# Specifications

## Week 2 Class

## CE202 Software Engineering

Cunjin Luo

Special thanks to Michael Ernst & John Chapin
MIT UPOP Program

# Specifications tell you what to do (but not how to do it)

- **A perfect implementation is no good if it solves the wrong problem**

- **It is difficult to create a specification that is**
  - complete
  - consistent
  - precise
  - concise

# What do these cases have in common?

**Ariane 5 explosion 1996**

# Ariane 5 launch vehicle, 1996

- **Went off course during launch**
  - Ariane 4 guidance software reused in Ariane 5
  - Ariane 5 accelerated much faster
  - velocity variable overflowed, computer crashed

- **"The failure of the Ariane 501 was caused by the complete loss of guidance and attitude information... due to specification and design errors in the software."**

  ESA Inquiry Board

# Berlin Bundestag 1992

# Bundestag Sound System, 1992

- **No sound from speakers in new building**
  - system requirement: no feedback
  - new all-glass room

- **"This glass does not absorb the sound. The computers, detecting feedback, turn down the volume. A steady state is only achieved when the microphones are turned off."**

  Dr. Debora Weber-Wulff

# Mars Polar Lander Mission Overview

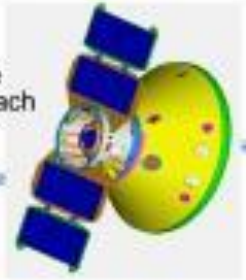
## Cruise

Thruster attitude control

Four trajectory-correction maneuvers, site-adjustment maneuver September 1, 1999, contingency 5th TCM at entry -24 hours

Eleven month cruise

Near-simultaneous tracking with Mars Climate Orbiter or Mars Global Surveyor during approach



## Entry, Descent, & Landing

Arrival: December 3, 1999

Jettison cruise stage; microprobes separate from cruise stage

Hypersonic entry

Parachute descent; propulsive landing

Descent imaging of landing site

## Launch

Delta II 7425

Launched January 3, 1999

Launch mass: 574 kilograms

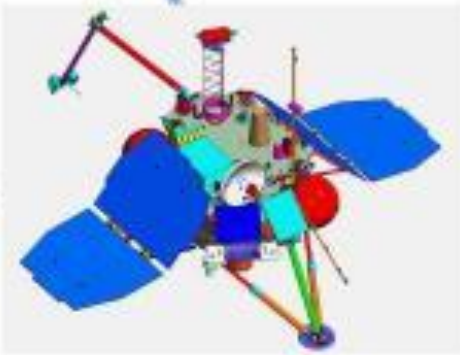
## Landed Operations

Lands in Martian spring at 76 degrees South latitude, 195 degrees West longitude (76° S, 195° W)

90-day landed mission

Meteorology, imaging, soil analysis, trenching

Data relay via Mars Climate Orbiter, Mars Global Surveyor, or direct-to-Earth high-gain antenna



# Mars Polar Lander, 1999

- **Crashed while landing on Mars**
  - sensor transient when legs deployed
  - software thought vehicle had landed
  - engine shut down during descent

- **"There was no software requirement to clear spurious signals prior to using the sensor information to determine that landing had occurred."**

  Mars program independent assessment team

# Specifications matter

- **A specification:**
  - connects customer and engineer
  - ensures parts of implementation work together
  - defines correctness of implementation
- **Therefore everyone must understand specs**
  - Designers, implementers, testers, managers, marketing, technical support, ... users!
- **Good specifications are essential**

# Specification Example

# Desktop telephone

**Handset (speaker and microphone)**

**Keypad**

- `talk`
- `redial`
- `ansmachine`
- `end`

**24-character display**

**Answering machine**

**Phone jack**

# Requirements

**Display indicates current functionality**

- caller ID
- number being called
- "Answering machine“
- "Ready"

**Answering machine picks up after 2 rings**

**There are other aspects of system behavior**

# Definitions

**Lineidle: phone is on-hook ("hung up")**

- sent from phone to phoneline

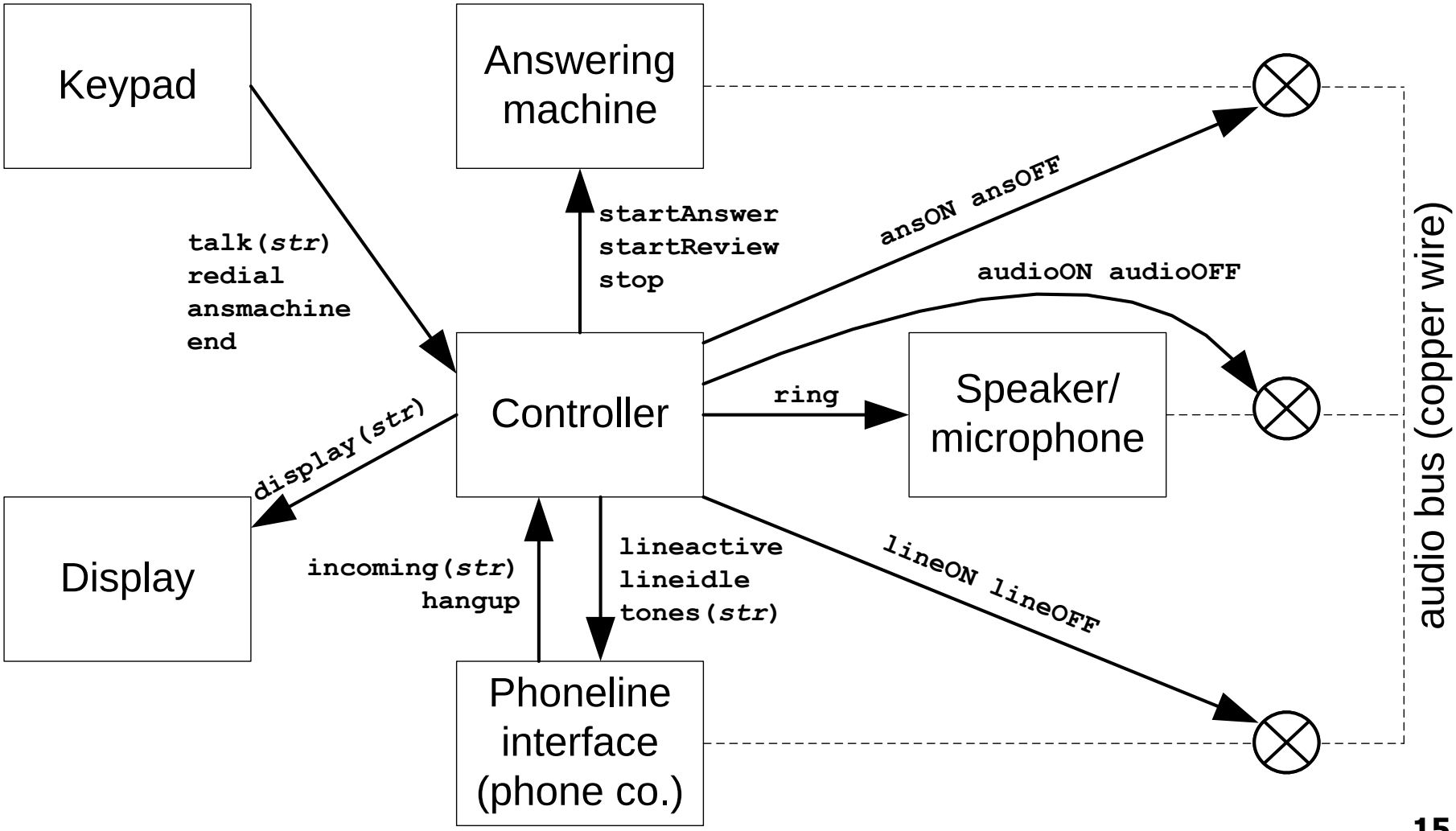
**Lineactive: phone is off-hook ("picked up")**

- sent from phone to phoneline

**Ring signal: causes phone to ring once**

- sent from phoneline to phone

# System architecture



Thank you

**cunjin.luo@essex.ac.uk**

Special thanks to Michael Ernst & John Chapin
MIT UPOP Program