Re: [mop] TFSM plugin

mop-bounces@cs.illinois.edu on behalf of Falcone, Ylies [ylies@illinois.edu]
Sent: Thursday, March 12, 2015 2:23 PM
To: Rosu, Grigore
Cc: mop@cs.uiuc.edu

A 2cts comment. The advantage of the limited expressiveness and the potential for efficient implementation is that we will need to make sure that the execution time of the monitor does not influence the satisfiability of the specification. When we are dealing with deadlines (arrow -17>), this could lead us to state false positives, and the converse with arrow of the form ->17>.
We will probably need to provide guarantees that such false verdicts do not happen.

> Le 12 mars 2015 à 12:46, Rosu, Grigore <grosu@illinois.edu> a écrit :
>
> Phil and others,
>
> After a discussion with Ylies today after the RV meeting, I think we should go ahead with our plan to add time on transitions in our tfsm plugin. Syntactically, it would just modify the fsm plugin to allow arrows of the form -17>, with the semantics that the transition should happen in less than 17 units (say ms), and arrows of the form ->17>, with the semantics that the transition should happen in at least 17 units, in addition to arrows of the form -> which are unbounded. For example, here is a property stating that if "next" happens then it should happen <5ms after "hasnext", and if the property fails, then we can start it over after at least 10ms:
>
```
> start [
>    next -> fail
>    hasnext -> safe
>  ]
>  safe [
>    next -5> start
>    hasnext -> safe
>  ]
>  fail [
>    hasnext ->10> safe
>  ]
```
>
> I know this is not as general as it can be, but it seems to go a long way on the practical side and it is easy to implement,
>
> What do you guys think?
>
> We need to move fast with this, because we need it both for the rewrite competition and for our Toyota/Denso project.
>
> Grigore
>
>
>
> _____
> mop mailing list
> mop@cs.illinois.edu
> http://lists.cs.uiuc.edu/mailman/listinfo/mop

_____
mop mailing list
mop@cs.illinois.edu

http://lists.cs.uiuc.edu/mailman/listinfo/mop