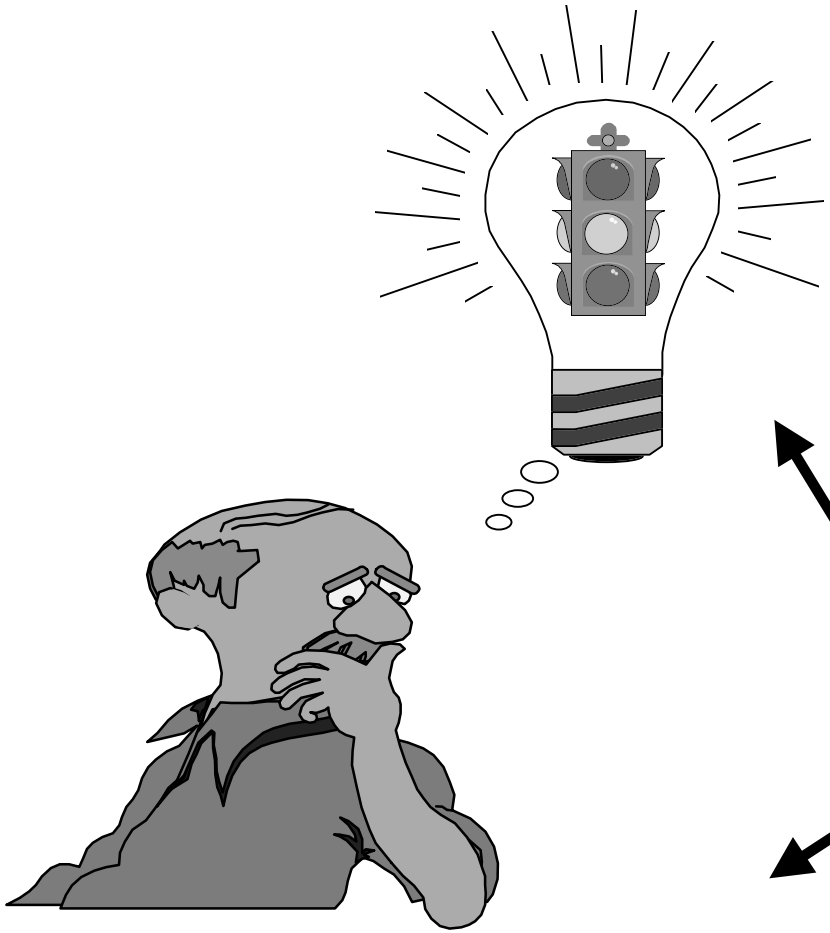
Formal Validation of System Specifications

Nancy Day
Department of Computer Science
University of British Columbia

Supervisor: Jeff Joyce, Hughes

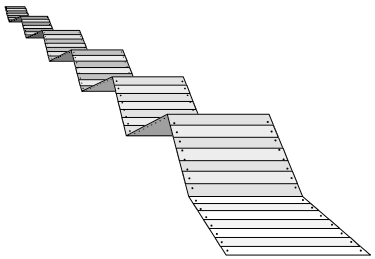
Thesis Committee:
Paul Gilmore, UBC
Alan Hu, UBC
Gail Murphy, UBC
Mark Greenstreet, UBC
Nancy Leveson, UW

Requirements Validation



?

Are we building the right system ?



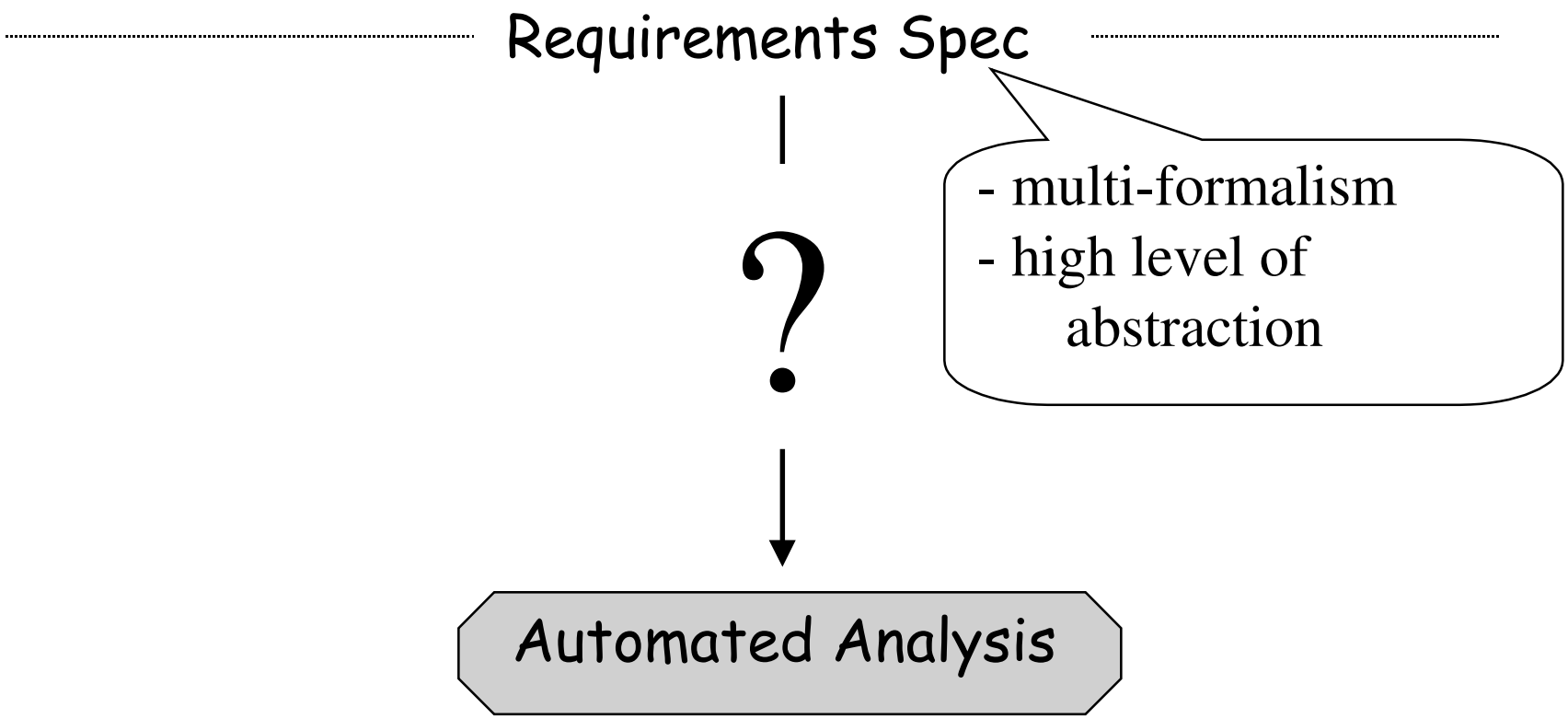
Requirements Specification

Analysis Techniques

- parsing
- typechecking
- simulation
- prototyping

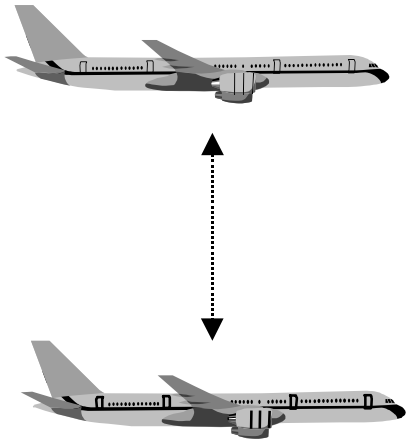
- completeness and consistency checking
- model checking: asking questions about the specification

Thesis: Formal Validation of System Specifications



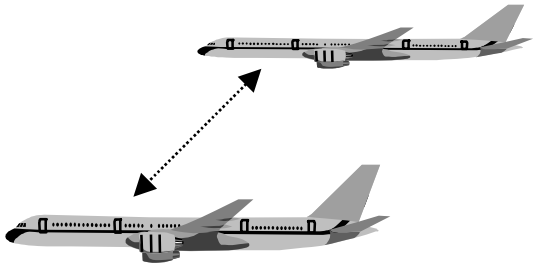
Separation Minima for NAT

rules for air traffic controllers



Vertical Separation

Lateral Separation



Longitudinal Separation

Samples from Spec

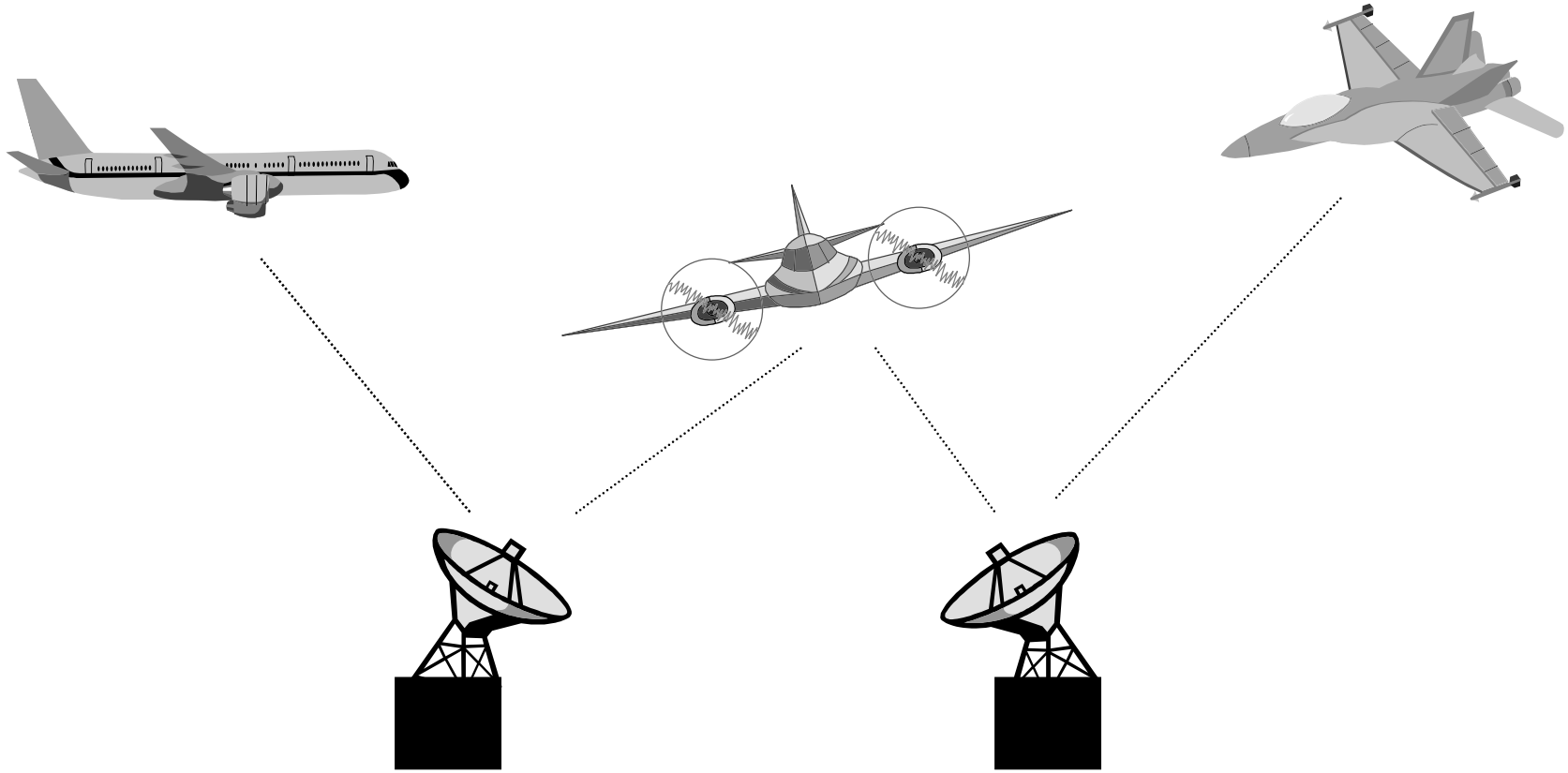
:flight;

FlightLevel: (flight -> num);

		1	2	3	4	Default
1	A.FlightLevel	__ <= 280	.	__>450	__>450	
2	B.FlightLevel	.	__ <= 280	__ > 450	__>450	
3	IsSupersonic A	.	.	__=T	.	
4	IsSupersonic B	.	.	.	__=T	
	VerticalSeparationRequired (A,B)	1000	1000	4000	4000	2000

forall (A:flight). NOT (IsLevel A AND InCruiseClimb A);

Analysis Results

- completeness analysis found:
  - missing assumptions “everyone knew about” (domain knowledge)
- consistency analysis found:
  - three places where the requirements are inconsistent
- symmetry analysis found:
  - assumptions about the uninterpreted terms

Aeronautical Telecommunications Network (ATN)