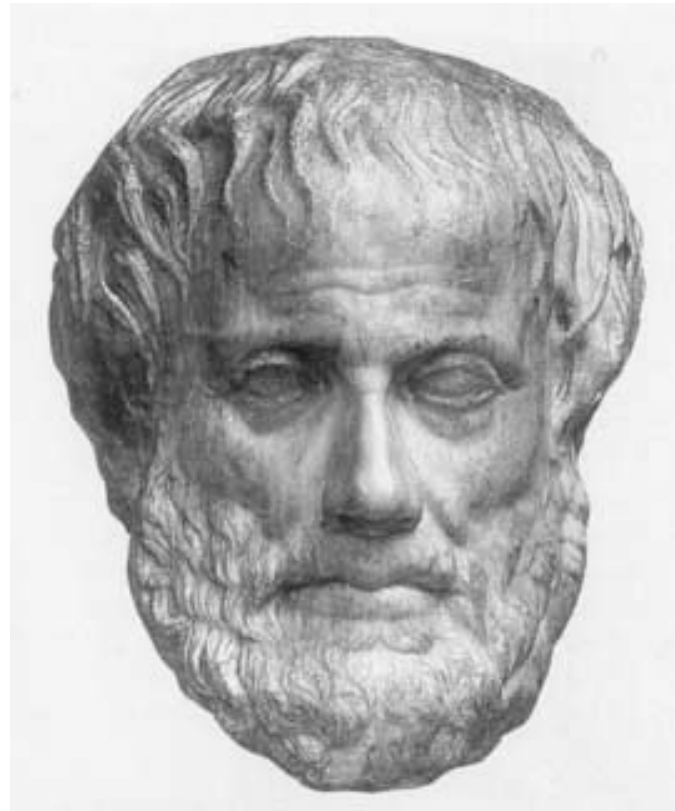


# WHAT ARE FORMAL METHODS?

CSSE 373, FORMAL METHODS  
CURT CLIFTON

# WHAT ARE FORMAL METHODS? (1/2)

- FORMAL METHODS ARE METHODS THAT USE FORMAL LANGUAGE.
- FORMAL METHODS USE FORMAL LOGIC.



# WHAT ARE FORMAL METHODS? (2/2)

- FORMAL METHODS USE FORMAL SPECIFICATION LANGUAGES. THAT IS, THEY USE LANGUAGES THAT HAVE A MATHEMATICALLY-DEFINED STATIC SEMANTICS.
- FORMAL METHODS EMPLOY ANALYSIS THAT IS MATHEMATICALLY SOUND.

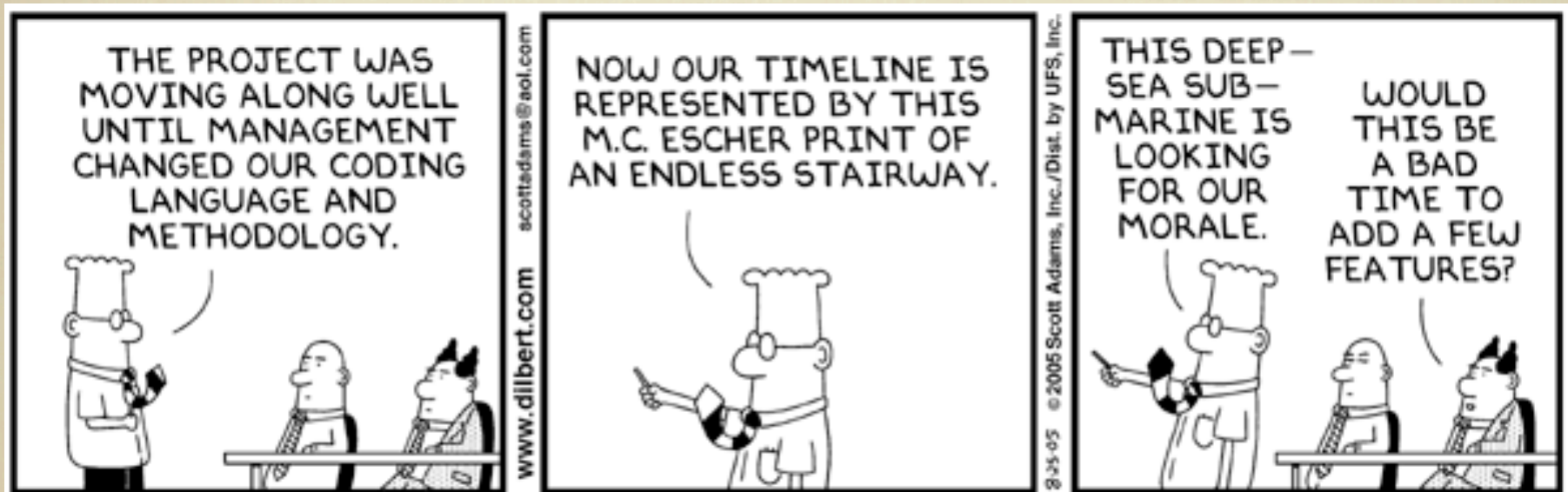
# WHEN ARE FORMAL METHODS MOST USEFUL?

- WHEN YOU HAVE TO GET IT RIGHT
- WHEN YOU CANNOT TEST IT ADEQUATELY
- EXAMPLES:
  - SAFETY-CRITICAL APPLICATIONS
    - AVIATION
    - MEDICAL EQUIPMENT
  - ECONOMICALLY-CRITICAL APPLICATIONS
    - STOCK EXCHANGE
    - ATMs

# JACKSON ON DESIGN

- **“SUCH MASSIVE FAILURES OCCUR BECAUSE CRUCIAL DESIGN FLAWS ARE DISCOVERED TOO LATE.”**
- **“NO AMOUNT OF REFACTORING, BAR STARTING FROM SCRATCH, CAN RESCUE A SYSTEM BUILT ON FLAWED CONCEPTS.”**
- **“WHEN GOOD ABSTRACTIONS ARE MISSING FROM THE DESIGN, OR ERODE AS THE SYSTEM EVOLVES, THE RESULTING PROGRAM GROWS BARNACLES OF COMPLEXITY.”**

# CARTOON OF THE DAY



© Scott Adams, Inc./Dist. by UFS, Inc.

# POSSIBLE WAYS TO GET THE ABSTRACTION RIGHT

- EVOLVE THE DESIGN
- FORMAL SPECIFICATION AND THEOREM PROVING
- MODEL CHECKING

# BENEFITS OF MODEL CHECKING

- NO TEST CASES
- AUTOMATICALLY DISCOVERS COUNTEREXAMPLES
- “A KIND OF EXPLORATION THEREFORE BECOMES POSSIBLE THAT COMBINES THE INCREMENTALITY AND IMMEDIACY OF EXTREME PROGRAMMING WITH THE DEPTH AND CLARITY OF FORMAL SPECIFICATION”

# FALLACIES ABOUT SOFTWARE – 1

- SOFTWARE IS TOO COMPLICATED TO GET COMPLETELY RIGHT.
- THE ONLY WAY TO KNOW WHETHER SOFTWARE WORKS IS TO TEST IT.
- USERS DON'T KNOW WHAT THEY WANT—ONLY TRIAL AND ERROR WILL LEAD TO THE RIGHT SOLUTION.

# FALLACIES ABOUT SOFTWARE – 2

- **EVERYTHING HAS BUGS IN IT, SO THERE IS NO POINT IN MAKING ANYTHING BETTER.**
- **IT COSTS TOO MUCH TO MAKE HIGHLY-RELIABLE SOFTWARE.**
- **COMPUTING IS STILL TOO IMMATURE TO BE RELIABLE.**

# INSTALLING ALLOY

- **ON CAMPUS:**

- <http://www.rose-hulman.edu/class/csse/binaries/Alloy>

- **OFF CAMPUS:**

- <http://alloy.mit.edu/alloy4>