theory *SALOverflowPlatform-deep* = *SALSafetyLogic-deep* + *TupleOrd*:

1 SAL Overflow Platform

In this theory we instantiate a wellformedness checker and the generic VCG from the PCC Framework.

1.1 Wellformedness Checker

consts
checkPos :: *SALprogram* ⇒ (*pos list*) ⇒ *bool*

primrec
checkPos prg [] = *True*
checkPos prg (*pc* # *pcs*) = (*if* (*let* (*pn*, *i*) = *pc in* (*case* (*cmd prg pc*) *of*
None ⇒ *False*
| *Some c* ⇒ (*case c of*
SET x n ⇒ *True*
| *ADD x y* ⇒ *True*
| *SUB x y* ⇒ *True*
| *INC x* ⇒ *True*
| *JMPEQ x y t* ⇒ (*t* = *0*) ⟶ ((*anF prg* (*pn*, *i*)) ≠ *None*)
| *JMPL x y t* ⇒ (*t* = *0*) ⟶ ((*anF prg* (*pn*, *i*)) ≠ *None*)
| *JLE x y t* ⇒ (*t* = *0*) ⟶ ((*anF prg* (*pn*, *i*)) ≠ *None*)
| *JMPB t* ⇒ ((*anF prg* (*pn*, *i* − *t*)) ≠ *None*)
| *CALL x pn′* ⇒ (*anF prg* (*pn′*, *0*) ≠ *None*)
| *RET x* ⇒ (*list-all* (λ (*pc*, *B*). *anF prg pc* ≠ *None*) (*ret-succs prg pc x* (*callpoints prg pn*))) ∧ (*0* < *pn*)
| *MOV s t* ⇒ *True*
| *HALT* ⇒ *True*
)))
then (*checkPos prg pcs*)
else False)

constdefs
wf :: *SALprogram* ⇒ *bool*
wf prg ≡ *checkPos prg* (*domC prg*)

constdefs
domA :: *SALprogram* ⇒ *pos list*
domA ≡ λ *prg*. [*pc*∈ *domC prg*. (*anF prg pc*) ≠ *None*]

constdefs
vcgSALDeep :: *SALprogram* ⇒ *SALform*
vcgSALDeep prg ≡ *vcG Conj Impl FalseF ipc initF safeF succsF wpF domC domA anF prg*

syntax
callmem :: *env* ⇒ *tram* ($\overleftarrow{m}$ -)
callpc :: *env* ⇒ *pos* ($\overleftarrow{pc}$ -)
callenv :: *env* ⇒ *env* ($\overleftarrow{e}$ -)

1.2 Generate ML code for the VCG

generate-code (*vcgSALDeep.ML*) [*term-of*]
vcg = *vcgSALDeep*

end