The proof obligations of the project `mcfsi0-safety`

A true but non-inductive safety property: generation, comparison with Rodin, proof

Dominique Méry
Telecom Nancy, Université de Lorraine

November 23, 2026

dominique.mery@loria.fr

© Dominique Méry

Outline

1. The model
2. Overview of the obligations
3. Machine `safety0`
4. Machine `safety1`
5. Summary

Current Section Summary

1. The model
2. Overview of the obligations
3. Machine `safety0`
4. Machine `safety1`
5. Summary

Two machines for the same property $x \leq 0$

Machine safety0

variable x

inv1 $x \in \mathbb{Z}$

theproperty $x \leq 0$

INITIALISATION $x := -1$

event1 when $x \geq 0$ then $x := x + 1$

event2 $x := x$

Machine safety1

variable x

inv1 $x \in \mathbb{Z}$

inv2 $x = -1$

safety1 (thm) $x \leq 0$

INITIALISATION $x := -1$

event1 when $x \geq 0$ then $x := x + 1$

event2 $x := x$

evt1 when $x \geq 6$ then $x := x + 1$

The two machines are independent (no refinement, no context). safety1 replaces the invariant $x \leq 0$ by $x = -1$ and makes it a theorem.

The reachable states

- Initially $x = -1$.
- `event1` (and `evt1`) requires $x \geq 0$ (resp. $x \geq 6$): never true when $x = -1$.
- `event2` does not change x.

Hence $x = -1$ **in every reachable state**: the safety property $x \leq 0$ holds.

But an invariant preservation obligation says nothing about the reachable states: it only assumes the invariants and the guard. The question is therefore: *is the invariant* $x \leq 0$ *inductive?*

Current Section Summary

1. The model
2. Overview of the obligations
3. Machine `safety0`
4. Machine `safety1`
5. Summary

8 obligations, a single false one

component	INV	THM	total	Rodin	z3
machine `safety0`	3	–	3	2/3	2/3
machine `safety1`	4	1	5	5/5	5/5
total	7	1	**8**	**7/8**	**7/8**

- `INV` (R4, R6): the initialisation or an event preserves an invariant; `THM` (R3): a theorem follows from the invariants.
- **Rodin**: same names and same goals for the 8 POs (`--comparer`); `safety0/event1/theproperty/INV` is not discharged.
- z3 proves the 7 others and gives a counterexample for that one: it is *false*, not merely hard.
- No `WD` (no partial operator); the `INV` of $x \in \mathbb{Z}$ are trivial.

© Dominique Méry

Current Section Summary

1. The model
2. Overview of the obligations
3. Machine `safety0`
4. Machine `safety1`
5. Summary

safety0: the three obligations

INITIALISATION/theproperty/INV

$$\vdash \quad -1 \leq 0$$

event2/theproperty/INV

inv1	$x \in \mathbb{Z}$
theproperty	$x \leq 0$
	$\vdash \quad x \leq 0$

Proved by Rodin and by z3.

event1/theproperty/INV

inv1	$x \in \mathbb{Z}$
theproperty	$x \leq 0$
event1.grd1	$x \geq 0$
	$\vdash \quad x + 1 \leq 0$

Not discharged by Rodin; z3: counterexample $x = 0$.

safety0: the counterexample $x = 0$

- The hypotheses $x \leq 0$ and $x \geq 0$ leave $x = 0$; `event1` then gives $x' = 1$, and $1 \leq 0$ is false.
- The state $x = 0$ **is not reachable** (x stays at -1), but nothing in the hypotheses rules it out: $x \leq 0$ *is not an inductive invariant*.
- The PO is therefore false: no proof, manual or automatic, will discharge it in `safety0`.

Two possible corrections

- **strengthen the invariant** to rule out the unreachable states (here $x = -1$, `safety1`);
- or **strengthen the guard** of `event1` (for instance $x < 0$).

Current Section Summary

1. The model
2. Overview of the obligations
3. Machine `safety0`
4. Machine `safety1`
5. Summary

safety1: the strengthened invariant $x = -1$

obligation	own hypotheses	goal	remark
`safety1/THM`	$x = -1$	$\vdash x \leq 0$	the property
`INITIALISATION/inv2/INV`		$\vdash -1 = -1$	
`event1/inv2/INV`	$x = -1$, `grd1` $x \geq 0$	$\vdash x + 1 = -1$	contradictory hypotheses
`event2/inv2/INV`	$x = -1$	$\vdash x = -1$	
`evt1/inv2/INV`	$x = -1$, `grd1` $x \geq 6$	$\vdash x + 1 = -1$	contradictory hypotheses

- The 5 POs are proved by Rodin and by z3.
- For `event1` and `evt1`, the guards are incompatible with $x = -1$: the goal $x + 1 = -1$ is false, but the PO holds because its hypotheses are contradictory; these events are never enabled.
- In the POs of the events, the theorem `safety1` ($x \leq 0$) is among the hypotheses.

© Dominique Méry

Current Section Summary

1. The model
2. Overview of the obligations
3. Machine `safety0`
4. Machine `safety1`
5. Summary

Summary and remarks

- 8 POs: 7 `INV`, 1 `THM`;
- `safety0/event1/theproperty/INV` is false: z3 exhibits $x = 0$, a state that satisfies the hypotheses without being reachable.
- **A true safety property is not always an inductive invariant**; it sometimes has to be strengthened: $x = -1$ is inductive, and $x \leq 0$ becomes a theorem (`safety1`, 5 POs, all proved).
- A *counterexample* from the solver distinguishes a false PO from a PO that Rodin merely did not prove.