Key Focus of Software Engineering

- How to describe software products?
- Processes to build software products?
  - And assure that the products are "good" at the end
- How to grow and evolve such products
  - At acceptable costs
  - And improving quality

Software Engineering = Products + Processes

Stakeholder Perspective Suggests an Approach

- How to manage the creation and maintenance of a software product that satisfies all needs of all stakeholders?
  - Implies understanding who stakeholders are; what questions they need answered; to what degree of thoroughness
  - Implies supporting reasoning needed to provide adequate answers to stakeholder questions (at acceptable cost)
  - Implies need for representation(s) of product sufficient to support such reasoning; and reasoning techniques

Stakeholder questions and concerns

The Problem of Providing Satisfactory Answers to Stakeholder Questions

- Most important questions are vague
  - Eg. Is this software user-friendly?
  - (ATCS) How to interact with pilots to assure user interfaces are going to be effective?
- Most important questions have open-ended answers
  - Eg. How fast is this system?
  - (ATCS) Different platforms, situations, conditions
- Different stakeholders require different degrees of assurance
  - Affects the degree of thoroughness of (eg.) testing
  - (ATCS) Some functions more critical than others
- Different stakeholders have differing degrees of technical sophistication
  - Affects the choice of formalism in which to couch answers

Using Models to Answer Questions

- What is a model?
- How have they been used elsewhere?
  - Most previous models have been tangible and have typically been models of physical objects
- Software Models
  - Model non-physical objects, are not tangible
  - What should they be like?
  - Should be driven by what they are for
Plato’s Cave

Plato’s Allegory

- Even tangible objects may be only models of what is “real”
- Plato: We see only images (representations) of reality
  - Like prisoners seeing only shadows on cave walls
- The images are not the reality
- What is most real is least tangible

Software is a lot like that

No one representation can be expected to suffice for all purposes

- That is the case in manufacturing other kinds of products:
  - Houses: Multiple diagrams and views; appliance user manuals; inspection reports and certificates, etc.
  - Cars: Owners manuals; shop manuals; EPA reports; NTSB reports;
  - Laws: Legislative blueprints; law; opinions; decisions in cases involving the law; impact assessments; agency budgeting reports
  - Movies: Story treatment; script; actual film; reviews; profit and loss accounting
- Representations are quite varied: Notations expressing them are too
- We should expect the same for computer software—products and processes
- Notations are better evolved, more effective, in cases of better established manufacturing disciplines

Typical Approach

- Select a (set of \[interconnected/overlapping\]?) representation(s?) (some of which are?) effective in communication with stakeholder constituent(s)
- Derive information/answers expressed in that representation that are able to satisfy stakeholder(s)
- Assure that the information is consistent with other parts of the product (e.g. the code!)
  - It helps if they are overlapping
- ATCS: FAA needs proof that all collisions will be detected
  - Statement of proof needed
  - Other artifacts: body of proof, code, code structure representations, etc. Must be derived and shown to be consistent with each other

Key Model Desiderata

- Precise
- Detailed
- Broad
- Clear

Precise

- Based upon rigorously defined semantics
- So that there is a meaning that can be definitively established to the satisfaction of all
  - To resolve disputes and disagreements
- So that definitive reasoning is possible
  - Deriving properties
  - Answering specific stakeholder questions
Detailed

- Stakeholder questions may need answers that require details
- Model must support getting down to the level of detail that is required
  - By the relevant stakeholder(s)

Broad

- Many semantic issues may need to be covered
  - Functionality, timing, robustness, precision, resource utilization, etc.
- More semantic richness is better
  - It is capable of supporting answering more questions from more stakeholder types
- Broad and Precise and NOT the same

Clear

- Understandable to the relevant stakeholder(s)
- So that they can understand what the model is saying
  - And what the results of reasoning mean
- This is definitely relative to the stakeholder community

The Great Compromise

- No single modeling approach is likely to excel in all four dimensions
- What is each one likely to be good for?
- Different needs under different circumstances
  - During conceptualization, contract negotiation
  - During development
  - During test and evaluation
  - During utilization
  - During evolution
- How to select one(s) that are appropriate for the stakeholder communities?
  - At the relevant time(s)

Some Software Representation Approaches

- Programming Languages
- Natural Language
- Structured Language
- Box-and-Arrow Charts
- Graphs
  - Flowgraphs
  - Callgraphs
  - Dataflow graphs
  - Petri Nets
- Databases
- Charts, Diagrams
- Mathematical formalisms (e.g. predicate logic)

Some Software Representation Approaches

- Programming Languages
- Natural Language
- Structured Language
- Box-and-Arrow Charts
- Graphs
  - Flowgraphs
  - Callgraphs
  - Dataflow graphs
  - Petri Nets
- Databases
- Charts, Diagrams
- Mathematical formalisms (e.g. predicate logic)
Course Strategy/Roadmap

- Look at some of them now
  - Separate and apart from when, where, and how they might eventually be used
- Understand about "precise, detailed, broad, clear"
- Then examine needs at different points during software development
- We will see many combinations of the basic approaches
  - Understand the basic approaches first

Do We Need Anything More than a Programming Language?

- Code is the ultimate
- Describes what is actually being done
- What more can you ask for?

Programming Languages

- Primary stakeholder constituency is Developers
  - Helps answer: What does the product do?
- Less useful to other stakeholder constituencies:
  - How do you get the product to do what it does? (users)
  - What is the product supposed to do? (users/investors)
  - Will the product ever fail disastrously? (bystanders)
  - Is the product’s development (almost) done? (managers/investors)
  - How extensible/adaptable is the product? (maintainers/managers/investors)
- (Some) Differences in Programming Languages are intended to help them be (more) effective in answering some of these sorts of questions.
- But additional representations are more suitable for most of these questions and stakeholder constituencies

Even Developers Need More

- "What does it do"—for
  - Complicated programs
  - Large programs
  - Badly written programs
  - Programs written poorly or in poor programming languages
- "How does it work"
  - NB: Languages that separate specification part from implementation part are attempting to address this question
  - What would happen if I changed.....
  - How should our team go about changing....

Even Developers Need More

Most programming languages answer MOST software questions poorly

Example: Elevator Controller

- What is it supposed to do?
  - Stop on every floor it is called to
  - Maybe not so easy: multiple elevators
  - Service users "first come, first served"
  - May conflict with optimal strategies
- These are hard to be precise about, reason about in "plain English"
- Code helps with some of these, but not all
- What should it never do?
  - Allow elevator to move with doors open
  - What else?
More Appropriate Representations(?)

• "How does it work"
  – Diagrams: Box-and-Arrow charts, data and control flow
  – Petri-Nets

• "What is it supposed to do"
  – Natural language
  – Finite State Machines

• "What can’t/won’t it do"
  – Natural language

• "How do I get it to work"
  – Structured Natural Language
  – Dependency diagrams

• "What would happen if I changed...."
  – Structured Natural Language
  – Dependency diagrams

• "How should our team go about changing ...."*
  – Process descriptions, using...
    – All of the above
Natural Language

- Write in "plain English"
- All stakeholders understand natural language (?)
- Possible to augment with defined terms
- Use of punctuation for clarification
- Text/word processing systems help automate/maintain/alter

Examples of Natural Language artifacts:
- User manuals
- Most requirements specifications
- Most test plans
- Development status reports

Advantages of Natural Language

- Easy to train users
- Clarity is possible (but may be difficult)
- Completeness is possible (but by no means assured)
- Easily modified
- It is the "least common denominator"

But--
Disadvantages are far more numerous and serious

Natural Language Disadvantages

- Determining consistency between natural language artifacts and anything else is hard/subjective
  --Ambiguity in natural language is easy and sometimes intentional
  --Clear natural language expression is very difficult
  --The longer the text, the more information, the more the risk of inconsistency, the harder it is to determine
- No way of knowing when a specification is "complete"

Main Problems are:
- Cannot reason definitively about natural language
- Cannot be sure that natural language artifacts are consistent with other artifacts
- Assurances to stakeholders are shaky

More Appropriate Representations (?)

- "How does it work"
  - Diagrams: Box-and-Arrow charts, data and control flow
  - Petri-Nets
- "What is it supposed to do"
  - Natural language
  - Finite State Machines
- "What can’t/won’t it do"
  - Natural language
- "How do I get it to work"
  - Structured Natural Language
- "What would happen if I changed....."
  - Dependency diagrams
- "How should our team go about changing ...."* 
  - Process descriptions, using...
  - All of the above
- "What does it do" for large, complex programs
  - Program models and abstractions

Create them, and assure that they are consistent with other artifact types

Discreted Use of Natural Language

- Response to natural language problems of:
  --imprecision
  --ambiguity
  --inconsistency (especially when due to size)
  --inability to reason effectively and definitively
- Familiar approaches:
  --Restricted use of reserved terms
  --Structuring (paragraph numbering, outline form, templates, etc.)
- Other, earlier examples of disciplined use of natural language:
  --Laws and other legal documents
  --Recipes
  --Help systems

Examples of Natural Language artifacts:
- Program models and abstractions
- Petri-Nets
- Finite State Machines
- Structured Natural Language
- Dependency diagrams
- Process descriptions, using...
- All of the above
- User manuals
- Most requirements specifications
- Most test plans
- Development status reports
- Text/word processing systems help automate/maintain/alter
A Software Engineering Example: PSL (Problem Statement Language)

**DESCRIPTION:**
This process performs those actions needed to interpret time records to produce a pay statement for each hourly employee.

**KEYWORDS:**
- independent;

**ATTRIBUTES ARE:**
- complexity-level high;

**GENERATES:**
- pay-statement, error-listing;

**RECEIVES:**
- time-card;

**SUBPARTS ARE:**
- hourly-paycheck-validation, hourly-emp-update, h-report-entry-generates, hourly-paycheck-production;

**PART OF:**
- payroll-processing;

**USES:**
- time-card, hourly-employee-record;

**DERIVES:**
- pay-statement;

**USING:**
- hourly-employee-report;

**USING:**
- time-card, hourly-employee-record;

**DERIVES:**
- error-listing;

**USING:**
- time-card, hourly-employee-record;

**HAPPENS:**
- number-of-payments TIMES-PER pay-period;

**TRIGGERED BY:**
- hourly-emp-processing-event;

**TERMINATION-CAUSES:**
- new-employee-processing-event;

**SECURITY IS:**
- company-only;

**Discipline Mechanisms in PSL**

- Use of keywords (defined elsewhere in specification)
  - fosters precision, clarity
  - helps support consistency determination: some keyword fields have defined relations to others (eg. input-to and output-from)

- Use of templates
  - facilitates determination of completeness
  - fosters clarity
  - facilitates consistency checking

- Use of structure:
  - HIERARCHY:
    - Standard practice for dealing with size, complexity
    - Exploits innate human capacity for abstraction

- DATA FLOW:
  - Can determine which data objects flow to what activities

**Evaluation of Disciplined Natural Language**

- Big step in the right direction: improvement over straight natural language
- Possible to determine some kinds of consistency thru:
  - mechanisms for reducing ambiguity
  - mechanisms for fostering completeness
  - structuring mechanisms for dealing with complexity

- Stilted form reduces clarity: less suitable for some key stakeholder groups
- Some residual reliance on natural language means ambiguity remains
- Size is still a problem: PSL specs (for example) can be huge: consistency determination is long/error prone

**Pictorial and Diagrammatic Approaches**

- Diagrams composed of visual elements having rigorously defined (definable?) semantics
- Diagrams used as modeling devices
- Diagrams depict key structural aspects of system
- Reduction or removal of natural language
- Clarity improved greatly
- Consistency improved greatly
- Completeness of diagrams facilitated
- Possibility of ambiguity considerably reduced

**Example: Elevator Controller**

- What is it supposed to do?
  - Stop on every floor it is called to
  - Maybe not so easy: multiple elevators
  - Service users "first come, first served"
  - May conflict with optimal strategies
  - These are hard to be precise about, reason about in "plain English"
  - Code helps with some of these, but not all
  - What should it never do?
    - Allow elevator to move with doors open
    - What else?

**Data Flow Diagram**

- New Request
- Get copy of Request List
- Satisfied
- New Request
- Update Request List
- New Floor
- Elevator
- Move
- Request List
- New Request
- Satisfied
- Get copy of Request List
- Update Request List
- Button Press
- Turn on Light
- Turn off Light
- Current Floor
- New Floor
Control Flow Diagram

Finite State Machine

Petri Net

Pictures are not enough

An Example: A Data Flow Diagram

The power of annotation:

Improper use of notation is not saved by annotation here:
What’s wrong with this diagram

There is ambiguity and misuse of notation here:
• one circle is a test, others are functions

There is ambiguity and misuse of notation here:
• one circle is a test, others are functions

There is ambiguity and misuse of notation here:
• one circle is a test, others are functions
• some edge annotations are data, some predicates

There is ambiguity and misuse of notation here:
• one circle is a test, others are functions
• some edge annotations are data, some predicates
• are multiple arrows in and out “and” or “or”? 

Very Simple DFD

Attempt to make this more precise
Relations:

A relation, \( R \), over a set, \( S = \{s_i\} \), is a set of tuples:

\[ R = \{r_i\} \quad \text{where} \quad r_i = \{s_{i_1}, s_{i_2}, \ldots, s_{i_n}\} \]

An n-ary relation is a relation where all of the tuples are n-tuples.

A binary relation is a relation where all of the tuples are 2-tuples.

If \( (s_i, s_j) \) is an element of \( R \), then we often write \( s_i R s_j \).

Some familiar properties of ordered binary relations, \( R \), over the set \( S = \{s_i\} \):

- **Symmetry**: \( s_i R s_j \) if and only if \( s_j R s_i \)
- **Reflexivity**: \( s_i R s_i \) for all \( s_i \) in \( S \)
- **Transitivity**: \( s_i R s_j \) and \( s_j R s_k \) implies \( s_i R s_k \)

A relation that is symmetric, reflexive, and transitive is called an equivalence relation.

\( R \) is transitive if for all \( s_i, s_j, s_k \) in \( S \), \( s_i R s_j \) and \( s_j R s_k \) implies \( s_i R s_k \).

\( R \) is reflexive if \( s_i R s_i \) for all \( s_i \) in \( S \).

\( R \) is symmetric if \( s_i R s_j \) implies \( s_j R s_i \).

\( R \) is transitive if \( s_i R s_j \) and \( s_j R s_k \) implies \( s_i R s_k \).

\( R \) is reflexive if \( s_i R s_i \) for all \( s_i \) in \( S \).

\( R \) is symmetric if \( s_i R s_j \) implies \( s_j R s_i \).

\( R \) is transitive if \( s_i R s_j \) and \( s_j R s_k \) implies \( s_i R s_k \).

Some examples of ordered relations:

Let \( L \) = \{(all integers)\},

Define \( F = \{ (x, y, z) \mid x, y, z \text{ are integers and} \ y = x^2, z = x^3 \} \)

Let \( S = \{\text{all states of the U.S.}, S_i\}, \)

Define \( B = \{ (S_i, S_j) \mid S_i \text{ and } S_j \text{ are states that share a border} \} \)

Let \( L = \{\text{all states of a program, } S\}, \)

Define \( \text{ImmFol} = \{(L_i, L_j) \mid \text{the execution of } L_i \text{ may immediately follow the execution of } L_j \text{ for some execution of } P \} \)

Some Properties of Relations

Some familiar properties of ordered binary relations, \( R \), over the set \( S = \{s_i\} \):

- **Symmetry**: \( s_i R s_j \) if and only if \( s_j R s_i \)
- **Reflexivity**: \( s_i R s_i \) for all \( s_i \) in \( S \)
- **Transitivity**: \( s_i R s_j \) and \( s_j R s_k \) implies \( s_i R s_k \)

A relation that is symmetric, reflexive, and transitive is called an equivalence relation.

If \( R = \{(s_i, s_j)\} \) is transitive, then \( C = \{s_i, s_j\} \) there exists a sequence, \( i_1, i_2, \ldots, i_n \), in \( S \), such that \( s_i R s_{i_1}, s_{i_1} R s_{i_2}, \ldots, s_n R s_j \).

Antisymmetry: \( s_i R s_j \) if and only if \( s_j R s_i \) for all \( s_i \) and \( s_j \) in \( S \).

Irreflexivity: \( s_i \neg R s_i \) for all \( s_i \) in \( S \).

Examples

- **If** \( S = \{\text{all subroutines written in Fortran}\} \), \( s_i R s_j \) if and only if \( s_i \text{ calls } s_j \), then \( R \) is an irreflexive relation.
- **Let** \( P = \{\text{all statements in a program that consists of a set of modules, } m_i = \{m_i\}\} \),
  - \( \text{INMOD} = \{ (c_i, c_j) \mid c_i \text{ and } c_j \text{ appear in the same module } m \} \)
  - \( \text{INMOD} \) is an equivalence relation.
- The relation \( \text{ImmFol} \) (earlier slide) is not transitive.
- Change \( \text{ImmFol} \) to \( \text{Fol} \), by defining \( \text{Fol} = \{(L_1, L_2) \mid \text{the execution of } L_2 \text{ may follow the execution of } L_1 \text{ for some execution of } P \} \).
**Graphs**

A graph, $G = (N, E)$ is an ordered pair, consisting of a node set, $N$, and an edge set, $E = \{(n, n)\}$

If $G = (N, E)$ is an ordered graph with
$E = \{(n, n)\}$ then its unordered version, $UG = (N, U)$, where $U = \{<n, n>\}$

**Paths**

A path, $P$, through an ordered graph $G = (N, E)$ is a sequence of edges, $\{(n_1, n_2), (n_2, n_3), \ldots, (n_i, n_j)\}$ such that $n_{i+1} = n_i$ for all $2 \leq k \leq n$

A path, $UP$, thru an unordered graph $UG = (N, U)$ is a sequence of edges, $\{<n_1, n_2>, <n_2, n_3>, \ldots, <n_i, n_j>\}$ such that all of the $<n_i, n_j>$ can be ordered to assure that $n_{i+1} = n_i$ for all $2 \leq k \leq n$

In either case, $n_1$ is called the start node and $n_j$ is called the end node.

The length of a path is the number of edges in the path.

A graph $G$ is connected if and only if, for every pair of nodes, $n_i, n_j$, there is a path from one of them to the other with $G$ considered to be an unordered graph.

**Other Types of Graphs**

A multigraph $MG$ is an ordered pair $MG = (N, C)$ where $N$ is a set of nodes $\{n\}$ and $C$ is a collection of pairs of nodes (edges) with repetitions allowed (ie. $C$ can be a multiset).

A hypergraph $HG$ is an ordered pair $HG = (N, T)$ where $N$ is a set of nodes $\{n\}$ and $T$ is a set of $t$-tuples of nodes, where $t \geq 2$.

A hypermultigraph is a hypergraph where the set of $t$-tuples can be a multiset.

A bipartite graph $BG$ is an ordered pair, $BG = (BN, E)$ where $BN$ is a node set that is the union of two disjoint subsets, $N \cup N_e$, and no edge in $E$ has both nodes in either $N$ or $N_e$.

A bipartite graph is often called a 2-colorable graph.

A $k$-colorable graph is defined analogously, with $BN$ being the disjoint union of $k$ subsets.

**Trees**

A cycle in a graph $G$ is a path whose start node and end node are the same.

A simple cycle in a graph $G$ is a cycle such that all of its nodes are different (except for the start and end nodes).

If a graph $G$ is connected and has no path through it that is a cycle, then the graph is called acyclic.

An acyclic, connected, unordered graph is called a tree.

A collection of trees is called a forest.

If the unordered version of an ordered connected graph is acyclic, the graph is called a directed tree. (In this course we drop this distinction and call both graphs trees).

If the unordered version of an ordered graph has cycles, but the ordered graph itself has no cycles, then the graph is called a Directed Acyclic Graph (DAG).

**Examples**

If $S=$ (all subroutines written in Fortran) $s \rightarrow R$ $s$, if and only if $s$ calls $s_n$, then $R$ is an irreflexive relation.

Let $PS = \{c_1, c_2, \ldots\}$ all the statements in a program that consists of a set of modules, $M = \{m_1, m_2, \ldots\}$.

$INMOD = \{(c_1, c_2) \mid c_1$ and $c_2$ are in the same module $m_1\}$.

$INMOD$ is an equivalence relation.

The relation $ImmFol$ (earlier slide) is not transitive.

$INMOD = \{\{(c_1, c_2), (c_2, c_3), (c_1, c_3)\} \mid c_1, c_2, c_3 \in C\}$.

$INMOD$ is a 2-colorable graph.

$INMOD$ is often called a 2-colorable graph.

A $k$-colorable graph is defined analogously, with $BN$ being the disjoint union of $k$ subsets.
Differences in Graphs Result from Different Choices for Nodes & Relations

- Hierarchy:
  - Models "consists of" or "is a part of"
  - Key to divide-and-conquer approaches to understanding
- Data Flow:
  - Nodes represent set of sites where data is generated/used
  - Each edge is a (data generated, data used) node pair
- Control Flow:
  - Nodes represent units of functionality
    - \((n_1, n_2)\) is an edge in this graph if and only if \(n_1\) can execute immediately after \(n_2\) executes (\(ImmFol\) relation)
- Finite State Machines
  - Nodes represent all possible different "execution states"
    - \((s_1, s_2)\) is an edge if and only if it is possible for state \(s_1\) to immediately succeed \(s_2\).
    - Called \(transition\) from \(s_1\) to \(s_2\)
- Edges annotated with transition condition
  - Annotations are relations too

Callgraphs

Let \(PROC = (\text{procedures S... that the program P comprises})\)

Let \(CALLS = (\text{S... S...})\) \(i S... \text{ is directly invoked from S... during some execution of P}\)

Then \(CG = (\text{PROC, CALLS})\) is called the Call Graph of P

CG is a directed graph
If P is written in a language that does not allow recursion, then CG will be acyclic
A cycle in CG indicates that the nodes along the cycle participate in a recursive calling chain

NOTE: DEPICTIONS OF THESE GRAPHS MAY BE SUPERIMPOSED OVER EACH OTHER TO CLARIFY (?!)

DATA FLOW DIAGRAMS

- Capture system functionality: What does system do? How?
- Basic components of a data flow diagram:
  - Nodes, represented by circles (boxes), are functional units
  - Edges, represented by arrows, are data flows between units
  - Both augmented by separate annotation relations
  - Boxes (sometimes circles), represent I/O data

Flowgraphs

Let \(S = \text{(all statements s... in a program, P)}\)

Let \(ImmFol = \text{((s_1, s_2) I The execution of s_1 immediately follows the execution of s_2 for some execution of P)}\)

Then: \(if FG = (S, \text{ImmFol})\), FG is called the flowgraph of P

FG is an ordered graph
Every execution sequence (ie. the sequence in which the statements of P are executed for a given execution of P) corresponds to a path in FG.

However—the converse is not true. A path through FG may not correspond to an execution sequence for P

A loop in P appears as a cycle in FG

Formalizing DFDs

- DataFlow(i, j) if node i creates data that node j uses
- INPUT--set of nodes (input) such that input is a provider of input from external source
- OUTPUT--set of nodes (output) such that output is a conveyor of computed artifacts to external source
- EdgeAnnotation(e, operand) where operand is the identification of the artifact that flows along edge e
  - Preferably the data artifact is defined rigorously
- NodeAnnotation(n, text) if the string text describes the functioning of node n

Questions this helps answer:
- Why create this data? Who uses this data? What results does the end user see? What does the end user have to input?
- Questions this can’t answer: What is the exact sequence of events?
  - How does a node do its job?

Adding Hierarchy

- Supports increased detail
- Increased precision too
- But creates complications
Consistency is a principal concern

• Are the diagrams consistent with each other?
• Top view consistent with elaborations?
  – Arrows consistent
  – Data flows consistent
  – Other semantics?
• Invitation to subtle errors