

MACHINE Cm0

This model contains the following abstract events:

- Moving connected and non ambiguous trains (2 events)
- Disconnecting connected and non ambiguous trains (2 events)
- Reconnecting disconnected trains (1 event)
- Introducing ghosts and ambiguous trains (2 events)
- Moving ambiguous trains (4 events)

Some events are missing for the disconnection of ambiguous trains

SEES Cc0

VARIABLES

frontv
 rearv
 FREEV
 OCCUPIEDV
 UNKNOWNV
 AMBIGUOUSV
 UNKNOWNV
 CONNECTED
 DISCONNECTED
 GHOST
 FREET
 OCCUPIEDT
 NOTRAIN
 lastU
 AMBTRAIN

INVARIANTS

- inv1:** *partition*(1 .. *maxtt*, *FREET*, *OCCUPIEDT*)
 TTD sections
 incompatibilities
- inv2:**
partition(1 .. *maxvss*, *FREEV*,
OCCUPIEDV, *UNKNOWNV*, *AMBIGUOUSV*,
UNKNOWNV)
 VSS incompatibilities. Notice the
 distinction between unknown VSS:
 those resulting from a
 disconnection (*UNKNOWNV*) and
 those resulting from a ghost
 trains (*UNKNOWNV*)
- inv3:**
partition(*TRAIN*, *CONNECTED*, *DISCONNECTED*,
GHOST, *NOTRAIN*)
 Train incompatibilities
- inv4:** *frontv* ∈ *CONNECTED* ∪ *DISCONNECTED* → 1 .. *maxvss*
 front end VSS
- inv5:** *rearv* ∈ *CONNECTED* ∪ *DISCONNECTED* → 1 .. *maxvss*
 rear end VSS
- inv6:**
 $\forall t. t \in \text{CONNECTED} \cup \text{DISCONNECTED}$
 \Rightarrow
 $\text{rearv}(t) \leq \text{frontv}(t)$
 Rear end VSS is smaller than or
 equal to the front end VSS for
 connected or disconnected trains
- inv7:** *AMBTRAIN* ⊆ *CONNECTED*
 An ambiguous train is a connected train

inv8:
 $\forall t. t \in \text{CONNECTED} \setminus \text{AMBTRAIN}$
 \Rightarrow
 $\text{rearv}(t) .. \text{frontv}(t) \subseteq \text{OCCUPIEDV}$
VSS of a connected
train are all occupied

inv9:
 $\forall t. t \in \text{AMBTRAIN}$
 \Rightarrow
 $\text{rearv}(t) .. \text{frontv}(t) \subseteq \text{AMBIGUOUSV}$
VSS of an ambiguous train
are all ambiguous

inv10:
 $\forall t. t \in \text{DISCONNECTED}$
 \Rightarrow
 $\text{rearv}(t) .. \text{frontv}(t) \subseteq \text{UNKNOWNV}$
VSS of a disconnected
train are all unknown

inv11: $\text{ttdv}[\text{OCCUPIEDV}] \subseteq \text{OCCUPIEDT}$
TTD sections of occupied VSS
are occupied

inv12: $\text{ttdv}^{-1}[\text{FREET}] \subseteq \text{FREEV}$
VSS of free TTD sections are free

inv13:
 $\forall t1, t2. t1 \in \text{CONNECTED} \cup \text{DISCONNECTED} \wedge$
 $t2 \in \text{CONNECTED} \cup \text{DISCONNECTED} \wedge$
 $t1 \neq t2$
 \Rightarrow
 $(\text{rearv}(t1) .. \text{frontv}(t1)) \cap$
 $(\text{rearv}(t2) .. \text{frontv}(t2)) = \emptyset$
connected or disconnected
trains do not overlap.
This safety property is
assumed in this case study.

inv14: $\text{lastU} \in \text{DISCONNECTED} \rightarrow 1 .. \text{maxvss}$
Last VSS which is made UNKNOWNV
when disconnecting

inv15:
 $\forall t. t \in \text{DISCONNECTED}$
 \Rightarrow
 $\text{lastU}(t) \geq \text{frontv}(t)$
This last VSS is greater then or equal
to the front end VSS of the disconnected
train. Equality occurs when no VSS are
made unknown besides those which were
occupied by the connected train before
disconnection

inv16:
 $\forall t. t \in \text{DISCONNECTED}$
 \Rightarrow
 $\text{frontv}(t) + 1 .. \text{lastU}(t) \subseteq \text{UNKNOWNV}$
VSS made unknown in a
disconnection besides those
which were occupied

inv17:
 $\forall t1, t2. t1 \in \text{DISCONNECTED} \wedge$
 $t2 \in \text{DISCONNECTED} \wedge$
 $t1 \neq t2$

\Rightarrow
 $rearv(t1) \dots frontv(t1) \cap$
 $frontv(t2) + 1 \dots lastU(t2) = \emptyset$
 Some incompatibilities between
 disconnected trains
inv18:
 $\forall t1, t2 \cdot t1 \in DISCONNECTED \wedge$
 $t2 \in DISCONNECTED \wedge$
 $t1 \neq t2$
 \Rightarrow
 $frontv(t1) + 1 \dots lastU(t1) \cap$
 $frontv(t2) + 1 \dots lastU(t2) = \emptyset$
 More incompatibilities between
 disconnected trains
inv19:
 $\forall tr, t \cdot tr \in AMBTRAIN \wedge$
 $t = ttdv(rearv(tr))$
 \Rightarrow
 $t > 1 \wedge$
 $t - 1 \in OCCUPIEDT \wedge$
 $ttdv^{-1}[\{t - 1\}] \subseteq UNKNOWNNG \wedge$
 $minvsst(t) \dots rearv(tr) - 1 \subseteq UNKNOWNNG$
 Properties of ambiguous
 trains
inv20: <theorem>
 $\forall tr \cdot tr \in CONNECTED \wedge$
 $rearv(tr) \dots frontv(tr) \subseteq OCCUPIEDV$
 \Rightarrow
 $tr \notin AMBTRAIN$
inv21:
 $\forall tr, t \cdot tr \in AMBTRAIN \wedge$
 $t \in DISCONNECTED$
 \Rightarrow
 $minvsst(ttdv(rearv(tr))) \dots rearv(tr) - 1 \cap$
 $rearv(t) \dots lastU(t) = \emptyset$
inv22:
 $\forall tr, t \cdot tr \in AMBTRAIN \wedge$
 $t \in DISCONNECTED$
 \Rightarrow
 $ttdv^{-1}[\{ttdv(rearv(tr)) - 1\}] \cap$
 $rearv(t) \dots lastU(t) = \emptyset$
inv23: $ttdv[AMBIGUOUSV] \subseteq OCCUPIEDT$
 TTD sections of ambiguous
 trains are all occupied
inv24:
 $\forall t1, t2 \cdot t1 \in AMBTRAIN \wedge$
 $t2 \in AMBTRAIN \wedge$
 $t1 \neq t2$
 \Rightarrow
 $ttdv(rearv(t1)) \neq ttdv(rearv(t2))$
inv25:
 $\forall t1, t2 \cdot t1 \in AMBTRAIN \wedge$
 $t2 \in AMBTRAIN \wedge$
 $t1 \neq t2$
 \Rightarrow
 $ttdv(rearv(t1)) - 1 \neq ttdv(rearv(t2))$

EVENTS

Initialisation

begin

act1: $FREET := 1 .. maxttd$
 TTD sections are all free initially
 act2: $OCCUPIEDT := \emptyset$
 act3: $CONNECTED := \emptyset$
 act4: $DISCONNECTED := \emptyset$
 act5: $GHOST := \emptyset$
 act6: $NOTRAIN := TRAIN$
 No trains initially
 act7: $FREEV := 1 .. maxvss$
 VSS are all free initially
 act8: $OCCUPIEDV := \emptyset$
 act9: $AMBIGUOUSV := \emptyset$
 act10: $UNKNOWNV := \emptyset$
 act11: $frontv := \emptyset$
 act12: $rearv := \emptyset$
 act13: $lastU := \emptyset$
 act14: $AMBTRAIN := \emptyset$
 act15: $UNKNOWNNG := \emptyset$

end

Event move_non_ambtrain_1 *(ordinary)* $\hat{=}$

Abstract move of a connected and
 non ambiguous train.

Parameters: u, newrear, newfront

Here newrear \leq frontv(u)

any

u
 newrear
 newfront

where

grd1: $u \in CONNECTED \setminus AMBTRAIN$
 grd2: $newrear \in 1 .. maxvss$
 grd3: $newfront \in 1 .. maxvss$
 grd4: $newfront \geq frontv(u)$
 grd5: $frontv(u) + 1 .. newfront \subseteq FREEV$
 grd6: $newrear \geq rearv(u)$
 grd7: $newrear \leq newfront$
 grd8: $ttdv[frontv(u) + 1 .. newfront] \subseteq OCCUPIEDT$
 grd9: $newrear \leq frontv(u)$
 grd10: *(theorem)* $newrear .. newfront = (newrear .. frontv(u)) \cup (frontv(u) + 1 .. newfront)$

then

act1: $frontv(u) := newfront$
 act2: $rearv(u) := newrear$
 act3:
 $OCCUPIEDV := (OCCUPIEDV \setminus rearv(u) .. newrear - 1) \cup$
 $(frontv(u) + 1 .. newfront)$
 act4:
 $FREEV := (FREEV \setminus frontv(u) + 1 .. newfront) \cup$
 $(rearv(u) .. newrear - 1)$

end

Event move_non_ambtrain_2 *(ordinary)* $\hat{=}$

Abstract move of a connected and
 non ambiguous train.

Parameters: u, newrear, newfront

Here newrear $>$ frontv(u)

any

u
 newrear
 newfront

where

grd1: $u \in \text{CONNECTED} \setminus \text{AMBTRAIN}$
 grd2: $\text{newrear} \in 1 \dots \text{maxvss}$
 grd3: $\text{newfront} \in 1 \dots \text{maxvss}$
 grd4: $\text{newfront} \geq \text{frontv}(u)$
 grd5: $\text{frontv}(u) + 1 \dots \text{newfront} \subseteq \text{FREEV}$
 grd6: $\text{newrear} \geq \text{rearv}(u)$
 grd7: $\text{newrear} \leq \text{newfront}$
 grd8: $\text{ttv}[\text{frontv}(u) + 1 \dots \text{newfront}] \subseteq \text{OCCUPIEDT}$
 grd9: $\text{newrear} > \text{frontv}(u)$

then

act1: $\text{frontv}(u) := \text{newfront}$
 act2: $\text{rearv}(u) := \text{newrear}$
 act3:
 $\text{OCCUPIEDV} := (\text{OCCUPIEDV} \setminus \text{rearv}(u) \dots \text{frontv}(u)) \cup$
 $(\text{newrear} \dots \text{newfront})$
 act4:
 $\text{FREEV} := (\text{FREEV} \setminus \text{newrear} \dots \text{newfront}) \cup$
 $(\text{rearv}(u) \dots \text{frontv}(u))$

end

Event disconnect_1 *<ordinary>* $\hat{=}$

Abstract disconnection (no mute timer)
 We suppose that the disconnected train
 is not an ambiguous train. Another
 event is needed for ambiguous train
 disconnection

any

t
 S

where

grd1: $t \in \text{CONNECTED} \setminus \text{AMBTRAIN}$
 grd2: $S = \{v \mid v \in 1 \dots \text{maxvss} \wedge v > \text{frontv}(t) \wedge (v \notin \text{FREEV} \vee \text{ttv}(v) \in \text{FREET})\}$
 grd3: $S \neq \emptyset$
 grd4: *<theorem>* $\text{rearv}(t) \dots \text{frontv}(t) \subseteq \text{OCCUPIEDV}$
 grd5: *<theorem>* $\text{frontv}(t) + 1 \dots \min(S) - 1 \subseteq \text{FREEV}$

then

act1: $\text{UNKNOWNV} := \text{UNKNOWNV} \cup \text{rearv}(t) \dots \text{frontv}(t) \cup \text{frontv}(t) + 1 \dots \min(S) - 1$
 act2: $\text{OCCUPIEDV} := \text{OCCUPIEDV} \setminus \text{rearv}(t) \dots \text{frontv}(t)$
 act3: $\text{FREEV} := \text{FREEV} \setminus \text{frontv}(t) + 1 \dots \min(S) - 1$
 act4: $\text{CONNECTED} := \text{CONNECTED} \setminus \{t\}$
 act5: $\text{DISCONNECTED} := \text{DISCONNECTED} \cup \{t\}$
 act6: $\text{lastU}(t) := \min(S) - 1$

end

Event disconnect_2 *<ordinary>* $\hat{=}$

Abstract disconnection (no mute timer)
 We suppose that the disconnected train
 is not an ambiguous train. Another
 event is needed for ambiguous train
 disconnection

any

t

where

grd1: $t \in \text{CONNECTED} \setminus \text{AMBTRAIN}$
 grd2: $\{v \mid v \in 1 \dots \text{maxvss} \wedge v > \text{frontv}(t) \wedge (v \notin \text{FREEV} \vee \text{ttv}(v) \in \text{FREET})\} = \emptyset$
 grd3: *<theorem>* $\text{rearv}(t) \dots \text{frontv}(t) \subseteq \text{OCCUPIEDV}$

then

act1: $\text{UNKNOWNV} := \text{UNKNOWNV} \cup \text{rearv}(t) \dots \text{frontv}(t)$
 act2: $\text{OCCUPIEDV} := \text{OCCUPIEDV} \setminus \text{rearv}(t) \dots \text{frontv}(t)$
 act3: $\text{CONNECTED} := \text{CONNECTED} \setminus \{t\}$

```

    act4: DISCONNECTED := DISCONNECTED  $\cup$  {t}
    act5: lastU(t) := frontv(t)
end
Event reconnect  $\langle$ ordinary $\rangle \hat{=}$ 
    Reconnection re-establishes the situation
    when the train was disconnected.
    We suppose that the disconnected train is
    still on the TTD section where it was
    before disconnection
    any
        t
    where
        grd1: t  $\in$  DISCONNECTED
        grd2: ttdv[rearv(t) .. frontv(t)]  $\subseteq$  OCCUPIEDT
            Probably not always true when reconnecting.
            It means that the disconnected train has
            not moved too much. It has not left any of
            the TTD sections where it was when
            disconnection has occurred.
            Another event is necessary for ambiguous
            train reconnection.
    then
        act1: DISCONNECTED := DISCONNECTED  $\setminus$  {t}
        act2: CONNECTED := CONNECTED  $\cup$  {t}
        act3: OCCUPIEDV := OCCUPIEDV  $\cup$  rearv(t) .. frontv(t)
        act4: UNKNOWNV := UNKNOWNV  $\setminus$  rearv(t) .. lastU(t)
        act5: FREEV := FREEV  $\cup$  frontv(t) + 1 .. lastU(t)
        act6: lastU := {t}  $\triangleleft$  lastU
    end
Event ghost_1  $\langle$ ordinary $\rangle \hat{=}$ 
    A ghost appears in TTD section t.
    t is free.
    Next TTD section (if any) is free.
    We just make all VSS of t be unknown
    any
        t
    where
        grd1: t  $\in$  FREET
            t is free.
        grd2: t < maxttd  $\Rightarrow$  t + 1  $\in$  FREET
            Next TTD section (if any) is free.
    then
        act1: UNKNOWNV := UNKNOWNV  $\cup$  ttdv-1{t}
        act2: FREEV := FREEV  $\setminus$  ttdv-1{t}
        act3: FREET := FREET  $\setminus$  {t}
        act4: OCCUPIEDT := OCCUPIEDT  $\cup$  {t}
    end
Event ghost_2  $\langle$ ordinary $\rangle \hat{=}$ 
    A ghost appears in TTD section t
    t is free.
    t is not the last TTD section
    Next TTD section is occupied
    There exists a train tr which is connected
    and non ambiguous. The rear end of tr is in
    the next TTD section (t+1). VSS before the
    rear end of tr in t+1 are all free.
    We make all VSS of t be unknown.
    We make all VSS of tr be ambiguous.
    We make VSS in t+1 before the rear end of tr

```

be unknown. tr becomes an ambiguous train.

Another event is needed when a train such

as tr does not exist in $t+1$

any

t

tr

where

grd1: $t \in FREET$

t is free

grd2: $t < maxttd$

t is not the last TTD section

grd3: $t + 1 \in OCCUPIEDT$

Next TTD section is occupied

grd4: $tr \in CONNECTED \setminus AMBTRAIN$

There exists a train tr which is connected and not ambiguous

grd5: $ttdv(rearv(tr)) = t + 1$

The rear end of tr is in $t+1$

grd6: $\langle \text{theorem} \rangle ttdv^{-1}[\{t\}] \subseteq FREEV$

grd7: $minvsst(t + 1) .. rearv(tr) - 1 \subseteq FREEV$

VSS before the rear end of tr in $t+1$ are all free

grd8: $\langle \text{theorem} \rangle ttdv^{-1}[\{t\}] \cup minvsst(t + 1) .. rearv(tr) - 1 \subseteq FREEV$

grd9: $\langle \text{theorem} \rangle ttdv^{-1}[\{t\}] \cap minvsst(t + 1) .. rearv(tr) - 1 = \emptyset$

then

act1: $UNKNOWNNG := UNKNOWNNG \cup (ttdv^{-1}[\{t\}] \cup minvsst(t + 1) .. rearv(tr) - 1)$

act2: $FREEV := FREEV \setminus (ttdv^{-1}[\{t\}] \cup minvsst(t + 1) .. rearv(tr) - 1)$

act3: $FREET := FREET \setminus \{t\}$

act4: $OCCUPIEDT := OCCUPIEDT \cup \{t\}$

act5: $AMBIGUOUSV := AMBIGUOUSV \cup rearv(tr) .. frontv(tr)$

act6: $OCCUPIEDV := OCCUPIEDV \setminus rearv(tr) .. frontv(tr)$

act7: $AMBTRAIN := AMBTRAIN \cup \{tr\}$

end

Event move_ambtrain_1 $\langle \text{ordinary} \rangle \hat{=}$

Abstract move of an ambiguous train

Parameters: u , newrear, newfront

Here $ttdv(newrear) = ttdv(rearv(u))$

and $newrear \leq frontv(u)$

any

u

newrear

newfront

where

grd1: $u \in AMBTRAIN$

grd2: $newrear \in 1 .. maxvss$

grd3: $newfront \in 1 .. maxvss$

grd4: $newfront \geq frontv(u)$

grd5: $frontv(u) + 1 .. newfront \subseteq FREEV$

grd6: $newrear \geq rearv(u)$

grd7: $newrear \leq newfront$

grd8: $ttdv[frontv(u) .. newfront] \subseteq OCCUPIEDT$

grd9: $ttdv(newrear) = ttdv(rearv(u))$

grd10: $newrear \leq frontv(u)$

then

act1: $frontv(u) := newfront$

act2: $rearv(u) := newrear$

act3:

$AMBIGUOUSV := (AMBIGUOUSV \setminus rearv(u) .. newrear - 1) \cup$
 $(frontv(u) + 1 .. newfront)$

act4: $FREEV := FREEV \setminus (frontv(u) + 1 .. newfront)$

act5: $UNKNOWNNG := UNKNOWNNG \cup (rearv(u) .. newrear - 1)$

end

Event move_ambtrain_2 *<ordinary>* $\hat{=}$

Abstract move of an ambiguous train

Parameters: u , newrear, newfront

Here $ttdv(newrear) = ttdv(rearv(u))$

and $newrear > frontv(u)$

any

u

newrear

newfront

where

grd1: $u \in AMBTRAIN$

grd2: $newrear \in 1 .. maxvss$

grd3: $newfront \in 1 .. maxvss$

grd4: $newfront \geq frontv(u)$

grd5: $frontv(u) + 1 .. newfront \subseteq FREEV$

grd6: $newrear \geq rearv(u)$

grd7: $newrear \leq newfront$

grd8: $ttdv[frontv(u) .. newfront] \subseteq OCCUPIEDT$

grd9: $ttdv(newrear) = ttdv(rearv(u))$

grd10: $newrear > frontv(u)$

then

act1: $frontv(u) := newfront$

act2: $rearv(u) := newrear$

act3:

$AMBIGUOUSV := (AMBIGUOUSV \setminus rearv(u) .. frontv(u)) \cup$
 $(newrear .. newfront)$

act4: $FREEV := FREEV \setminus (frontv(u) + 1 .. newfront)$

act5: $UNKNOWNNG := UNKNOWNNG \cup (rearv(u) .. newrear - 1)$

end

Event move_ambtrain_3 *<ordinary>* $\hat{=}$

Abstract move of an ambiguous train

Parameters: u , newrear, newfront

Here $ttdv(newrear) > ttdv(rearv(u))$

and $newrear \leq frontv(u)$

any

u

newrear

newfront

where

grd1: $u \in AMBTRAIN$

grd15: *<theorem>* $AMBTRAIN \subseteq CONNECTED$

grd2: $newrear \in 1 .. maxvss$

grd3: $newfront \in 1 .. maxvss$

grd4: $newfront \geq frontv(u)$

grd5: $frontv(u) + 1 .. newfront \subseteq FREEV$

grd6: $newrear \geq rearv(u)$

grd7: $newrear \leq newfront$

grd8: $ttdv[frontv(u) .. newfront] \subseteq OCCUPIEDT$

grd9: $ttdv(newrear) > ttdv(rearv(u))$

grd10: $newrear \leq frontv(u)$

grd11: $ttdv(newrear) \in FREET$

grd12: *<theorem>* $minvsst(ttdv(rearv(u))) .. newrear - 1 = minvsst(ttdv(rearv(u))) .. rearv(u) -$
 $1 \cup rearv(u) .. newrear - 1$

grd13: *<theorem>* $newrear .. newfront = newrear .. frontv(u) \cup frontv(u) + 1 .. newfront$

grd14: *<theorem>* $rearv(u) .. frontv(u) = rearv(u) .. newrear - 1 \cup newrear .. frontv(u)$

then

act1: $UNKNOWNNG := UNKNOWNNG \setminus minvsst(ttdv(rearv(u))) .. rearv(u) - 1$

act2: $AMBIGUOUSV := AMBIGUOUSV \setminus rearv(u) .. frontv(u)$


```

act3:  $FREEV := (FREEV \setminus frontv(u) + 1 .. newfront) \cup minvsst(tdv(rearv(u))) .. newrear - 1$ 
act4:  $OCCUPIEDV := OCCUPIEDV \cup newrear .. newfront$ 
act5:  $AMBTRAIN := AMBTRAIN \setminus \{u\}$ 
act6:  $frontv(u) := newfront$ 
act7:  $rearv(u) := newrear$ 

end

Event move_ambtrain_4 ⟨ordinary⟩  $\hat{=}$ 
  Abstract move of an ambiguous train
  Parameters: u, newrear, newfront
  Here  $ttdv(newrear) > ttdv(rearv(u))$ 
  and  $newrear > frontv(u)$ 
  any
    u
    newrear
    newfront
  where
    grd1:  $u \in AMBTRAIN$ 
    grd15: ⟨theorem⟩  $AMBTRAIN \subseteq CONNECTED$ 
    grd2:  $newrear \in 1 .. maxvss$ 
    grd3:  $newfront \in 1 .. maxvss$ 
    grd4:  $newfront \geq frontv(u)$ 
    grd5:  $frontv(u) + 1 .. newfront \subseteq FREEV$ 
    grd6:  $newrear \geq rearv(u)$ 
    grd7:  $newrear \leq newfront$ 
    grd8:  $ttdv[frontv(u) .. newfront] \subseteq OCCUPIEDT$ 
    grd9:  $ttdv(newrear) > ttdv(rearv(u))$ 
    grd10:  $newrear > frontv(u)$ 
    grd12: ⟨theorem⟩
       $minvsst(tdv(rearv(u))) .. frontv(u) =$ 
       $minvsst(tdv(rearv(u))) .. rearv(u) - 1 \cup rearv(u) .. frontv(u)$ 
  then
    act1:  $UNKNOWN := UNKNOWN \setminus minvsst(tdv(rearv(u))) .. rearv(u) - 1$ 
    act2:  $AMBIGUOUSV := AMBIGUOUSV \setminus rearv(u) .. frontv(u)$ 
    act3:  $FREEV := (FREEV \setminus newrear .. newfront) \cup minvsst(tdv(rearv(u))) .. frontv(u)$ 
    act4:  $OCCUPIEDV := OCCUPIEDV \cup newrear .. newfront$ 
    act5:  $AMBTRAIN := AMBTRAIN \setminus \{u\}$ 
    act6:  $frontv(u) := newfront$ 
    act7:  $rearv(u) := newrear$ 
  end
END

```