Recommended Changes to the SVA Formal Semantics

31 August 2003

1 Overview

These recommendations for changes are the result of reviewing the SV 3.1 version of Annex G and careful scrutiny by the SVA/PSL Alignment Subcommittee of the semantics that it defines. There are several groups of changes represented in the list:

- Minor errata.
- Changes needed to add the finite neutral semantics, which was omitted from the SV 3.1 version due to an oversight.
- Addition of a derived form for multiple local variable assignments, another oversight.
- Errata discovered in the SVA/PSL alignment effort.
- Changes to require non-degeneracy of top-level sequences used in properties. Non-degeneracy is needed in order for the semantics of "disable iff" to be intuitive. The need for non-degeneracy was not discovered until the SVA/PSL alignment effort.

2 Recommended Changes

1. p. 344, Subsection G.2.1, after line 19. Add non-degeneracy requirement.
   NEW: Each instance of R in this production must be a non-degenerate unclocked sequence. See G.3.2 and G.3.5 for the definition of non-degeneracy.
   REASON: Non-degeneracy is required in order for the semantics of "disable iff" to be intuitive.

2. p. 344, Subsection G.2.1, after line 23. Add non-degeneracy requirement.
   NEW: Each instance of S in this production must be a non-degenerate clocked sequence. See G.3.2 and G.3.5 for the definition of non-degeneracy.
   REASON: Non-degeneracy is required in order for the semantics of "disable iff" to be intuitive.

3. p. 346, Subsection G.2.3.5, new final bullet.
   NEW: `(` b`,` $v_1 = e_1$`,...,` $v_k = e_k$ `)`
   $\equiv$ `(` `(` b`,` $v_1 = e_1$ `)` `##0` `(` `1,` $v_2 = e_2$`,...,` $v_k = e_k$ `)` `)` for $k > 1$.
   REASON: Oversight in 3.1 version. Neglected to define this derived form.

4. p. 346, Section G.3, line 3. Change "$\vee$" to "$\top$".
   NEW: $\Sigma = 2^{\mathbf{P}} \cup \{\top, \bot\}$.
   OLD: $\Sigma = 2^{\mathbf{P}} \cup \{\vee, \bot\}$.
   REASON: Erratum.

5. p. 346, Section G.3, line 12. Change "$\vee$" to "$\top$".
   NEW: interchanging $\top$ with $\bot$.
   OLD: interchanging $\vee$ with $\bot$.
   REASON: Erratum.

6. p. 346, Section G.3, line 12. Fix poor line break and change "$\vee$" to "$\top$".
   NEW: $\bar{w}^i = \top$.
   OLD: $\bar{w}$ ⟨line break⟩ $^i = \vee$.
   REASONS: Errata.

7. p. 346, Section G.3, line 13. Change "$\vee$" to "$\top$".
   NEW: if $w^i = \top$.
   OLD: if $w^i = \vee$.
   REASON: Erratum.

8. p. 346, Section G.3, line 18. Change "$\vee$" to "$\top$".
   NEW: $\top \models b$.
   OLD: $\vee \models b$.
   REASON: Erratum.

9. p. 347, Subsection G.3.2, line 3.
   NEW: $w \models\!\models b$ iff $|w| = 1$ and $w^0 \models b$.
   OLD: $w \models\!\models b$ iff $|w| = 1$ and $w \models b$.
   REASON: Erratum. The document fails to identify a word of length one with its letter, so the old definition leads to a circularity.

10. p. 347, Subsection G.3.2, line 11.
    NEW: if there exist x, y such that $w = xy$ and $\bar{x} \models\!\models R$, then
    OLD: if there exist x, y such that $w = xy$ and $x \models\!\models R$, then
    REASON: Erratum. Not discovered until the study of non-degeneracy.

11. p. 347, Subsection G.3.2, end. Add definition of non-degeneracy.
    NEW: An unclocked sequence R is *non-degenerate* iff there exists a non-empty finite word w over Σ such that $w \models\!\models R$. A clocked sequence S is *non-degenerate* iff the unclocked sequence S' that results from S by applying the rewrite rules is non-degenerate.
    REASON: Non-degeneracy is required in order for the semantics of "disable iff" to be intuitive.

12. p. 347, Subsection G.3.3.1 heading. Change heading.
    NEW: Neutral satisfaction.
    OLD: Satisfaction by infinite words.
    REASON: Addition of finite neutral semantics.

13. p. 347, Subsection G.3.3.1, line 1.
    NEW: w denotes a non-empty finite or infinite word over Σ.
    OLD: w denotes an infinite word over Σ.
    REASON: Addition of finite neutral semantics.

14. p. 347, Subsection G.3.3.1, line 3. Change heading.
    NEW: **Neutral satisfaction of assertions:**
    OLD: **Assertion Satisfaction:**
    REASON: Addition of finite neutral semantics.

15. p. 347, Subsection G.3.3.1, line 4.
    NEW: For the definition of neutral satisfaction of assertions, b denotes the boolean
    OLD: For the definition of assertion satisfaction, b denotes the boolean
    REASON: Addition of finite neutral semantics.

16. p. 347, Subsection G.3.3.1, line 7.
    NEW: for every $0 \leq i < |w|$ such that $\bar{w}^i \models c$ and $\bar{w}^i \models b$, $w^{i\cdot\cdot} \models$ `@(`c`)` P .
    OLD: for every $i \geq 0$ such that $w^i \models c$, if $\bar{w}^i \models b$ then $w^{i\cdot\cdot} \models$ `@(`c`)` P .
    REASONS: Addition of finite neutral semantics and missing bar on w^i in $w^i \models c$ (erratum discovered in SVA/PSL alignment).

17. p. 347, Subsection G.3.3.1, line 9.
    NEW: for every $0 \leq i < |w|$, if $\bar{w}^i \models b$ then $w^{i\cdot\cdot} \models Q$.
    OLD: for every $i \geq 0$, if $\bar{w}^i \models b$ then $w^{i\cdot\cdot} \models Q$.
    REASON: Addition of finite neutral semantics.

18. p. 347, Subsection G.3.3.1, line 10.
    NEW: for every $0 \leq i < |w|$ such that $\bar{w}^{0,i} \models$ `!`c `[*0:$] ##1` c and $\bar{w}^i \models b$,
    OLD: if there exists $i \geq 0$ such that $w^i \models c$, then for the first such i, if $\bar{w}^i \models b$ then
    REASONS: Addition of finite neutral semantics, missing bar on w^i in $w^i \models c$ (erratum discovered in SVA/PSL alignment), incorrect use of "for the first such" in the presence of $\top, \bot$ (erratum discovered in SVA/PSL alignment), and change of "if there exists" to "for every" to simplify SVA/PSL alignment proofs (this last change does not affect the semantics).

19. p. 348, Subsection G.3.3.1, line 2. Change heading.
    NEW: **Neutral satsifaction of properties:**
    OLD: **Property Satisfaction:**
    REASON: Addition of finite neutral semantics.

20. p. 348, Subsection G.3.3.1, line 4.
    NEW: $w \models \varphi$ or there exists $0 \leq k < |w|$ such that $w^k \models b$ and
    OLD: $w \models \varphi$ or there exists $k \geq 0$ such that $w^k \models b$ and
    REASON: Addition of finite neutral semantics.

21. p. 348, Subsection G.3.3.1, line 7.
NEW: $w \models R$ iff there exists $0 \leq j < |w|$ such that
OLD: $w \models R$ iff there exists $j \geq 0$ such that
REASON: Addition of finite neutral semantics.

22. p. 348, Subsection G.3.3.1, line 8.
NEW: iff for every $0 \leq j < |w|$ such that $\bar{w}^{0,j} \models\!\models R_1$, $w^{j\cdot\cdot} \models N\ R_2$.
OLD: iff for every $j \geq 0$ such that $\bar{w}^{0,j} \models\!\models R_1$, $w^{j\cdot\cdot} \models N\ R_2$.
REASON: Addition of finite neutral semantics.

23. p. 348, Subsection G.3.3.2, heading. Change heading.
NEW: Weak and strong satisfaction by finite words
OLD: Satisfaction by finite words
REASON: Addition of finite neutral semantics.

24. p. 348, Subsection G.3.3.2, line 1.
NEW: of an assertion A by a finite (possibly empty) word w over Σ. These relations are defined in terms of the relation of neutral satisfaction by infinite words as follows:
OLD: of an assertion A by a finite word w over Σ. These relations are defined in terms of the relation of satisfaction by infinite words as follows:
REASON: Clarification.

25. p. 348, Subsection G.3.3.2, line 4. Change "$\vee$" to "$\top$".
NEW: $w\top^\omega \models A$
OLD: $w\vee^\omega \models A$
REASON: Erratum.

26. p.348, Subsection G.3.3.3. Change subsection number.
NEW: G.3.4
OLD: G.3.3.3.
REASON: Erratum.

27. p.349, Subsection G.3.4. Change subsection number.
NEW: G.3.5
OLD: G.3.4
REASON: Erratum.

28. p. 350, Subsection G.3.4, line 10.
NEW: first according to L_0 and second according to w^0. In case $w^0 \in \{\top, \bot\}$, $e[L_0, \top]$ and $e[L_0, \bot]$ can be any constant values of the type of e.
OLD: first according to L_0 and second according to w^0.
REASON: Clarification. The old definition does not say what $e[L_0, \top]$ and $e[L_0, \bot]$ mean. It turns out that their particular choice is irrelevant as long as they are constants (or expressions) of the type of e.

29. p. 350, Subsection G.3.4, line 28.
NEW: $\bar{x}, L_0, L' \models\!\models R$, then y is empty.
OLD: $x, L_0, L' \models\!\models R$, then y is empty.
REASON: Erratum. Not discovered until the study of non-degeneracy.

30. p. 350, Subsection G.3.4, end. Add definition of non-degeneracy.
    NEW: An unclocked sequence R is *non-degenerate* iff there exist a non-empty finite word w over Σ and local variable contexts L_0, L_1 such that $w, L_0, L_1 \models R$. A clocked sequence S is *non-degenerate* iff the unclocked sequence S' that results from S by applying the rewrite rules is non-degenerate.
    REASON: Non-degeneracy is required in order for the semantics of "disable iff" to be intuitive.

31. p. 350, Subsection G.3.5. Change subsection number.
    NEW: G.3.6
    OLD: G.3.5
    REASON: Erratum.

32. p.350, Subsection G.3.5.1. Change subsection number.
    NEW: G.3.6.1
    OLD: G.3.5.1
    REASON: Erratum.

33. p. 350, Subsection G.3.5.1, heading.
    NEW: Neutral satisfaction
    OLD: Satisfaction by infinite words
    REASON: Addition of finite neutral semantics.

34. p. 350, Subsection G.3.5.1, line 1.
    NEW: w denotes a non-empty finite or infinite word over Σ.
    OLD: w denotes an infinite word over Σ.
    REASON: Addition of finite neutral semantics.

35. p. 351, Subsection G.3.5.1, line 1.
    NEW: The rules defining neutral satisfaction of an assertion are identical to those without
    OLD: The rules defining assertion satisfaction are identical to those without
    REASON: Addition of finite neutral semantics.

36. p. 351, Subsection G.3.5.1, line 3. Change heading
    NEW: **Neutral satisfaction of properties:**
    OLD: Property Satisfaction:
    REASONS: Addition of finite neutral semantics and font correction.

37. p. 351, Subsection G.3.5.1, new first bullet.
    NEW: $w \models Q$ iff $w, \{\} \models Q$.
    REASON: To uniformize the bullets in this subsection. Before, some bullets required empty local variable context, while others allowed general local variable context.

38. p. 351, Subsection G.3.5.1, line 4.
    NEW: $w, L_0 \models Q$ iff $w, L_0 \models Q'$, where Q' is the unclocked
    OLD: $w \models Q$ iff $w, \{\} \models Q'$, where Q' is the unclocked
    REASON: To uniformize the bullets in this subsection. Before, some bullets required empty local variable context, while others allowed general local variable context.

39. p. 351, Subsection G.3.5.1, line 5.
NEW: $w, L_0 \models$ `disable iff (`b`)` φ iff either $w, L_0 \models \varphi$ or there exists $0 \leq k < |w|$ such that $w^k \models b[L_0]$ and $w^{0,k-1}\top^\omega, L_0 \models \varphi$. Here, $w^{0,-1}$ denotes the
OLD: $w, \{\} \models$ `disable iff (`b`)` φ iff either $w, \{\} \models \varphi$ or there exists $k \geq 0$ such that $w^k \models b$ and $w^{0,k-1}\top^\omega, \{\} \models \varphi$. Here, $w^{0,-1}$ denotes the
REASONS: Addition of finite neutral semantics and to uniformize the bullets in this subsection. Before, some bullets required empty local variable context, while others allowed general local variable context.

40. p. 351, Subsection G.3.5.1, line 8.
NEW: $w, L_0 \models R$ iff there exist $0 \leq j < |w|$ and L_1 such that
OLD: $w, L_0 \models R$ iff there exist $j \geq 0$ and L_1 such that
REASON: Addition of finite neutral semantics.

41. p. 351, Subsection G.3.5.1, line 9.
NEW: iff for every $0 \leq j < |w|$ and L_1 such that $\bar{w}^{0,j}, L_0, L_1 \models\!\!\models R_1$,
OLD: iff for every $j \geq 0$ and L_1 such that $\bar{w}^{0,j}, L_0, L_1 \models\!\!\models R_1$,
REASON: Addition of finite neutral semantics.

42. p. 351, Subsection G.3.5.2, heading. Change heading and subsection number.
NEW: **G.3.6.2 Weak and strong satisfaction by finite words**
OLD: **G.3.5.2 Satisfaction by finite words**
REASON: Addition of finite neutral semantics, erratum.

43. p. 351, Subsection G.4.1, line 1.
NEW: w denotes a non-empty finite or infinite word over Σ, j denotes an integer such that $0 \leq j < |w|$, and
OLD: w denotes an infinite word over Σ,
REASON: Addition of finite neutral semantics.

44. p. 351, Subsection G.4.1, line 2.
NEW: $w^j \models T$`.ended` iff there exist $0 \leq i \leq j$ and L such that
OLD: $w^j \models T$`.ended` iff there exist $i \leq j$ and L such that
REASON: Addition of finite neutral semantics.

45. p. 351, Subsection G.4.1, line 3.
NEW: iff there exists $0 \leq i < j$ such that $w^i \models T$`.ended` and
OLD: iff there exists $i < j$ such that $w^i \models T$`.ended` and
REASON: Addition of finite neutral semantics.

46. p. 351, Subsection G.4.1, line 5.
NEW: $0 \leq i < j$ such that
OLD: $i < j$ such that
REASON: Addition of finite neutral semantics.

47. p. 351, Subsection G.4.1, line 6.
NEW: $0 \leq i < j$ such that
OLD: $i < j$ such that
REASON: Addition of finite neutral semantics.

48. p. 351, Subsection G.4.1, line 8.
NEW: $0 \leq i < j$ such that
OLD: $i < j$ such that
REASON: Addition of finite neutral semantics.

49. p. 351, Subsection G.4.2, line 1.
NEW: w denotes a non-empty finite or infinite word over Σ, and j denotes an integer such that $0 \leq j < |w|$.
OLD: w denotes an infinite word over Σ.
REASON: Addition of finite neutral semantics.

50. p. 351, Subsection G.4.2, line 2.
NEW: If there exists $0 \leq i < j$ such that $w^{i,j}, \{\}, \{\} \models$
OLD: If there exist $i < j$ such that $w^{i,j}, \{\}, \{\} \models$
REASON: Addition of finite neutral semantics.