

**theory** *SALTimeFWInst* = *SALTimePlatform* + *SALOverflowFWInst*:

— Instantiating the VCG Framework

**lemma** *safeF-mono*:

$(\text{safeF } \text{prg } p) s \implies (\text{SALSafetyLogic.safeF } \text{prg } p) s$   
**by** (*simp add: safeF-def Conj-def*)

**lemma** *wpF-mono*:

$\llbracket (\text{wpF } \text{prg } p \ p' \ Q) s; (\forall s. Q \ s \longrightarrow Q' \ s) \rrbracket \implies (\text{wpF } \text{prg } p \ p' \ Q') \text{ sdone}$

**lemma** *isafe-mono*:

$\bigwedge s. \text{valid } \text{prg } s \ (\text{isafe } (\text{domC } \text{prg}, \text{prg}, \text{anF } \text{prg}, p, \text{FalseF}, \text{Conj}, \text{Impl}, \text{safeF}, \text{succsF}, \text{wpF}))$   
 $\implies \text{valid } \text{prg } s \ (\text{isafe } (\text{domC } \text{prg}, \text{prg}, \text{anF } \text{prg}, p, \text{FalseF}, \text{Conj}, \text{Impl}, \text{SALSafetyLogic.safeF}, \text{succsF}, \text{wpF}))$   
**done**

**lemma** *isafeP-mono*:

$\bigwedge s \ \text{prg}. \llbracket s \in \text{isafeP } \text{prg} \rrbracket \implies s \in (\text{SALSafetyLogic.isafeP } \text{prg}) \text{done}$

**theorem** *SAL-VCG-Ins*:

*VerificationConditionGenerator Conj Impl TrueF FalseF valid provable effS wpF succsF initF ipc SALTimePlatform.safeF anF domC wf done*

## 1 Platform Soundness

**constdefs** *isSafe::SALprogram*  $\Rightarrow$  *bool*

$\text{isSafe } \text{prg} \equiv (\forall s \ s'. \text{prg}, s \models \text{initF } \text{prg} \wedge (s, s') \in (\text{effS } \text{prg})^* \longrightarrow \text{prg}, s' \models \text{safeF } \text{prg} \ (\text{fst } s'))$

**theorem** *platform-soundness*:

$\llbracket \text{wf } \text{prg}; \text{provable } \text{prg} \ (\text{vcgSALT } \text{prg}) \rrbracket \implies \text{isSafe } \text{prg} \text{done}$

**end**