Gear Controller Case-study (Time Added by the Improved Plugin)

Table of Contents

Context c0

CONTEXT
c0
CONSTANTS
ChangeDL
AXIOMS
axm1 :ChangeDL > 0
END

Context c1

CONTEXT
c1
EXTENDS
c0
CONSTANTS
R_TN *// ToNeu Releasing deadline*
R_NN *// NoNeu Releasing deadline*
S_NN *// NoNeu Setting deadline after a normal releasing process*
S_NN_RC *// NoNeu Setting deadline with opened clutch during releasing process*
S_FN *// FromNeu Setting deadline*
R_NN_NC_EX *// NoNeu Releasing without clutch expiry (500)*
AXIOMS
axm1 :R_TN > 0
axm2 :R_NN> 0
axm3 :S_NN> 0
axm4 :S_NN_RC > 0
axm5 :R_TN> 0
axm6 :R_TN ≤ ChangeDL
axm7 :R_NN + S_NN_RC ≤ ChangeDL
axm8 :R_NN_NC_EX + S_NN ≤ ChangeDL
axm9 :S_FN≤ ChangeDL
axm10 :S_FN> 0
END

Context c2

CONTEXT
c2
EXTENDS
c1
CONSTANTS
SyncOpen_DL *// 355*
SetGear_DL *// 350*
CloseClutch_DL *// 200*
Sync_EX *// 150*
AXIOMS
axm1 :SyncOpen_DL > 0
axm2 :SetGear_DL > 0
axm3 :CloseClutch_DL > 0
axm4 :SyncOpen_DL + SetGear_DL + CloseClutch_DL ≤ S_FN
axm5 :Sync_EX > 0
axm6 :Sync_EX ≤ SyncOpen_DL
END

Context c3

CONTEXT
c3
EXTENDS
c2
CONSTANTS
ZeroOpen_DL *// 455*
Release_DL *// 250*
Zero_EX *// 250*
AXIOMS
axm1 :ZeroOpen_DL > 0
axm2 :Release_DL >0
axm3 :ZeroOpen_DL + Release_DL + CloseClutch_DL ≤ R_TN

axm4 :Zero_EX >0
axm5 :Zero_EX ≤ ZeroOpen_DL
END

Context c4

CONTEXT
c4
EXTENDS
c3
AXIOMS
axm2 :Zero_EX + Release_DL ≤ R_NN_NC_EX
axm3 :ZeroOpen_DL + Release_DL + CloseClutch_DL ≤ R_NN
axm4 :SyncOpen_DL + SetGear_DL + CloseClutch_DL ≤ S_NN
axm5 :SetGear_DL + CloseClutch_DL ≤ S_NN_RC
END

Context c5

CONTEXT
c5
EXTENDS
c4
CONSTANTS
Zero_DL *// 155*
OpenClutch_DL *// 200*
Sync_DL *// 255*
OpenClutch_Zero_DE *// 250*
OpenClutch_Sync_DE *// 150*
AXIOMS
axm1 :Zero_DL > 0
axm2 :OpenClutch_DL > 0
axm3 :Zero_DL + OpenClutch_DL ≤ ZeroOpen_DL
axm4 :Sync_DL > 0
axm5 :Sync_DL + OpenClutch_DL ≤ SyncOpen_DL
axm6 :Zero_DL ≥ Zero_EX
axm7 :Sync_DL ≥ Sync_EX
axm8 :OpenClutch_Zero_DE > 0
axm9 :OpenClutch_Sync_DE > 0
axm10 :OpenClutch_Zero_DE > Zero_EX
axm11 :OpenClutch_Sync_DE > Sync_EX
axm12 :OpenClutch_Zero_DE ≤ Zero_DL
axm13 :OpenClutch_Sync_DE ≤ Sync_DL
END

Context c6

CONTEXT
c6
EXTENDS
c5
CONSTANTS
Channel_DL *// 5*
Engine_Sync_DL *// 100*
Engine_Zero_DL *// 200*
Clutch_Open_DL *// 150*
Clutch_Close_DL *// 150*
Gear_Set_DL *// 300*
Gear_Release_DL *// 200*
AXIOMS
axm1 :Channel_DL > 0
axm2 :Engine_Sync_DL > 0
axm3 :Engine_Zero_DL > 0
axm4 :2∗Channel_DL + Engine_Sync_DL ≤ Sync_EX
axm5 :2∗Channel_DL + Engine_Zero_DL ≤ Zero_EX
axm6 :Clutch_Open_DL > 0
axm7 :Clutch_Close_DL > 0
axm8 :2∗Channel_DL + Clutch_Open_DL < OpenClutch_DL
axm9 :2∗Channel_DL + Clutch_Close_DL < CloseClutch_DL
axm10 :Gear_Set_DL > 0

```
    axm11 :Gear_Release_DL >0
    axm12 :2∗Channel_DL + Gear_Set_DL < SetGear_DL
    axm13 :2∗Channel_DL + Gear_Release_DL < Release_DL
END
```

Machine m0

MACHINE

m0 // *Deadline(Request, Response ∨ Error, ChangingDL)*

SEES

c0

VARIABLES

Request
Response
Error // *Flags*
time
tRequest
tError
tResponse

INVARIANTS

inv1 : Request ∈ BOOL
inv2 : Error ∈ BOOL
inv3 : Response ∈ BOOL
time : time∈ℕ
tRequest : tRequest ∈ ℕ
tError : tError ∈ ℕ
tResponse : tResponse ∈ ℕ

TIMING

Deadline1 : Deadline (Request, Error ∨ Response, ChangeDL)

EVENTS

INITIALISATION ≙
STATUS
ordinary

BEGIN
act1 : Error ≔FALSE
act2 : Request ≔FALSE
act3 : Response ≔FALSE
time : time ≔0
tRequest : tRequest ≔ 0
tError : tError ≔ 0
tResponse : tResponse ≔ 0
END

Request ≙
STATUS
ordinary

WHEN
grd1 : Request = FALSE
THEN
act1 : Request ≔ TRUE
tRequest : tRequest ≔time
END

Response ≙
STATUS
ordinary

WHEN
grd1 : Request = TRUE
grd2 : Error = FALSE
grd3 : Response = FALSE
THEN
act1 : Response ≔ TRUE
tResponse : tResponse ≔time

```
END

    Error ≜
        STATUS
      ordinary
WHEN
      grd1  :  Error = FALSE
      grd2  :  Request = TRUE
      grd3  :  Response = FALSE
THEN
      act1  :  Error ≔ TRUE
      tError  :  tError ≔time
END

    FINAL ≜
        STATUS
      ordinary
WHEN
      grd1  :  Response = TRUE
THEN
      act1  :  Request ≔ FALSE
      act2  :  Response ≔ FALSE
END

    Tick_Tock ≜
        STATUS
      ordinary
ANY
      tick
WHERE
      tick  :  tick > 0
      Deadline1  :  Request = TRUE ∧ Error = FALSE ∧ Response = FALSE ⇒ time + tick ≤ tRequest + Change
                    DL
THEN
      act1  :  time ≔time+tick
END

END
```

Machine m1

MACHINE

m1

// *Deadline(RequestFromNeu, FromNeu ∨ Error_FromNeu, ChangingDL)*
// *Deadline(RequestNoNeu, NoNeu ∨ Error_NoNeu, ChangingDL)*
// *Deadline(RequestToNeu, ToNeu ∨ Error_ToNeu, ChangingDL)*

REFINES

m0

SEES

c0

VARIABLES

RequestFromNeu
RequestNoNeu
RequestToNeu
FromNeu // *Changing from the neutral gear to a gear*
ToNeu // *Changing from a gear to another gear*
NoNeu // *Changing from a gear to the neutral gear*
Error_FromNeu // *Flags*
Error_NoNeu
Error_ToNeu // *Flags*
isNeu // *Gear Status*
time
tRequestFromNeu
tError_FromNeu
tFromNeu
tRequestNoNeu
tError_NoNeu
tNoNeu
tRequestToNeu
tError_ToNeu
tToNeu

INVARIANTS

inv1 : {ToNeu, FromNeu, NoNeu, isNeu, RequestFromNeu, RequestNoNeu, RequestToNeu, Error_FromNeu, Error_NoNeu, Error_ToNeu} ∈ ℙ(BOOL)
inv2 : (FromNeu = TRUE ∨ ToNeu = TRUE ∨ NoNeu = TRUE) ⇒ Response = TRUE
inv3 : (FromNeu = FALSE ∧ ToNeu = FALSE ∧ NoNeu = FALSE) ⇒ Response = FALSE
inv4 : (RequestFromNeu = TRUE ∨ RequestNoNeu = TRUE ∨ RequestToNeu = TRUE) ⇒ Request = TRUE
inv5 : (RequestFromNeu = FALSE ∧ RequestNoNeu = FALSE ∧ RequestToNeu = FALSE) ⇒ Request = FALSE
inv6 : RequestFromNeu = TRUE ⇒RequestToNeu = FALSE ∧ RequestNoNeu = FALSE
inv7 : RequestToNeu = TRUE ⇒RequestFromNeu = FALSE ∧ RequestNoNeu = FALSE
inv8 : RequestNoNeu = TRUE ⇒RequestFromNeu = FALSE ∧ RequestToNeu = FALSE
inv9 : RequestNoNeu = TRUE ⇒ ToNeu = FALSE ∧ FromNeu = FALSE
inv10 : RequestToNeu = TRUE ⇒ FromNeu = FALSE ∧ NoNeu = FALSE
inv11 : RequestFromNeu = TRUE ⇒ ToNeu = FALSE ∧ NoNeu = FALSE
inv12 : NoNeu = TRUE ⇒ RequestNoNeu = TRUE
inv13 : FromNeu = TRUE ⇒ RequestFromNeu = TRUE
// *@inv16 RequestFromNeu= TRUE ⇒RequestFromNeuT = RequestT*
inv14 : ToNeu = TRUE ⇒ RequestToNeu = TRUE
// *@inv17 RequestNoNeu= TRUE ⇒RequestNoNeuT = RequestT*
// *@inv18 RequestToNeu= TRUE ⇒RequestToNeuT = RequestT*
inv15 : Error_FromNeu = TRUE ∨ Error_NoNeu = TRUE ∨ Error_ToNeu = TRUE ⇒ Error = TRUE
inv16 : Error_FromNeu = FALSE ∧ Error_NoNeu = FALSE ∧ Error_ToNeu= FALSE ⇒ Error = FALSE
inv17 : Error_FromNeu = TRUE ⇒ RequestFromNeu= TRUE
inv18 : Error_NoNeu = TRUE ⇒ RequestNoNeu= TRUE

inv19 : Error_ToNeu = TRUE ⇒ RequestToNeu= TRUE
inv20 : RequestFromNeu= TRUE ⇒ Error_NoNeu = FALSE ∧ Error_ToNeu = FALSE
inv21 : RequestNoNeu= TRUE ⇒ Error_FromNeu = FALSE ∧ Error_ToNeu = FALSE
inv22 : RequestToNeu= TRUE ⇒ Error_FromNeu = FALSE ∧ Error_NoNeu = FALSE
inv23 : FromNeu = TRUE ⇒ RequestFromNeu= TRUE
inv24 : NoNeu = TRUE ⇒ RequestNoNeu= TRUE
inv25 : ToNeu = TRUE ⇒ RequestToNeu= TRUE
inv26 : RequestFromNeu= TRUE ⇒ NoNeu = FALSE ∧ ToNeu = FALSE
inv27 : RequestNoNeu= TRUE ⇒ FromNeu = FALSE ∧ ToNeu = FALSE
inv28 : RequestToNeu= TRUE ⇒ FromNeu = FALSE ∧ NoNeu = FALSE
inv29 : FromNeu = TRUE ⇒ Error_FromNeu = FALSE
inv30 : NoNeu = TRUE ⇒ Error_NoNeu = FALSE
inv31 : ToNeu = TRUE ⇒ Error_ToNeu = FALSE
inv32 : FromNeu = TRUE ∨ ToNeu = TRUE ∨ NoNeu = TRUE ⇒ Error = FALSE
tRequestFromNeu : tRequestFromNeu ∈ ℕ
tError_FromNeu : tError_FromNeu ∈ ℕ
tFromNeu : tFromNeu ∈ ℕ
abstractRequestFromNeu : RequestFromNeu = TRUE ⇒ tRequestFromNeu = tRequest
tRequestNoNeu : tRequestNoNeu ∈ ℕ
tError_NoNeu : tError_NoNeu ∈ ℕ
tNoNeu : tNoNeu ∈ ℕ
abstractRequestNoNeu : RequestNoNeu = TRUE ⇒ tRequestNoNeu = tRequest
tRequestToNeu : tRequestToNeu ∈ ℕ
tError_ToNeu : tError_ToNeu ∈ ℕ
tToNeu : tToNeu ∈ ℕ
abstractRequestToNeu : RequestToNeu = TRUE ⇒ tRequestToNeu = tRequest

TIMING

Deadline1 : Deadline (RequestFromNeu, Error_FromNeu ∨ FromNeu, ChangeDL)
Deadline2 : Deadline (RequestNoNeu, Error_NoNeu ∨ NoNeu, ChangeDL)
Deadline3 : Deadline (RequestToNeu, Error_ToNeu ∨ ToNeu, ChangeDL)

EVENTS

INITIALISATION ≙
STATUS
ordinary

BEGIN
act1 : ToNeu ≔ FALSE
act2 : FromNeu ≔ FALSE
act3 : NoNeu ≔ FALSE
act4 : isNeu ≔ TRUE
act5 : RequestNoNeu ≔ FALSE
act6 : RequestToNeu ≔ FALSE
act7 : RequestFromNeu ≔ FALSE
act8 : Error_FromNeu ≔ FALSE
act9 : Error_NoNeu ≔ FALSE
act10 : Error_ToNeu ≔ FALSE
time : time ≔ 0
tRequestFromNeu : tRequestFromNeu ≔ 0
tError_FromNeu : tError_FromNeu ≔ 0
tFromNeu : tFromNeu ≔ 0
tRequestNoNeu : tRequestNoNeu ≔ 0
tError_NoNeu : tError_NoNeu ≔ 0
tNoNeu : tNoNeu ≔ 0
tRequestToNeu : tRequestToNeu ≔ 0
tError_ToNeu : tError_ToNeu ≔ 0
tToNeu : tToNeu ≔ 0
END

RequestFromNeu ≙
STATUS
ordinary

```
REFINES
        Request
WHEN
        grd1   :   RequestFromNeu = FALSE
        grd2   :   RequestNoNeu = FALSE
        grd3   :   RequestToNeu = FALSE
        grd4   :   isNeu = TRUE
THEN
        act1   :   RequestFromNeu ≔ TRUE
        tRequestFromNeu   :   tRequestFromNeu ≔time
END

      RequestNoNeu   ≙
            STATUS
        ordinary
REFINES
        Request
WHEN
        grd1   :   RequestFromNeu = FALSE
        grd2   :   RequestNoNeu = FALSE
        grd3   :   RequestToNeu = FALSE
        grd4   :   isNeu = FALSE
THEN
        act1   :   RequestNoNeu ≔ TRUE
        tRequestNoNeu   :   tRequestNoNeu ≔time
END

      RequestToNeu   ≙
            STATUS
        ordinary
REFINES
        Request
WHEN
        grd1   :   RequestFromNeu = FALSE
        grd2   :   RequestNoNeu = FALSE
        grd3   :   RequestToNeu = FALSE
        grd4   :   isNeu = FALSE
THEN
        act1   :   RequestToNeu ≔ TRUE
        tRequestToNeu   :   tRequestToNeu ≔time
END

      FromNeu   ≙
            STATUS
        ordinary
REFINES
        Response
WHEN
        grd1   :   RequestFromNeu = TRUE
        grd2   :   Error_FromNeu = FALSE
        grd3   :   FromNeu = FALSE
THEN
        act1   :   FromNeu ≔ TRUE
        act2   :   isNeu ≔ FALSE
        tFromNeu   :   tFromNeu ≔time
END

      NoNeu   ≙
            STATUS
        ordinary
REFINES
```

```
        Response
WHEN
        grd1  :  RequestNoNeu = TRUE
        grd2  :  Error_NoNeu = FALSE
        grd3  :  NoNeu = FALSE
THEN
        act1  :  NoNeu ≔ TRUE
        tNoNeu  :  tNoNeu ≔time
END

    ToNeu  ≙
        STATUS
        ordinary
REFINES
        Response
WHEN
        grd1  :  RequestToNeu = TRUE
        grd2  :  Error_ToNeu = FALSE
        grd3  :  ToNeu = FALSE
THEN
        act1  :  ToNeu ≔ TRUE
        act2  :  isNeu ≔ TRUE
        tToNeu  :  tToNeu ≔time
END

    Error_FromNeu  ≙
        STATUS
        ordinary
REFINES
        Error
WHEN
        grd1  :  Error_FromNeu = FALSE
        grd2  :  RequestFromNeu = TRUE
        grd3  :  FromNeu = FALSE
THEN
        act1  :  Error_FromNeu ≔ TRUE
        tError_FromNeu  :  tError_FromNeu ≔time
END

    Error_NoNeu  ≙
        STATUS
        ordinary
REFINES
        Error
WHEN
        grd1  :  Error_NoNeu = FALSE
        grd2  :  RequestNoNeu = TRUE
        grd3  :  NoNeu = FALSE
THEN
        act1  :  Error_NoNeu ≔ TRUE
        tError_NoNeu  :  tError_NoNeu ≔time
END

    Error_ToNeu  ≙
        STATUS
        ordinary
REFINES
        Error
WHEN
        grd1  :  Error_ToNeu = FALSE
        grd2  :  RequestToNeu = TRUE
```

```
        grd3  :  ToNeu = FALSE
THEN
        act1  :  Error_ToNeu ≔ TRUE
        tError_ToNeu  :  tError_ToNeu ≔time
END

    FINAL  ≙
        STATUS
        ordinary
REFINES
        FINAL
WHEN
        grd1  :  FromNeu = TRUE ∨    ToNeu = TRUE ∨    NoNeu = TRUE
THEN
        act1  :  RequestFromNeu ≔ FALSE
        act2  :  RequestNoNeu ≔ FALSE
        act3  :  RequestToNeu ≔ FALSE
        act4  :  FromNeu ≔ FALSE
        act5  :  ToNeu ≔ FALSE
        act6  :  NoNeu ≔ FALSE
END

    Tick_Tock  ≙
        STATUS
        ordinary
REFINES
        Tick_Tock
ANY
        tick
WHERE
        tick  :  tick > 0
        Deadline1  RequestFromNeu = TRUE ∧ Error_FromNeu = FALSE ∧ FromNeu = FALSE ⇒ time + tick ≤ tR
          :          equestFromNeu + ChangeDL
        Deadline2  RequestNoNeu = TRUE ∧ Error_NoNeu = FALSE ∧ NoNeu = FALSE ⇒ time + tick ≤ tRequest
        :            NoNeu + ChangeDL
        Deadline3  RequestToNeu = TRUE ∧ Error_ToNeu = FALSE ∧ ToNeu = FALSE ⇒ time + tick ≤ tRequest
        :            ToNeu + ChangeDL
THEN
        act1  :  time ≔time+tick
END

END
```

Machine m2

MACHINE

m2 // Deadline(RequestFromNeu, FromNeuNoClutch ∨ FromNeuClutch ∨ Error_FromNeu, ChangingDL)
// Deadline(RequestNoNeu, NoNeuNoClutch ∨ NoNeuClutch ∨ Error_NoNeu, ChangingDL)
// Deadline(RequestToNeu, ToNeuNoClutch ∨ ToNeuClutch ∨ Error_ToNeu, ChangingDL)

REFINES

m1

SEES

c0

VARIABLES

RequestFromNeu
RequestNoNeu
RequestToNeu
FromNeuNoClutch
NoNeuClutch // Flags
ToNeuNoClutch
NoNeuNoClutch
FromNeuClutch
ToNeuClutch // nextline
Error_FromNeu // Flags
Error_NoNeu // Flage
Error_ToNeu // Flags
isNeu // Gear Status
time
tRequestFromNeu
tError_FromNeu
tFromNeuClutch
tFromNeuNoClutch
tRequestNoNeu
tError_NoNeu
tNoNeuClutch
tNoNeuNoClutch
tRequestToNeu
tError_ToNeu
tToNeuClutch
tToNeuNoClutch

INVARIANTS

inv1 : FromNeuClutch ∈ BOOL
inv2 : FromNeuNoClutch ∈ BOOL
inv3 : ToNeuNoClutch ∈ BOOL
inv4 : ToNeuClutch ∈ BOOL
inv5 : NoNeuNoClutch ∈ BOOL
inv6 : NoNeuClutch ∈ BOOL
inv7 : FromNeuNoClutch = TRUE ∨ FromNeuClutch = TRUE ⇔FromNeu = TRUE
inv8 : ToNeuNoClutch = TRUE ∨ ToNeuClutch = TRUE ⇔ToNeu = TRUE
inv9 : NoNeuNoClutch = TRUE ∨ NoNeuClutch = TRUE ⇔NoNeu = TRUE
inv10 : FromNeuNoClutch = FALSE ∧ FromNeuClutch = FALSE ⇔FromNeu = FALSE
inv11 : ToNeuNoClutch = FALSE ∧ ToNeuClutch = FALSE ⇔ToNeu = FALSE
inv12 : NoNeuNoClutch = FALSE ∧ NoNeuClutch = FALSE ⇔NoNeu = FALSE
tFromNeuClutch : tFromNeuClutch ∈ ℕ
tFromNeuNoClutch : tFromNeuNoClutch ∈ ℕ
tNoNeuClutch : tNoNeuClutch ∈ ℕ
tNoNeuNoClutch : tNoNeuNoClutch ∈ ℕ
tToNeuClutch : tToNeuClutch ∈ ℕ
tToNeuNoClutch : tToNeuNoClutch ∈ ℕ

TIMING

Deadline1 : Deadline (RequestFromNeu, Error_FromNeu ∨ FromNeuClutch ∨ FromNeuNoClutch, Change DL)
Deadline2 : Deadline (RequestNoNeu, Error_NoNeu ∨ NoNeuClutch ∨ NoNeuNoClutch, ChangeDL)
Deadline3 : Deadline (RequestToNeu, Error_ToNeu ∨ ToNeuClutch ∨ ToNeuNoClutch, ChangeDL)

EVENTS

INITIALISATION ≙
STATUS
ordinary
BEGIN
act1 : ToNeuNoClutch ≔FALSE
act2 : FromNeuNoClutch ≔FALSE
act3 : NoNeuNoClutch ≔FALSE
act4 : ToNeuClutch ≔FALSE
act5 : FromNeuClutch ≔FALSE
act6 : NoNeuClutch ≔FALSE
act7 : RequestNoNeu ≔FALSE
act8 : RequestToNeu ≔FALSE
act9 : RequestFromNeu ≔FALSE
act10 : isNeu ≔TRUE
act11 : Error_FromNeu ≔FALSE
act12 : Error_NoNeu ≔FALSE
act13 : Error_ToNeu ≔FALSE
time : time ≔0
tRequestFromNeu : tRequestFromNeu ≔ 0
tError_FromNeu : tError_FromNeu ≔ 0
tFromNeuClutch : tFromNeuClutch ≔ 0
tFromNeuNoClutch : tFromNeuNoClutch ≔ 0
tRequestNoNeu : tRequestNoNeu ≔ 0
tError_NoNeu : tError_NoNeu ≔ 0
tNoNeuClutch : tNoNeuClutch ≔ 0
tNoNeuNoClutch : tNoNeuNoClutch ≔ 0
tRequestToNeu : tRequestToNeu ≔ 0
tError_ToNeu : tError_ToNeu ≔ 0
tToNeuClutch : tToNeuClutch ≔ 0
tToNeuNoClutch : tToNeuNoClutch ≔ 0
END

RequestFromNeu ≙
STATUS
ordinary
REFINES
RequestFromNeu
WHEN
grd1 : RequestFromNeu = FALSE
grd2 : RequestNoNeu = FALSE
grd3 : RequestToNeu = FALSE
grd4 : isNeu = TRUE
THEN
act1 : RequestFromNeu ≔ TRUE
tRequestFromNeu : tRequestFromNeu ≔time
END

RequestNoNeu ≙
STATUS
ordinary
REFINES
RequestNoNeu
WHEN
grd1 : RequestFromNeu = FALSE
grd2 : RequestNoNeu = FALSE
grd3 : RequestToNeu = FALSE
grd4 : isNeu = FALSE

```
THEN
        act1  :  RequestNoNeu ≔ TRUE
        tRequestNoNeu  :  tRequestNoNeu ≔time
END

    RequestToNeu  ≙
        STATUS
        ordinary
REFINES
        RequestToNeu
WHEN
        grd1  :  RequestFromNeu = FALSE
        grd2  :  RequestNoNeu = FALSE
        grd3  :  RequestToNeu = FALSE
        grd4  :  isNeu = FALSE
THEN
        act1  :  RequestToNeu ≔ TRUE
        tRequestToNeu  :  tRequestToNeu ≔time
END

    FromNeuNoClutch  ≙
        STATUS
        ordinary
REFINES
        FromNeu
WHEN
        grd1  :  RequestFromNeu = TRUE
        grd2  :  Error_FromNeu = FALSE
        grd3  :  FromNeuNoClutch = FALSE
        grd4  :  FromNeuClutch = FALSE
THEN
        act1  :  FromNeuNoClutch ≔ TRUE
        act2  :  isNeu ≔ FALSE
        tFromNeuNoClutch  :  tFromNeuNoClutch ≔time
END

    NoNeuNoClutch  ≙
        STATUS
        ordinary
REFINES
        NoNeu
WHEN
        grd1  :  RequestNoNeu = TRUE
        grd2  :  Error_NoNeu = FALSE
        grd3  :  NoNeuNoClutch = FALSE
        grd4  :  NoNeuClutch = FALSE
THEN
        act1  :  NoNeuNoClutch ≔ TRUE
        tNoNeuNoClutch  :  tNoNeuNoClutch ≔time
END

    ToNeuNoClutch  ≙
        STATUS
        ordinary
REFINES
        ToNeu
WHEN
        grd1  :  RequestToNeu = TRUE
        grd2  :  Error_ToNeu = FALSE
        grd3  :  ToNeuNoClutch = FALSE
        grd4  :  ToNeuClutch = FALSE
```

```
THEN
        act1  :  ToNeuNoClutch ≔ TRUE
        act2  :  isNeu ≔ TRUE
        tToNeuNoClutch  :  tToNeuNoClutch ≔time
END

    FromNeuClutch  ≙
        STATUS
        ordinary
REFINES
        FromNeu
WHEN
        grd1  :  RequestFromNeu = TRUE
        grd2  :  Error_FromNeu = FALSE
        grd3  :  FromNeuClutch = FALSE
        grd4  :  FromNeuNoClutch = FALSE
THEN
        act1  :  FromNeuClutch ≔ TRUE
        act2  :  isNeu ≔ FALSE
        tFromNeuClutch  :  tFromNeuClutch ≔time
END

    NoNeuClutch  ≙
        STATUS
        ordinary
REFINES
        NoNeu
WHEN
        grd1  :  RequestNoNeu = TRUE
        grd2  :  Error_NoNeu = FALSE
        grd3  :  NoNeuClutch = FALSE
        grd4  :  NoNeuNoClutch = FALSE
THEN
        act1  :  NoNeuClutch ≔ TRUE
        tNoNeuClutch  :  tNoNeuClutch ≔time
END

    ToNeuClutch  ≙
        STATUS
        ordinary
REFINES
        ToNeu
WHEN
        grd1  :  RequestToNeu = TRUE
        grd2  :  Error_ToNeu = FALSE
        grd3  :  ToNeuClutch = FALSE
        grd4  :  ToNeuNoClutch = FALSE
THEN
        act1  :  ToNeuClutch ≔ TRUE
        act2  :  isNeu ≔ TRUE
        tToNeuClutch  :  tToNeuClutch ≔time
END

    Error_FromNeu  ≙
        STATUS
        ordinary
REFINES
        Error_FromNeu
WHEN
        grd1  :  Error_FromNeu = FALSE
        grd2  :  RequestFromNeu = TRUE
```

```
        grd3  :  FromNeuClutch = FALSE
        grd4  :  FromNeuNoClutch = FALSE
THEN
        act1  :  Error_FromNeu ≔ TRUE
        tError_FromNeu  :  tError_FromNeu ≔time
END

    Error_NoNeu  ≜
        STATUS
        ordinary
REFINES
        Error_NoNeu
WHEN
        grd1  :  Error_NoNeu = FALSE
        grd2  :  RequestNoNeu = TRUE
        grd3  :  NoNeuClutch = FALSE
        grd4  :  NoNeuNoClutch = FALSE
THEN
        act1  :  Error_NoNeu ≔ TRUE
        tError_NoNeu  :  tError_NoNeu ≔time
END

    Error_ToNeu  ≜
        STATUS
        ordinary
REFINES
        Error_ToNeu
WHEN
        grd1  :  Error_ToNeu = FALSE
        grd2  :  RequestToNeu = TRUE
        grd3  :  ToNeuClutch = FALSE
        grd4  :  ToNeuNoClutch = FALSE
THEN
        act1  :  Error_ToNeu ≔ TRUE
        tError_ToNeu  :  tError_ToNeu ≔time
END

    FINAL  ≜
        STATUS
        ordinary
REFINES
        FINAL
WHEN
        grd1  :  FromNeuNoClutch = TRUE ∨  ToNeuNoClutch = TRUE ∨  NoNeuNoClutch = TRUE ∨
                 FromNeuClutch = TRUE ∨  ToNeuClutch = TRUE ∨  NoNeuClutch = TRUE
THEN
        act1  :  RequestFromNeu ≔ FALSE
        act2  :  RequestNoNeu ≔ FALSE
        act3  :  RequestToNeu ≔ FALSE
        act4  :  FromNeuNoClutch ≔ FALSE
        act5  :  ToNeuNoClutch ≔ FALSE
        act6  :  NoNeuNoClutch ≔ FALSE
        act7  :  FromNeuClutch ≔ FALSE
        act8  :  ToNeuClutch ≔ FALSE
        act9  :  NoNeuClutch ≔ FALSE
END

    Tick_Tock  ≜
        STATUS
        ordinary
REFINES
```

```
        Tick_Tock
ANY
        tick
WHERE
        tick   :   tick > 0
        Deadlin  RequestFromNeu = TRUE ∧ Error_FromNeu = FALSE ∧ FromNeuClutch = FALSE ∧ FromNeuN
        e1   :      oClutch = FALSE ⇒ time + tick ≤ tRequestFromNeu + ChangeDL
        Deadline RequestNoNeu = TRUE ∧ Error_NoNeu = FALSE ∧ NoNeuClutch = FALSE ∧ NoNeuNoClutch
        2   :        = FALSE ⇒ time + tick ≤ tRequestNoNeu + ChangeDL
        Deadline RequestToNeu = TRUE ∧ Error_ToNeu = FALSE ∧ ToNeuClutch = FALSE ∧ ToNeuNoClutch =
        3   :         FALSE ⇒ time + tick ≤ tRequestToNeu + ChangeDL
THEN
        act1   :   time ≔time+tick
END

END
```

Machine m3

MACHINE

m3

// Deadline(RequestFromNeu, Setting_FromNeu_NoClutch ∨ Setting_FromNeu_Clutch ∨ Error_FromNeu, ChangingDL)

// Deadline(RequestNoNeu, Setting_NoNeu_ReleaseClutch ∨ Setting_NoNeu_NoClutch ∨ Setting_NoNeu_Clutch

// Error_Releasing_NoNeu ∨ Error_Setting_NoNeu, ChangingDL)

// Deadline(RequestToNeu, Releasing_ToNeu_NoClutch ∨ Releasing_ToNeu_Clutch ∨ Error_ToNeu, ChangingDL)

REFINES

m2

SEES

c0

VARIABLES

isNeu *// Gear Status*
RequestFromNeu
RequestNoNeu
RequestToNeu
Setting_NoNeu_NoClutch *// Flags*
Setting_FromNeu_NoClutch
Releasing_ToNeu_NoClutch
Releasing_NoNeu_NoClutch *// Flags*
Setting_FromNeu_Clutch
Releasing_ToNeu_Clutch
Releasing_NoNeu_Clutch *// Flags*
Setting_NoNeu_Clutch
Setting_NoNeu_ReleaseClutch *// Flags*
Error_FromNeu *// Flags*
Error_Releasing_NoNeu *// Flage*
Error_Setting_NoNeu *// Flage*
Error_ToNeu *// Flags*
time
tRequestFromNeu
tError_FromNeu
tSetting_FromNeu_Clutch
tSetting_FromNeu_NoClutch
tRequestToNeu
tError_ToNeu
tReleasing_ToNeu_Clutch
tReleasing_ToNeu_NoClutch
tRequestNoNeu
tError_Releasing_NoNeu
tError_Setting_NoNeu
tSetting_NoNeu_Clutch
tSetting_NoNeu_NoClutch
tSetting_NoNeu_ReleaseClutch

INVARIANTS

{Setting_FromNeu_Clutch, Releasing_ToNeu_Clutch, Releasing_NoNeu_Clutch, Setting_NoNeu_Clutch,

inv1 : Setting_NoNeu_ReleaseClutch, Releasing_ToNeu_NoClutch, Releasing_NoNeu_NoClutch, Setting_NoNeu_NoClutch,

Setting_FromNeu_NoClutch, Error_FromNeu ,Error_Releasing_NoNeu ,Error_Setting_NoNeu,Error_ToNeu} ∈ ℙ(BOOL)

inv2 : Setting_FromNeu_NoClutch = TRUE ⇔FromNeuNoClutch = TRUE

inv3 : Setting_NoNeu_NoClutch = TRUE ⇔NoNeuNoClutch = TRUE

inv4 : Releasing_ToNeu_NoClutch = TRUE ⇔ToNeuNoClutch = TRUE

inv5 : Setting_FromNeu_Clutch = TRUE ⇔FromNeuClutch = TRUE

inv6 : Setting_NoNeu_Clutch = TRUE ∨ Setting_NoNeu_ReleaseClutch = TRUE ⇔NoNeuClutch = TRUE

inv7 : Releasing_ToNeu_Clutch = TRUE ⇔ToNeuClutch = TRUE
inv8 : Releasing_NoNeu_NoClutch =TRUE ∨ Releasing_NoNeu_Clutch =TRUE ⇒ RequestNoNeu = TRUE
inv9 : Releasing_NoNeu_NoClutch =TRUE ⇒ Releasing_NoNeu_Clutch =FALSE
inv10 : Releasing_NoNeu_Clutch =TRUE ⇒ Releasing_NoNeu_NoClutch =FALSE
inv11 : Setting_NoNeu_Clutch = TRUE ∨ Setting_NoNeu_NoClutch = TRUE ⇒ Releasing_NoNeu_NoClutch = TRUE
inv12 : Setting_NoNeu_ReleaseClutch = TRUE ⇒ Releasing_NoNeu_Clutch = TRUE
inv13 : Error_Releasing_NoNeu = FALSE ∧ Error_Setting_NoNeu = FALSE ⇒ Error_NoNeu = FALSE
inv14 : Error_Releasing_NoNeu = TRUE ∨ Error_Setting_NoNeu = TRUE ⇒ Error_NoNeu = TRUE
inv15 : Releasing_NoNeu_Clutch = TRUE ∨ Releasing_NoNeu_NoClutch = TRUE ⇒ Error_Releasing_NoNeu = FALSE
inv16 : RequestNoNeu = TRUE ∧ Releasing_NoNeu_Clutch = FALSE ∧ Releasing_NoNeu_NoClutch = FALSE ⇒ Error_Setting_NoNeu = FALSE
tSetting_FromNeu_Clutch : tSetting_FromNeu_Clutch ∈ ℕ
tSetting_FromNeu_NoClutch : tSetting_FromNeu_NoClutch ∈ ℕ
tReleasing_ToNeu_Clutch : tReleasing_ToNeu_Clutch ∈ ℕ
tReleasing_ToNeu_NoClutch : tReleasing_ToNeu_NoClutch ∈ ℕ
tError_Releasing_NoNeu : tError_Releasing_NoNeu ∈ ℕ
tError_Setting_NoNeu : tError_Setting_NoNeu ∈ ℕ
tSetting_NoNeu_Clutch : tSetting_NoNeu_Clutch ∈ ℕ
tSetting_NoNeu_NoClutch : tSetting_NoNeu_NoClutch ∈ ℕ
tSetting_NoNeu_ReleaseClutch : tSetting_NoNeu_ReleaseClutch ∈ ℕ

TIMING

Deadline1 : Deadline (RequestFromNeu, Error_FromNeu ∨ Setting_FromNeu_Clutch ∨ Setting_FromNeu_NoClutch, ChangeDL)
Deadline2 : Deadline (RequestToNeu, Error_ToNeu ∨ Releasing_ToNeu_Clutch ∨ Releasing_ToNeu_NoClutch, ChangeDL)
Deadline3 : Deadline (RequestNoNeu, Error_Releasing_NoNeu ∨ Error_Setting_NoNeu ∨ Setting_NoNeu_Clutch ∨ Setting_NoNeu_NoClutch ∨ Setting_NoNeu_ReleaseClutch, ChangeDL)

EVENTS

INITIALISATION ≙
STATUS
ordinary

BEGIN

act1 : isNeu ≔TRUE
act2 : RequestNoNeu ≔FALSE
act3 : RequestToNeu ≔FALSE
act4 : RequestFromNeu ≔FALSE
act5 : Releasing_ToNeu_NoClutch ≔FALSE
act6 : Setting_FromNeu_NoClutch ≔FALSE
act7 : Releasing_NoNeu_NoClutch ≔FALSE
act8 : Setting_NoNeu_NoClutch ≔FALSE
act9 : Releasing_ToNeu_Clutch ≔FALSE
act10 : Setting_FromNeu_Clutch ≔FALSE
act11 : Releasing_NoNeu_Clutch ≔FALSE
act12 : Setting_NoNeu_Clutch ≔FALSE
act13 : Setting_NoNeu_ReleaseClutch ≔FALSE
act14 : Error_FromNeu ≔FALSE
act15 : Error_Releasing_NoNeu≔ FALSE
act16 : Error_Setting_NoNeu≔ FALSE
act17 : Error_ToNeu≔ FALSE
time : time ≔0
tRequestFromNeu : tRequestFromNeu ≔ 0
tError_FromNeu : tError_FromNeu ≔ 0
tSetting_FromNeu_Clutch : tSetting_FromNeu_Clutch ≔ 0
tSetting_FromNeu_NoClutch : tSetting_FromNeu_NoClutch ≔ 0
tRequestToNeu : tRequestToNeu ≔ 0
tError_ToNeu : tError_ToNeu ≔ 0
tReleasing_ToNeu_Clutch : tReleasing_ToNeu_Clutch ≔ 0
tReleasing_ToNeu_NoClutch : tReleasing_ToNeu_NoClutch ≔ 0

```
        tRequestNoNeu  :  tRequestNoNeu ≔ 0
        tError_Releasing_NoNeu  :  tError_Releasing_NoNeu ≔ 0
        tError_Setting_NoNeu  :  tError_Setting_NoNeu ≔ 0
        tSetting_NoNeu_Clutch  :  tSetting_NoNeu_Clutch ≔ 0
        tSetting_NoNeu_NoClutch  :  tSetting_NoNeu_NoClutch ≔ 0
        tSetting_NoNeu_ReleaseClutch  :  tSetting_NoNeu_ReleaseClutch ≔ 0
END

    RequestFromNeu  ≙
        STATUS
        ordinary
REFINES
        RequestFromNeu
WHEN
        grd1  :  RequestFromNeu = FALSE
        grd2  :  RequestNoNeu = FALSE
        grd3  :  RequestToNeu = FALSE
        grd4  :  isNeu = TRUE
THEN
        act1  :  RequestFromNeu ≔ TRUE
        tRequestFromNeu  :  tRequestFromNeu ≔time
END

    RequestNoNeu  ≙
        STATUS
        ordinary
REFINES
        RequestNoNeu
WHEN
        grd1  :  RequestFromNeu = FALSE
        grd2  :  RequestNoNeu = FALSE
        grd3  :  RequestToNeu = FALSE
        grd4  :  isNeu = FALSE
THEN
        act1  :  RequestNoNeu ≔ TRUE
        tRequestNoNeu  :  tRequestNoNeu ≔time
END

    RequestToNeu  ≙
        STATUS
        ordinary
REFINES
        RequestToNeu
WHEN
        grd1  :  RequestFromNeu = FALSE
        grd2  :  RequestNoNeu = FALSE
        grd3  :  RequestToNeu = FALSE
        grd4  :  isNeu = FALSE
THEN
        act1  :  RequestToNeu ≔ TRUE
        tRequestToNeu  :  tRequestToNeu ≔time
END

    Setting_FromNeu_NoClutch  ≙
        STATUS
        ordinary
REFINES
        FromNeuNoClutch
WHEN
        grd1  :  RequestFromNeu = TRUE
        grd2  :  Error_FromNeu = FALSE
        grd3  :  Setting_FromNeu_NoClutch = FALSE
```

```
        grd4  :  Setting_FromNeu_Clutch = FALSE
THEN
        act1  :  Setting_FromNeu_NoClutch ≔ TRUE
        act2  :  isNeu ≔ FALSE
        tSetting_FromNeu_NoClutch  :  tSetting_FromNeu_NoClutch ≔time
END

    Setting_FromNeu_Clutch  ≙
        STATUS
        ordinary
REFINES
        FromNeuClutch
WHEN
        grd1  :  RequestFromNeu = TRUE
        grd2  :  Error_FromNeu = FALSE
        grd3  :  Setting_FromNeu_Clutch = FALSE
        grd4  :  Setting_FromNeu_NoClutch = FALSE
THEN
        act1  :  Setting_FromNeu_Clutch ≔ TRUE
        act2  :  isNeu ≔ FALSE
        tSetting_FromNeu_Clutch  :  tSetting_FromNeu_Clutch ≔time
END

    Releasing_NoNeu_NoClutch  ≙
        STATUS
        ordinary
WHEN
        grd1  :  RequestNoNeu = TRUE
        grd2  :  Error_Releasing_NoNeu = FALSE
        grd3  :  Releasing_NoNeu_NoClutch = FALSE
        grd4  :  Releasing_NoNeu_Clutch = FALSE
THEN
        act1  :  Releasing_NoNeu_NoClutch ≔ TRUE
END

    Releasing_NoNeu_Clutch  ≙
        STATUS
        ordinary
WHEN
        grd1  :  RequestNoNeu = TRUE
        grd2  :  Error_Releasing_NoNeu = FALSE
        grd3  :  Releasing_NoNeu_Clutch = FALSE
        grd4  :  Releasing_NoNeu_NoClutch = FALSE
THEN
        act1  :  Releasing_NoNeu_Clutch ≔ TRUE
END

    Setting_NoNeu_NoClutch  ≙
        STATUS
        ordinary
REFINES
        NoNeuNoClutch
WHEN
        grd1  :  Releasing_NoNeu_NoClutch = TRUE
        grd2  :  Error_Setting_NoNeu = FALSE
        grd3  :  Setting_NoNeu_NoClutch = FALSE
        grd4  :  Setting_NoNeu_Clutch = FALSE
THEN
        act1  :  Setting_NoNeu_NoClutch ≔ TRUE
        tSetting_NoNeu_NoClutch  :  tSetting_NoNeu_NoClutch ≔time
END
```

```
    Setting_NoNeu_Clutch  ≙
        STATUS
      ordinary
REFINES
      NoNeuClutch
WHEN
      grd1  :  Releasing_NoNeu_NoClutch = TRUE
      grd2  :  Error_Setting_NoNeu = FALSE
      grd3  :  Setting_NoNeu_Clutch = FALSE
      grd4  :  Setting_NoNeu_NoClutch = FALSE
THEN
      act1  :  Setting_NoNeu_Clutch ≔ TRUE
      tSetting_NoNeu_Clutch  :  tSetting_NoNeu_Clutch ≔time
END

    Setting_NoNeu_ReleaseClutch  ≙
        STATUS
      ordinary
REFINES
      NoNeuClutch
WHEN
      grd1  :  Releasing_NoNeu_Clutch = TRUE
      grd2  :  Error_Setting_NoNeu = FALSE
      grd3  :  Setting_NoNeu_ReleaseClutch = FALSE
THEN
      act1  :  Setting_NoNeu_ReleaseClutch ≔ TRUE
      tSetting_NoNeu_ReleaseClutch  :  tSetting_NoNeu_ReleaseClutch ≔time
END

    Releasing_ToNeu_NoClutch  ≙
        STATUS
      ordinary
REFINES
      ToNeuNoClutch
WHEN
      grd1  :  RequestToNeu = TRUE
      grd2  :  Error_ToNeu = FALSE
      grd3  :  Releasing_ToNeu_NoClutch = FALSE
      grd4  :  Releasing_ToNeu_Clutch = FALSE
THEN
      act1  :  Releasing_ToNeu_NoClutch ≔ TRUE
      act2  :  isNeu ≔ TRUE
      tReleasing_ToNeu_NoClutch  :  tReleasing_ToNeu_NoClutch ≔time
END

    Releasing_ToNeu_Clutch  ≙
        STATUS
      ordinary
REFINES
      ToNeuClutch
WHEN
      grd1  :  RequestToNeu = TRUE
      grd2  :  Error_ToNeu = FALSE
      grd3  :  Releasing_ToNeu_Clutch = FALSE
      grd4  :  Releasing_ToNeu_NoClutch = FALSE
THEN
      act1  :  Releasing_ToNeu_Clutch ≔ TRUE
      act2  :  isNeu ≔ TRUE
      tReleasing_ToNeu_Clutch  :  tReleasing_ToNeu_Clutch ≔time
END
```

```
    Error_ToNeu ≜
        STATUS
      ordinary
REFINES
      Error_ToNeu
WHEN
      grd1  :  Error_ToNeu = FALSE
      grd2  :  RequestToNeu = TRUE
      grd3  :  Releasing_ToNeu_NoClutch = FALSE
      grd4  :  Releasing_ToNeu_Clutch = FALSE
THEN
      act1  :  Error_ToNeu ≔ TRUE
      tError_ToNeu  :  tError_ToNeu ≔time
END

    Error_Releasing_NoNeu ≜
        STATUS
      ordinary
REFINES
      Error_NoNeu
WHEN
      grd1  :  Error_Releasing_NoNeu = FALSE
      grd2  :  RequestNoNeu = TRUE
      grd3  :  Releasing_NoNeu_Clutch = FALSE
      grd4  :  Releasing_NoNeu_NoClutch = FALSE
THEN
      act1  :  Error_Releasing_NoNeu ≔ TRUE
      tError_Releasing_NoNeu  :  tError_Releasing_NoNeu ≔time
END

    Error_Setting_NoNeu ≜
        STATUS
      ordinary
REFINES
      Error_NoNeu
WHEN
      grd1  :  Error_Setting_NoNeu = FALSE
      grd2  :  Releasing_NoNeu_Clutch = TRUE ∨ Releasing_NoNeu_NoClutch = TRUE
      grd3  :  Setting_NoNeu_NoClutch = FALSE
      grd4  :  Setting_NoNeu_Clutch = FALSE
      grd5  :  Setting_NoNeu_ReleaseClutch = FALSE
THEN
      act1  :  Error_Setting_NoNeu ≔ TRUE
      tError_Setting_NoNeu  :  tError_Setting_NoNeu ≔time
END

    Error_FromNeu ≜
        STATUS
      ordinary
REFINES
      Error_FromNeu
WHEN
      grd1  :  Error_FromNeu = FALSE
      grd2  :  RequestFromNeu = TRUE
      grd3  :  Setting_FromNeu_NoClutch = FALSE
      grd4  :  Setting_FromNeu_Clutch = FALSE
THEN
      act1  :  Error_FromNeu ≔ TRUE
      tError_FromNeu  :  tError_FromNeu ≔time
END
```

```
    FINAL ≙
        STATUS
      ordinary
REFINES
      FINAL
WHEN
          Setting_FromNeu_NoClutch = TRUE ∨ Setting_NoNeu_NoClutch = TRUE ∨ Releasing_ToNeu_NoC
      grd1 lutch = TRUE ∨
       :          Setting_FromNeu_Clutch = TRUE ∨ Setting_NoNeu_Clutch = TRUE ∨ Setting_NoNeu_Relea
          seClutch = TRUE ∨ Releasing_ToNeu_Clutch = TRUE
THEN
      act1  :  RequestFromNeu ≔ FALSE
      act2  :  RequestNoNeu ≔ FALSE
      act3  :  RequestToNeu ≔ FALSE
      act4  :  Releasing_ToNeu_NoClutch ≔ FALSE
      act5  :  Setting_NoNeu_NoClutch ≔ FALSE
      act6  :  Setting_FromNeu_NoClutch ≔ FALSE
      act7  :  Releasing_NoNeu_NoClutch ≔FALSE
      act8  :  Releasing_ToNeu_Clutch ≔ FALSE
      act9  :  Setting_NoNeu_Clutch ≔ FALSE
      act10  :  Setting_NoNeu_ReleaseClutch ≔ FALSE
      act11  :  Setting_FromNeu_Clutch ≔ FALSE
      act12  :  Releasing_NoNeu_Clutch ≔FALSE
END

    Tick_Tock ≙
        STATUS
      ordinary
REFINES
      Tick_Tock
ANY
      tick
WHERE
      tick  :  tick > 0
      DeadlinRequestFromNeu = TRUE ∧ Error_FromNeu = FALSE ∧ Setting_FromNeu_Clutch = FALSE ∧ Set
      e1  :    ting_FromNeu_NoClutch = FALSE ⇒ time + tick ≤ tRequestFromNeu + ChangeDL
      Deadlin RequestToNeu = TRUE ∧ Error_ToNeu = FALSE ∧ Releasing_ToNeu_Clutch = FALSE ∧ Releasi
      e2  :    ng_ToNeu_NoClutch = FALSE ⇒ time + tick ≤ tRequestToNeu + ChangeDL
      Dead RequestNoNeu = TRUE ∧ Error_Releasing_NoNeu = FALSE ∧ Error_Setting_NoNeu = FALSE ∧ Se
      line3 tting_NoNeu_Clutch = FALSE ∧ Setting_NoNeu_NoClutch = FALSE ∧ Setting_NoNeu_ReleaseClutc
        :    h = FALSE ⇒ time + tick ≤ tRequestNoNeu + ChangeDL
THEN
      act1  :  time ≔time+tick
END

END
```

Machine m4

MACHINE

m4

// Deadline(RequestFromNeu, Setting_FromNeu_NoClutch ∨ Setting_FromNeu_Clutch ∨ Error_FromNeu, S_FN)

// Deadline(RequestNoNeu, Releasing_NoNeu_Clutch ∨ Releasing_NoNeu_NoClutch ∨ Error_Releasing_NoNeu, R_NN)

// Deadline(Releasing_NoNeu_NoClutch, Setting_NoNeu_NoClutch ∨ Setting_NoNeu_Clutch ∨ Error_Setting_NoNeu, S_NN)

// Deadline(Releasing_NoNeu_Clutch, Setting_NoNeu_ReleaseClutch ∨ Error_Setting_NoNeu, S_NN_RC)

// Expiry(RequestNoNeu, Releasing_NoNeu_NoClutch, R_NN_NC_EX)

// Deadline(RequestToNeu, Releasing_ToNeu_NoClutch ∨ Releasing_ToNeu_Clutch ∨ Error_ToNeu, R_TN)

REFINES

m3

SEES

c1

VARIABLES

isNeu *// Gear Status*
Setting_FromNeu_NoClutch
Releasing_ToNeu_NoClutch
Releasing_NoNeu_NoClutch *// Flags*
Setting_NoNeu_NoClutch
RequestFromNeu
RequestNoNeu
RequestToNeu
Setting_FromNeu_Clutch
Releasing_ToNeu_Clutch
Releasing_NoNeu_Clutch
Setting_NoNeu_Clutch
Setting_NoNeu_ReleaseClutch
Error_FromNeu *// Flags*
Error_Releasing_NoNeu *// Flage*
Error_Setting_NoNeu *// Flage*
Error_ToNeu *// Flags*
time
tRequestNoNeu
tError_Releasing_NoNeu
tReleasing_NoNeu_Clutch
tReleasing_NoNeu_NoClutch
tRequestFromNeu
tError_FromNeu
tSetting_FromNeu_Clutch
tSetting_FromNeu_NoClutch
tRequestToNeu
tError_ToNeu
tReleasing_ToNeu_Clutch
tReleasing_ToNeu_NoClutch
tSetting_NoNeu_Clutch
tSetting_NoNeu_NoClutch
tError_Setting_NoNeu
tSetting_NoNeu_ReleaseClutch

INVARIANTS

tReleasing_NoNeu_Clutch : tReleasing_NoNeu_Clutch ∈ ℕ
tReleasing_NoNeu_NoClutch : tReleasing_NoNeu_NoClutch ∈ ℕ
Releasing_NoNeu_ClutchDurationDeadline3 : RequestNoNeu = TRUE ∧ Releasing_NoNeu_Clutch = TRUE ⇒ tReleasing_NoNeu_Clutch ≤ tRequestNoNeu + R_NN

Releasing_NoNeu_NoClutchDurationDeadline3 : RequestNoNeu = TRUE ∧ Releasing_NoNeu_NoClutch = TRUE ⇒ tReleasing_NoNeu_NoClutch ≤ tRequestNoNeu + R_NN

Deadline3 : RequestNoNeu = TRUE ∧ Error_Releasing_NoNeu = FALSE ∧ Releasing_NoNeu_Clutch = FALSE ∧ Releasing_NoNeu_NoClutch = FALSE ⇒ time ≤ tRequestNoNeu + R_NN

Releasing_NoNeu_NoClutchDurationExpiry1 : RequestNoNeu = TRUE ∧ Releasing_NoNeu_NoClutch = TRUE ⇒ tReleasing_NoNeu_NoClutch ≤ tRequestNoNeu + R_NN_NC_EX

TIMING

Deadline3 : Deadline (RequestNoNeu, Error_Releasing_NoNeu ∨ Releasing_NoNeu_Clutch ∨ Releasing_NoNeu_NoClutch, R_NN)

Deadline4 : Deadline (RequestFromNeu, Error_FromNeu ∨ Setting_FromNeu_Clutch ∨ Setting_FromNeu_NoClutch, S_FN)

Deadline5 : Deadline (RequestToNeu, Error_ToNeu ∨ Releasing_ToNeu_Clutch ∨ Releasing_ToNeu_NoClutch, R_TN)

Expiry1 : Expiry (RequestNoNeu, Releasing_NoNeu_NoClutch, R_NN_NC_EX)

Deadline6 : Deadline (Releasing_NoNeu_NoClutch, Setting_NoNeu_Clutch ∨ Setting_NoNeu_NoClutch, S_NN)

Deadline7 : Deadline (Releasing_NoNeu_Clutch, Error_Setting_NoNeu ∨ Setting_NoNeu_ReleaseClutch, S_NN_RC)

EVENTS

INITIALISATION ≙

STATUS

ordinary

BEGIN

act1 : isNeu ≔ TRUE
act2 : RequestNoNeu ≔ FALSE
act3 : RequestToNeu ≔ FALSE
act4 : RequestFromNeu ≔ FALSE
act5 : Releasing_ToNeu_NoClutch ≔ FALSE
act6 : Setting_FromNeu_NoClutch ≔ FALSE
act7 : Releasing_NoNeu_NoClutch ≔ FALSE
act8 : Setting_NoNeu_NoClutch ≔ FALSE
act9 : Releasing_ToNeu_Clutch ≔ FALSE
act10 : Setting_FromNeu_Clutch ≔ FALSE
act11 : Releasing_NoNeu_Clutch ≔ FALSE
act12 : Setting_NoNeu_Clutch ≔ FALSE
act13 : Setting_NoNeu_ReleaseClutch ≔ FALSE
act14 : Error_FromNeu ≔ FALSE
act15 : Error_Releasing_NoNeu ≔ FALSE
act16 : Error_Setting_NoNeu ≔ FALSE
act17 : Error_ToNeu ≔ FALSE
time : time ≔ 0
tRequestNoNeu : tRequestNoNeu ≔ 0
tError_Releasing_NoNeu : tError_Releasing_NoNeu ≔ 0
tReleasing_NoNeu_Clutch : tReleasing_NoNeu_Clutch ≔ 0
tReleasing_NoNeu_NoClutch : tReleasing_NoNeu_NoClutch ≔ 0
tRequestFromNeu : tRequestFromNeu ≔ 0
tError_FromNeu : tError_FromNeu ≔ 0
tSetting_FromNeu_Clutch : tSetting_FromNeu_Clutch ≔ 0
tSetting_FromNeu_NoClutch : tSetting_FromNeu_NoClutch ≔ 0
tRequestToNeu : tRequestToNeu ≔ 0
tError_ToNeu : tError_ToNeu ≔ 0
tReleasing_ToNeu_Clutch : tReleasing_ToNeu_Clutch ≔ 0
tReleasing_ToNeu_NoClutch : tReleasing_ToNeu_NoClutch ≔ 0
tSetting_NoNeu_Clutch : tSetting_NoNeu_Clutch ≔ 0
tSetting_NoNeu_NoClutch : tSetting_NoNeu_NoClutch ≔ 0
tError_Setting_NoNeu : tError_Setting_NoNeu ≔ 0
tSetting_NoNeu_ReleaseClutch : tSetting_NoNeu_ReleaseClutch ≔ 0

END

RequestFromNeu ≙

```
        STATUS
    ordinary
REFINES
    RequestFromNeu
WHEN
    grd1  :  RequestFromNeu = FALSE
    grd2  :  RequestNoNeu = FALSE
    grd3  :  RequestToNeu = FALSE
    grd4  :  isNeu = TRUE
THEN
    act1  :  RequestFromNeu ≔ TRUE
    tRequestFromNeu  :  tRequestFromNeu ≔time
END

  RequestNoNeu  ≙
        STATUS
    ordinary
REFINES
    RequestNoNeu
WHEN
    grd1  :  RequestFromNeu = FALSE
    grd2  :  RequestNoNeu = FALSE
    grd3  :  RequestToNeu = FALSE
    grd4  :  isNeu = FALSE
THEN
    act1  :  RequestNoNeu ≔ TRUE
    tRequestNoNeu  :  tRequestNoNeu ≔time
END

  RequestToNeu  ≙
        STATUS
    ordinary
REFINES
    RequestToNeu
WHEN
    grd1  :  RequestFromNeu = FALSE
    grd2  :  RequestNoNeu = FALSE
    grd3  :  RequestToNeu = FALSE
    grd4  :  isNeu = FALSE
THEN
    act1  :  RequestToNeu ≔ TRUE
    tRequestToNeu  :  tRequestToNeu ≔time
END

  Setting_FromNeu_NoClutch  ≙
        STATUS
    ordinary
REFINES
    Setting_FromNeu_NoClutch
WHEN
    grd1  :  RequestFromNeu = TRUE
    grd2  :  Error_FromNeu = FALSE
    grd3  :  Setting_FromNeu_NoClutch = FALSE
    grd4  :  Setting_FromNeu_Clutch = FALSE
THEN
    act1  :  Setting_FromNeu_NoClutch ≔ TRUE
    act2  :  isNeu ≔ FALSE
    tSetting_FromNeu_NoClutch  :  tSetting_FromNeu_NoClutch ≔time
END

  Setting_FromNeu_Clutch  ≙
```

```
        STATUS
    ordinary
REFINES
    Setting_FromNeu_Clutch
WHEN
    grd1  :  RequestFromNeu = TRUE
    grd2  :  Error_FromNeu = FALSE
    grd3  :  Setting_FromNeu_Clutch = FALSE
    grd4  :  Setting_FromNeu_NoClutch = FALSE
THEN
    act1  :  Setting_FromNeu_Clutch ≔ TRUE
    act2  :  isNeu ≔ FALSE
    tSetting_FromNeu_Clutch  :  tSetting_FromNeu_Clutch ≔time
END

  Releasing_NoNeu_NoClutch  ≙
    extended
        STATUS
    ordinary
REFINES
    Releasing_NoNeu_NoClutch
WHEN
    grd1  :  RequestNoNeu = TRUE
    grd2  :  Error_Releasing_NoNeu = FALSE
    grd3  :  Releasing_NoNeu_NoClutch = FALSE
    grd4  :  Releasing_NoNeu_Clutch = FALSE
    Expiry1  :  time ≤ tRequestNoNeu + R_NN_NC_EX
THEN
    act1  :  Releasing_NoNeu_NoClutch ≔ TRUE
    tReleasing_NoNeu_NoClutch  :  tReleasing_NoNeu_NoClutch ≔time
END

  Releasing_NoNeu_Clutch  ≙
    extended
        STATUS
    ordinary
REFINES
    Releasing_NoNeu_Clutch
WHEN
    grd1  :  RequestNoNeu = TRUE
    grd2  :  Error_Releasing_NoNeu = FALSE
    grd3  :  Releasing_NoNeu_Clutch = FALSE
    grd4  :  Releasing_NoNeu_NoClutch = FALSE
THEN
    act1  :  Releasing_NoNeu_Clutch ≔ TRUE
    tReleasing_NoNeu_Clutch  :  tReleasing_NoNeu_Clutch ≔time
END

  Setting_NoNeu_NoClutch  ≙
        STATUS
    ordinary
REFINES
    Setting_NoNeu_NoClutch
WHEN
    grd1  :  Releasing_NoNeu_NoClutch = TRUE
    grd2  :  Error_Setting_NoNeu = FALSE
    grd3  :  Setting_NoNeu_NoClutch = FALSE
    grd4  :  Setting_NoNeu_Clutch = FALSE
THEN
    act1  :  Setting_NoNeu_NoClutch ≔ TRUE
    tSetting_NoNeu_NoClutch  :  tSetting_NoNeu_NoClutch ≔time
END
```

```
    Setting_NoNeu_Clutch  ≙
        STATUS
      ordinary
REFINES
      Setting_NoNeu_Clutch
WHEN
      grd1  :  Releasing_NoNeu_NoClutch = TRUE
      grd2  :  Error_Setting_NoNeu = FALSE
      grd3  :  Setting_NoNeu_Clutch = FALSE
      grd4  :  Setting_NoNeu_NoClutch = FALSE
THEN
      act1  :  Setting_NoNeu_Clutch ≔ TRUE
      tSetting_NoNeu_Clutch  :  tSetting_NoNeu_Clutch ≔time
END

    Setting_NoNeu_ReleaseClutch  ≙
        STATUS
      ordinary
REFINES
      Setting_NoNeu_ReleaseClutch
WHEN
      grd1  :  Releasing_NoNeu_Clutch = TRUE
      grd2  :  Error_Setting_NoNeu = FALSE
      grd3  :  Setting_NoNeu_ReleaseClutch = FALSE
THEN
      act1  :  Setting_NoNeu_ReleaseClutch ≔ TRUE
      tSetting_NoNeu_ReleaseClutch  :  tSetting_NoNeu_ReleaseClutch ≔time
END

    Releasing_ToNeu_NoClutch  ≙
        STATUS
      ordinary
REFINES
      Releasing_ToNeu_NoClutch
WHEN
      grd1  :  RequestToNeu = TRUE
      grd2  :  Error_ToNeu = FALSE
      grd3  :  Releasing_ToNeu_NoClutch = FALSE
      grd4  :  Releasing_ToNeu_Clutch = FALSE
THEN
      act1  :  Releasing_ToNeu_NoClutch ≔ TRUE
      act2  :  isNeu ≔ TRUE
      tReleasing_ToNeu_NoClutch  :  tReleasing_ToNeu_NoClutch ≔time
END

    Releasing_ToNeu_Clutch  ≙
        STATUS
      ordinary
REFINES
      Releasing_ToNeu_Clutch
WHEN
      grd1  :  RequestToNeu = TRUE
      grd2  :  Error_ToNeu = FALSE
      grd3  :  Releasing_ToNeu_Clutch = FALSE
      grd4  :  Releasing_ToNeu_NoClutch = FALSE
THEN
      act1  :  Releasing_ToNeu_Clutch ≔ TRUE
      act2  :  isNeu ≔ TRUE
      tReleasing_ToNeu_Clutch  :  tReleasing_ToNeu_Clutch ≔time
END
```

```
    Error_ToNeu ≙
        STATUS
      ordinary
REFINES
      Error_ToNeu
WHEN
      grd1  :  Error_ToNeu = FALSE
      grd2  :  RequestToNeu = TRUE
      grd3  :  Releasing_ToNeu_NoClutch = FALSE
      grd4  :  Releasing_ToNeu_Clutch = FALSE
THEN
      act1  :  Error_ToNeu ≔ TRUE
      tError_ToNeu  :  tError_ToNeu ≔time
END

    Error_Releasing_NoNeu ≙
        STATUS
      ordinary
REFINES
      Error_Releasing_NoNeu
WHEN
      grd1  :  Error_Releasing_NoNeu = FALSE
      grd2  :  RequestNoNeu = TRUE
      grd3  :  Releasing_NoNeu_Clutch = FALSE
      grd4  :  Releasing_NoNeu_NoClutch = FALSE
THEN
      act1  :  Error_Releasing_NoNeu ≔ TRUE
      tError_Releasing_NoNeu  :  tError_Releasing_NoNeu ≔time
END

    Error_Setting_NoNeu ≙
        STATUS
      ordinary
REFINES
      Error_Setting_NoNeu
WHEN
      grd1  :  Error_Setting_NoNeu = FALSE
      grd2  :  Releasing_NoNeu_Clutch = TRUE ∨ Releasing_NoNeu_NoClutch = TRUE
      grd3  :  Setting_NoNeu_NoClutch = FALSE
      grd4  :  Setting_NoNeu_Clutch = FALSE
      grd5  :  Setting_NoNeu_ReleaseClutch = FALSE
THEN
      act1  :  Error_Setting_NoNeu ≔ TRUE
      tError_Setting_NoNeu  :  tError_Setting_NoNeu ≔time
END

    Error_FromNeu ≙
        STATUS
      ordinary
REFINES
      Error_FromNeu
WHEN
      grd1  :  Error_FromNeu = FALSE
      grd2  :  RequestFromNeu = TRUE
      grd3  :  Setting_FromNeu_NoClutch = FALSE
      grd4  :  Setting_FromNeu_Clutch = FALSE
THEN
      act1  :  Error_FromNeu ≔ TRUE
      tError_FromNeu  :  tError_FromNeu ≔time
END
```

FINAL ≙
extended
STATUS
ordinary
REFINES
FINAL
WHEN
Setting_FromNeu_NoClutch = TRUE ∨ Setting_NoNeu_NoClutch = TRUE ∨ Releasing_ToNeu_NoClutch = TRUE ∨
grd1 : *Setting_FromNeu_Clutch = TRUE ∨ Setting_NoNeu_Clutch = TRUE ∨ Setting_NoNeu_ReleaseClutch = TRUE ∨ Releasing_ToNeu_Clutch = TRUE*
THEN
act1 : RequestFromNeu ≔ FALSE
act2 : RequestNoNeu ≔ FALSE
act3 : RequestToNeu ≔ FALSE
act4 : Releasing_ToNeu_NoClutch ≔ FALSE
act5 : Setting_NoNeu_NoClutch ≔ FALSE
act6 : Setting_FromNeu_NoClutch ≔ FALSE
act7 : Releasing_NoNeu_NoClutch ≔FALSE
act8 : Releasing_ToNeu_Clutch ≔ FALSE
act9 : Setting_NoNeu_Clutch ≔ FALSE
act10 : Setting_NoNeu_ReleaseClutch ≔ FALSE
act11 : Setting_FromNeu_Clutch ≔ FALSE
act12 : Releasing_NoNeu_Clutch ≔FALSE
END

Tick_Tock ≙
STATUS
ordinary
REFINES
Tick_Tock
ANY
tick
WHERE
tick : tick > 0
Deadline3 : RequestNoNeu = TRUE ∧ Error_Releasing_NoNeu = FALSE ∧ Releasing_NoNeu_Clutch = FALSE ∧ Releasing_NoNeu_NoClutch = FALSE ⇒ time + tick ≤ tRequestNoNeu + R_NN
Deadline4 : RequestFromNeu = TRUE ∧ Error_FromNeu = FALSE ∧ Setting_FromNeu_Clutch = FALSE ∧ Setting_FromNeu_NoClutch = FALSE ⇒ time + tick ≤ tRequestFromNeu + S_FN
Deadline5 : RequestToNeu = TRUE ∧ Error_ToNeu = FALSE ∧ Releasing_ToNeu_Clutch = FALSE ∧ Releasing_ToNeu_NoClutch = FALSE ⇒ time + tick ≤ tRequestToNeu + R_TN
Deadline6 : Releasing_NoNeu_NoClutch = TRUE ∧ Setting_NoNeu_Clutch = FALSE ∧ Setting_NoNeu_NoClutch = FALSE ⇒ time + tick ≤ tReleasing_NoNeu_NoClutch + S_NN
Deadline7 : Releasing_NoNeu_Clutch = TRUE ∧ Error_Setting_NoNeu = FALSE ∧ Setting_NoNeu_ReleaseClutch = FALSE ⇒ time + tick ≤ tReleasing_NoNeu_Clutch + S_NN_RC
THEN
act1 : time ≔time+tick
END

END