Modelling and verifying IEEE 11073-20601 session setup with mCRL2

Jeroen Keiren  Martijn Klabbers

Bamberg, September 18, 2012
What is IEEE 11073-20601?

Health informatics — Personal health device communication —
Part 20601: Application profile — Optimized exchange protocol

and many more
What are personal health devices?

Agent devices

Manager devices
What is the purpose of IEEE 11073-20601?

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>“[...] define[...] a common framework for making an abstract model of personal health data available in transport-independent transfer syntax required to establish logical connections between systems and to provide presentation capabilities and services needed to perform communication tasks.” [IEEE std 11073-20601]</td>
</tr>
</tbody>
</table>
Agent and manager cycle through states:

- Unassociated
- Associating
- Sending configuration
- Waiting approval
- Operating
- Disassociating
Protocol (sketch)

Agent and manager cycle through states:

- Unasssociated
- Associating
- Sending configuration
- Waiting approval
- Operating
- Disassociating
Objectives

- Assess understandability, consistency, and completeness
- Establish correctness
- Fix bugs
Methodology

- Formalise protocol in mCRL2
- Formulate desired properties in temporal logic
- Use model checker to verify the properties
Understandability, consistency and completeness
Am I too stupid, or the standards committee too smart?

- Requirements are not explicit
- Formalisms not introduced
- Information inconsistently duplicated between representations
  - Inconsistent terminology/abbreviations
  - Different state changes for same event
- Unexpected messages not fully treated
Deadlocks caused by incompleteness
Correctness

Property

Data shall not be transmitted in inconsistent operating states.
But it does...
Conclusions

- Omissions and inconsistencies cause easy to fix bugs
- Session setup contains a severe bug
- Agent and manager devices can transfer data in inconsistent configurations
- Rest of the protocol should be verified
Lessons learned

- Formal modelling allows detection of problems in short timespan
- Standards should provide clear requirements
- Bugs cannot be fixed without breaking standard conformance
- Formal verification should be part of the development process of every communication standard
Take home message

Unverified standards contain subtle, hard to find errors!