Messing around with timeouts. In contracts?

Øyvind Teig
www.teigfam.net/oyvind/home

@CPA 2016 fringe http://www.wotug.org/cpa2016/
Can time be part of a contract?

- Is it a contract when time is included?

- “Shall we meet at half past eight at the pub for a beer?”
  - Let’s call it agreement for this presentation?

- Expecting a proper contractual response
  - But you can’t figure out why that timeout was added?
  - Was it needed?
Real contract **without time**

<table>
<thead>
<tr>
<th>Assumed “contract”</th>
<th>Real contract</th>
</tr>
</thead>
<tbody>
<tr>
<td>start(some_event)</td>
<td>start(some_event)</td>
</tr>
<tr>
<td>delay(duration)</td>
<td>wait(for_dataReady_signal)</td>
</tr>
<tr>
<td>get(&amp;assumedData_orStatus)</td>
<td>get(&amp;theData_orStatus)</td>
</tr>
</tbody>
</table>

- for some time
- forever
Real contract **without** time out

<table>
<thead>
<tr>
<th>Assumed “contract”</th>
<th>Real contract</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>start(some_event)</code></td>
<td><code>start(some_event)</code></td>
</tr>
<tr>
<td><code>delay(duration)</code></td>
<td><code>wait(for_dataReady_signal)</code></td>
</tr>
<tr>
<td><code>get(&amp;assumedData_orStatus)</code></td>
<td><code>get(&amp;theData_orStatus)</code></td>
</tr>
</tbody>
</table>

..at a **layer** below:

Connection down after some time
Periodic task certainly needs timeouts

<table>
<thead>
<tr>
<th>Assumed “contract”</th>
<th>Real contract</th>
</tr>
</thead>
<tbody>
<tr>
<td>start(some_event)</td>
<td>start(some_event)</td>
</tr>
<tr>
<td>delay(duration)</td>
<td>wait(for_dataReady_signal)</td>
</tr>
<tr>
<td>get(&amp;assumedData_orStatus)</td>
<td>get(&amp;theData_orStatus)</td>
</tr>
</tbody>
</table>

then action

```c
if (Status==OK) Blink_LED (Colour);
```

Periodic task certainly needs timeouts
P6 \[\rightarrow \text{X67} \rightarrow \text{P7} \]

P6 \[\rightarrow \text{X76} \rightarrow \text{P7} \]

X3 \[\rightarrow \text{t6} \rightarrow \text{P6} \]

H \[\rightarrow \text{T} \rightarrow \text{P7} \]

t7 \[\rightarrow \text{P7} \]

B

assert()
ASSERT (ok): «Design by contract»

Design by Contract ® (DbC) is trademarked by Eiffel Software
Timeouts to loosen or tighten?

• For Safety Critical systems, in IEC 61508 [4] 2010 part 3, Annex F 61508-3 there is an informative chapter called «Techniques for achieving non-interference between software elements on a single computer»

• «Independence of execution»
  • Spatial domain (don’t modify)
  • Temporal domain (don’t disturb)
IEC 61508

• Differing «systematic capability»

• Is progress guarantee, i.e. no deadlock and livelock not enough?

• Do we need timeouts or layers? Like at
Safety critical components
Rather layered / hidden timeout than interfering timeouts?
This CPA 2016 fringe presentation is based on a blog note
«Timing out design by contract with a stopwatch»

Preprint of the fringe presentation

Programme
http://www.wotug.org/cpa2016/programme.shtml
CPA @ CPH