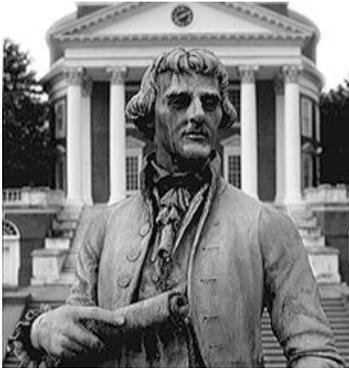


# FAA National Software Conference, May 2002

## Erroneous Requirements

### Erroneous Requirements: A Linguistic Basis For Their Occurrence and an Approach to Their Reduction.



**John C. Knight**  
Department of Computer Science  
University of Virginia

### University of Virginia

- Faculty:
  - John Knight
  - David Evans
- Graduate students:
  - Kimberly Hanks, Elisabeth Strunk, William Greenwell
  - David Laroche, Greg Yukl, Joel Winstead
- Undergraduate students:
  - Lisa Filemyr, Stavan Parikh, Brian Rowe
  - David Friedman, Mike Lanouette, Hien Phan
- NASA technical manager:
  - Kelly Hayhurst

# FAA National Software Conference, May 2002

## Erroneous Requirements

**Aviation Systems**



Increased Aviation *Functionality*

Improved Aviation *Safety*

Complex *Digital* Systems  
- *Air* and *Ground*

*Extensive Software*

3

FAA Software Conference

**Current Air Transports**



4

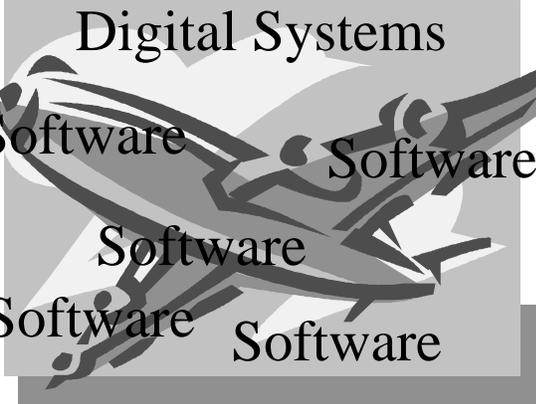
FAA Software Conference

Images courtesy of Boeing Corporation

# FAA National Software Conference, May 2002

## Erroneous Requirements

### Future Air Transports



Software is a pervasive *enabling* technology.

*Lots of ultra-dependable software required.*

5 FAA Software Conference

### Sometimes Simple Systems Fail

- Challenge:  
What is the shortest production program (measured in machine instructions) delivered by a major manufacturer that contained a bug?

6 FAA Software Conference

# FAA National Software Conference, May 2002

## Erroneous Requirements

### Why Do Software Systems Fail?

To a first approximation, requirements specification is the **dominant source** of problems in safety-critical and high-assurance **software** systems

7

FAA Software Conference

### Why Do Software Systems Fail?

- “Majority of safety-critical defects derive from poor requirements”  
-- *Lutz*
- “Majority of *all* defects derive from poor requirements”  
-- *AF Rome Laboratory*
- “The hardest single part of building a software system is deciding precisely what to build”  
-- *Brooks*

8

FAA Software Conference

# FAA National Software Conference, May 2002

## Erroneous Requirements

### Why Do Software Systems Fail?

- “It is not the internal complexity of a module but the complexity of the module’s connection to its environment that yields the persistent safety-related errors seen”  
-- *Lutz*
- “More has been screwed up on the battlefield and misunderstood at the Pentagon because of the lack of understanding of the English language than any other single factor”  
-- *Vessey*

9

FAA Software Conference

### Why Do Software Systems Fail?

#### ***Again:***

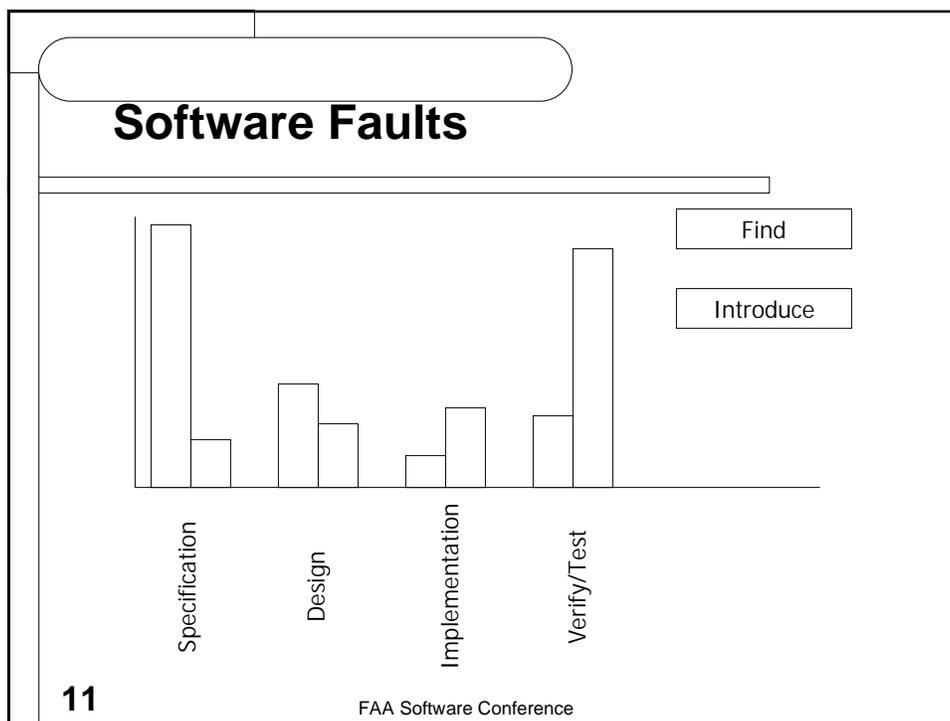
To a first approximation, requirements specification is the **dominant source** of problems in safety-critical and high-assurance **software** systems

10

FAA Software Conference

# FAA National Software Conference, May 2002

## Erroneous Requirements



### Hypotheses

The cause of many requirements errors is ***improper understanding*** of information from one domain by engineers who are not experts in that domain.

Proper acquisition, representation, and propagation of information from all relevant domains is ***crucial***.

12

FAA Software Conference

# FAA National Software Conference, May 2002

## Erroneous Requirements

### Examples

- There are many causes of failure, many are complex combinations of circumstances. But these examples are suggestive of the problem of *understanding*:
  - **Misunderstood** units:
    - Mars Polar Lander
  - **Misunderstood** term:
    - UK batch chemical reactor
  - **Misunderstood** context:
    - Ariane V
- All could be avoided by specific process changes
- What is the underlying cause? What is the general solution?

13

FAA Software Conference

### The General Solution Is Not

- Ad hoc process changes:
  - That deals only with specific symptoms
  - Does not necessarily deal even with a class of symptoms
- Ad hoc technological change—same reasons
- Switch to formal techniques:
  - In practice, formal languages *alone* cannot specify software completely

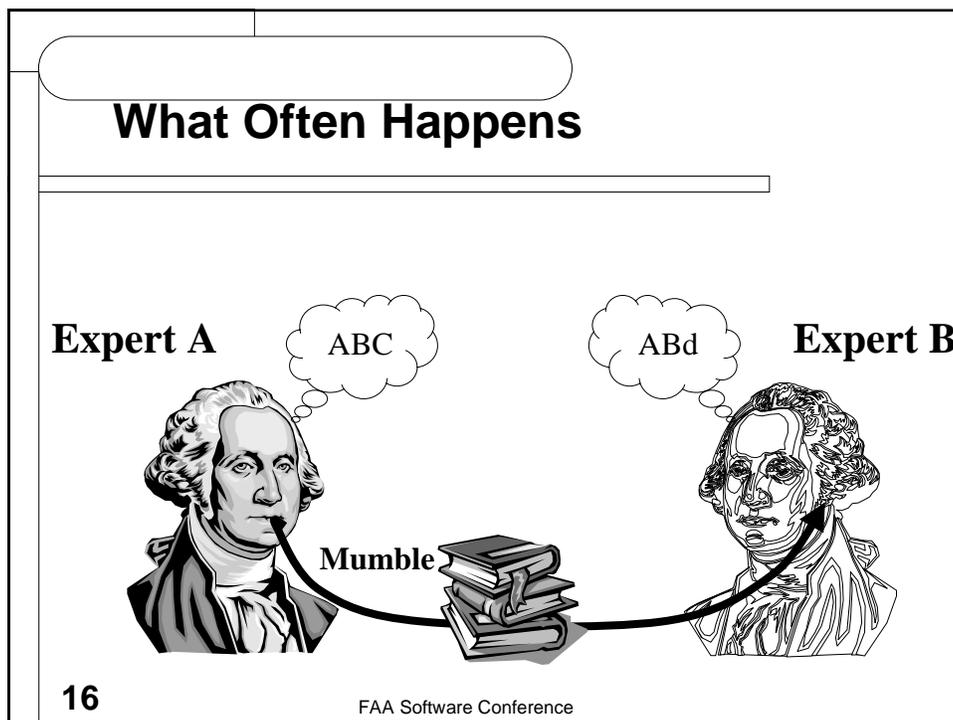
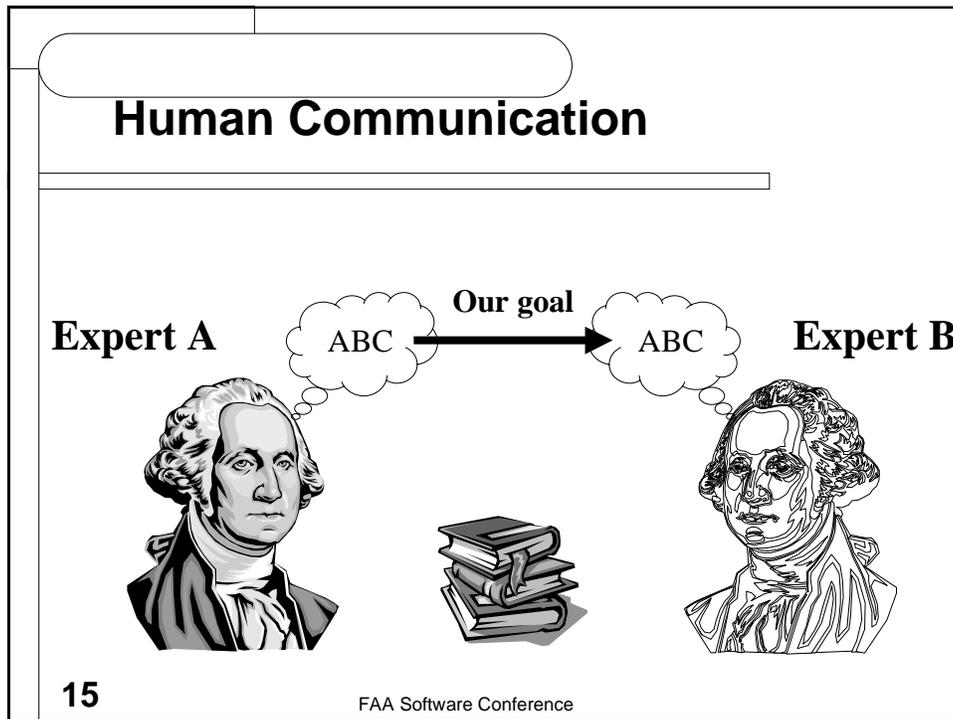
*Natural language is essential*

14

FAA Software Conference

# FAA National Software Conference, May 2002

## Erroneous Requirements



# FAA National Software Conference, May 2002

## Erroneous Requirements

### The Problem

- Miscommunication in software engineering is very common
- It is responsible for serious failures
- Natural language **cannot** be avoided, yet we don't know how to use it
- Engineering approach to natural language is essential

17

FAA Software Conference

### Cognitive Linguistics

- There is a rich, rigorous theory of linguistics that offers:
  - **Explanation** of much that we see in software engineering
  - **Structure** upon which to build approach to use of natural language
- Three major elements:
  - Cognitive categories
  - Cognitive economy
  - Hierarchical structure

18

FAA Software Conference

# FAA National Software Conference, May 2002

## Erroneous Requirements

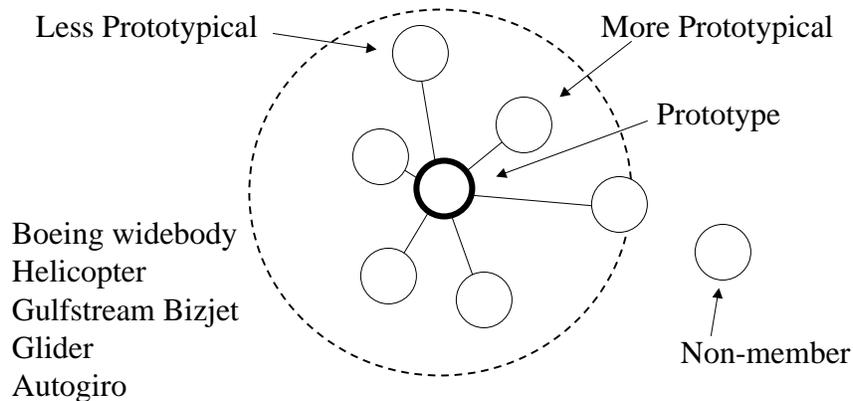
### Cognitive Categories

- Collections of entities judged to be the same:
  - Example: aircraft
- Mechanism by which humans store semantics
- Highly structured:
  - Central prototype
  - More and less prototypical members
  - Non members

19

FAA Software Conference

### Cognitive Category



20

FAA Software Conference

# FAA National Software Conference, May 2002

## Erroneous Requirements

### Cognitive Economy

- Human communication is low bandwidth
- Attributes ***assumed*** based on category name
- What is implied by the word “aircraft”?
- Problem:
  - Implied attributes not necessarily the same
  - If you know you don’t know, you ***ask***
  - If you don’t know you don’t know, you ***assume***

***This is a very serious source of mistakes***

21

FAA Software Conference

### Hierarchical Structure

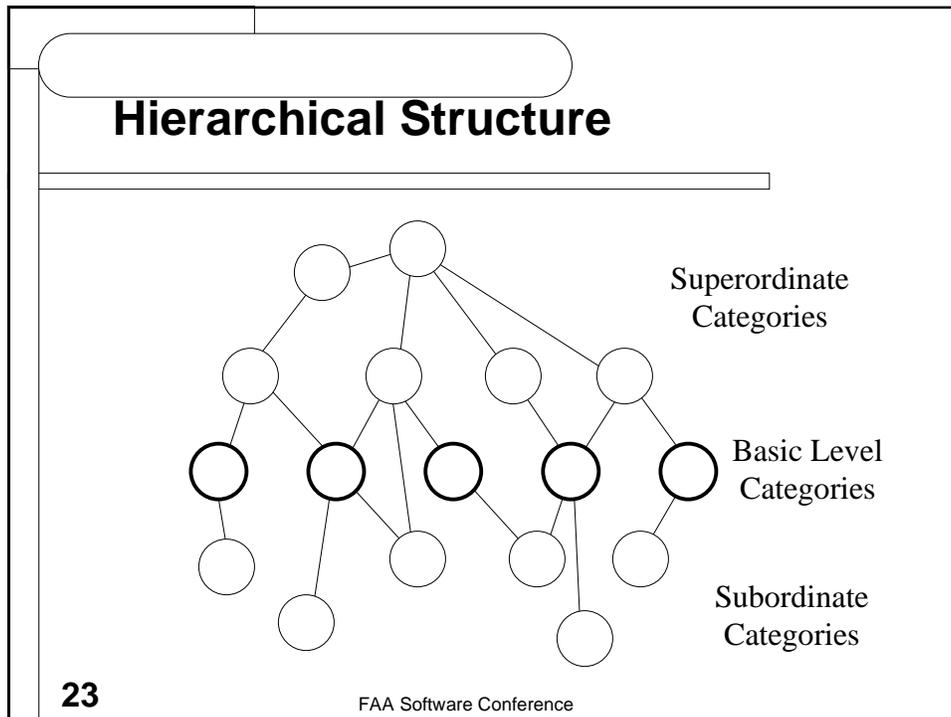
- Cognitive categories organized as a hierarchy
- Example:
  - Aircraft, commercial transports, widebodies
- Basic level in hierarchy has special significance
- Basic level is ***basic*** (fundamental) not ***lowest***
  - Retriever, ***dog***, mammal

22

FAA Software Conference

# FAA National Software Conference, May 2002

## Erroneous Requirements



### Basic Level Categories

- Basic Level: Levels at which members of a category have most in common with each other and least in common with members of other categories
- Category attributes are the basis

*Experts have been exposed to more attributes for categories in their domain*

24

FAA Software Conference

# FAA National Software Conference, May 2002

## Erroneous Requirements

### Basic Level Categories

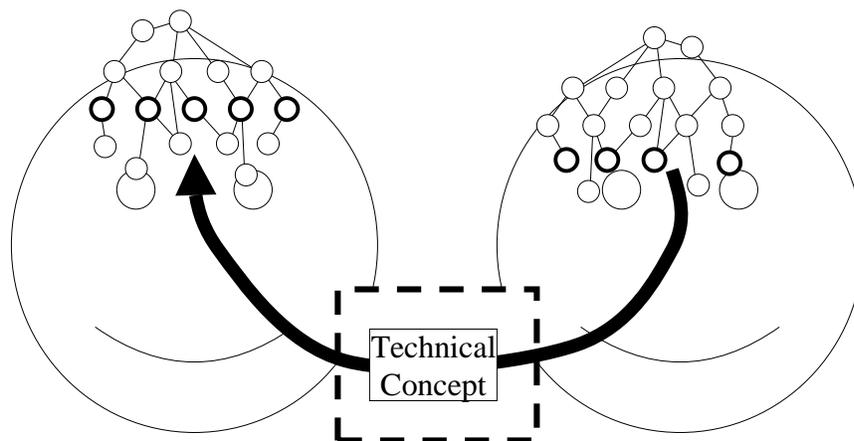
Experts tend to use lower levels as basic and use them in ways that basic level categories are used

This translates into proportionately more opportunities for miscommunication

25

FAA Software Conference

### Linguistic Theory Summary



26

FAA Software Conference

# FAA National Software Conference, May 2002

## Erroneous Requirements

### The Fundamental Problem

Human cognitive machinery is optimized, and communication across a domain boundary is not the common case.

But this is the very thing we have to do.....

*It is not part of human nature to get it right without serious and explicit intervention.*

27

FAA Software Conference

### Uses Of The Linguistic Theory

- Shows where problems come from and where to apply solutions
- Explains many reported observations
- Provides theoretical basis for several existing proposals, e.g., *smart ignoramus*
- Independent of any specific formal notation, applies to all

28

FAA Software Conference

# FAA National Software Conference, May 2002

## Erroneous Requirements

### Specification Material

- Computation
- *Real-world* meaning (domain information)
- Both are essential
- Both are *always* present during development
- Solution direction:

*Systematize the combination*

29

FAA Software Conference

### The Domain Map

- An *initial* approach to solution
- Integral part of any and every specification
- Systematic and complete repository of domain terminology—*make the implicit explicit*
- The only source of reference for domain semantics
- Heavily supported by software tools

30

FAA Software Conference

# FAA National Software Conference, May 2002

## Erroneous Requirements

### The Domain Map

- All domain terms defined
- Definitions use other definitions
- No cycles
- All definitions grounded in common terms
- Developed by iteration involving:
  - Software engineers
  - Domain experts

31

FAA Software Conference

### Preliminary Experiment

- Formal rewrite of informal maritime track control specification for ocean-going ships
- Operator enters waypoints, system steers ship
- 1600 word excerpt, 102 domain terms
- Domain map development:
  - Initial list of terms developed by software engineers
  - Reviewed by domain experts
  - Software engineers created domain map
  - Domain expert inspected and corrected

32

FAA Software Conference

# FAA National Software Conference, May 2002

## Erroneous Requirements

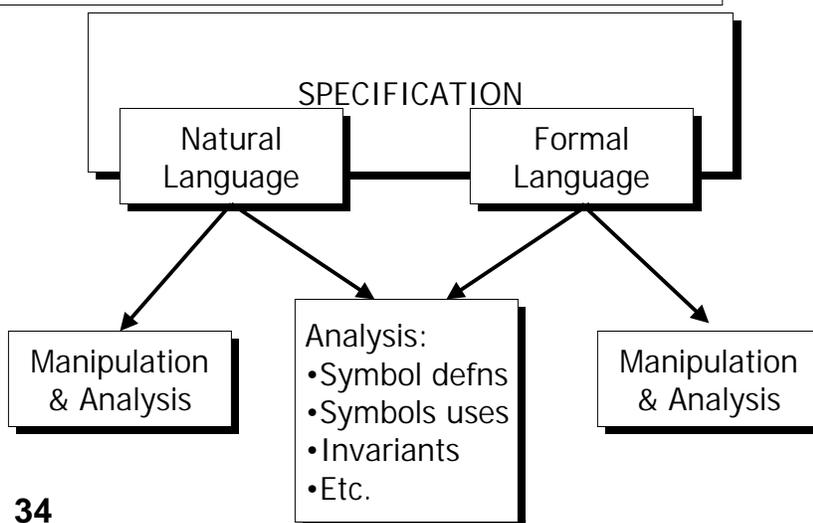
### Preliminary Results

- Initial informal source material:
  - Vague, incomplete, inconsistent, disorganized
- Review of initial list led to 55 corrections (54%)
- Example “bearing”:
  - Defined incorrectly
  - Used by 38 other definitions
  - Misused in definition of “heading” with many descendents
- Domain map max height 12, average 5

33

FAA Software Conference

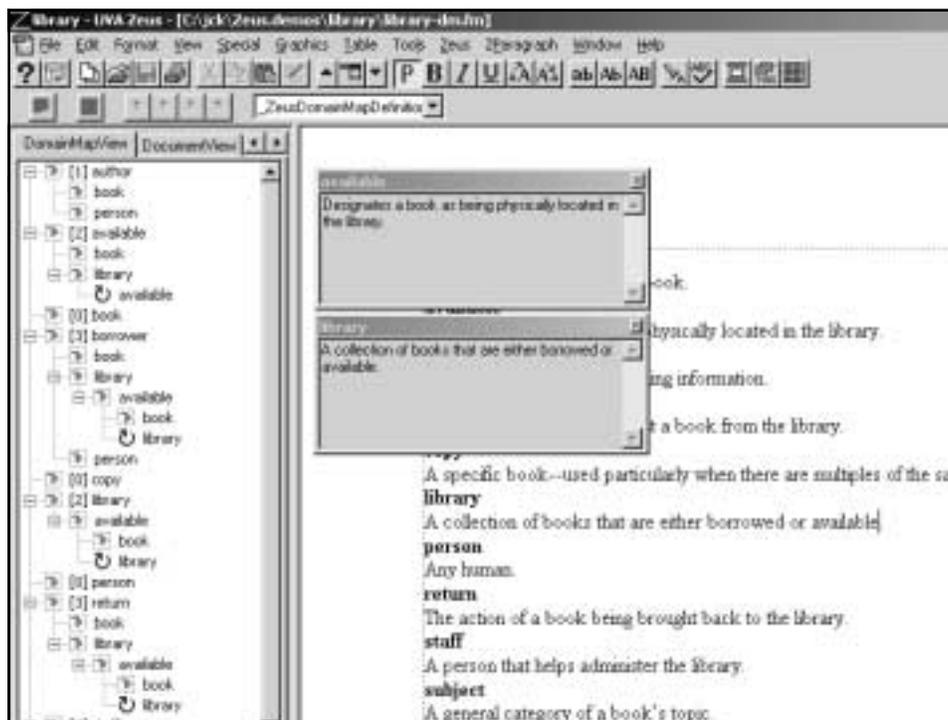
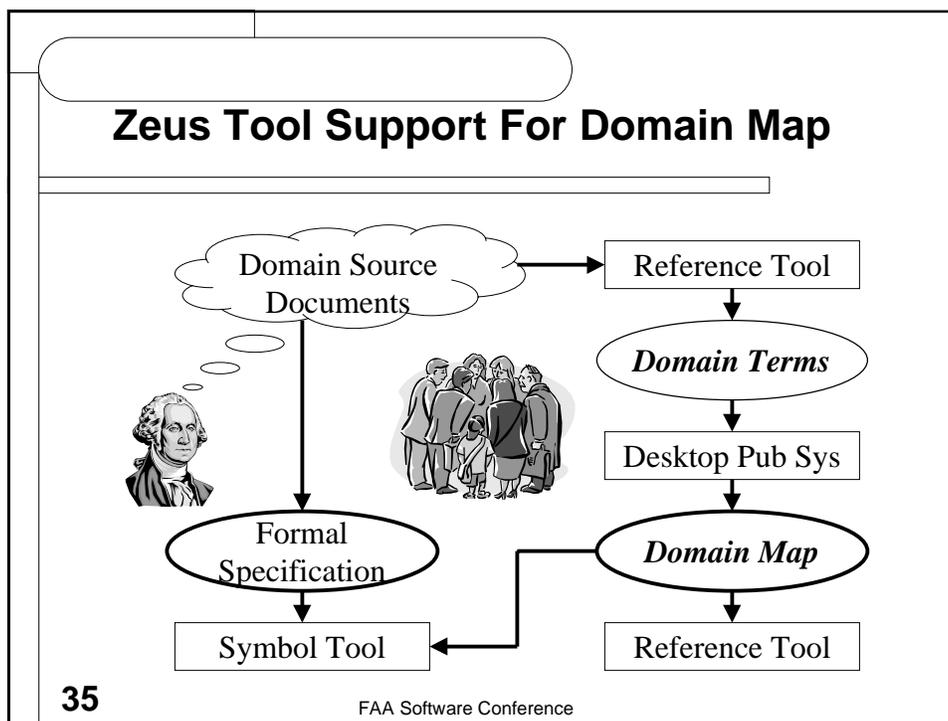
### Zeus Specification Tools



34

# FAA National Software Conference, May 2002

## Erroneous Requirements



# FAA National Software Conference, May 2002

## Erroneous Requirements

### Summary

- Natural language is **essential** in software development:
  - No other choice
  - Supplies the real-world meaning for software
  - Present now in all systems in an ad hoc way
- Natural language needs to be used **properly** in safety-critical aviation systems
- Formal linguistics provides **theoretical basis** for locating sources of problems and developing proper use
- Preliminary ideas based on **domain map** structure
- Preliminary data suggests positive direction

37

FAA Software Conference

### Contact

- E-mail addresses:  
[knight@cs.virginia.edu](mailto:knight@cs.virginia.edu)
- For more information see:  
<http://www.cs.virginia.edu/knight/>  
<http://www.cs.virginia.edu/zeus>

38

FAA Software Conference