1 VCG Invariant

theory *VCG-Invariant* = *VCG*:

— In invariantVCG we show that if wpF computes weakest(!) preconditions and if branch conditions of succsF ensure progress then VCG emits invariants.

locale *invariantVCG* = *VCG* +

fixes *isSafe'*::'*prog* ⇒ *bool*
defines *isSafe'* ≡ λ *prg*. ∀ *s s'*. *s* ∈ *initS prg* ∧ (*s*,*s'*) ∈ (*effS prg*)* ⟶ *prg*,*s'* ⊨ *saF prg* (*fst s'*)

assumes *semImpI*: ⟦ *prg*,*s* ⊨ *f1* ⟹ *prg*,*s* ⊨ *f2* ⟧ ⟹ *prg*,*s* ⊨ *f1* ⌞⇒⌟ *f2*

assumes *succsFprogress*: ⟦ *wf prg*; *correctAn prg*; *isSafe prg*; (*p*,*m*) ∈ *Reachables prg*;
prg,(*p*,*m*) ⊨ *B*; (*p'*,*B*) ∈ *set* (*succsF prg p''*) ⟧ ⟹ *p*=*p''* ∧ (∃ *m'*. ((*p*,*m*),(*p'*,*m'*)) ∈ (*effS prg*))

assumes *completeWpF*: ⟦ *wf prg*; *correctAn prg*; *isSafe prg*; (*p*,*m*) ∈ *Reachables prg*;
((*p*,*m*),(*p'*,*m'*)) ∈ (*effS prg*) ; *prg*,(*p'*,*m'*) ⊨ *Q*; ∃ *B*. (*p'*,*B*) ∈ *set* (*succsF prg p*) ⟧ ⟹ *prg*,(*p*,*m*) ⊨ *wpF prg p p' Q*

assumes *ipc-domC*:
wf prg ⟹ *ipc prg* ∈ *set* (*domC prg*)

assumes *succsF-domC*:
⟦ *wf* Π; (*p'*,*B*) ∈ *set* (*succsF* Π *p*) ⟧ ⟹ (*p* ∈ *set* (*domC* Π)) ∧ (*p'* ∈ *set* (*domC* Π))

lemma (**in** *invariantVCG*) *isSafe'-correctAn-isSafe*:
isSafe' Π = (*isSafe* Π ∧ *correctAn* Π)

lemma (**in** *invariantVCG*) *isSafe'-isafeF*:
⟦ *wf* Π; *isSafe'* Π; *s* ∈ *initS* Π; (*s*,*s'*) ∈ (*effS* Π)* ; *fst s'* ∈ *set* (*domC* Π)⟧ ⟹ Π,*s'* ⊨ *isafeF* Π (*fst s'*)

lemma (**in** *invariantVCG*) *vcg-invariant*:
⟦ *wf* Π; *isSafe'* Π ⟧ ⟹ (∀ *s* ∈ *Reachables* Π. Π,*s* ⊨ *vcg* Π)

lemma (**in** *invariantVCG*) *vcg-inv-completeness*:

$[\![$ *wf* Π; *isSafe* Π; *correctAn* Π; $(\forall\ s \in \mathit{Reachables}\ \Pi.\ \Pi,s \models \mathit{vcg}\ \Pi) \longrightarrow \Pi \vdash \mathit{vcg}\ \Pi\ ]\!] \Longrightarrow \Pi \vdash \mathit{vcg}\ \Pi$
end