

**MACHINE**

**Battery+Hardware\_M0**      *// 抽象モデル(SL1の安全性の核)*

**SEES**

**Battery+Hardware\_C0**

**VARIABLES**

batteryLevel      *// ローバの現在のバッテリーレベル(BatteryMonitorが監視)*

**INVARIANTS**

inv1 : batteryLevel ∈ N

inv2 : batteryLevel ≤ MAX\_BATTERY      *// ローバのバッテリーレベルは最大以下*

inv3 : batteryLevel ≥ MIN\_BATTERY      *// ローバのバッテリーレベルは最小以上(バッテリー切れになってはならない(SL1))*

**EVENTS**

**INITIALISATION**    ≐

**STATUS**

ordinary

**BEGIN**

act\_init\_battLevel : batteryLevel = MAX\_BATTERY      *// バッテリーレベルの初期状態は満充電状態*

**END**

**Consume\_Battery**    ≐      *// バッテリーの消費*

**STATUS**

ordinary

**WHEN**

grd\_batt\_min : batteryLevel > MIN\_BATTERY      *// バッテリーレベルが最小より大きい場合だけ消費可能*

**THEN**

act1 : batteryLevel :| batteryLevel' < batteryLevel ∧ batteryLevel' ≥ MIN\_BATTERY

**END**

**Charge\_Battery**    ≐      *// バッテリーの充電*

**STATUS**

ordinary

**WHEN**

grd1 : batteryLevel < MAX\_BATTERY      *// バッテリーレベルが最大より小さい時だけ充電可能*

**THEN**

act1 : batteryLevel :| batteryLevel' > batteryLevel ∧ batteryLevel' ≤ MAX\_BATTERY

**END**

**END**