Contents

CONTEXT c_status

SETS

STATUS

CONSTANTS

PO

PA

CC

PC

UNDEFINED

BRAKE

AXIOMS

axm1: $partition(STATUS, \{PO\}, \{PA\}, \{CC\}, \{PC\}, \{UNDEFINED\}, \{BRAKE\})$

END

CONTEXT c_user_action

SETS

USER_ACTION

CONSTANTS

pa

pac

cc

pc

pcc

br

ccc

AXIOMS

axm1: $partition(USER\_ACTION, \{pa\}, \{pac\}, \{cc\}, \{pc\}, \{pcc\}, \{br\}, \{ccc\})$

END

MACHINE M0
SEES c_status
VARIABLES

status
beforecc
engrun

INVARIANTS

inv1: $status \subseteq STATUS$
inv3: $beforecc \subseteq \{PO, PA, UNDEFINED\}$
inv4: $engrun \in BOOL$

EVENTS
Initialisation

```
    begin
        act1: $status := \{PO\}$
        act2: $beforecc := \{UNDEFINED\}$
        act3: $engrun := FALSE$
    end
```

Event PedalOnly ⟨ordinary⟩ $\widehat{=}$

```
    when
        grd1:
            $status = \{PA\} \lor status = \{PC\} \lor$
            $(status = \{CC\} \land beforecc = \{PO\})$
    then
        act1: $status := \{PO\}$
        act2: $engrun := FALSE$
    end
```

Event PedalAssist ⟨ordinary⟩ $\widehat{=}$

```
    when
        grd1:
            $status = \{PO\} \lor$
            $(status = \{CC\} \land beforecc = \{PA\})$
    then
        act1: $status := \{PA\}$
        act2: $engrun := TRUE$
    end
```

Event PedalOnly2CruiseControl ⟨ordinary⟩ $\widehat{=}$

```
    when
        grd1: $status = \{PO\}$
    then
        act1: $status := \{CC\}$
        act2: $beforecc := \{PO\}$
        act3: $engrun := TRUE$
    end
```

Event PedalAssist2CruiseControl ⟨ordinary⟩ $\widehat{=}$

```
    when
        grd1: $status = \{PA\}$
    then
        act1: $status := \{CC\}$
        act2: $beforecc := \{PA\}$
        act3: $engrun := TRUE$
    end
```

Event PedalCharge ⟨ordinary⟩ $\widehat{=}$

```
    when
        grd1: $status = \{PO\}$
    then
        act1: $status := \{PC\}$
        act2: $engrun := TRUE$
    end
Event Brake ⟨ordinary⟩ $\widehat{=}$
    when
        grd1: $status = \{PO\} \lor status = \{PA\} \lor status = \{PC\}$
    then
        act1: $status := \{BRAKE\}$
        act2: $engrun := FALSE$
    end
Event BrakeCruiseControl2PedalOnly ⟨ordinary⟩ $\widehat{=}$
    when
        grd1: $status = \{CC\} \land beforecc = \{PO\}$
    then
        act1: $status := \{PO\}$
        act2: $engrun := FALSE$
    end
Event BrakeCruiseControl2PedalAssist ⟨ordinary⟩ $\widehat{=}$
    when
        grd1: $status = \{CC\} \land beforecc = \{PA\}$
    then
        act1: $status := \{PA\}$
        act2: $engrun := TRUE$
    end
END
```

MACHINE M1

REFINES M0

SEES c_status,c_user_action

VARIABLES

status

beforecc

engrun

useraction

INVARIANTS

inv1: $useraction \in STATUS \mathrel{+\!\!\!\!\rightarrow} USER\_ACTION$

EVENTS

Initialisation

begin

act1: $status := \{PO\}$

act2: $beforecc := \{UNDEFINED\}$

act3: $engrun := FALSE$

act4: $useraction :\in \{\{PO \mapsto pc\}, \{PO \mapsto pa\}, \{PO \mapsto cc\}\}$

end

Event PedalAssist ⟨ordinary⟩ $\widehat{=}$

refines PedalAssist

when

grd1:

$status = \{PO\} \lor$

$(status = \{CC\} \land beforecc = \{PA\})$

status∈ ℙ (STATUS)\{{PA},{PC},{BRAKE},{UNDEFINED}}

then

act1: $status := \{PA\}$

act2: $engrun := TRUE$

act3: $useraction := \{PO \mapsto pa, CC \mapsto ccc\}$

end

Event PedalOnly ⟨ordinary⟩ $\widehat{=}$

refines PedalOnly

when

grd1:

$status = \{PA\} \lor status = \{PC\} \lor$

$(status = \{CC\} \land beforecc = \{PO\})$

status∈ ℙ (STATUS)\{{PO},{BRAKE},{UNDEFINED}}

then

act1: $status := \{PO\}$

act2: $engrun := FALSE$

act3: $useraction := \{PA \mapsto pac, CC \mapsto ccc, PC \mapsto pcc\}$

end

Event PedalOnly2CruiseControl ⟨ordinary⟩ $\widehat{=}$

refines PedalOnly2CruiseControl

any

s

where

grd1: $s = PO$

grd2: $status \in \{\{PO\}\}$

then

act1: $status := \{CC\}$

act2: $beforecc := \{PO\}$

act3: $engrun := TRUE$

act4: $useraction(s) := cc$

end

Event PedalAssist2CruiseControl ⟨ordinary⟩ $\widehat{=}$

refines PedalAssist2CruiseControl

any

s

where

grd1: $s = PA$

grd2: $status \in \{\{PA\}\}$

then

act1: $status := \{CC\}$

act2: $beforecc := \{PA\}$

act3: $engrun := TRUE$

act4: $useraction(s) := cc$

end

Event PedalCharge ⟨ordinary⟩ $\widehat{=}$

refines PedalCharge

any

s

where

grd1: $s = PO$

grd2: $status \in \{\{PO\}\}$

then

act1: $status := \{PC\}$

act2: $engrun := TRUE$

act3: $useraction(s) := pc$

end

Event Brake ⟨ordinary⟩ $\widehat{=}$

refines Brake

any

s

where

grd1: $s \in STATUS \setminus \{CC, BRAKE, UNDEFINED\}$

grd2: $status = \{PO\} \lor status = \{PA\} \lor status = \{PC\}$

status∈ ℙ (STATUS)\{{CC},{BRAKE},{UNDEFINED}}

then

act1: $status := \{BRAKE\}$

act2: $engrun := FALSE$

act3: $useraction(s) := br$

end

Event BrakeCruiseControl2PedalOnly ⟨ordinary⟩ $\widehat{=}$

refines BrakeCruiseControl2PedalOnly

any

s

where

grd1: $s = CC \land beforecc = \{PO\}$

grd2: $status \in \{\{CC\}\}$

then

act1: $status := \{PO\}$

act2: $engrun := FALSE$

act3: $useraction(s) := br$

end

Event BrakeCruiseControl2PedalAssist ⟨ordinary⟩ $\widehat{=}$

refines BrakeCruiseControl2PedalAssist

any

s

where

grd1: $s = CC \land beforecc = \{PA\}$

grd2: $status \in \{\{CC\}\}$

then

act1: $status := \{PA\}$

```
            act2: $engrun := TRUE$
            act3: $useraction(s) := br$
      end
END
```