

An Event-B Specification of ProofFailures

A machine with unproven, reviewed and manually proven POs.

1	CONTEXT	Direction	u	2
1.1	DIR			2
1.2	LEFT RIGHT			2
2	MACHINE	Machine	u r	3
2.1	its power thing			3
2.2	go			3

SETS

1.1

DIR

CONSTANTS

1.2

LEFT

RIGHT

AXIOMS

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

THEOREM

thm1: 1 = 2 Not provable.

thm2: 1 = max({1, 2, 3}) Woot?

END

u inv4/WD
r thm2/THM

VARIABLES

2.1

power
thing
its

INVARIANTS

inv1: $power \in \text{BOOL}$
inv2: $thing \in \mathbb{N}$
inv3: $its \subseteq \mathbb{N}$
inv4: $thing = \max(its)$
theorem thm1:
1 = $\max(\{1\})$ Manual proof of WD
theorem thm2:
2 = $\max(\{17\})$ Reviewed badly! Manual proof WD

EVENT INITIALISATION

THEN

init1: $power := \text{FALSE}$
init2: $thing := 1$
init3: $its := \emptyset$ Why is this auto-proved?

END

EVENT go

2.2

THEN

act1: $its := its \cup \{47\}$ PO cannot be proven

END

Direction, 2

go, 3

INITIALISATION, 3

its, 3

Machine, 3

power, 3

thing, 3