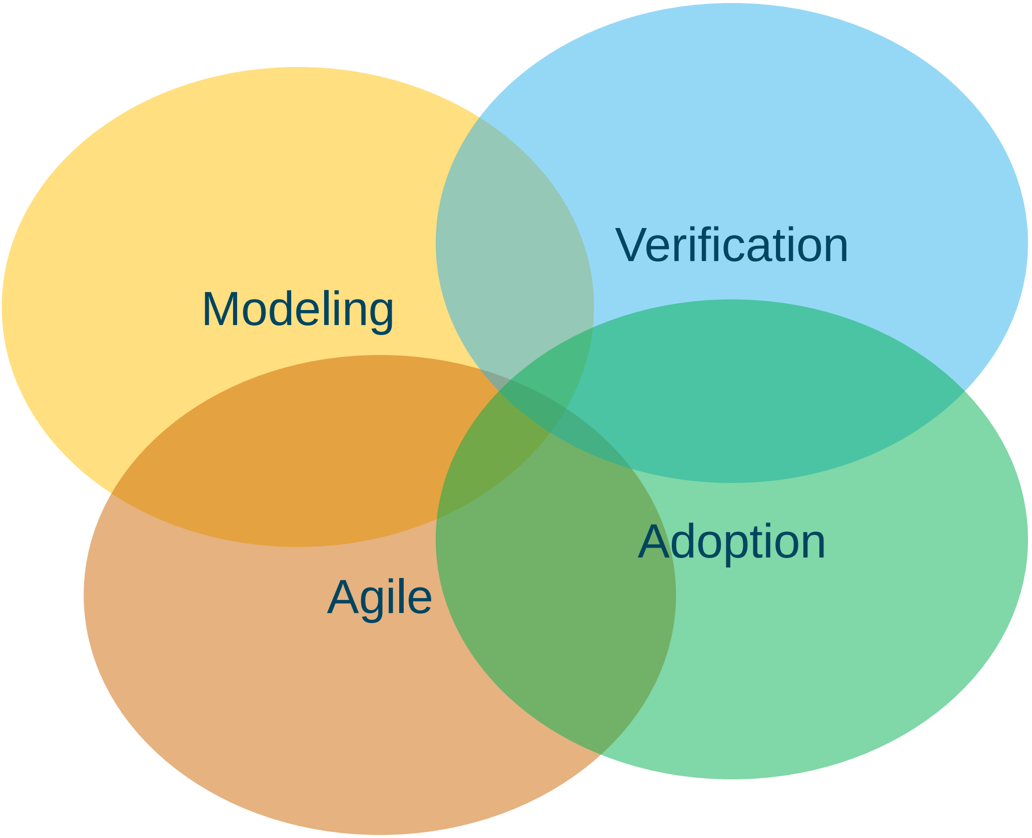




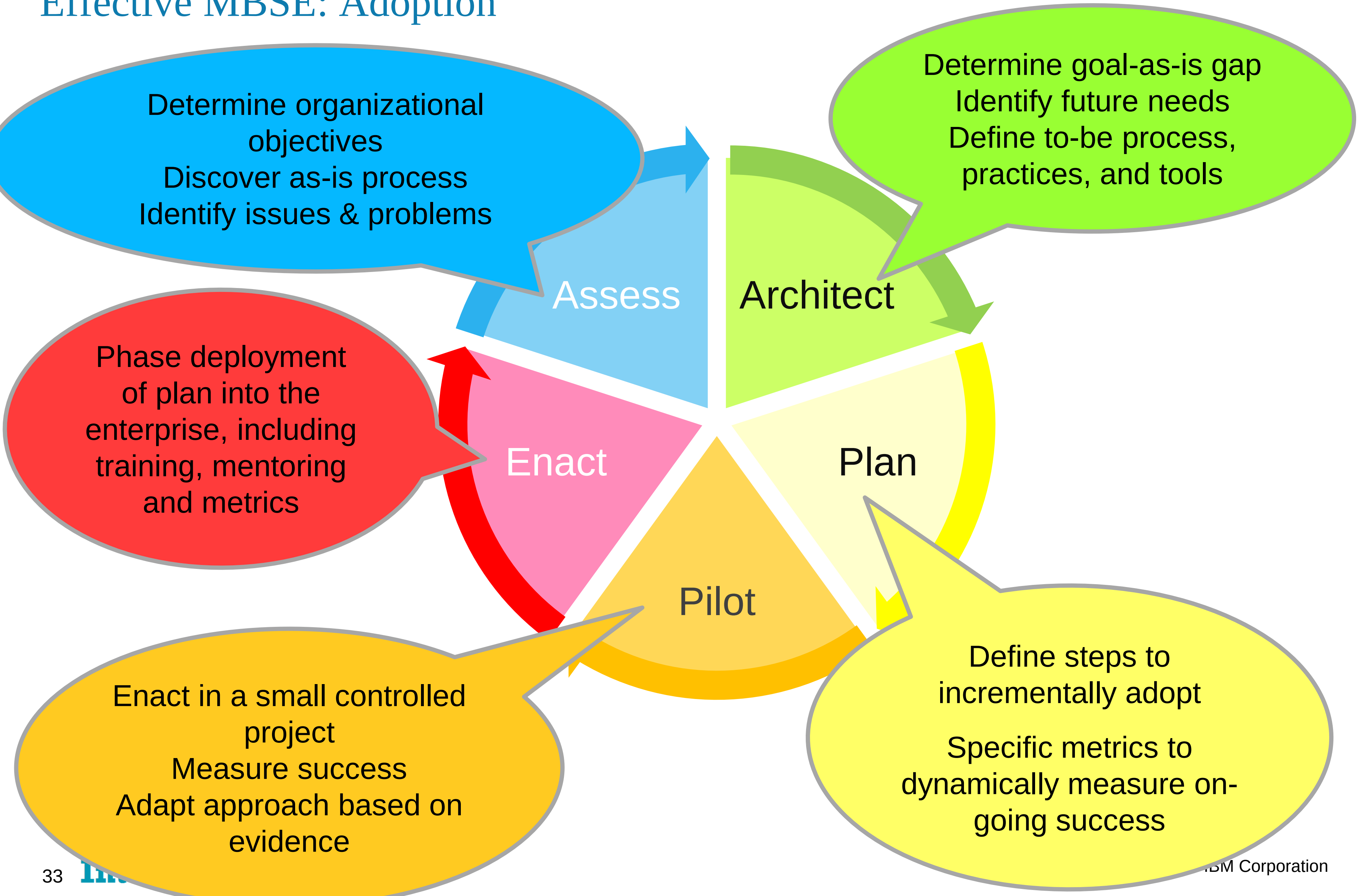




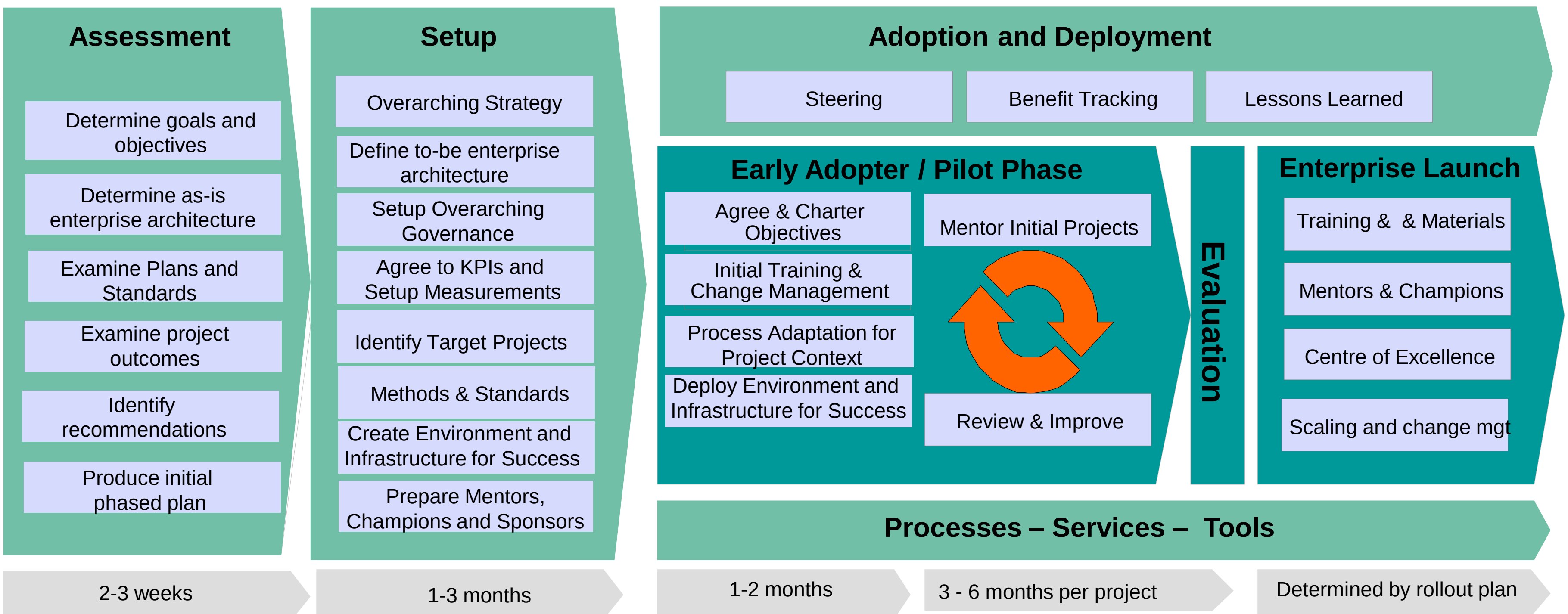
Key Topics



Effective MBSE: Adoption

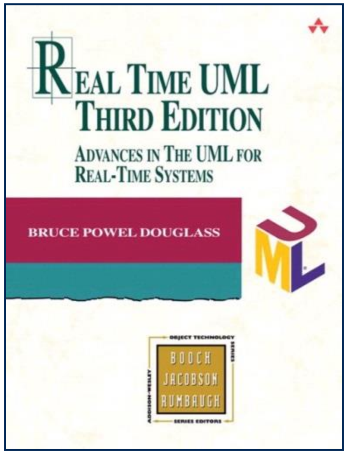


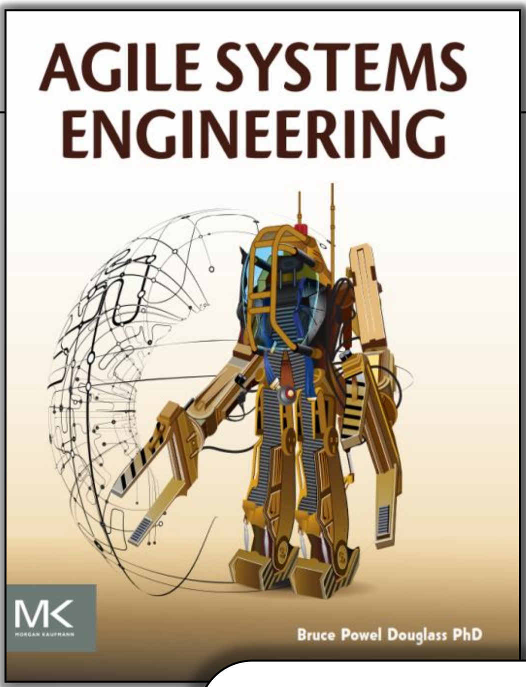
Approach for Adoption: Engineering Capability Improvement

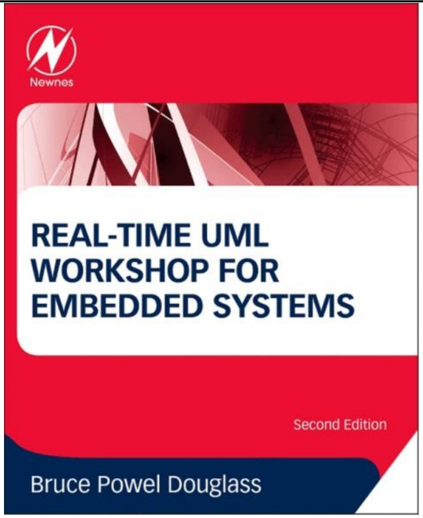


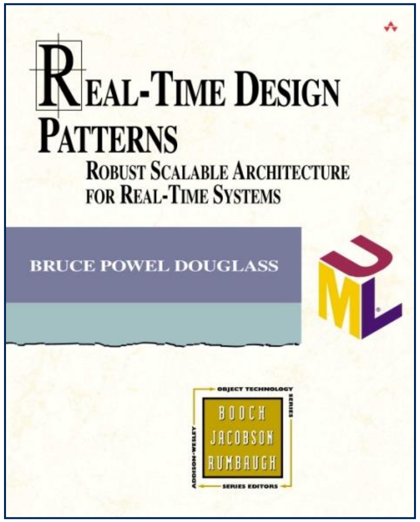
Evidence:

- Interviews
- Internal standards
- Project data









Want to know more?