

```

1 MACHINE
2     Ferroviaire0
3 SEES
4     FerroviaireCtx
5 VARIABLES
6     circulation    //  站台以外的铁轨上行驶火车
7     voies          //  停靠在站台的火车
8     sortie         //  在驶出站台和正常铁轨部分之间的火车
9 INVARIANTS
10    inv1   :   circulation  $\subseteq$  TRAINS
11    inv2   :   sortie  $\subseteq$  TRAINS
12    inv3   :   voies  $\in$  TRAINS  $\rightarrow$  VOIES
13    inv4   :   card(sortie)  $\leq$  1           //  在sortie部分的火车数量最多为1
14    inv5   :   circulation  $\cap$  sortie  $\cap$  dom(voies) =  $\emptyset$            //  一辆火车不能同时在三个地方
15    inv6   :    $\forall v.(v \in \text{VOIES} \Rightarrow \text{card}(\text{voies} \sim [\{v\}]) \leq 1)$            //  站台最多只能有一辆火车(未通
过P0)
16
17 EVENTS
18     INITIALISATION  $\triangleq$ 
19         STATUS ordinary
20         BEGIN
21             act1   :   circulation  $\equiv$  TRAINS
22             act2   :   sortie  $\equiv \emptyset$ 
23             act3   :   voies  $\equiv \emptyset$ 
24         END
25
26     Arriver  $\triangleq$            //  到达 (未通过grd3, inv3, inv6)
27         STATUS ordinary
28         ANY
29             tc      //  正常运行的火车
30             voie     //  站台
31         WHERE
32             grd1   :   tc  $\in$  circulation           //  正常运行的火车
33             grd2   :   voie  $\in$  VOIES           //  站台
34             grd3   :   card(voies  $\sim [\{voie\}]) = 0$            //  空闲的站台
35         THEN
36             act1   :   circulation  $\equiv$  circulation  $\setminus \{tc\}$ 
37             act2   :   voies  $\equiv$  voies  $\cup \{tc \rightarrow voie\}$ 
38         END
39
40     Partir  $\triangleq$            //  出发 (未通过inv6)
41         STATUS ordinary
42         ANY
43             tv      //  停在站台的和火车
44             voie
45         WHERE
46             grd1   :   card(sortie)=0           //  sortie 区域是空闲的
47             grd2   :   voie  $\in$  VOIES
48             grd3   :   tv  $\in$  TRAINS
49             grd4   :   tv  $\in$  voies  $\sim [\{voie\}]$            //  火车来自站台
50         THEN

```

```

51         act1    :    sortie = sortie U {tv}
52         act2    :    voies = voies \ {tv ↦ voie}
53     END
54
55     Circuler    ≜        //    正常运行
56         STATUS ordinary
57         ANY
58         t
59         WHERE
60             grd1    :    t ∈ sortie        //    火车在sortie区域
61         THEN
62             act1    :    sortie = sortie \ {t}
63             act2    :    circulation = circulation U {t}
64         END
65     END
66 END

```

```

1  MACHINE
2      Ferroviaire1
3  REFINES
4      Ferroviaire0
5  SEES
6      FerroviaireCtx
7  VARIABLES
8      circulation    //    站台以外的铁轨上行驶火车
9      voies          //    停靠在站台的火车
10     sortie         //    在驶出站台和正常铁轨部分之间的火车
11     horloge        //    时钟
12     departs        //    火车出发时间
13 INVARIANTS        //    extended
14     inv1    :    horloge ∈ ℕ
15     inv2    :    departs ∈ TRAINS ↗ ℕ
16     inv3    :    dom(departs) = dom(voies)
17
18 EVENTS
19     INITIALISATION    ≜
20         extended
21         STATUS ordinary
22         BEGIN
23             act1    :    circulation = TRAINS
24             act2    :    sortie = ∅
25             act3    :    voies = ∅
26             act4    :    horloge :∈ ℕ
27             act5    :    departs = ∅
28         END
29
30     Arriver    ≜        //    到达 (未通过inv3)
31         extended
32         STATUS ordinary
33         REFINES Arriver
34         ANY

```

```

35         tc      // 正常运行的火车
36         voie     // 站台
37     WHERE
38         grd1 : tc ∈ circulation      // 正常运行的火车
39         grd2 : voie ∈ VOIES          // 站台
40         grd3 : card(voies~[{voie}]) = 0      // 空闲的站台
41     THEN
42         act1 : circulation = circulation \ {tc}
43         act2 : voies = voies U {tc ↦ voie}
44     END
45
46     Partir ≜      // 出发 (未通过inv3)
47     extended
48     STATUS ordinary
49     REFINES Partir
50     ANY
51         tv      // 停在站台的和火车
52         voie
53     WHERE
54         grd1 : card(sortie)=0      // sortie 区域是空闲的
55         grd2 : voie ∈ VOIES
56         grd3 : tv ∈ TRAINS
57         grd4 : tv ∈ voies~[{voie}]      // 火车来自站台
58         grd5 : departs(tv) ≤ horloge    // 当前系统时间大于出发时间时
59     THEN
60         act1 : sortie = sortie U {tv}
61         act2 : voies = voies \ {tv ↦ voie}
62     END
63
64     Circuler ≜      // 正常运行
65     extended
66     STATUS ordinary
67     REFINES Circuler
68     ANY
69         t
70     WHERE
71         grd1 : t ∈ sortie      // 火车在sortie区域
72     THEN
73         act1 : sortie = sortie \ {t}
74         act2 : circulation = circulation U {t}
75     END
76
77     Tick ≜      // 系统时间
78     STATUS ordinary
79     BEGIN
80         act1 : horloge = horloge + 1      // 系统时钟
81     END
82
83     END

```