








An Event-B Specification of ProofFailures

A machine with unproven, reviewed and manually proven POs.

1	CONTEXT	Direction		2
1.1		DIR		2
1.2		LEFT RIGHT		2
2	MACHINE	Machine	 	3
2.1	<i>its power thing</i>			3
2.2		go		3

 thm1/THM

SETS

1.1

DIR

CONSTANTS

1.2

LEFT

RIGHT

AXIOMS

axm1: partition(DIR, {LEFT}, {RIGHT})

theorem thm1:

1 = 2



Not provable.

theorem thm2:

1 = max({1, 2, 3})

Woot?

END

 inv4/WD
 thm2/THM

VARIABLES

2.1

power
thing
its

INVARIANTS

inv1: *power* ∈ BOOL
inv2: *thing* ∈ ℕ
inv3: *its* ⊆ ℕ
inv4: *thing* = max(*its*)
theorem thm1:
 1 = max({1})
theorem thm2:
 2 = max({17})

Manual proof of WD

Reviewed badly! Manual proof WD

EVENT INITIALISATION
THEN

init1: *power* := FALSE
init2: *thing* := 1
init3: *its* := ∅

Why is this auto-proved?

END

EVENT go
THEN

2.2

act1: *its* := *its* ∪ {47}
END

PO cannot be proven

Direction, 2

go, 3

INITIALISATION, 3

its, 3

Machine, 3

power, 3

thing, 3