Messing around with timeouts.
In contracts?

Øyvind Teig
www.teigfam.net/oyvind/home

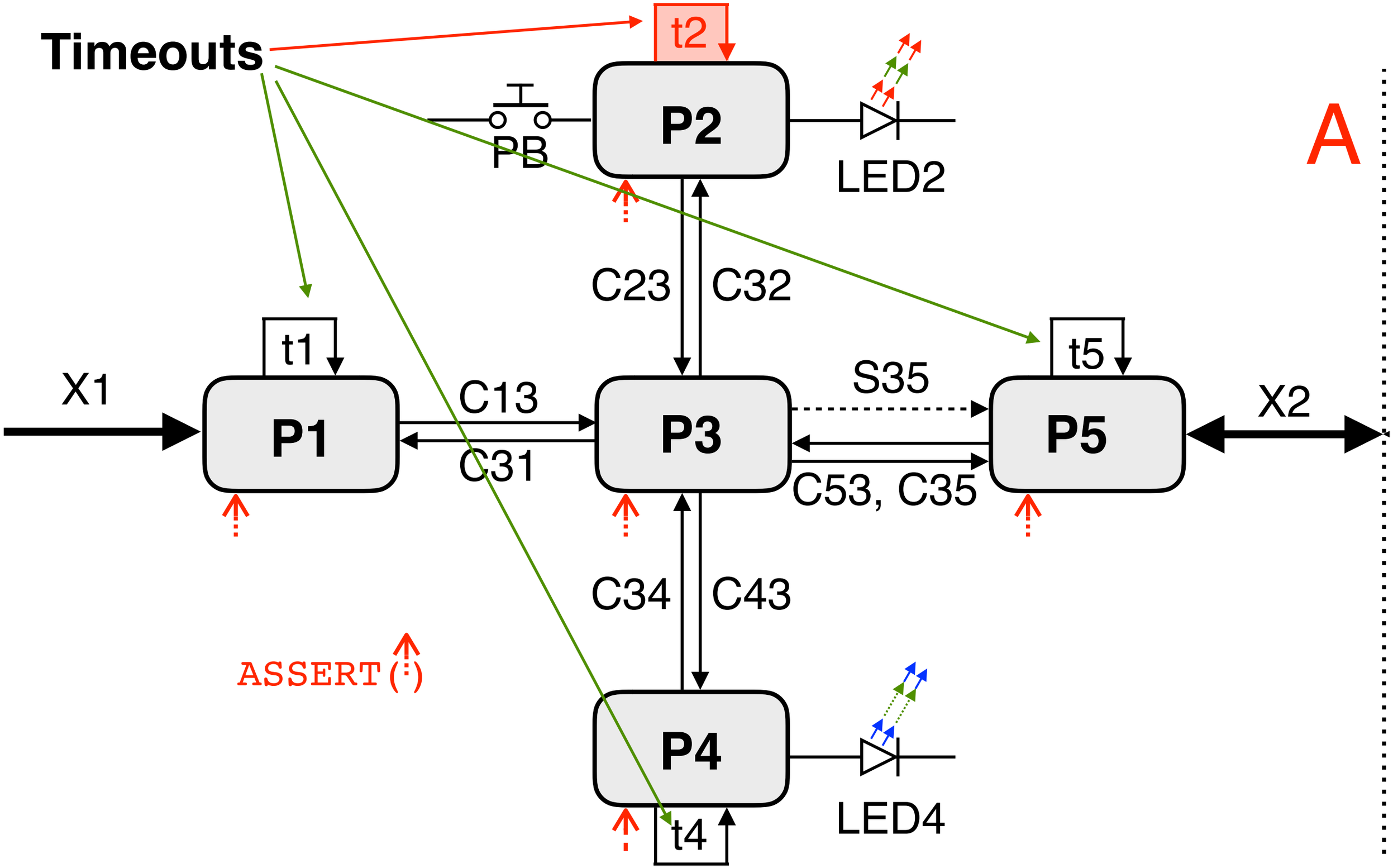
@CPA 2016 fringe http://www.wotug.org/cpa2016/

)

Autronica Fire and Security AS, Trondheim, Norway. Autronica is a part of UTC Climate, controls and security, a unit of United Technologies Corporation

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 cant’ figure out why that timeout was added?
  - Was it needed?


Timeouts
t2
P2
PB
LED2
A
C23
C32
t1
t5
X1
P1
C13
C31
P3
S35
P5
X2
C53, C35
C34
C43
ASSERT(·)
P4
LED4
t4

Real contract without time

Assumed "contract"	Real contract
`start(some_event)`	`start(some_event)`
`delay(duration)`	`wait(for_dataReady_signal)`
`get(&assumedData_orStatus)`	`get(&theData_orStatus)`

for some time

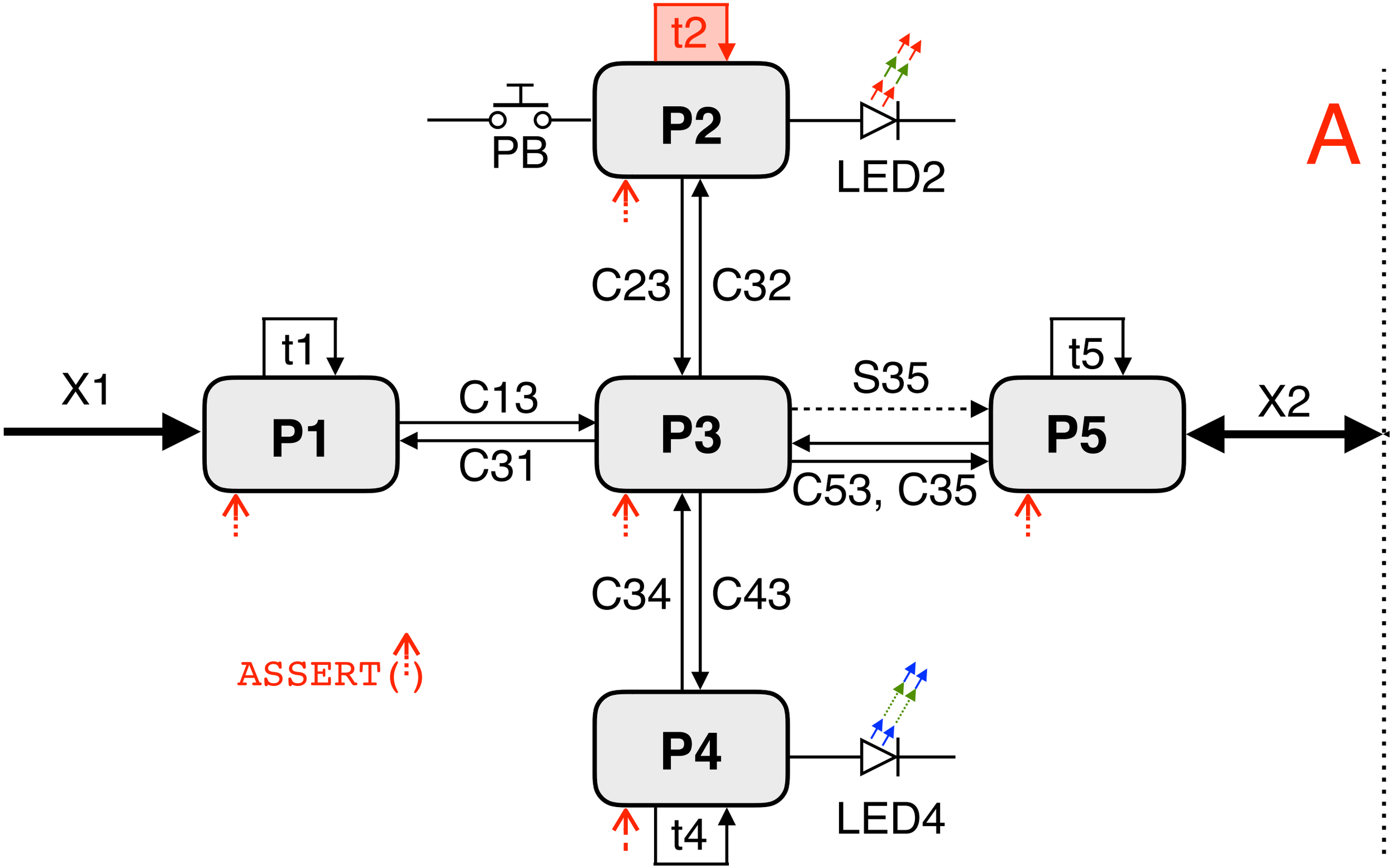
forever

Real contract without time out

Assumed "contract"	Real contract
`start(some_event)`	`start(some_event)`
`delay(duration)`	`wait(for_dataReady_signal)`
`get(&assumedData_orStatus)`	`get(&theData_orStatus)`

Connection down after some time

..at a layer below:


t2
P2
PB
LED2
A
C23
C32
t1
t5
X1
P1
C13
C31
P3
S35
P5
X2
C53, C35
C34
C43
ASSERT(·)
P4
LED4
t4

`delay` **or** `sleep` **also needed**

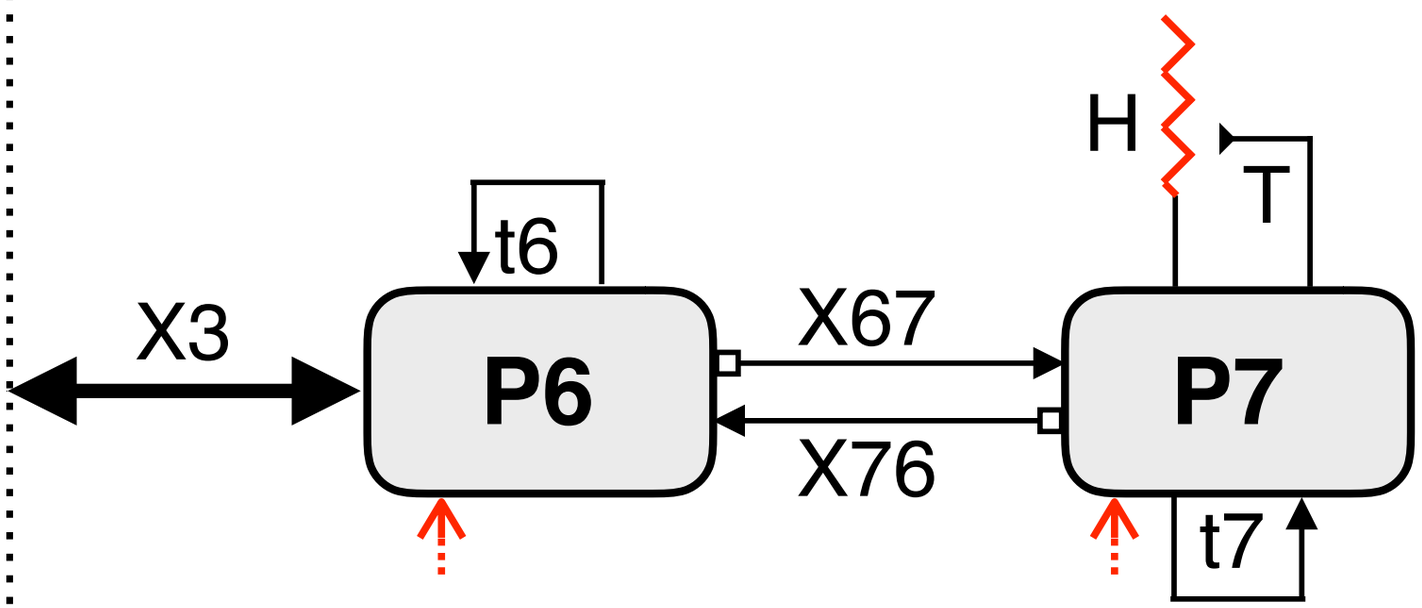
Assumed "contract"	Real contract
`start(some_event)`	`start(some_event)`
`delay(duration)`	`wait(for_dataReady_signal)`
`get(&assumedData_orStatus)`	`get(&theData_orStatus)`

then action

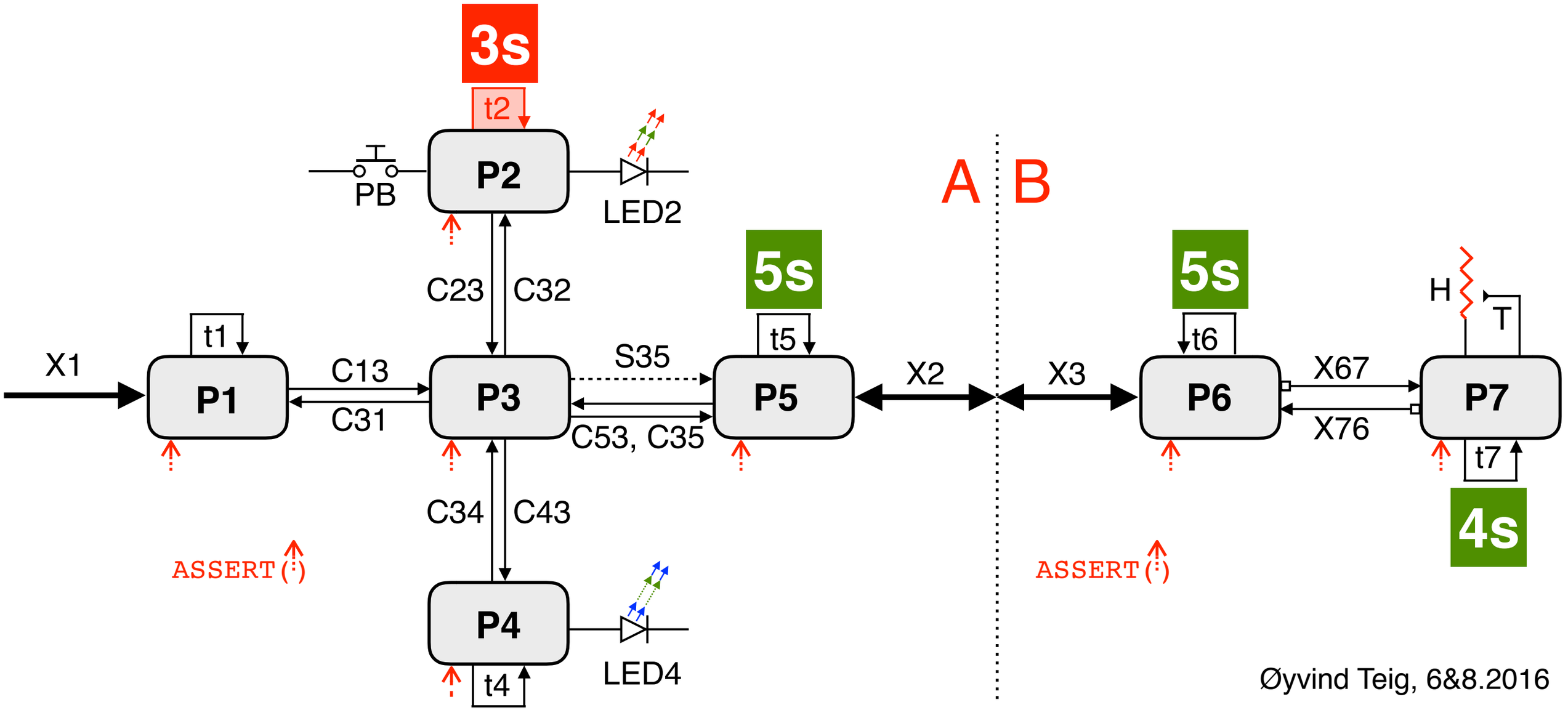
```
if (Status==OK) Blink_LED (Colour);
```

Periodic task certainly needs timeouts

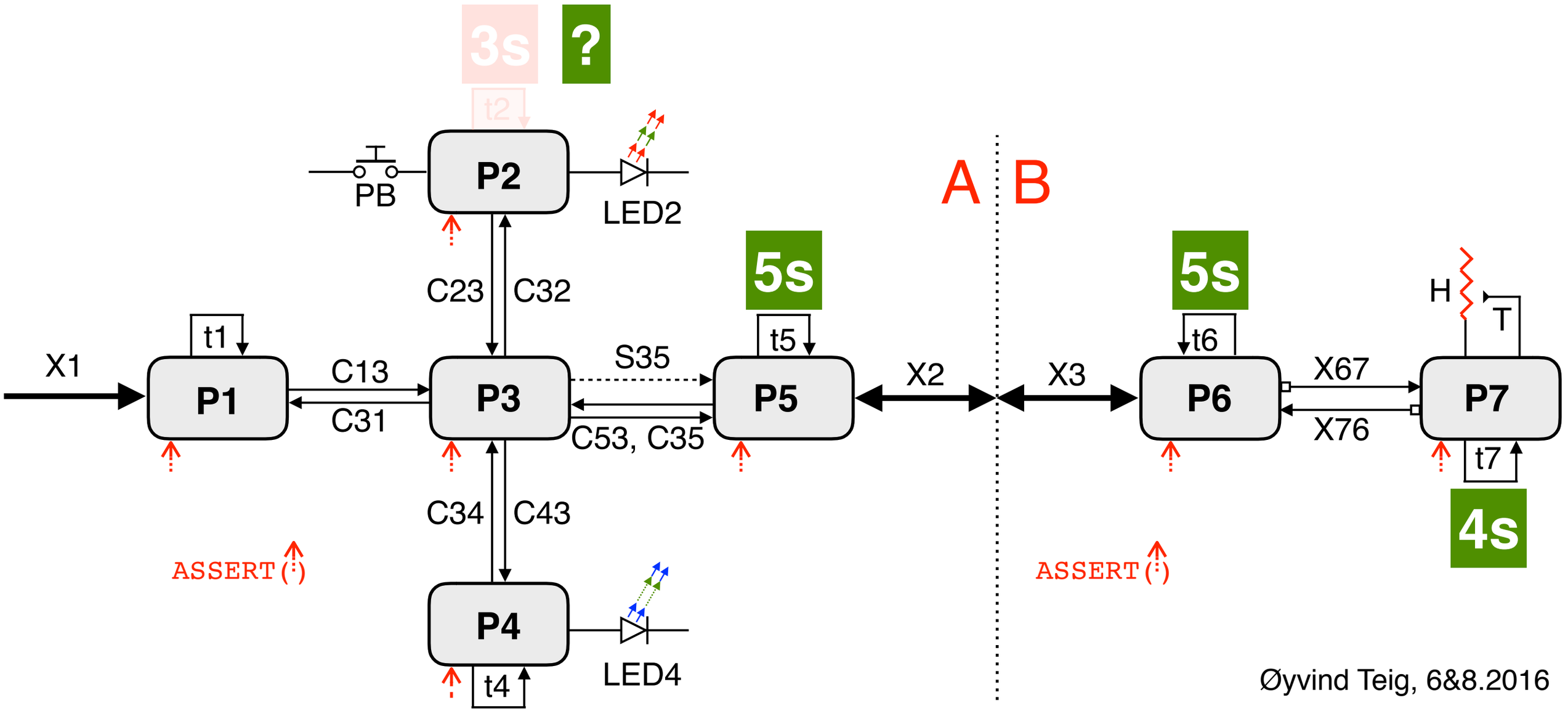
B



ASSERT(⋮)

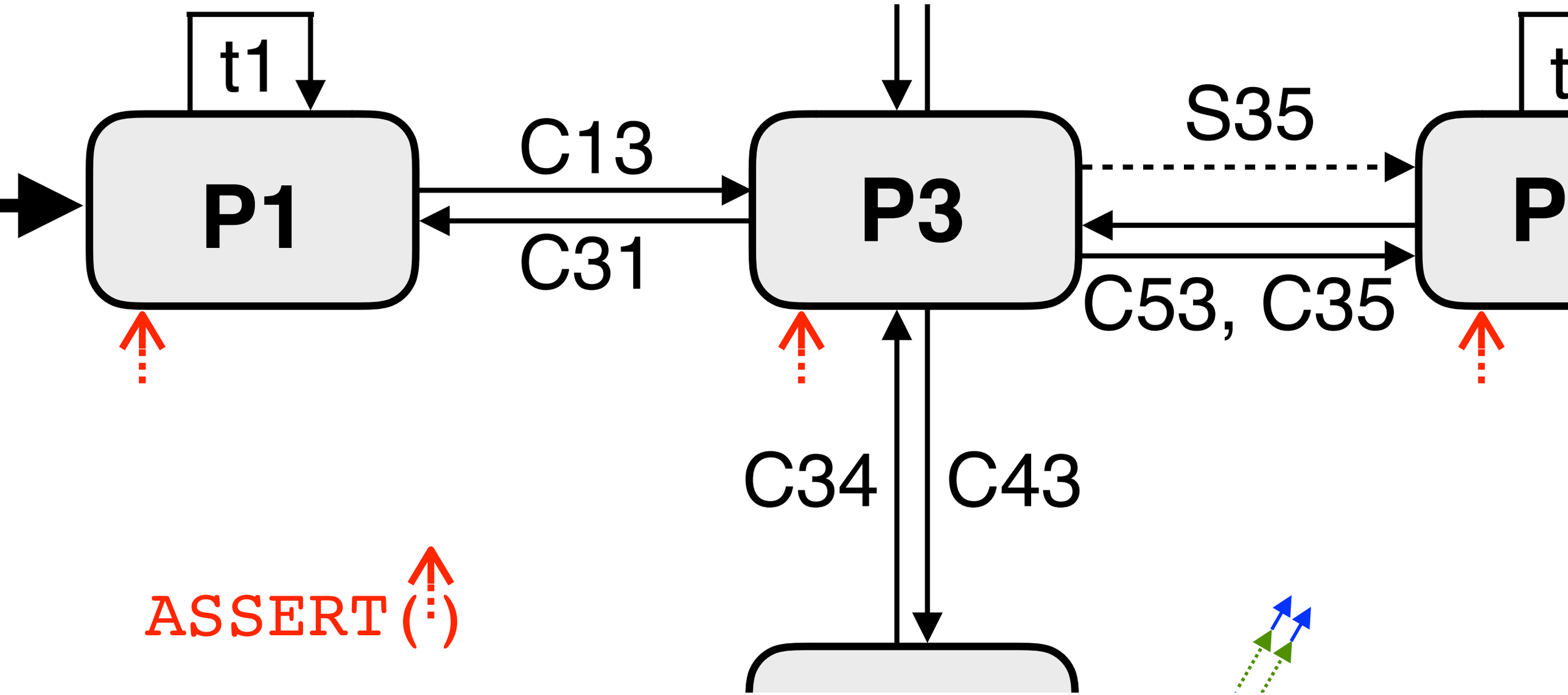


Øyvind Teig, 6&8.2016



Øyvind Teig, 6&8.2016

ASSERT (ok): «Design by contract»



Design by Contract ® (DbC) is trademarked by Eiffel Software

Timeouts to loosen or tighten?

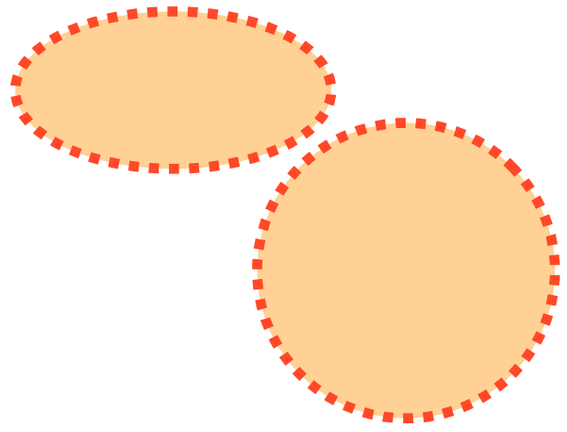
- For Safety Critical systems, in IEC 61508 [4] 2010 part 3, Annex F 61508-3 there is an informative chapter called «Techniques for achieving **non-interference** between software elements on a single computer»

- «**Independence of execution**»
  - **Spatial domain** (dont' modify)
  - **Temporal domain** (don't disturb)

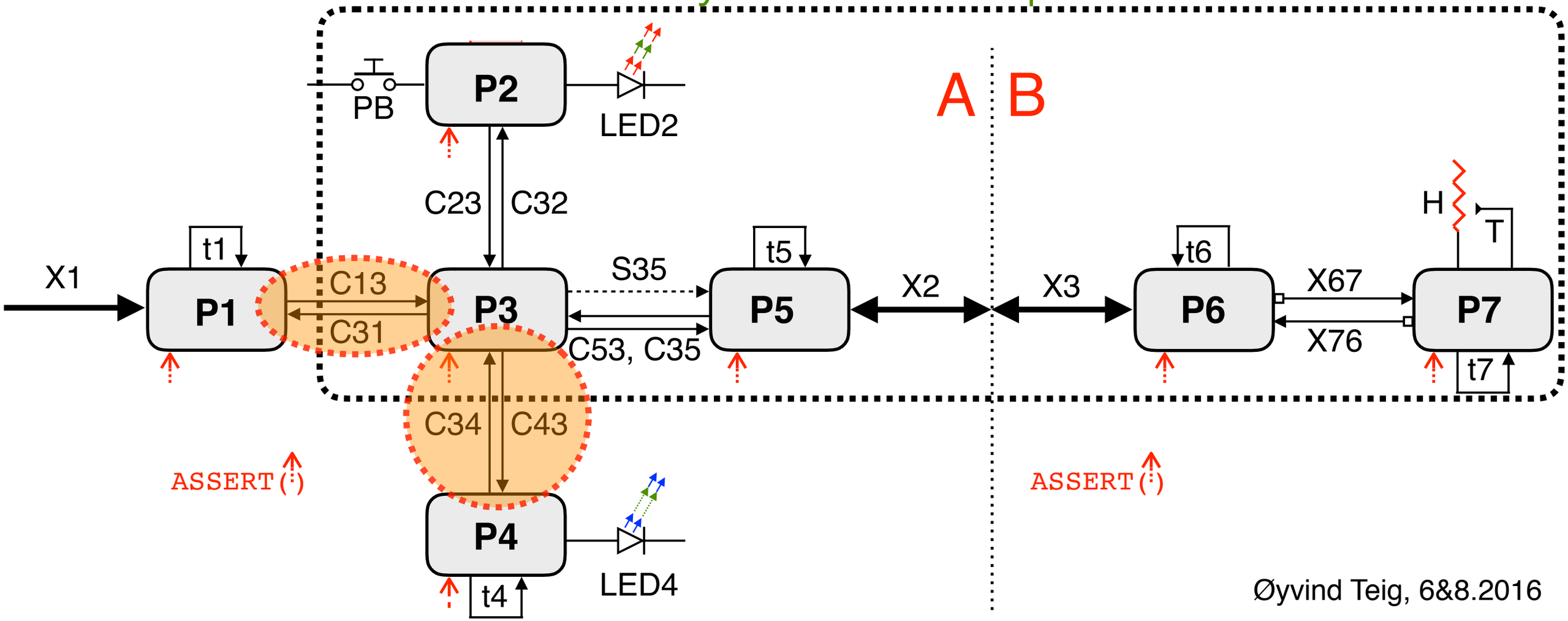
Progress guarantee or timeouts?

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



Øyvind Teig, 6&8.2016

Montecatini Alto Chiesa dei Santi Jacopo e Filippo (o del Carmine), Italy
Minus some modern antenna wires!

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»

www.teigfam.net/oyvind/home/technology/128-timing-out-design-by-contract-with-a-stopwatch/

Preprint of the fringe presentation

http://www.wotug.org/cpa2016/preprints/30-preprint.pdf

Programme

http://www.wotug.org/cpa2016/programme.shtml

«CPA @ CPH»