Introduction to CS655
System Modeling and Analysis

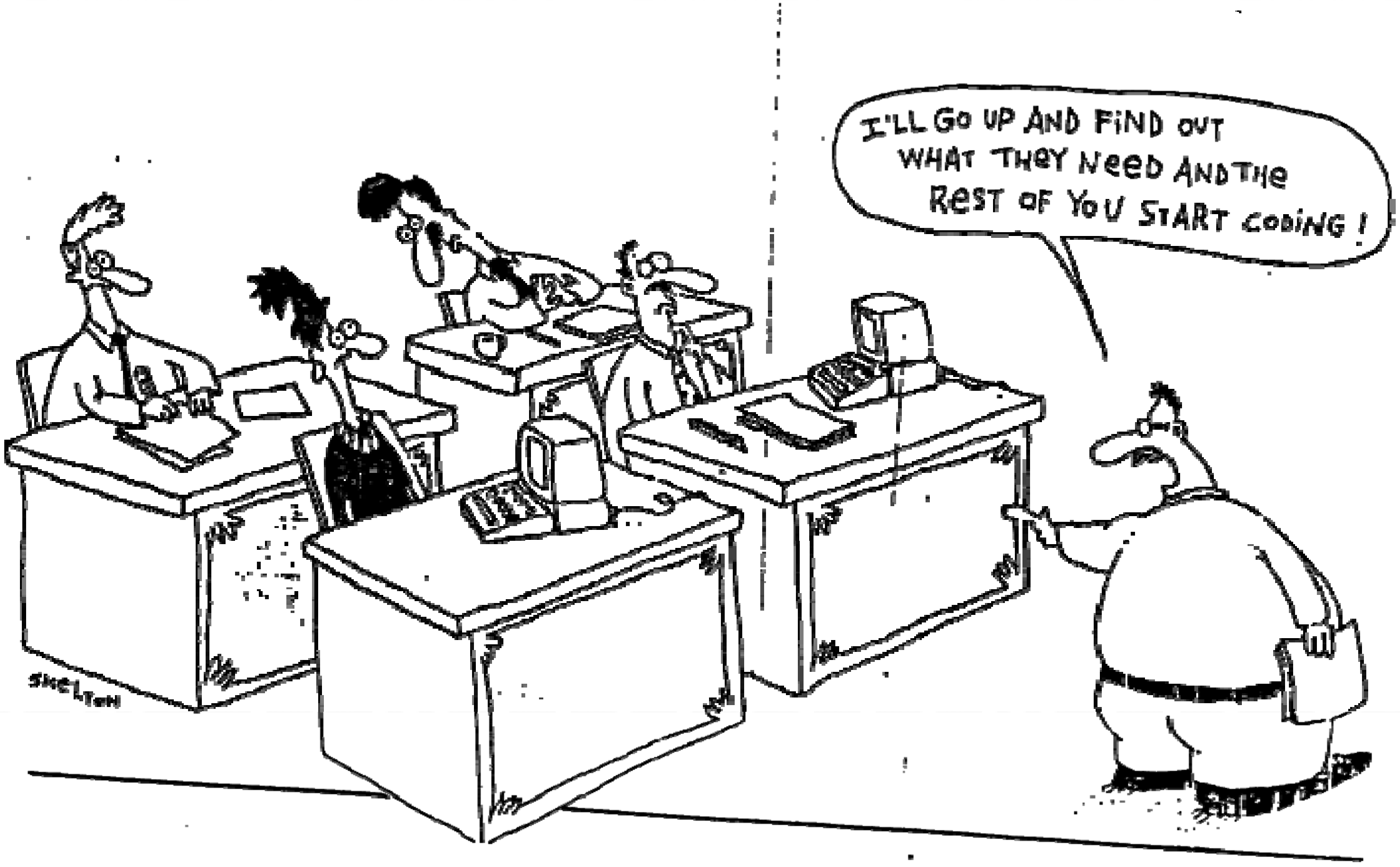
Moonzoo Kim

Provable Software Laboratory

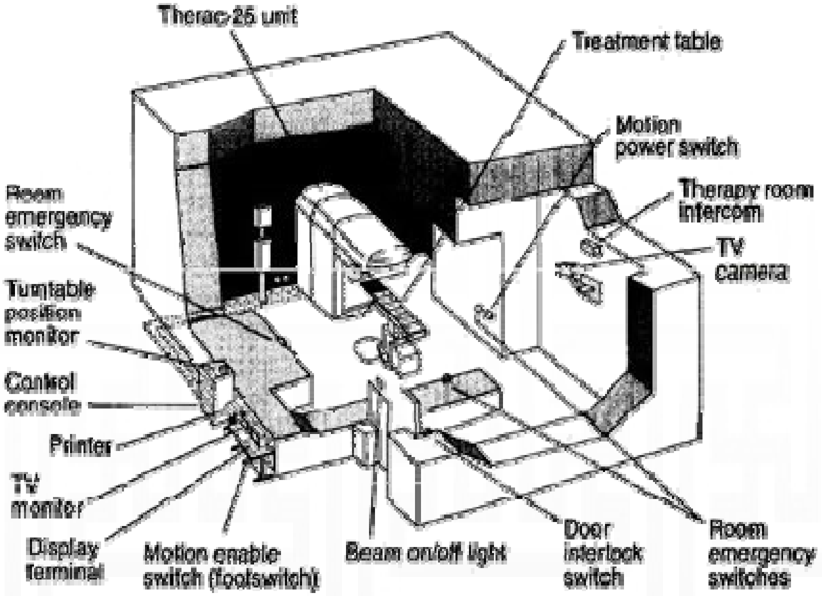
CS Dept. KAIST

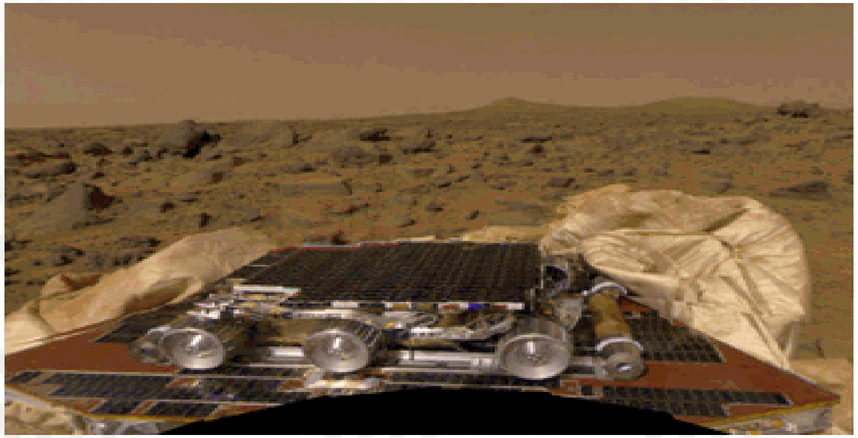
Main Theme of the Class

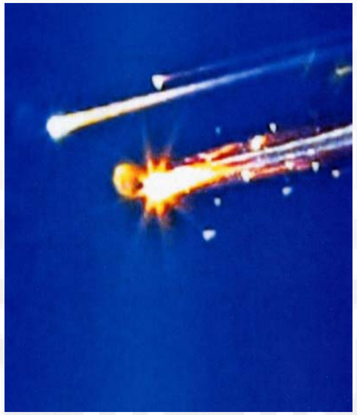
- **To improve the understanding of the target system through formal modeling and analysis**
  - In many cases, we do NOT know what we are building exactly !!!


I'LL GO UP AND FIND OUT WHAT THEY NEED AND THE REST OF YOU START CODING!
SKELTON

Tragic Accidents due to SW Bugs

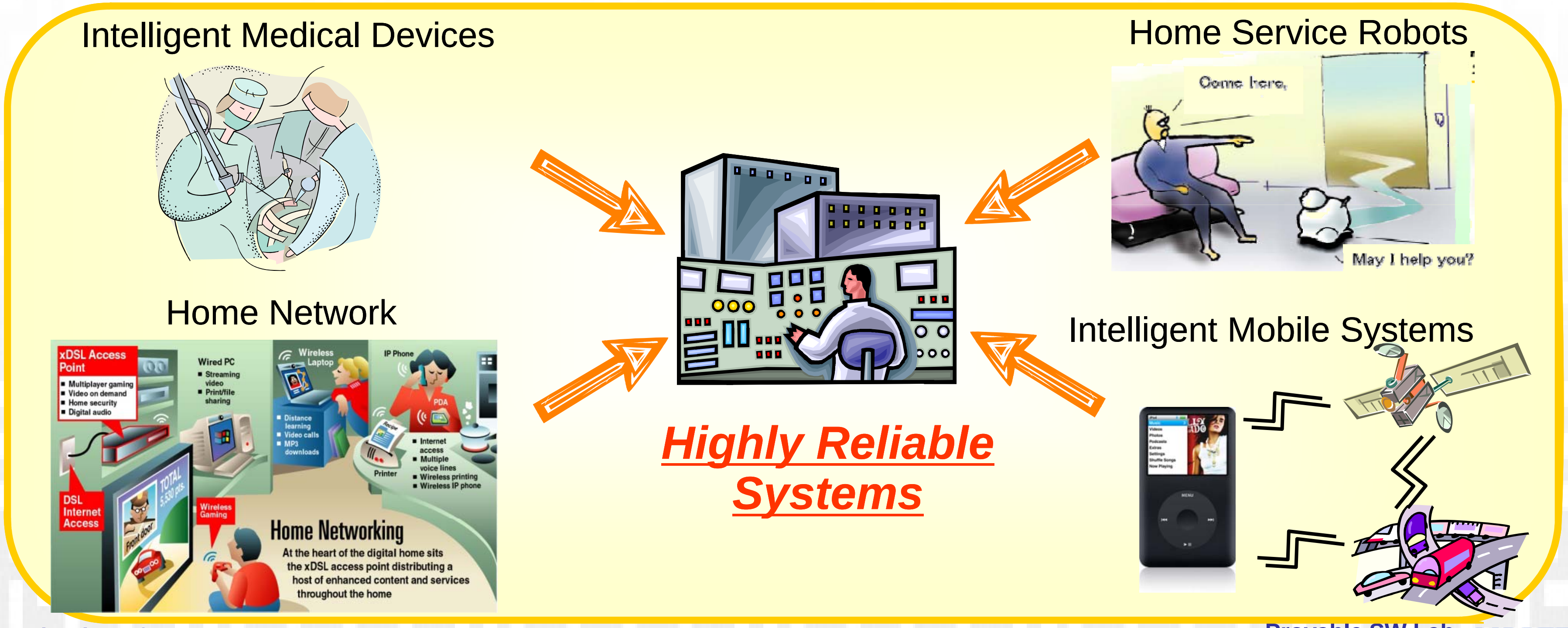






Main Target Systems

- **Embedded systems where highly reliable SW technology is a key to the success**
  - The portion of SW in commercial embedded devices increases continuously
  - More than 50% of development time is spent on SW testing and debugging



Intelligent Medical Devices

Home Service Robots

Home Network

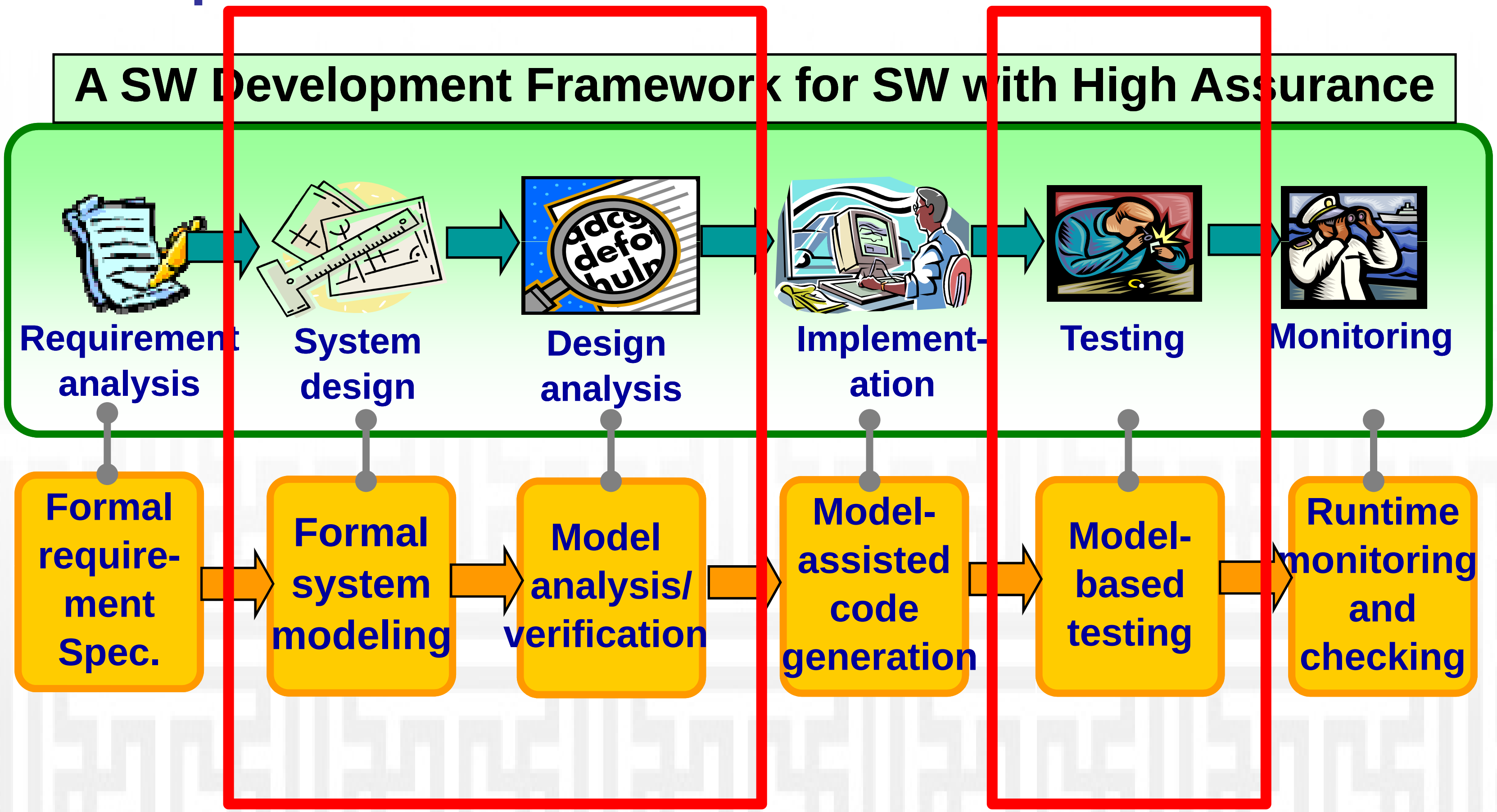
Intelligent Mobile Systems

Highly Reliable Systems

At the heart of the digital home sits the xDSL access point distributing a host of enhanced content and services throughout the home

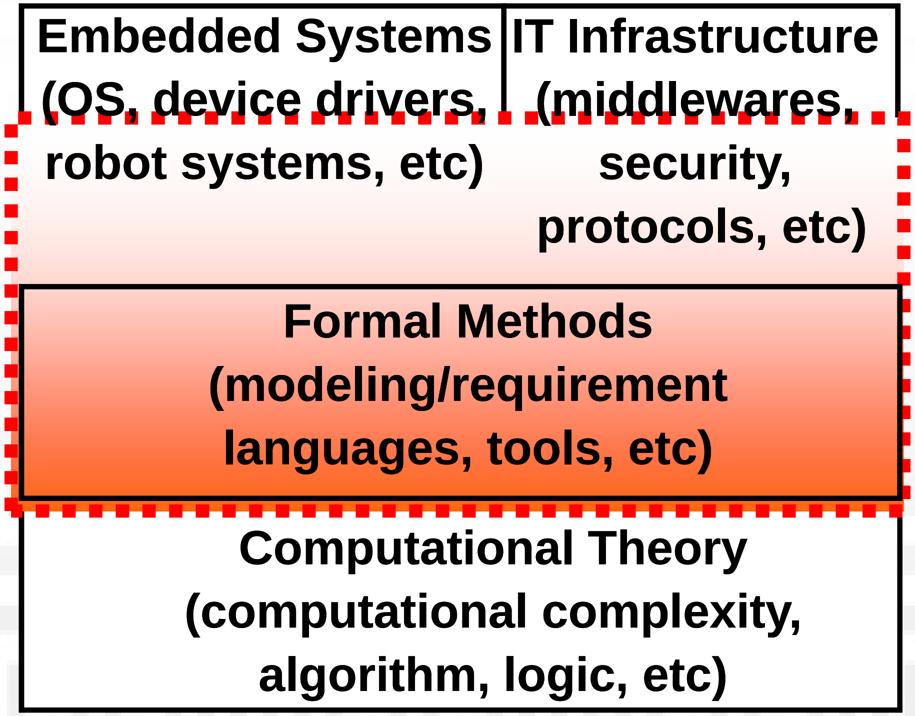
Software Development Cycle

- A practical end-to-end formal framework for software development


A SW Development Framework for SW with High Assurance
Requirement analysis
System design
Design analysis
Implement-ation
Testing
Monitoring
Formal require-ment Spec.
Formal system modeling
Model analysis/ verification
Model-assisted code generation
Model-based testing
Runtime monitoring and checking

Main Research Approach

- Practical formal methods that can be applied to software intensive systems to enhance reliability

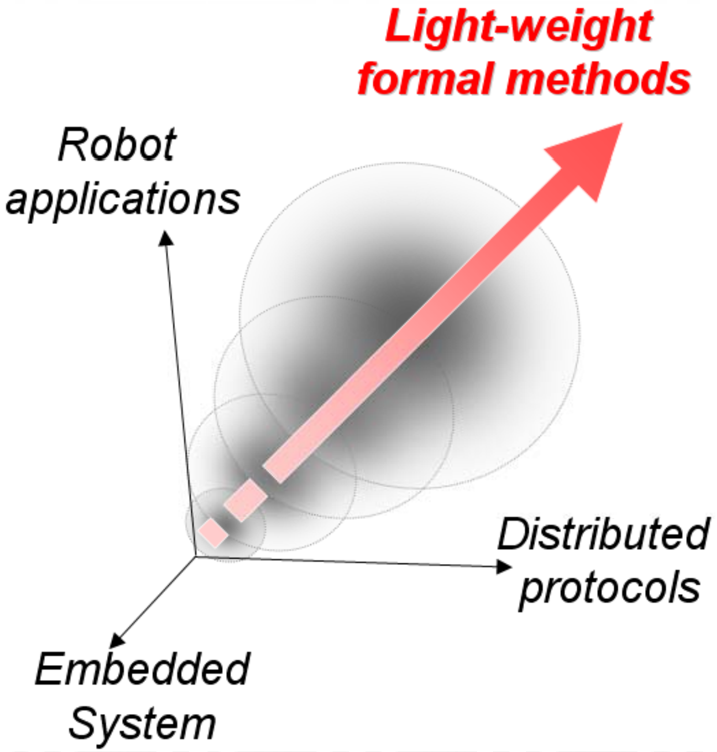


Embedded Systems (OS, device drivers, robot systems, etc)

IT Infrastructure (middlewares, security, protocols, etc)

Formal Methods (modeling/requirement languages, tools, etc)

Computational Theory (computational complexity, algorithm, logic, etc)

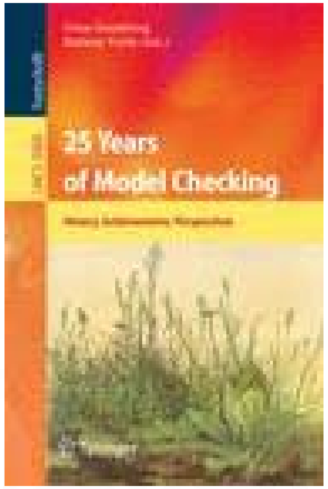


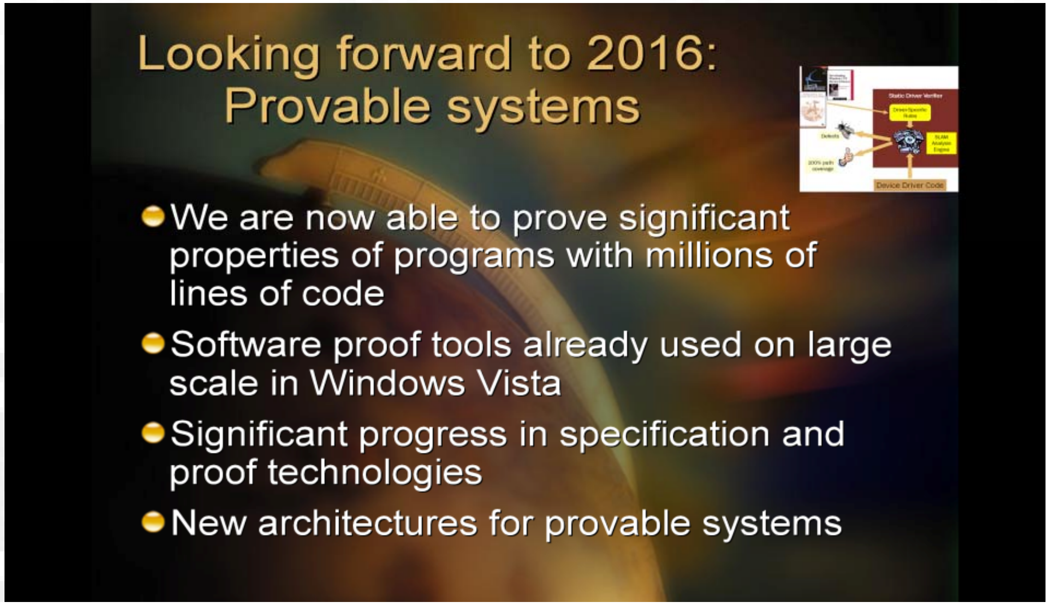
Research Trends toward Quality Systems

- **Academic research on developing embedded systems has reached stable stage**
  - just adding a new function to a target system is not considered as an academic contribution anymore
- **Research focus has moved on to the quality of the systems from the mere functionalities of the systems**
  - Energy efficient design, ez-maintenance, dynamic configuration, etc
- **Software reliability is one of the highly pursued qualities**
  - NSDI 2007 Best paper
    - "Life, Death, and the Critical Transition: Finding Liveness Bugs in Systems Code" @ U.C. San Diego
      - Heuristic application of model checking to detect liveness bug
  - OSDI 2004 Best paper
    - "Using Model Checking to Find Serious File System Errors" @ Stanford
      - Application of software model checking to find FS bugs

Formal Modeling and Analysis as a Foundational and Promising CS Research

- **2007 ACM Turing Awardees**
  - Prof. Edmund Clarke
  - Dr. Joseph Sipfakis
  - Prof. E. Allen Emerson
- **For the contribution of migrating from pure research to industrial reality**
- **One of the four Microsoft Research main areas**



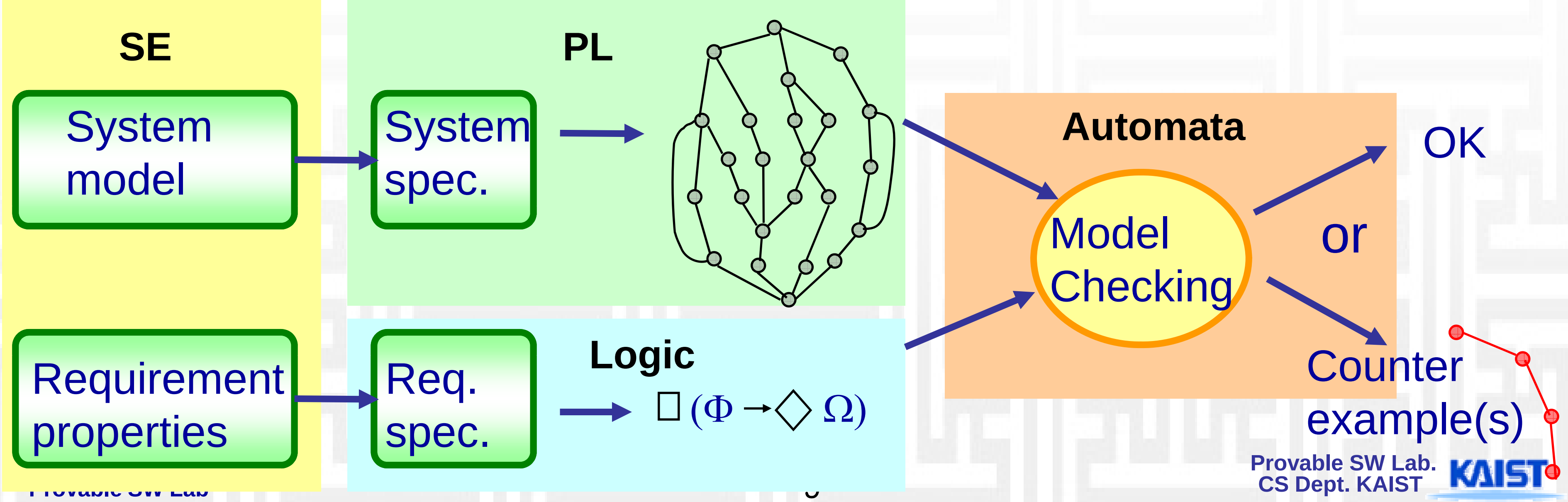


Looking forward to 2016:
Provable systems

- We are now able to prove significant properties of programs with millions of lines of code
- Software proof tools already used on large scale in Windows Vista
- Significant progress in specification and proof technologies
- New architectures for provable systems

Model Checking Basics (cont.)

- Undergraduate foundational CS classes contribute this area
  - CS204 Discrete mathematics
  - CS300 Algorithm
  - CS320 Programming language
  - CS322 Automata and formal language
  - CS350 Introduction to software engineering
  - CS402 Introduction to computational logic



SE

System model

Requirement properties

PL

System spec.

Logic

Req. spec.

$\square(\Phi \rightarrow \Diamond \Omega)$

Automata

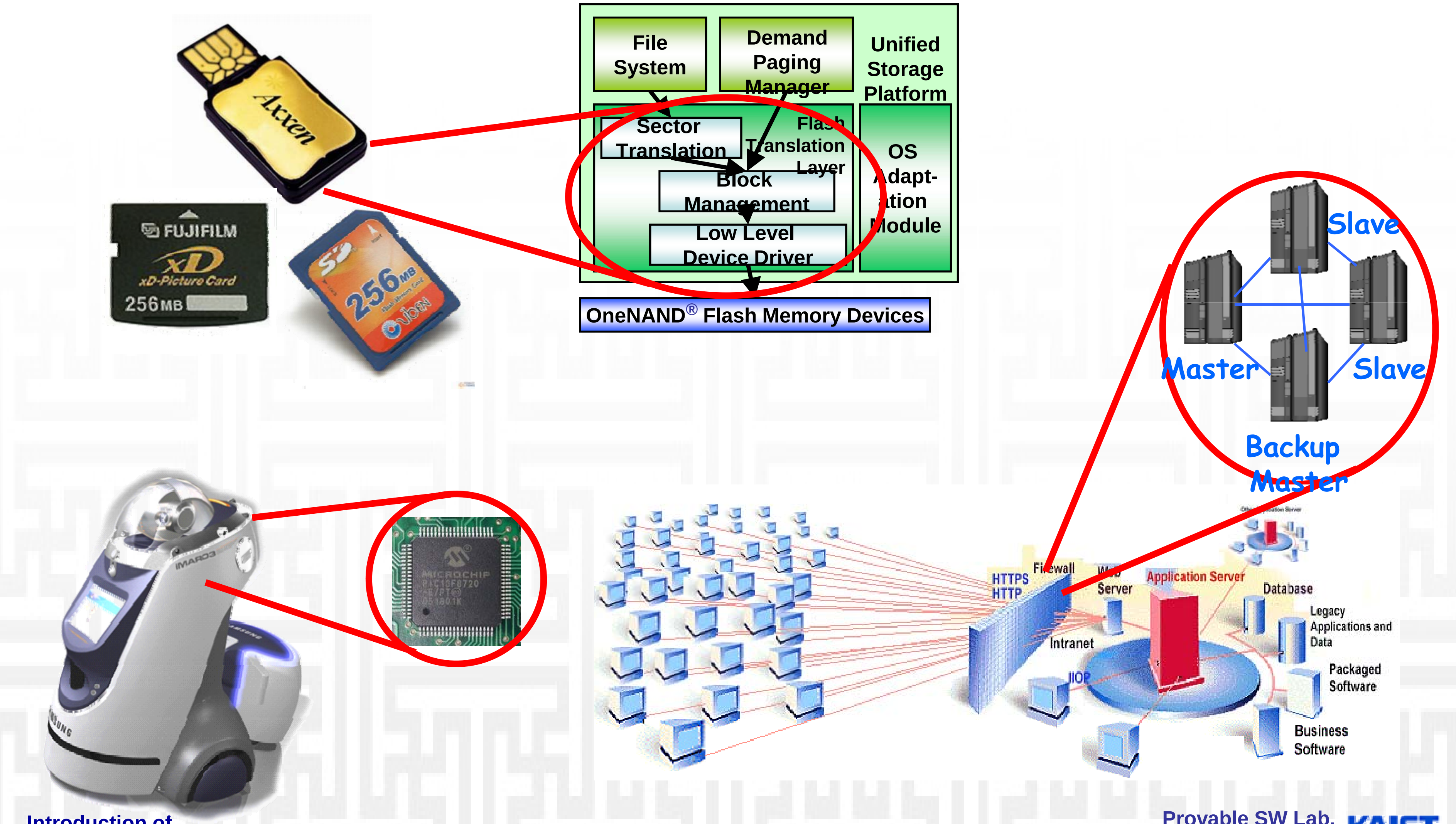
Model Checking

OK

or

Counter example(s)

Samples of Korean Industrial Application of Formal Modeling and Analysis



File System

Demand Paging Manager

Unified Storage Platform

Sector Translation

Flash Translation Layer

Block Management

Low Level Device Driver

OS Adapt-ation Module

OneNAND® Flash Memory Devices