```
CONTEXT
   System_Ctx
CONSTANTS
   TIME
   sigma
   plantV0
AXIOMS
   axm1   :   TIME = RRealPlus
   axm2   :   sigma ∈ RRealPlus ∧ sigma ↦Rzero ∈gt
   axm3   :   plantV0∈ RReal
END
```

```
CONTEXT
   Theorems
AXIOMS
   axm1   :   ∀a,b,c,d·a↦b∈ leq ∧ c↦d ∈leq ⇒ plus(a↦c) ↦plus(b↦d) ∈ leq
   axm2   :   ∀a,b,c,d·Rzero↦a ∈ leq ∧ Rzero↦b ∈ leq ∧ Rzero↦c ∈ leq ∧ Rzero↦d ∈ leq ∧ a↦b∈ leq ∧ c↦d ∈leq ⇒ times
              (a↦c) ↦times(b↦d) ∈ leq
   axm3   :   ∀a,b,c· a↦b ∈ leq ∧ b↦c ∈ leq⇒ a ↦c ∈ leq
              ∀a,b· a∈ RReal ∧ b ∈ RReal
   axm4   :   ⇒
              minus(times(a↦a) ↦times(b↦b))=times(plus(a↦b)↦minus(a↦b))
   axm5   :    ∀a· a∈ RReal ⇒ uminus(a)=minus(Rzero↦a)
              ∀a· a∈ RReal ⇒
              a=plus(
                     times(divide(Rone ↦ Rtwo) ↦a)
   axm6   :      ↦
                     times(divide(Rone ↦ Rtwo) ↦a)
                   )
              ∀a,b· a∈ RReal ∧ b∈ RReal ∧ times(a↦b)∈ RRealStar
   axm7   :   ⇒
              inverse(times(a↦b))=times(inverse(a)↦inverse(b))
END
```

```
MACHINE
   System_M
SEES
   System_Ctx
   Theorems
VARIABLES
   t
   plantV
INVARIANTS
   inv1   :   t ∈ TIME
   inv2   :   plantV ∈ Closed2Closed(Rzero, t) ⇸ RReal
EVENTS
   INITIALISATION   ≙
   STATUS
     ordinary
   BEGIN
     act1   :   t≔Rzero
     act2   :   plantV ≔{Rzero↦plantV0}
   END

   Progress   ≙
   STATUS
     ordinary
   BEGIN
     act1   :   t :∣ t' ∈ TIME ∧ (t ↦ t' ∈ lt ∧ minus(t'↦t) ↦ sigma ∈ geq)
   END

   Plant   ≙
   STATUS
     ordinary
   ANY
     e
     plant1
   WHERE
     grd1   :   e ∈ DE(RReal)
     grd2   :   Solvable(Closed2Closed(Rzero, t)\dom(plantV),e)
                plant1 ∈ Closed2Closed(Rzero, t)\dom(plantV) ⟶ RReal ∧
     grd3   :   AppendSolutionBAP(e,
                Closed2Closed(Rzero, t)\dom(plantV),
                Closed2Closed(Rzero, t)\dom(plantV), plant1)
   THEN
     act1   :   plantV≔plantV⩤plant1
   END

END
```

```
CONTEXT
    EventTriggered_Ctx
EXTENDS
    System_Ctx
SETS
    EXEC
    PROP
CONSTANTS
    prop_safe
    prop_evt_trig
    ctrl
    plant
    prg
    f_evol
    f_evol_plantV
    prop_evade_values
AXIOMS
    axm1   :   prop_safe ∈ PROP⟶((RReal  × RReal) ⟶ BOOL)
    axm2   :   prop_evt_trig ∈ PROP⟶((RReal×RReal)×RReal ⟶ BOOL)
    axm3   :   partition(EXEC,  {ctrl},{plant},{prg})
    axm4   :   f_evol ∈ RReal ⟶ RReal
    axm5   :   f_evol_plantV ∈ (RReal ⟶ (TIME × RReal ⟶ RReal))
    axm6   :   ∀ ctrlV · ctrlV ∈ RReal ⇒ (f_evol_plantV(ctrlV) =
                     (λ t ↦ plantV · t ∈ TIME ∧ plantV ∈ RReal | f_evol(ctrlV)))
    axm7   :    prop_evade_values∈PROP⟶ℙ1(RReal)
END
```

```
MACHINE
   EventTriggered_M
REFINES
   System_M
SEES
   EventTriggered_Ctx
VARIABLES
   t
   plantV
   ctrlV
   exec
INVARIANTS
   inv1   :   ctrlV ∈ RReal
   inv2   :   exec ∈ EXEC
   inv3   :   exec≠plant ⇒ dom(plantV)=Closed2Closed(Rzero, t)
   inv4   :   exec=plant ⇒ t∉ dom(plantV)
EVENTS
   INITIALISATION   ≙
     extended
   STATUS
     ordinary
   BEGIN
     act1   :   t≔Rzero
     act2   :   plantV ≔{Rzero↦plantV0}
     act3   :   ctrlV :∈ RReal
     act4   :   exec ≔ ctrl
   END

   Progress   ≙
   STATUS
     ordinary
   REFINES
     Progress
   ANY
     t1
   WHERE
     grd1   :   exec=prg
     grd2   :   t1 ∈ TIME ∧ (t ↦ t1 ∈ lt ∧ minus(t1↦t) ↦ sigma ∈ geq)
                ∀x· x∈ PROP ⇒
     grd3   :     (ctrlV∉ prop_evade_values(x)⇒
                       (prop_evt_trig(x))(plantV(t)↦minus(t1↦t)↦ctrlV) = TRUE)
   THEN
     act1   :   t≔t1
     act2   :   exec ≔ plant
   END

   Plant   ≙
   STATUS
     ordinary
   REFINES
     Plant
   ANY
     plant1
   WHERE
     grd1   :   exec=plant
     grd2   :   plant1 ∈ Closed2Closed(Rzero, t)\dom(plantV) ⟶ RReal
     grd3   :   ode(f_evol_plantV(ctrlV),plant1(t),t) ∈ DE(RReal)
                Solvable(Closed2Closed(Rzero, t)\dom(plantV),
     grd4   :                 ode(f_evol_plantV(ctrlV),plant1(t),t))
                AppendSolutionBAP(ode(f_evol_plantV(ctrlV),plant1(t),t),
     grd5   :   Closed2Closed(Rzero, t)\dom(plantV),
                Closed2Closed(Rzero, t)\dom(plantV), plant1)
   WITH
     e   :   e = ode(f_evol_plantV(ctrlV),plant1(t),t)
   THEN
     act1   :   plantV≔plantV⩤plant1
     act2   :   exec≔ctrl
   END
```

```
Ctrl  ≙
STATUS
  ordinary
ANY
  value
WHERE
  grd1  :   exec = ctrl
  grd2  :   value∈RReal
            ∀x· x∈ PROP ⇒
  grd3  :     (value∉ prop_evade_values(x)
            ⇒(prop_safe(x))(plantV(t)↦value) = TRUE)
THEN
  act1  :   ctrlV ≔value
  act2  :   exec ≔ prg
END

END
```

```
CONTEXT
   TimeTriggered_Ctx
EXTENDS
   EventTriggered_Ctx
CONSTANTS
   epsilon
   prop_safeEpsilon
AXIOMS
   axm1   :   epsilon ∈ TIME ∧ sigma↦epsilon ∈leq
   axm2   :   prop_safeEpsilon ∈ PROP⟶((RReal × RReal) ⟶ BOOL)
   axm3   :   Rzero↦epsilon ∈lt
END
```

```
MACHINE
   TimeTriggered_M
REFINES
   EventTriggered_M
SEES
   TimeTriggered_Ctx
   Theorems
VARIABLES
   t
   plantV
   ctrlV
   exec
EVENTS
   INITIALISATION  ≙
     extended
   STATUS
     ordinary
   BEGIN
     act1  :  t≔Rzero
     act2  :  plantV ≔{Rzero↦plantV0}
     act3  :  ctrlV :∈ RReal
     act4  :  exec ≔ ctrl
   END

   Progress  ≙
   STATUS
     ordinary
   REFINES
     Progress
   ANY
     t1
   WHERE
     grd1  :  exec=prg
     grd2  :  t1 ∈ TIME ∧ (t ↦ t1 ∈ lt ∧ minus(t1↦t) ↦ sigma ∈ geq)
              ∀x· x∈ PROP ⇒
     grd3  :    (ctrlV∉ prop_evade_values(x)⇒
                     (prop_evt_trig(x))(plantV(t)↦minus(t1↦t)↦ctrlV) = TRUE)
     grd4  :   t1 ∈ TIME ∧ (t ↦ t1 ∈ lt) ∧ minus(t1↦t) ↦ sigma ∈ geq ∧ minus(t1↦t) ↦ epsilon ∈ leq
   THEN
     act1  :  t≔t1
     act2  :  exec ≔ plant
   END

   Plant  ≙
   STATUS
     ordinary
   REFINES
     Plant
   ANY
     plant1
   WHERE
     grd1  :  exec=plant
     grd2  :  plant1 ∈ Closed2Closed(Rzero, t)\dom(plantV) ⟶ RReal
     grd3  :  ode(f_evol_plantV(ctrlV),plant1(t),t) ∈ DE(RReal)
     grd4  :  Solvable(Closed2Closed(Rzero, t)\dom(plantV),
                           ode(f_evol_plantV(ctrlV),plant1(t),t))
              AppendSolutionBAP(ode(f_evol_plantV(ctrlV),plant1(t),t),
     grd5  :  Closed2Closed(Rzero, t)\dom(plantV),
              Closed2Closed(Rzero, t)\dom(plantV), plant1)
   THEN
     act1  :  plantV≔plantV⊲plant1
     act2  :  exec≔ctrl
   END

   Ctrl  ≙
   STATUS
     ordinary
   REFINES
     Ctrl
```

```
ANY
  value
WHERE
  grd1   :   exec = ctrl
  grd2   :   value∈RReal
             ∀ x· x∈ PROP ⇒
  grd3   :     (value∉ prop_evade_values(x)
             ⇒(prop_safe(x))(plantV(t)↦value) = TRUE)
             ∀ x· x∈ PROP ⇒
  grd4   :          (value∉ prop_evade_values(x)
             ⇒(prop_safeEpsilon(x))(plantV(t)↦value) = TRUE)
THEN
  act1   :   ctrlV ≔value
  act2   :   exec ≔ prg
END

END
```

```
CONTEXT
   Desolve
EXTENDS
   TimeTriggered_Ctx
CONSTANTS
   B_desolve
   prop
AXIOMS
   axm1   :   B_desolve ∈  ℕ × RReal × (TIME ⇸ RReal ) ×TIME × (TIME × RReal) → (RReal ⇸ RReal)
   axm2   :   prop∈ RReal →BOOL
   axm3   :   prop(plantV0)=TRUE
END
```

```
MACHINE
   TimeTriggered_desolve_M
REFINES
   TimeTriggered_M
SEES
   Desolve
   Theorems
VARIABLES
   t
   plantV
   ctrlV
   exec
INVARIANTS
   inv1   :   ∀x· x∈ dom(plantV)⇒prop(plantV(x))=TRUE
EVENTS
   INITIALISATION   ≙
     extended
   STATUS
     ordinary
   BEGIN
     act1   :   t≔Rzero
     act2   :   plantV ≔{Rzero↦plantV0}
     act3   :   ctrlV :∈ RReal
     act4   :   exec ≔ ctrl
   END

   Progress   ≙
   STATUS
     ordinary
   REFINES
     Progress
   ANY
     t1
   WHERE
     grd1   :   exec=prg
     grd2   :   t1 ∈ TIME ∧ (t ↦ t1 ∈ lt ∧ minus(t1↦t) ↦ sigma ∈ geq)
                ∀x· x∈ PROP ⇒
     grd3   :     (ctrlV∉ prop_evade_values(x)⇒
                       (prop_evt_trig(x))(plantV(t)↦minus(t1↦t)↦ctrlV) = TRUE)
     grd4   :   t1 ∈ TIME ∧ (t ↦ t1 ∈ lt) ∧ minus(t1↦t) ↦ sigma ∈ geq ∧ minus(t1↦t) ↦ epsilon ∈ leq
   THEN
     act1   :   t≔t1
     act2   :   exec ≔ plant
   END

   Plant   ≙
   STATUS
     ordinary
   REFINES
     Plant
   ANY
     plant1
     lastTime
   WHERE
     grd1   :   exec=plant
     grd2   :   lastTime∈ TIME ∧ dom(plantV)=Closed2Closed(Rzero,lastTime)
     grd3   :   plant1 =B_desolve(1 ↦ ctrlV ↦ plantV ↦ t ↦ (lastTime↦plantV(lastTime)))
     grd4   :   plant1 ∈ Closed2Closed(Rzero, t)\dom(plantV) ⟶ RReal
     grd5   :    ode(f_evol_plantV(ctrlV),plant1(t),t) ∈ DE(RReal)
     grd6   :   Solvable(Closed2Closed(Rzero, t)\dom(plantV),
                             ode(f_evol_plantV(ctrlV),plant1(t),t))
     grd7   :     AppendSolutionBAP(ode(f_evol_plantV(ctrlV),plant1(t),t),
                Closed2Closed(Rzero, t)\dom(plantV),Closed2Closed(Rzero, t)\dom(plantV), plant1)
     grd8   :    ∀xx· xx∈ dom(plant1)⇒ prop(plant1(xx))=TRUE
   THEN
     act1   :   plantV≔plantV⊲plant1
     act2   :   exec≔ctrl
   END
```

```
Ctrl  ≙
STATUS
  ordinary
REFINES
  Ctrl
ANY
  value
WHERE
  grd1   :   exec = ctrl
  grd2   :   value∈RReal
             ∀x· x∈ PROP ⇒
  grd3   :     (value∉ prop_evade_values(x)
             ⇒(prop_safe(x))(plantV(t)↦value) = TRUE)
             ∀x· x∈ PROP ⇒
  grd4   :          (value∉ prop_evade_values(x)
             ⇒(prop_safeEpsilon(x))(plantV(t)↦value) = TRUE)
THEN
  act1   :   ctrlV ≔value
  act2   :   exec ≔ prg
END

END
```

```
CONTEXT
   WaterTank_ctx
EXTENDS
   Desolve
CONSTANTS
   p1
   p2
   prop_val
   V_high
   V_low
   V0
   f_in
   f_out
AXIOMS
   axm1   :  V_high ∈ RReal
   axm2   :  V_high↦ V_low ∈ gt
   axm3   :  V_low ∈ RReal
   axm4   :  V_low ↦ Rzero ∈ gt
   axm5   :  V0 ∈ RRealPlus
   axm6   :  f_in ∈ RReal ∧ f_out∈RReal
   axm7   :  f_in ↦ Rzero ∈ gt ∧ f_out ↦ Rzero ∈ gt
   axm8   :  prop_val∈PROP⟶ℙ(RReal×BOOL)
   axm9   :  PROP={p1,p2}
   axm10   :  prop_val={p1↦(λ t· t ∈ RReal | bool(V_low↦t∈leq)),
                        p2↦(λ t· t ∈ RReal | bool(t↦V_high∈ leq))}
   axm11   :  prop=(λ t· t ∈ RReal | bool((prop_val(p1))(t)=TRUE ∧
                                        (prop_val(p2))(t)=TRUE))
              prop_safe ={
   axm12   :  p1↦(λ T↦ctrlV · T ∈ RReal ∧ ctrlV ∈ RReal | bool(T ↦ V_high ∈ leq)),
              p2↦(λ T↦ctrlV · T ∈ RReal ∧ ctrlV ∈ RReal | bool(T ↦ V_low ∈ geq))
              }
              prop_safeEpsilon = {
              p1↦(λ T↦ctrlV · T ∈ RReal ∧ ctrlV ∈ RReal |
   axm13   :  bool(plus(T↦ times(ctrlV ↦ epsilon))↦V_high ∈ leq)),
              p2↦(λ T↦ctrlV· T ∈ RReal ∧ ctrlV ∈ RReal |
              bool(plus(T↦ times(ctrlV ↦ epsilon)) ↦ V_low ∈ geq))
              }
              prop_evt_trig ={
              p1↦(λ v↦t1↦ctrlV· v ∈ RReal ∧ t1∈ RReal ∧ ctrlV ∈ RReal |
                 bool(plus(v ↦times(ctrlV↦t1))↦V_high ∈ leq)),
   axm14   :  p2↦(λ v↦t1↦ctrlV · v ∈ RReal ∧ t1∈ RReal ∧ ctrlV ∈ RReal |
                 bool(plus(v ↦times(ctrlV↦t1)) ↦ V_low ∈ geq))
              }
   axm15   :  Rzero↦epsilon ∈ lt
   axm16   :  V0 ↦ V_high ∈ leq ∧ V0 ↦ V_low ∈ geq
   axm17   :  V0 =plantV0
   axm18   :  prop_evade_values={p1↦{uminus(f_out)}, p2↦{f_in}}
END
```

```
MACHINE
    WaterTank
REFINES
    TimeTriggered_desolve_M
SEES
    WaterTank_ctx
    Theorems
VARIABLES
    t
    V
    ctrlV
    exec
INVARIANTS
    inv1   :   V=plantV ∧ ran(V)⊆ RReal
    inv2   :   ctrlV∈{f_in,uminus(f_out)}
    inv3   :   exec≠plant ⇒ dom(V)=Closed2Closed(Rzero, t)
    inv4   :   exec=plant ⇒ t∉dom(V)
    inv5   :   ∀x· x∈ dom(V)⇒ V(x) ↦ V_high ∈ leq ∧ V(x) ↦ V_low ∈ geq
               ∃ t1 · t1 ∈ RRealPlus ∧ dom(V) = Closed2Closed(Rzero, t1) ∧
               minus(t ↦ t1) ↦ epsilon ∈ leq ∧
                   (exec ≠ plant ⇒ t1 = t) ∧
    inv6   :        (exec =plant ⇒ t ↦ t1 ∈ gt) ∧
               (∀x· x∈ PROP ∧ ctrlV∉ prop_evade_values(x) ∧ exec=plant
                   ⇒
                     (prop_safeEpsilon(x))(V(t1)↦ctrlV) = TRUE)
               ∀x· x∈ PROP ∧ ctrlV∉ prop_evade_values(x) ∧ exec=prg
    inv7   :       ⇒
                     (prop_safeEpsilon(x))(V(t)↦ctrlV) = TRUE
               ∀ t1, t2 · t1 ∈ RRealPlus ∧ t2 ∈ RRealPlus ∧
    inv8   :   dom(V) = Closed2Closed(Rzero, t1) ∧
               dom(V) = Closed2Closed(Rzero, t2)
               ⇒ t1 = t2
EVENTS
    INITIALISATION  ≙
    STATUS
      ordinary
    BEGIN
      act1   :   t≔Rzero
      act2   :   V≔{Rzero↦V0}
      act3   :   exec ≔ ctrl
      act4   :   ctrlV ≔f_in
    END

    Progress   ≙
    STATUS
      ordinary
    REFINES
      Progress
    ANY
      t1
    WHERE
      grd1   :   exec=prg
      grd2   :   t1 ∈ TIME ∧ (t ↦ t1 ∈ lt) ∧ minus(t1↦t) ↦ sigma ∈ geq ∧ minus(t1↦t) ↦ epsilon ∈ leq
    THEN
      act1   :   t≔t1
      act2   :   exec ≔ plant
    END

    plant  ≙
    STATUS
      ordinary
    REFINES
      Plant
    ANY
      lastTime
      plant1
      dvar
      ivar
      ics
```

```
WHERE
  grd1   :   exec=plant
  grd2   :   lastTime∈ TIME ∧ dom(V)=Closed2Closed(Rzero, lastTime)
  grd3   :   dvar=V
  grd4   :   ivar=t
  grd5   :   ics=(lastTime↦V(lastTime))
  grd6   :   plant1 =B_desolve(1 ↦ ctrlV ↦ dvar ↦ ivar ↦ ics)
             ode(f_evol_plantV(ctrlV),
  grd7   :   plant1(t),t) ∈ DE(RReal)
             Solvable(Closed2Closed(Rzero, t)\dom(V),
  grd8   :   ode(f_evol_plantV(ctrlV),
             plant1(t),t))
             AppendSolutionBAP(ode(f_evol_plantV(ctrlV),plant1(t),t),
  grd9   :          Closed2Closed(Rzero, t)\dom(V),
                    Closed2Closed(Rzero, t)\dom(V), plant1)
THEN
  skip
END

Ctrl   ≙
STATUS
  ordinary
REFINES
  Ctrl
ANY
  value
WHERE
  grd1   :   exec = ctrl
  grd2   :   value∈ {f_in,uminus(f_out)}
             ∀x· x∈ PROP ⇒
  grd3   :          (value∉ prop_evade_values(x)
             ⇒(prop_safeEpsilon(x))(V(t)↦value) = TRUE)
THEN
  act1   :   ctrlV ≔value
  act2   :   exec≔ prg
END

END
```