Veri£cation of Asbru

Utrecht, 14.02.2002, Michael Balser

Current State

Asbru plans are translated into parallel programs

Current State

Asbru plans are translated into parallel programs

Is this the original protocol?

ASBRU in KIV

Protocure

Current State

Asbru plans are translated into parallel programs

Is this the original protocol?

(Far) Future

Proof method of

symbolic execution with induction

is general enough to allow arbitrary operators

ASBRU in KIV

Protocure

Current State

Asbru plans are translated into parallel programs

Is this the original protocol?

(Far) Future

Proof method of

symbolic execution with induction

is general enough to allow arbitrary operators

Best Solution

$\Rightarrow$ add ASBRU syntax to KIV
$\Rightarrow$ design proof rules in analogy to formal semantics

ASBRU syntax in KIV (1)

Protocure

Scheme

```
ASBRU(<state>, <start>, <ctrl>, <time>,
      <fc>, <actc>, <ac>, <cc>,
      <body>)
```

ASBRU syntax in KIV (2)

Protocure

Example

```
   Blood-tests-state = activated,
   ASBRU(Blood-tests-state, Blood-tests-start,
         Blood-tests-ctrl, Blood-tests-time,
         true,
         automatic,
         Chck-state.abrtd /\ Prfrm-state.abrtd
            Chck-state.cmpltd \/ Prfrm-state.cmpl
         /\ Chck-state.trmintd /\ Prfrm-state.trm
         DO-SEQ(Chck-state, Chck-ctrl,
                Prfrm-state, Prfrm-ctrl )),
   ASBRU(Chck-state, ...),
   ASBRU(Prfrm-state, ...)
|- [] ...
```

Previous and Next Steps

Protocure

Proof support for Asbru syntax is a lot of work

Previous and Next Steps

Protocure

Proof support for Asbru syntax is a lot of work

Previous Steps

- correctness of proof method (symbolic execution with induction)
- trials with additional operators

Previous and Next Steps

Protocure

Proof support for Asbru syntax is a lot of work

Previous Steps

- correctness of proof method (symbolic execution with induction)
- trials with additional operators

Next Steps

- correctness of modular proof method
- continue with translation to parallel plans
- handle gap between Asbru and KIV representation manually