CS 228 : Logic in Computer Science

Krishna. S

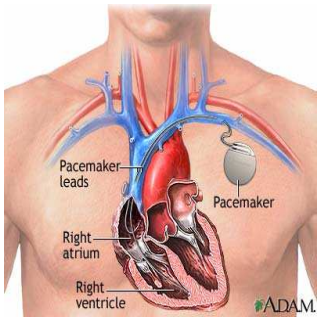
So Far

- Dwelt on classical logics : propositional logic, FO and MSO on finite words
- Words : good abstraction for capturing properties to be checked on systems built
- Moving on to Temporal logics

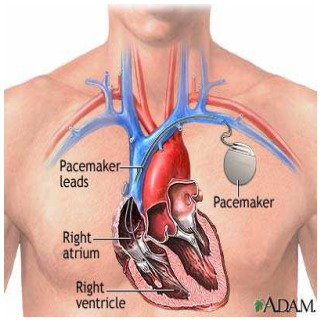
Safety Critical Systems

Safety Critical Systems

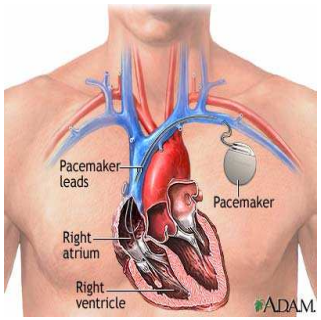
Safety Critical Systems

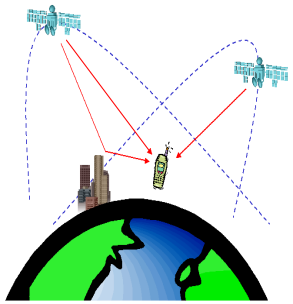


Safety Critical Systems

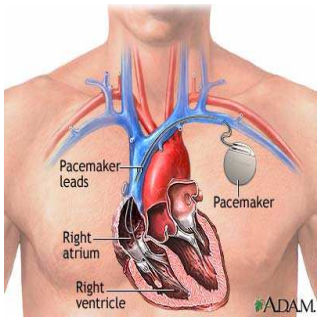


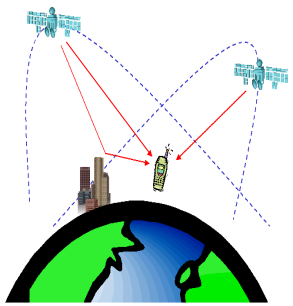
Safety Critical Systems



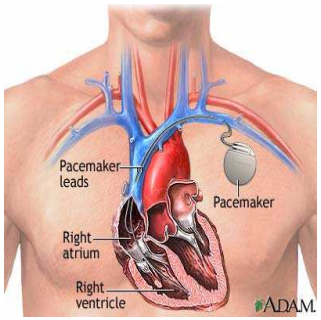


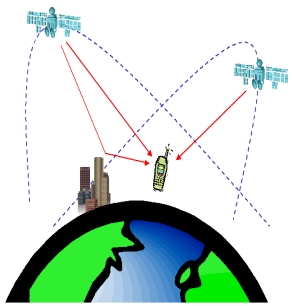
Safety Critical Systems



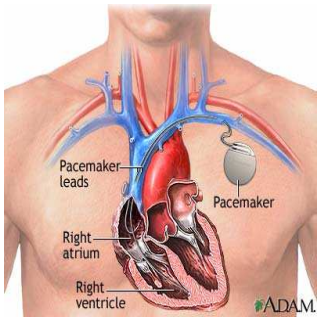


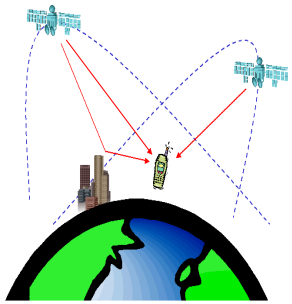
Safety Critical Systems



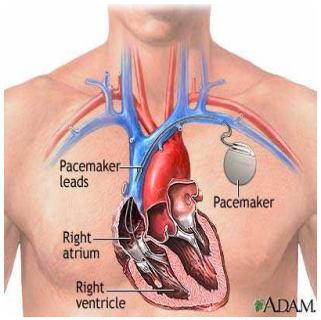


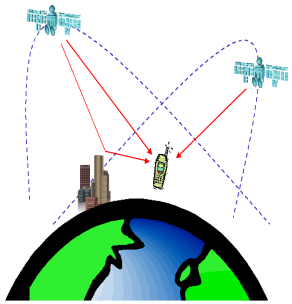
Safety Critical Systems





Safety Critical Systems

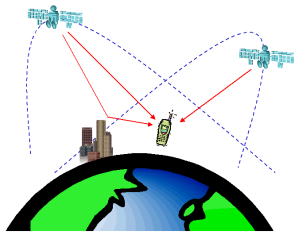


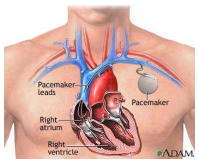


The role of Automata and Logics

- Systems modeled as certain kinds of automata
- Safety critical properties written in some logic
- Check if the property is satisfied by all runs of the system

Verification through Model Checking

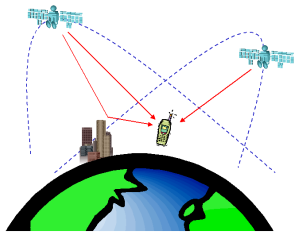




System → satisfy? → specification

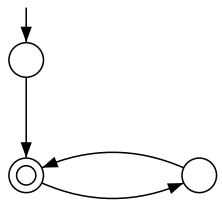
good/bad properties

Verification through Model Checking



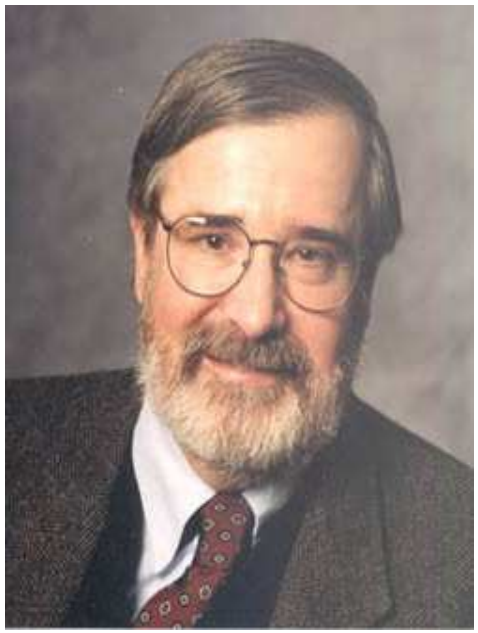
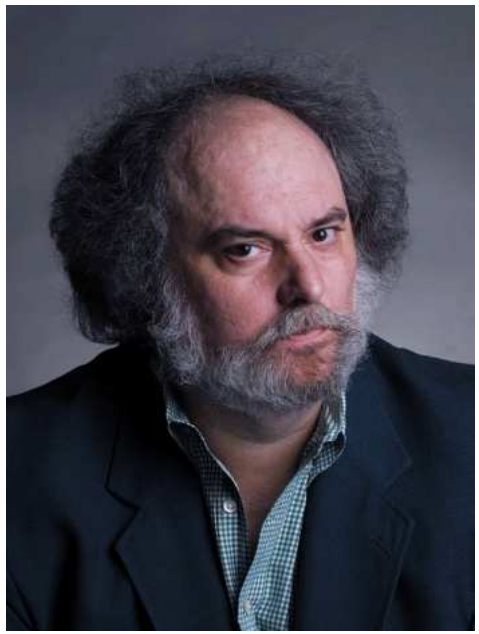
System — satisfy? → specification

System Model — model-checking, $\models$? → Spec Model



ϕ

Model Checking : Pioneers


- Year 2008 : ACM confers the Turing Award to the pioneers of Model Checking: Ed Clarke, Allen Emerson, and Joseph Sifakis

Properties of the Infinite

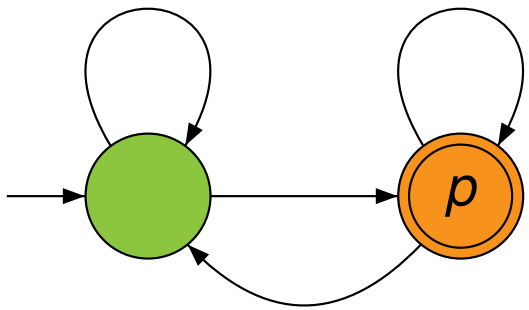
- Modelling Reactive Systems
  - Computer Program that continously interacts with the environment
  - Correctness cannot be specified by correct output
- Infinitely often *a* (Liveness)
- Never *b* (Safety)
- Eventually forever *a* (Persistence)

A Simple Example

Property : p occurs infinitely often

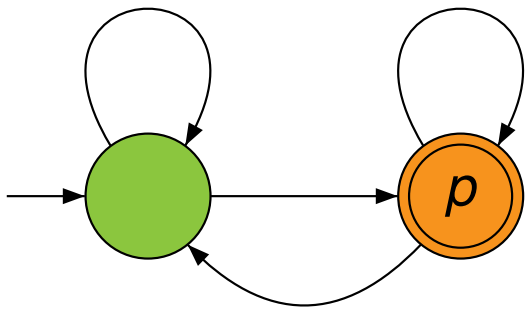
A Simple Example

Property : p occurs infinitely often



A Simple Example

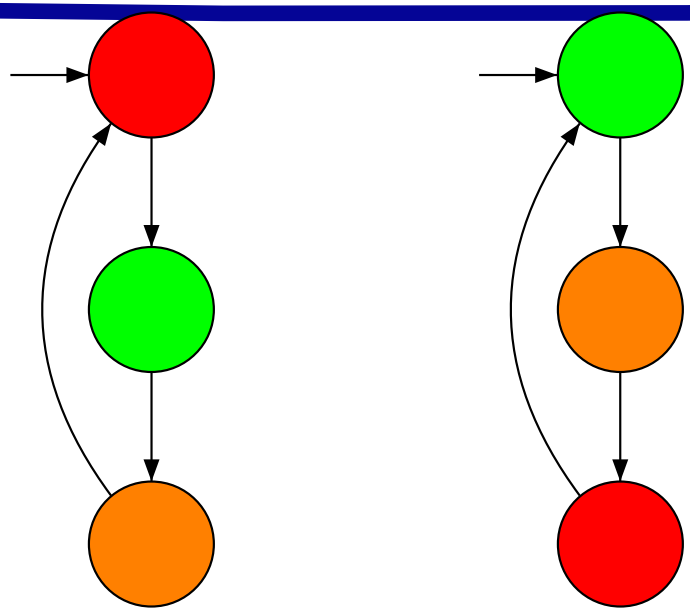
Property : p occurs infinitely often



$\Box\Diamond p$

$\forall x\, \exists y\, (x < y \wedge p(y))$

Two Traffic Lights



1. The traffic lights are never green simultaneously
   $\forall x(\neg(green_1(x) \wedge green_2(x)))$ or $\Box(\neg(green_1 \wedge green_2))$
2. The first traffic light is infinitely often green
   $\forall x \exists y(x < y \wedge green_1(y))$ or $\Box\Diamond green_1$
3. Between every two occurrences of traffic light 1 becoming red, traffic light 2 becomes red once.

Temporal Logics

- It will rain tomorrow and it does not rain today

Temporal Logics

- It will rain tomorrow and it does not rain today
- Linear Temporal Logic (LTL) for specification of programs (Amir Pnueli, 1977)
  - Turing Award 1996(Amir Pnueli)
  - For seminal work introducing temporal logic into computing science and for outstanding contributions to program and system verification.

Temporal Logics

- It will rain tomorrow and it does not rain today
- Linear Temporal Logic (LTL) for specification of programs (Amir Pnueli, 1977)
  - Turing Award 1996(Amir Pnueli)
  - For seminal work introducing temporal logic into computing science and for outstanding contributions to program and system verification.
- Temporal Logic CTL for program correctness; introduction of model-checking (Emerson and Clarke; Sifakis, 1982)
  - Turing Award 2008 (Clarke, Emerson and Sifakis).
  - For their role in developing model-checking into a highly effective verification technology that is widely adopted in the hardware and software industries.
  - See *http://www-verimag.imag.fr/ sifakis/TuringAwardPaper-Apr14.pdf*.