An Event-B Specification of

ProofFailures

A machine with unproven, reviewed and manually proven POs.

CONTEXT Direction 1

SETS 1.1

DIR

CONSTANTS 1.2

LEFT
RIGHT

AXIOMS

axm1: $\text{partition}(\text{DIR}, \{\text{LEFT}\}, \{\text{RIGHT}\})$

THEOREM

thm1: $1 = 2$ Not provable.
thm2: $1 = max(\{1, 2, 3\})$ Woot?

END

MACHINE Machine 6 a 2 m 1 r 1 u 2

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: $its := \varnothing$ Why is this auto-proved?

END

EVENT go 2.2
THEN

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

END