MODELING DISTRIBUTED SYSTEMS

HERMANN HÄRTIG, DISTRIBUTED OPERATING SYSTEMS, SS2020
use models to analyze, prove, predict, ... properties of concrete system AND
to establish fundamental insights

- abstract from details
- concentrate on functionality, properties, ... considered important for a specific system/application/question
- models in engineering disciplines very common, increasingly in CS as well
Purpose

- describe the timing requirements of an application
- describe available resources
- question: can the application run on/use these resources such that timing requirements are fulfilled

Model elements:

- periodic tasks, deadlines, worst-case exec time, ...

 Hopefully RTS class is offered in future (by my successor)
<table>
<thead>
<tr>
<th>Model</th>
<th>Objective/Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Trees</td>
<td>are all failures and their combinations taken into account</td>
</tr>
<tr>
<td>statics models</td>
<td>does a house fall down (snow, quake)</td>
</tr>
<tr>
<td></td>
<td>what kind of vehicles on a bridge</td>
</tr>
<tr>
<td>control laws</td>
<td>stability of controllers</td>
</tr>
<tr>
<td>Ohm’s Law</td>
<td>behavior of circuits</td>
</tr>
</tbody>
</table>
WELL KNOWN EXAMPLES FOR MODELS

\[ I = \frac{V}{R} \]
Q1: Is it possible to build arbitrarily reliable Systems out of unreliable components?

Q2: Can we achieve consensus in the presence of faults (consensus: all non-faulty components agree on action)?

Q3: Is there an algorithm to determine for a system with a given setting of access control permissions, whether or not a Subject A can obtain a right on Object B?

2 Models per Question!
SYSTEMS MODELS: GENERAL APPROACH

Reasoning:
- Common sense
- Formal Verification
- Careful Inspection
- Mathematics
Reasoning:
- Common sense
- Formal Verification
- Careful Inspection
- Mathematics

“Refinement”:
- Abstraction
- Implementation
- Formal Refinement

Property

Model

Reasoning

Refinement

Model M

Reasoning

Refinement

Model L

Reasoning

System

OK?
<table>
<thead>
<tr>
<th>Model</th>
<th>Objective/Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amdahl’s Law</td>
<td>Scalability</td>
</tr>
<tr>
<td>Turing Machine</td>
<td>Halting problem, Decidability</td>
</tr>
<tr>
<td>Logic</td>
<td>Correctness, Precision, ...</td>
</tr>
</tbody>
</table>
Objective of lecture:
understand the power of models and the need for their careful understanding
models in detail, but math results by intuition not proofs

Try to find answers to question Q1 ... Q3
BEFORE viewing the other pieces of the lecture and the full slide set
Q1: Is it possible to build arbitrarily reliable Systems out of unreliable components?

Q2: Can we achieve consensus in the presence of faults (consensus: all non-faulty components agree on action)?

Q3: Is there an algorithm to determine for a system with a given setting of access control permissions, whether or not a Subject A can obtain a right on Object B?

2 Models per Question!