System Validation: An Introduction

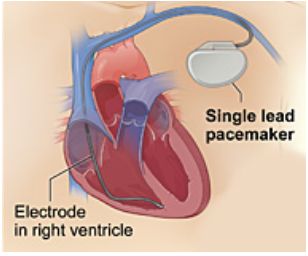
Mohammad Mousavi and Jeroen Keiren

PSI Conference 2015, Innopolis

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.

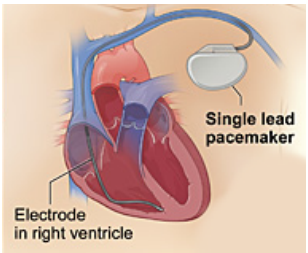
XYZ said it has not received any reports of deaths of clinical complications resulting from the glitch, which appears in about 53 out of every 199,100 cases.



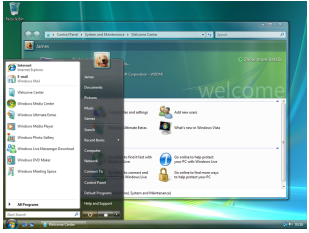
Software at Your Heart...

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]



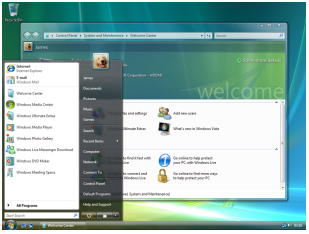
Which one is more complex?



Used with permission from Microsoft.

Which one is more complex?

1.5 Bil.USD



Used with permission from Microsoft.

6 Bil. USD

Why Formal?

- Mathematics: source of precision in all engineering disciplines

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?

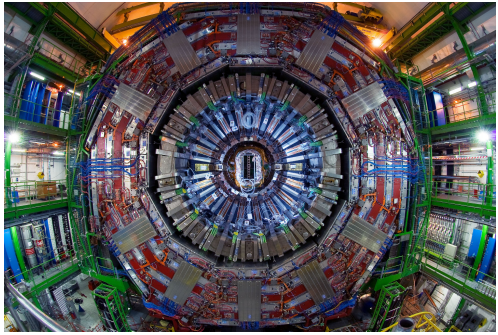
- Can be used for several purposes:
  e.g., code generation, testing and verification
- Verification provides a precise proof of correctness
- Your verification results are as good as your models

Subject Matter

- Application,
- Tools, and
- Theory of

proving system correctness with respect to abstract properties.

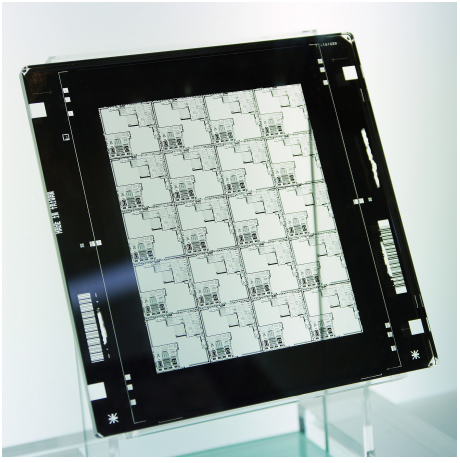
Applications: CERN Hadron Collider



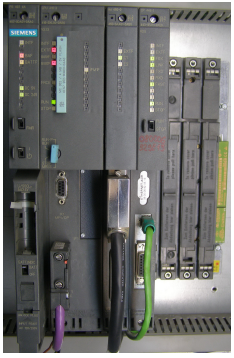
Source: CERN

Applications: FlexRay Protocol

Applications: ASML Wafer Stepper

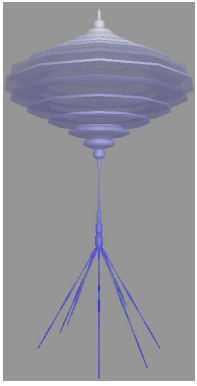


Applications: Many Others



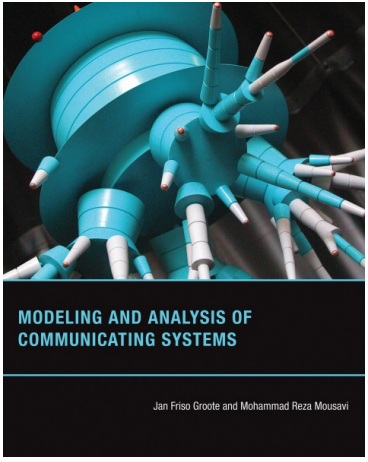
Source: Wikimedia

Tool: mCRL2

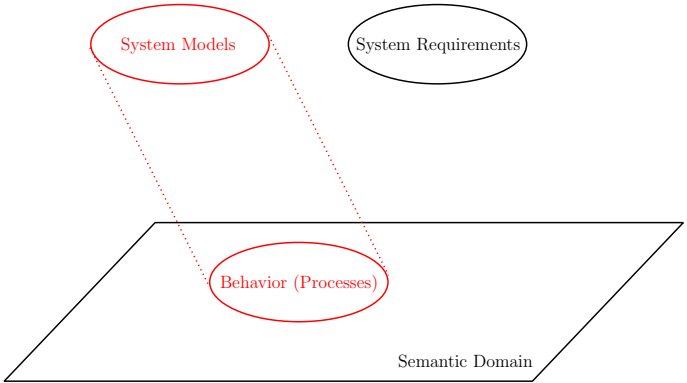


See: `http://www.mcrl2.org/`

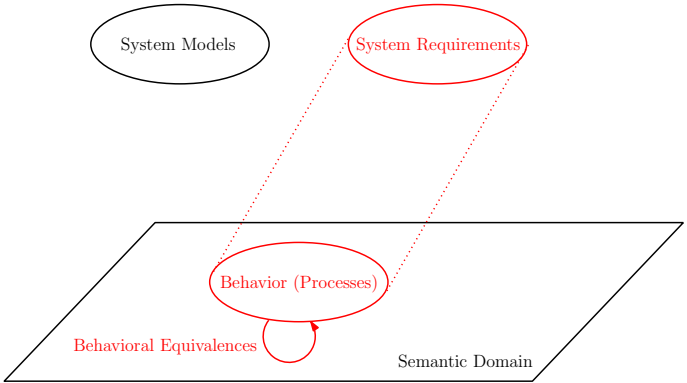
Book: MACS


MODELING AND ANALYSIS OF
COMMUNICATING SYSTEMS
Jan Friso Groote and Mohammad Reza Mousavi

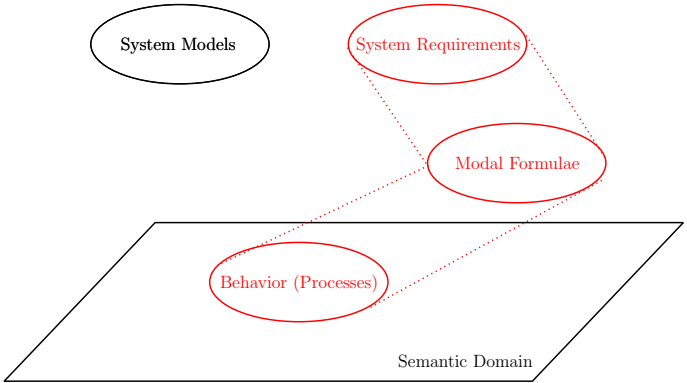
General Outline



General Outline



General Outline



Summary

Motivation Computer systems are:

- omnipresent, and
- complex.

Modeling is essential

Verification provides rigorous proof of Correctness

To do Download mCRL2 and try it

Acknowledgments

The material presented in this tutorial has been developed in collaboration with Jan Friso Groote and his group at TU/Eindhoven.

Michel Reniers of TU/Eindhoven has contributed to the material on modal mu-calculus.

Mousavi's research is supported by grants from Swedish Research Council (VR) and Swedish Knowledge Foundation (KKS).

Thank you very much.