# System Validation

Mohammad Mousavi

1. System Validation: an introduction

TU Delft

# System Validation: An Introduction

Mohammad Mousavi

TU/Eindhoven

System Validation, 2012-2013
StayOk, Doorwerth

# Outline

1. Organizational Matters

2. Formal Modeling Verification

# Contact information

## Course Web Page

`http://www.win.tue.nl/~mousavi/IN4387/`

Check for news, updates, course material and much more!

| | |
|---|---|
| Office | EWI Building, Floor 9, Room 160 |
| Office Hours | Wednesdays from 10:30 to 16:00 |
| E-mail | M.R.Mousavi@tue.nl |
| WWW | `http://www.win.tue.nl/~mousavi/` |

# Audience

- Embedded Systems – Master's degree program (year 1) – Compulsory
- Computer Engineering – Master's degree program (year 1) – Elective
- Others?

# Objectives and assessment

## Learning objectives

1. Know the concepts of behavioral specification and equivalence **(Knowledge)**
2. Know the realization of these concepts in mCRL2 **(Knowledge)**
3. Know how to specify logical properties **(Knowledge)**
4. Specify the behavior of embedded systems **(Application)**
5. Experience the design of a provably correct system **(Application)**

## Evaluation method

Items 1-3: Written exams. No material allowed.
Item 4-5: Practical project

# Examination(s)

Theory:

- E1 End of Quarter 1, 8-11-2012, 14:00-17:00
- E2 Resit: End of Quarter 2, 30-01-2013, 14:00-17:00

Do register using Osiris.

Practical project P (compulsory, no pass without the project)

$$M = \frac{Max(E1, E2) + P}{2}$$

# Project: Procedure

- Formulate informal requirements

# Project: Procedure

- Formulate informal requirements
- Define interactions with the outside world

# Project: Procedure

- Formulate informal requirements
- Define interactions with the outside world
- Rephrase the requirements in terms of interactions

# Project: Procedure

- Formulate informal requirements
- Define interactions with the outside world
- Rephrase the requirements in terms of interactions
- Define the system architecture and internal interactions

# Project: Procedure

- Formulate informal requirements
- Define interactions with the outside world
- Rephrase the requirements in terms of interactions
- Define the system architecture and internal interactions
- Model the system behavior

# Project: Procedure

- Formulate informal requirements
- Define interactions with the outside world
- Rephrase the requirements in terms of interactions
- Define the system architecture and internal interactions
- Model the system behavior
- Verify the requirements on the model

# Project: Procedure

- Formulate informal requirements
- Define interactions with the outside world
- Rephrase the requirements in terms of interactions
- Define the system architecture and internal interactions
- Model the system behavior
- Verify the requirements on the model

Iterate the last two items until requirements are satisfied.

# Project: Procedure

- Carried out in groups of 4; form your groups and email them to me.

# Project: Procedure

- Carried out in groups of 4; form your groups and email them to me.
- Weekly progress meetings of 15 minutes with all group members; prepare well beforehand

# Project: Procedure

- Carried out in groups of 4; form your groups and email them to me.
- Weekly progress meetings of 15 minutes with all group members; prepare well beforehand
- Deadlines and deliverables:

First deliverable October 5: Report including requirements, interactions and architecture

cond deliverable October 19: Report (complete structure)

Final deliverable November Report, source files for models, and reflections

# Project: Short Description

- Inspired by the packet storage system, by Vanderlande Industries
- 5 controllers for elevators, conveyor belts and racks
- Several requirements: deadlock freedom, avoiding clash, maximum efficiency

# Project: Short Description

## Design Decision

No extra functionality, unless strictly needed.

# Project: Short Description

### Design Decision

No extra functionality, unless strictly needed.

Make design decisions, when needed, but keep them:

- consistent,
- motivated, and
- documented.

# Reading material

Course Notes J.F. Groote and M.R. Mousavi. Modelling and Analysis of Communicating Systems, 2011. (Mandatory, available on the course page.)

Slides Available on-line (after each session) on the course page.

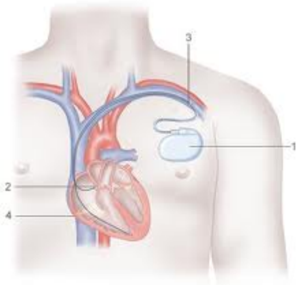
Chapters Chapters 3b-6 of L. Aceto, A. Ingólfsdóttir, K.G. Larsen, and J. Šrba. Reactive Systems: Modelling, Specification and Verification, Cambridge University Press, 2007. (Recommended)

Book W.J. Fokkink, Introduction to Process Algebra (2nd edition), April 2007 (Recommended)

# Software at Your Heart...

XYZ Medical Inc. said Thursday that it has identified a glitch in software used to program three of its pacemaker models.

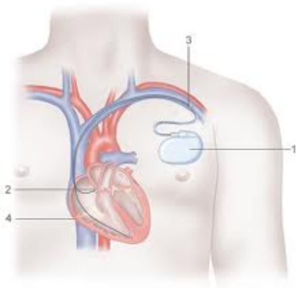
XYZ said it has not received any reports of deaths of clinical complications resulting from the glitch, which appears in about 53 out of every 199,100 cases.



# Software at Your Heart...

At least 212 deaths from device failure in five different brands of implantable cardioverter-defibrillator (ICD) according to a study reported to the FDA ... .

[Killed by Code, 2010]



# Which one is more complex?

# Which one is more complex?

1.5 Mil.USD

6 Mil. USD

# Modeling and Verification

## Why Formal?

- Mathematics: source of precision in all engineering disciplines

# Modeling and Verification

## Why Models?

- Common practice in all mature engineering disciplines
  (imagine building the Empire State or a Boeing 747 without a model)
- Provides the basis for calculation, reasoning, sanity- and consistency-check
- Closes the gap between phases: software development as model transformation

# Modeling and Verification

## Why Verification?

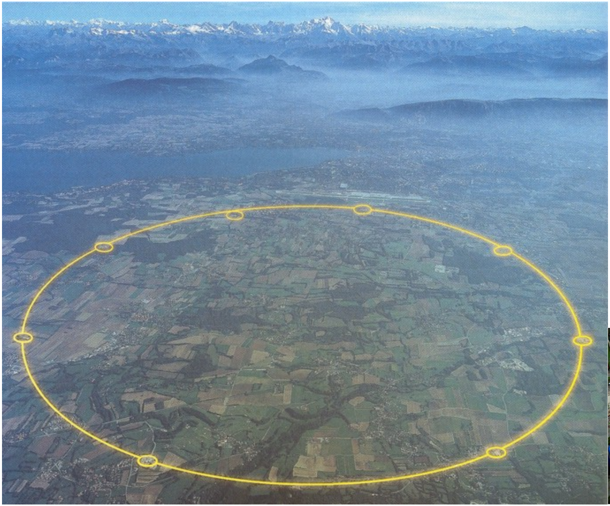
- Can be used for several purposes: e.g., code generation, testing and verification
- Verification provides a precise proof of correctness
- Your verification results are as good as your models

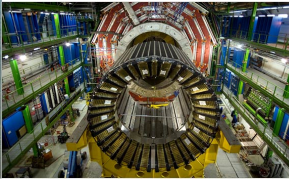
# Subject Matter

- Application,
- Tools, and
- Theory of

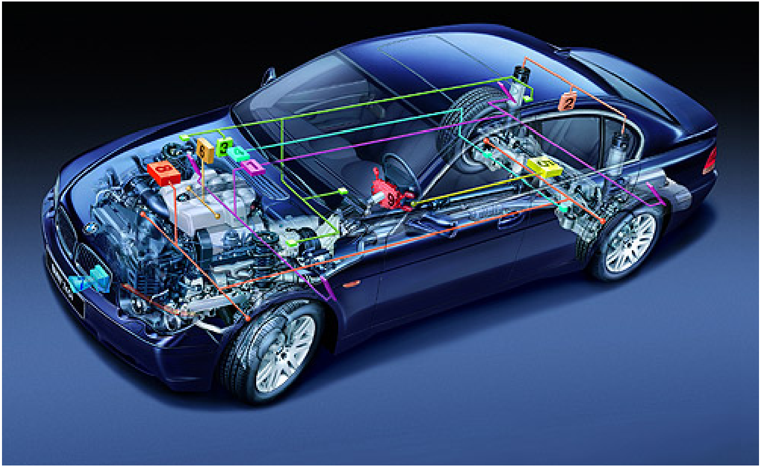
proving system correctness with respect to abstract properties.

# Applications: CERN Hadron Collider



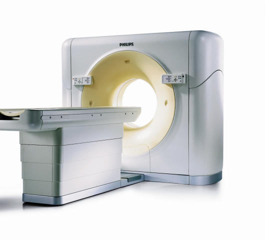


# Applications: FlexRay Protocol

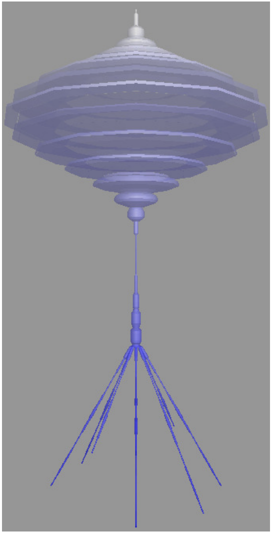


# Applications: ASML Wafer Stepper

# Applications: Many Others



# Tool: mCRL2



See: `http://www.mcrl2.org/`

# General Outline

## Plan

| | |
|---|---|
| September 4 | Introduction, Behavioral Equivalences |
| September 12 | Behavioral Equivalences |
| September 19 | Abstract Data Types |
| September 26 | Sequential Processes: Theory |
| October 3 | Sequential Processes: Reasoning and Examples |
| October 10 | Parallel Processes: Theory |
| October 17 | Parallel Processes: Reasoning and Examples |
| October 24 | Modal mu-Calculus |

# Thank you very much.

Questions?