Dear Reviewers,

Thank you for recognizing the potential of our work, for your time and effort in reviewing our paper, for the diversity of your comments, and the perseverance in our discussions. All these discussions and interactions have shown to us what needed to be explained better.

We are particularly grateful to Reviewer_C for the three separate rounds of discussion, and their patience to explain their views to us.

We now are submitting

- The improved versions of our paper (as two pdfs, with and without the supplementary material),
- A summary of improvements in the current version (next in this pdf),
- A response to the more recent comments from Reviewer*B and Reviewer*C (below in this pdf),
- A diff between the February version and the improved version (as a seperate *pdf).

Summary of improvements in the current version

Improvements Requested by Reviewers

1. We ensured that any terms in Section 2 are used only after their definition.
2. We repaired annoying typos in the Definition of “protected”, and “deep satisfaction”.
3. We extended the discussion of Stbl, Stbl+, and Enc. We added examples that demonstrate their differences, and explanations why these properties are needed.
4. We clarified how the type system is used in reasoning about protection.
5. We added the definition of well-formed specifications (Def 5.6), explained why the various requirements are made. Moreover in the definition of well-formed modules (line 978), we. reminded the reader about the requirement for well-formed specifications.
6. We explained how to obtain sound logics for assertions, even though “protection” is a new concept.
7. We replaced the term “scoped satisfaction” by “deep satisfaction” (lines 1033-1044). We improved the explanation that “deep satisfaction” as well as satisfaction (lines 719-723) are based on scoped execution.
8. We improved the bibliography.

9. We shrunk the subsection on expressiveness to just 4 lines.

10. We discuss the rationale of ghost code in lines 420-425, and give an example where ghost fields are used in Appendix A.3

11. We implemented all further requests made by the reviewers.

Further Improvements -- not Requested by the Reviewers

1. We introduced the notation $^\sigma\lceil A\rceil$ to substitute all free variables in A by their values in σ -- cf. Def. 4.5. This allows us to avoid some clutter in the notations -- cf Def. 5.2.

2. Amalgamated old section 4 into section 3, and old section 6 into old section 5. Now the paper has 8 rather than 10 secretions, and is better balanced.

3. Explained that our approach relies on the platform's guarantees and could also be used for interlanguage safety -- footnote 4.

Reasoning about External Calls

– Responses to February Reviews –

March 25, 2025

1 Response to Reviewer_A

Thank you for your comments in the First Round of reviewing.

2 Response to Reviewer_B

> *Fig. 1 is unreadable; please enlarge it*

Done. We enlarged it, and removed from Fig. 2 the parts that were repeated from Fig. 1.

> *line 222: "objects, Object o4" −− > "objects. Object o4"*

Done.

> *line 480: "Fig. 9" −− > "Fig. 5"*

Done.

> *line 526: two dots are hanging after the beginning of the definition.*
> *I think some text is missing here*

Repaired

> *line 552: something is broken in this definition. There are two dots after f_n, and then the square bracket is open but not close.*

Repaired: Removed superfluous dot, and added missing closing bracket.

> *line 572: "field,," −− > "fields,"*

Repaired.

> *line 622-625: also here I have the feeling the definition is broken. In particular, I would expect that α' appears on the right-hand side of the implication.*
> *As written now, I read the definition as: α' is [locally] reachable from α_0 and external, and we cannot reach α from α_0 in one step. Instead, in the description, I would have expected that the right-hand side would check if α' has a field reaching α (instead of α_0 as it is written now).*

Am I missing something?

You are spot on. The definition should have said $\alpha'.f \neq \alpha$ – thank you for spotting this error in a very crucial definition in our paper.

> line 739, definition 7.4:
$\overline{M}$ is quantified but not used, maybe shuold be $\overline{M}; M$ instead of just M at line 740?
Also, I do not see the need to define A'_3, just use A_3 at line 740.

Exactly as you say! line 740 should have been $\overline{M}; M$ instead of just M.
And as we do not need A'_3, we have slightly re-formatted the definition.
Thank you.

> line 759: "invariants. but" −− > "invariants, but"

Done.

> line 791, section 7.1: I would remove this section.
It presents examples of applications of the approach at a too-high level that, on the one hand, does not allow us to understand if this is really the case; on the other hand, it looks like a bit of overselling.

Done; we only kept a summary of this section.

> bibliography: the various citations are not homogenous, and sometimes some pieces are missing. Just as examples, [25, 30, 33, 39 56, 64, 77] all refer to ECOOP papers, but some of them report page numbers and others do not, some of them have the doi and others do not, and some reports Springer/LNCS others not, etc. The bibliographic entries should be carefully revised.

Done. We have made the bibliographic entries more consistent, ensuring that each entry has a link and page numbers.

3 Response to Reviewer_C

We are deeply grateful to you, for the many pertinent comments, and for engaging with us in several rounds of discussion on hotcrp. In the below we summarize the outcome of these discussions (hopefully Reviewer_C agrees with our summary), and give our responses:

> 1. Section 2 suffers in places from imprecision and bad technical writing. For example, - the important notion of internal and external states ...

We moved the definition of internal/external states to lines 199/200, ie the reader will have seen some states.

> - the critical idea behind the key notion of scoped invariants that internal states are not included shows up just in the final sentence in the para that introduces the scoped assertions, almost like an afterthought.

That is not quite true. In February's submission, the text (lines 250-252) used to say

> "... $\forall \overline{x : C}.A$ expresses that if a state σ has objects $\overline{x}$ of class $\overline{C}$, and satisfies A, then all σ's external, scoped future states will also satisfy A."

However, we have now rephrased for better clarity, to

"... all external states which are part of the scoped future of σ will also satisfy A "

Cf – line 248 in current submission.

> *the last part of section 2 that sketches the proof references for the first time well-formedness conditions about invariants, which are not explained earlier and are only described in the technical sections where it becomes apparent that they are an important for soundness"*

That is a very important point, which had escaped us. Thank you for alerting us. We have given a short description of the requirement for $Stbl^+$ in sect 2.2, we have moved the Def. of well-formed specs to main paper (Def. 5.4) and discuss the rationale of the definition (lines762-772). Moreover, we remind the reader that well-formed specs are required for Module well-formedness (line978).
We did not move these point to Sect 2.2 as you had suggested, because we believe that this would be too much information too early.

> *not sure how the type system plays a role in the argument that* `account.key` *is protected by account*

Another important point; thank you. We explain the role of types in sect 2 (lines 386-391), and also in section 6 (lines 1010-1015).

> *- in the well-formed modules para at the end of 2, the first sentence of this para is only indirectly connected to the rest of the para. In fact, the rest of the para is closer to the external calls para*

We added explanations for what it means for a specification to be well-formed (and why the requirement needs to be made), and made a better bridge to the requirement for a proof of the method body of `Shop::buy`. We also started the paragraph called "External Calls" with a discussion of proofs of method bodies.

> *- make sure that in section 2, all technical terms are introduced together or after all the other technical terms their meaning depends on.*

We moved the Definition of "external state" to line 199. We have carefully read section 2, and checked that all terms are used only after their definition.

> *2. scoped semantics - definition 7.4 i...I do not see how it achieves the "stopping before returning from the active call in " part of the scoped semantics and also - explain in section 7 in detail how 7.4 captures the scoping constraints, in particular for invariants.*

This is now Definition 5.4. We have improved the explanation of Def. 5.2, where we say "then any terminating scoped execution of its continuation" (line 716).
In example 5.3 we mention the $\rightsquigarrow$ relation, and explicitly talk of the states not covered because of stopping before returning.
Similarly, in section 2, line 255 and 273 we say which states are not included, as they are not part of the scoped future.

> *3. Section 9 references in passing the judgment form for assertions and says that this is assumed to be sound with respect to the semantics in section 6.*

However, assertions include protection assertions that are new to this work. So I do not think the workings of the proof system for assertions is obvious

This is now Section 7. Right after Lemma 7.1, we added an argument that sound logics for assertions (including assertions which talk about protection) exist.
We expanded appendix G.1 to show that such an assertion logic can be built out of an assertion logic which does not talk about soundness, and that such a logic would preserve soundness.
We also argue after Lemma 9.1, that a sound underlying Hoare logic which does not talk about protection can be taken from the literature.
Thank you for pointing this out.

> 4. I am confused about the role of $Stbl^+$ and Enc in the proof system of the logic. These are important requirements for preservation of satisfaction.
However, it is not clear how they are connected to the rest of the proof system. I suspect this is through module well-formedness and its premise that Spec(M) is well-formed. But it is unclear if this is the case because this relation is not explained in the paper.

Thank you for pointing this out to us.
Upon further reflection we realized how crucial it is to explain these concepts well. As a result, we expanded the discussion of $Stbl^+$ and *Enc* in sections 4.3.1 and 4.3.2, and added Fig. 6 to demonstrate examples and differences.

> 5. Some secondary parts of the formalism need a bit more fleshing out. Eg
- the expression evaluation that first appears in def 6., is straightforward but there should be a sentence that explains it.
- the ghost fields and their role — I cannot find an example in the main body of the paper where they are needed.

Ghost fields are not needed for our work; they are supported, because they are convenient. We wrote some more explanations about ghost-fields in lines 417-424, discuss the rationale of ghost code in lines 420-425, and give an example where ghost fields are used in Appendix A.3.

> 6. typos and grammatical errors

We have gone through the paper thoroughly and tried to remove all such errors.

> 7. ... nomenclature used in 9 (scoped vs shallow) made things even worse in my mind.

Indeed, it was misleading nomenclature. We now talk of "deep" vs "shallow" satisfaction.
We have added explanations for what it means for a specification to be well-formed (and why the requirement needs to be made), and made a better bridge to the requirement for a proof of the method body of `Shop::buy`.
We also started the paragraph called "External Calls" with a discussion of proofs of method bodies.