```
MACHINE
    Ferroviaire0
SEES
    FerrovaireCtx
VARIABLES
    circulation    //   站台以外的铁轨上行驶的火车
    voies      //   停靠在站台的火车
    sortie     //   在驶出站台和正常铁轨部分之间的火车
INVARIANTS
    inv1   :    circulation ⊆ TRAINS
    inv2   :    sortie ⊆ TRAINS
    inv3   :    voies ∈ TRAINS ⇸ VOIES
    inv4   :    card(sortie) ≤ 1       //   在sortie部分的火车数量最多为1
    inv5   :    circulation ∩ sortie ∩ dom(voies) = ∅      //   一辆火车不能同时在三个地方
    inv6   :    ∀v·(v∈VOIES ⇒ card(voies~[{v}]) ≤ 1 )      //   站台最多只能有一辆火车(未通过PO)

EVENTS
    INITIALISATION   ≙
        STATUS ordinary
        BEGIN
            act1   :    circulation ≔ TRAINS
            act2   :    sortie ≔ ∅
            act3   :    voies ≔ ∅
    END

    Arriver   ≙        //   到达 (未通过grd3, inv3, inv6)
        STATUS ordinary
        ANY
            tc     //   正常运行的火车
            voie       //   站台
        WHERE
            grd1   :    tc ∈ circulation       //   正常运行的火车
            grd2   :    voie ∈ VOIES       //   站台
            grd3   :    card(voies~[{voie}]) = 0       //   空闲的站台
        THEN
            act1   :    circulation ≔ circulation \ {tc}
            act2   :    voies ≔ voies ∪ {tc ↦ voie}
    END

    Partir   ≙         //   出发 (未通过inv6)
        STATUS ordinary
        ANY
            tv     //   停在站台的和火车
            voie
        WHERE
            grd1   :    card(sortie)=0     //   sortie 区域是空闲的
            grd2   :    voie ∈VOIES
            grd3   :    tv ∈ TRAINS
            grd4   :    tv ∈  voies~[{voie}]       //   火车来自站台
        THEN
```

```
            act1   :    sortie ≔ sortie ∪ {tv}
            act2   :    voies ≔ voies ⩤ {tv ↦ voie}
    END

    Circuler   ≙       //   正常运行
        STATUS ordinary
        ANY
            t
        WHERE
            grd1   :    t ∈ sortie     //   火车在sortie区域
        THEN
            act1   :    sortie ≔ sortie ∖ {t}
            act2   :    circulation ≔ circulation ∪ {t}
    END

END
```

```
MACHINE
    Ferroviaire1
REFINES
    Ferroviaire0
SEES
    FerrovaireCtx
VARIABLES
    circulation    //   站台以外的铁轨上行驶的火车
    voies      //   停靠在站台的火车
    sortie     //   在驶出站台和正常铁轨部分之间的火车
    horloge    //   时钟
    departs    //   火车出发时间
INVARIANTS      // extended
    inv1   :    horloge ∈ ℕ
    inv2   :    departs ∈ TRAINS ⇸ ℕ
    inv3   :    dom(departs) = dom(voies)

EVENTS
    INITIALISATION   ≙
        extended
        STATUS ordinary
        BEGIN
            act1   :    circulation ≔ TRAINS
            act2   :    sortie ≔ ∅
            act3   :    voies ≔ ∅
            act4   :    horloge :∈ ℕ
            act5   :    departs ≔ ∅
    END

    Arriver   ≙        //   到达 (未通过inv3)
        extended
        STATUS ordinary
        REFINES Arriver
        ANY
```

```
            tc      //   正常运行的火车
            voie        //   站台
        WHERE
            grd1   :    tc ∈ circulation        //   正常运行的火车
            grd2   :    voie ∈ VOIES        //   站台
            grd3   :    card(voies~[{voie}]) = 0        //   空闲的站台
        THEN
            act1   :    circulation ≔ circulation \ {tc}
            act2   :    voies ≔ voies ∪ {tc ↦ voie}
    END

    Partir   ≙          //   出发 (未通过inv3)
        extended
        STATUS ordinary
        REFINES Partir
        ANY
            tv      //   停在站台的和火车
            voie
        WHERE
            grd1   :    card(sortie)=0      //   sortie 区域是空闲的
            grd2   :    voie ∈VOIES
            grd3   :    tv ∈ TRAINS
            grd4   :    tv ∈  voies~[{voie}]        //   火车来自站台
            grd5   :    departs(tv)≤horloge     //   当前系统时间大于出发时间时
        THEN
            act1   :    sortie ≔ sortie ∪ {tv}
            act2   :    voies ≔ voies \ {tv ↦ voie}
    END

    Circuler   ≙        //   正常运行
        extended
        STATUS ordinary
        REFINES Circuler
        ANY
            t
        WHERE
            grd1   :    t ∈ sortie      //   火车在sortie区域
        THEN
            act1   :    sortie ≔ sortie \ {t}
            act2   :    circulation ≔ circulation ∪ {t}
    END

    Tick   ≙            // 系统时间
        STATUS ordinary
        BEGIN
            act1   :    horloge ≔ horloge + 1       //   系统时钟
    END

END
```