Contents

1 projectTypes Theory

Built: 27 December 2018
Parent Theories: indexedLists, patternMatches

1.1 Datatypes

commands =
    PlatoonLeaderCOM platoonLeaderCom
  | PlatoonSergeantCOM platoonSergeantCom
  | OmniCOM omniCom

omniCom = none | omniNA

output = Secure | Withdraw | Complete | ActionsIn
       | NoActionTaken | UnAuthenticated | UnAuthorized

platoonLeaderCom = secure | withdraw | complete

platoonSergeantCom = actionsIn | psgNA

principal = PlatoonLeader | PlatoonSergeant | Omni

state = CONDUCT_PB | SECURE | ACTIONS_IN | WITHDRAW | COMPLETE

1.2 Theorems

[commands_distinct_clauses]

$\vdash$ $(\forall a'\ a.$ PlatoonLeaderCOM $a \neq$ PlatoonSergeantCOM $a') \wedge$
  $(\forall a'\ a.$ PlatoonLeaderCOM $a \neq$ OmniCOM $a') \wedge$
  $\forall a'\ a.$ PlatoonSergeantCOM $a \neq$ OmniCOM a'

[commands_one_one]

$\vdash$ $(\forall a\ a'.$
    (PlatoonLeaderCOM a = PlatoonLeaderCOM $a') \iff (a = a')) \wedge$
  $(\forall a\ a'.$
    (PlatoonSergeantCOM a = PlatoonSergeantCOM $a') \iff$
    $(a = a')) \wedge \forall a\ a'.$ (OmniCOM a = OmniCOM $a') \iff (a = a')$

[omniCom_distinct_clauses]

$\vdash$ none $\neq$ omniNA

[output_distinct_clauses]
⊢ Secure ≠ Withdraw ∧ Secure ≠ Complete ∧ Secure ≠ ActionsIn ∧
Secure ≠ NoActionTaken ∧ Secure ≠ UnAuthenticated ∧
Secure ≠ UnAuthorized ∧ Withdraw ≠ Complete ∧
Withdraw ≠ ActionsIn ∧ Withdraw ≠ NoActionTaken ∧
Withdraw ≠ UnAuthenticated ∧ Withdraw ≠ UnAuthorized ∧
Complete ≠ ActionsIn ∧ Complete ≠ NoActionTaken ∧
Complete ≠ UnAuthenticated ∧ Complete ≠ UnAuthorized ∧
ActionsIn ≠ NoActionTaken ∧ ActionsIn ≠ UnAuthenticated ∧
ActionsIn ≠ UnAuthorized ∧ NoActionTaken ≠ UnAuthenticated ∧
NoActionTaken ≠ UnAuthorized ∧ UnAuthenticated ≠ UnAuthorized

[platoonLeaderCom_distinct_clauses]
⊢ secure ≠ withdraw ∧ secure ≠ complete ∧ withdraw ≠ complete

[platoonSergeantCom_distinct_clauses]
⊢ actionsIn ≠ psgNA

[principal_distinct_clauses]
⊢ PlatoonLeader ≠ PlatoonSergeant ∧ PlatoonLeader ≠ Omni ∧
PlatoonSergeant ≠ Omni

[state_distinct_clauses]
⊢ CONDUCT_PB ≠ SECURE ∧ CONDUCT_PB ≠ ACTIONS_IN ∧
CONDUCT_PB ≠ WITHDRAW ∧ CONDUCT_PB ≠ COMPLETE ∧
SECURE ≠ ACTIONS_IN ∧ SECURE ≠ WITHDRAW ∧ SECURE ≠ COMPLETE ∧
ACTIONS_IN ≠ WITHDRAW ∧ ACTIONS_IN ≠ COMPLETE ∧
WITHDRAW ≠ COMPLETE

2 projectUtilities Theory

Built: 27 December 2018
Parent Theories: projectTypes, satList

2.1 Theorems

[getOmniCOM_def]
⊢ (getOmniCOM [] = NONE) ∧
(∀ *xs cmd*.
getOmniCOM (SOME (OmniCOM *cmd*)::*xs*) =
SOME (OmniCOM *cmd*)) ∧
(∀ *xs*. getOmniCOM (NONE::*xs*) = getOmniCOM *xs*) ∧
(∀ *xs* v_4.
getOmniCOM (SOME (PlatoonLeaderCOM v_4)::*xs*) =
getOmniCOM *xs*) ∧
∀ *xs* v_5.
getOmniCOM (SOME (PlatoonSergeantCOM v_5)::*xs*) =
getOmniCOM *xs*

[getOmniCOM_ind]

```
⊢ ∀P.
    P [] ∧ (∀cmd xs. P (SOME (OmniCOM cmd)::xs)) ∧
    (∀xs. P xs ⇒ P (NONE::xs)) ∧
    (∀v4 xs. P xs ⇒ P (SOME (PlatoonLeaderCOM v4)::xs)) ∧
    (∀v5 xs. P xs ⇒ P (SOME (PlatoonSergeantCOM v5)::xs)) ⇒
    ∀v. P v
```

[getOmniCOMx_def]

```
⊢ (getOmniCOMx [] = NONE) ∧
  (∀xs cmd.
     getOmniCOMx
       (Name Omni says prop (SOME (OmniCOM cmd))::xs) =
     SOME (OmniCOM cmd)) ∧
  (∀xs. getOmniCOMx (TT::xs) = getOmniCOMx xs) ∧
  (∀xs. getOmniCOMx (FF::xs) = getOmniCOMx xs) ∧
  (∀xs v2. getOmniCOMx (prop v2::xs) = getOmniCOMx xs) ∧
  (∀xs v3. getOmniCOMx (notf v3::xs) = getOmniCOMx xs) ∧
  (∀xs v5 v4. getOmniCOMx (v4 andf v5::xs) = getOmniCOMx xs) ∧
  (∀xs v7 v6. getOmniCOMx (v6 orf v7::xs) = getOmniCOMx xs) ∧
  (∀xs v9 v8. getOmniCOMx (v8 impf v9::xs) = getOmniCOMx xs) ∧
  (∀xs v11 v10.
     getOmniCOMx (v10 eqf v11::xs) = getOmniCOMx xs) ∧
  (∀xs v12. getOmniCOMx (v12 says TT::xs) = getOmniCOMx xs) ∧
  (∀xs v12. getOmniCOMx (v12 says FF::xs) = getOmniCOMx xs) ∧
  (∀xs v134.
     getOmniCOMx (Name v134 says prop NONE::xs) =
     getOmniCOMx xs) ∧
  (∀xs v144.
     getOmniCOMx
       (Name PlatoonLeader says prop (SOME v144)::xs) =
     getOmniCOMx xs) ∧
  (∀xs v144.
     getOmniCOMx
       (Name PlatoonSergeant says prop (SOME v144)::xs) =
     getOmniCOMx xs) ∧
  (∀xs v146.
     getOmniCOMx
       (Name Omni says prop (SOME (PlatoonLeaderCOM v146))::
            xs) =
     getOmniCOMx xs) ∧
  (∀xs v147.
     getOmniCOMx
       (Name Omni says prop (SOME (PlatoonSergeantCOM v147))::
            xs) =
     getOmniCOMx xs) ∧
  (∀xs v68 v136 v135.
     getOmniCOMx (v135 meet v136 says prop v68::xs) =
     getOmniCOMx xs) ∧
```

```
(∀ xs v68 v138 v137.
   getOmniCOMx (v137 quoting v138 says prop v68::xs) =
   getOmniCOMx xs) ∧
(∀ xs v69 v12.
   getOmniCOMx (v12 says notf v69::xs) = getOmniCOMx xs) ∧
(∀ xs v71 v70 v12.
   getOmniCOMx (v12 says (v70 andf v71)::xs) =
   getOmniCOMx xs) ∧
(∀ xs v73 v72 v12.
   getOmniCOMx (v12 says (v72 orf v73)::xs) =
   getOmniCOMx xs) ∧
(∀ xs v75 v74 v12.
   getOmniCOMx (v12 says (v74 impf v75)::xs) =
   getOmniCOMx xs) ∧
(∀ xs v77 v76 v12.
   getOmniCOMx (v12 says (v76 eqf v77)::xs) =
   getOmniCOMx xs) ∧
(∀ xs v79 v78 v12.
   getOmniCOMx (v12 says v78 says v79::xs) =
   getOmniCOMx xs) ∧
(∀ xs v81 v80 v12.
   getOmniCOMx (v12 says v80 speaks_for v81::xs) =
   getOmniCOMx xs) ∧
(∀ xs v83 v82 v12.
   getOmniCOMx (v12 says v82 controls v83::xs) =
   getOmniCOMx xs) ∧
(∀ xs v86 v85 v84 v12.
   getOmniCOMx (v12 says reps v84 v85 v86::xs) =
   getOmniCOMx xs) ∧
(∀ xs v88 v87 v12.
   getOmniCOMx (v12 says v87 domi v88::xs) =
   getOmniCOMx xs) ∧
(∀ xs v90 v89 v12.
   getOmniCOMx (v12 says v89 eqi v90::xs) = getOmniCOMx xs) ∧
(∀ xs v92 v91 v12.
   getOmniCOMx (v12 says v91 doms v92::xs) =
   getOmniCOMx xs) ∧
(∀ xs v94 v93 v12.
   getOmniCOMx (v12 says v93 eqs v94::xs) = getOmniCOMx xs) ∧
(∀ xs v96 v95 v12.
   getOmniCOMx (v12 says v95 eqn v96::xs) = getOmniCOMx xs) ∧
(∀ xs v98 v97 v12.
   getOmniCOMx (v12 says v97 lte v98::xs) = getOmniCOMx xs) ∧
(∀ xs v99 v12 v100.
   getOmniCOMx (v12 says v99 lt v100::xs) = getOmniCOMx xs) ∧
(∀ xs v15 v14.
   getOmniCOMx (v14 speaks_for v15::xs) = getOmniCOMx xs) ∧
(∀ xs v17 v16.
   getOmniCOMx (v16 controls v17::xs) = getOmniCOMx xs) ∧
```

```
   (∀ xs v20 v19 v18.
      getOmniCOMx (reps v18 v19 v20::xs) = getOmniCOMx xs) ∧
   (∀ xs v22 v21.
      getOmniCOMx (v21 domi v22::xs) = getOmniCOMx xs) ∧
   (∀ xs v24 v23.
      getOmniCOMx (v23 eqi v24::xs) = getOmniCOMx xs) ∧
   (∀ xs v26 v25.
      getOmniCOMx (v25 doms v26::xs) = getOmniCOMx xs) ∧
   (∀ xs v28 v27.
      getOmniCOMx (v27 eqs v28::xs) = getOmniCOMx xs) ∧
   (∀ xs v30 v29.
      getOmniCOMx (v29 eqn v30::xs) = getOmniCOMx xs) ∧
   (∀ xs v32 v31.
      getOmniCOMx (v31 lte v32::xs) = getOmniCOMx xs) ∧
   ∀ xs v34 v33. getOmniCOMx (v33 lt v34::xs) = getOmniCOMx xs
```

[getOmniCOMx_ind]

```
⊢ ∀ P.
    P [] ∧
    (∀ cmd xs.
       P (Name Omni says prop (SOME (OmniCOM cmd))::xs)) ∧
    (∀ xs. P xs ⇒ P (TT::xs)) ∧ (∀ xs. P xs ⇒ P (FF::xs)) ∧
    (∀ v2 xs. P xs ⇒ P (prop v2::xs)) ∧
    (∀ v3 xs. P xs ⇒ P (notf v3::xs)) ∧
    (∀ v4 v5 xs. P xs ⇒ P (v4 andf v5::xs)) ∧
    (∀ v6 v7 xs. P xs ⇒ P (v6 orf v7::xs)) ∧
    (∀ v8 v9 xs. P xs ⇒ P (v8 impf v9::xs)) ∧
    (∀ v10 v11 xs. P xs ⇒ P (v10 eqf v11::xs)) ∧
    (∀ v12 xs. P xs ⇒ P (v12 says TT::xs)) ∧
    (∀ v12 xs. P xs ⇒ P (v12 says FF::xs)) ∧
    (∀ v134 xs. P xs ⇒ P (Name v134 says prop NONE::xs)) ∧
    (∀ v144 xs.
       P xs ⇒
       P (Name PlatoonLeader says prop (SOME v144)::xs)) ∧
    (∀ v144 xs.
       P xs ⇒
       P (Name PlatoonSergeant says prop (SOME v144)::xs)) ∧
    (∀ v146 xs.
       P xs ⇒
       P
         (Name Omni says prop (SOME (PlatoonLeaderCOM v146))::
              xs)) ∧
    (∀ v147 xs.
       P xs ⇒
       P
         (Name Omni says
          prop (SOME (PlatoonSergeantCOM v147))::xs)) ∧
    (∀ v135 v136 v68 xs.
       P xs ⇒ P (v135 meet v136 says prop v68::xs)) ∧
```

$(\forall\, v137\ v138\ v_{68}\ xs.$
$\quad P\ xs \Rightarrow P\ (v137\ \texttt{quoting}\ v138\ \texttt{says prop}\ v_{68}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{69}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says notf}\ v_{69}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{70}\ v_{71}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ (v_{70}\ \texttt{andf}\ v_{71})\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{72}\ v_{73}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ (v_{72}\ \texttt{orf}\ v_{73})\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{74}\ v_{75}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ (v_{74}\ \texttt{impf}\ v_{75})\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{76}\ v_{77}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ (v_{76}\ \texttt{eqf}\ v_{77})\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{78}\ v_{79}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{78}\ \texttt{says}\ v_{79}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{80}\ v_{81}\ xs.$
$\quad P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{80}\ \texttt{speaks\_for}\ v_{81}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{82}\ v_{83}\ xs.$
$\quad P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{82}\ \texttt{controls}\ v_{83}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{84}\ v_{85}\ v_{86}\ xs.$
$\quad P\ xs \Rightarrow P\ (v_{12}\ \texttt{says reps}\ v_{84}\ v_{85}\ v_{86}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{87}\ v_{88}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{87}\ \texttt{domi}\ v_{88}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{89}\ v_{90}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{89}\ \texttt{eqi}\ v_{90}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{91}\ v_{92}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{91}\ \texttt{doms}\ v_{92}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{93}\ v_{94}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{93}\ \texttt{eqs}\ v_{94}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{95}\ v_{96}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{95}\ \texttt{eqn}\ v_{96}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{97}\ v_{98}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{97}\ \texttt{lte}\ v_{98}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{99}\ v100\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{99}\ \texttt{lt}\ v100\texttt{::}xs)) \wedge$
$(\forall\, v_{14}\ v_{15}\ xs.\ P\ xs \Rightarrow P\ (v_{14}\ \texttt{speaks\_for}\ v_{15}\texttt{::}xs)) \wedge$
$(\forall\, v_{16}\ v_{17}\ xs.\ P\ xs \Rightarrow P\ (v_{16}\ \texttt{controls}\ v_{17}\texttt{::}xs)) \wedge$
$(\forall\, v_{18}\ v_{19}\ v_{20}\ xs.\ P\ xs \Rightarrow P\ (\texttt{reps}\ v_{18}\ v_{19}\ v_{20}\texttt{::}xs)) \wedge$
$(\forall\, v_{21}\ v_{22}\ xs.\ P\ xs \Rightarrow P\ (v_{21}\ \texttt{domi}\ v_{22}\texttt{::}xs)) \wedge$
$(\forall\, v_{23}\ v_{24}\ xs.\ P\ xs \Rightarrow P\ (v_{23}\ \texttt{eqi}\ v_{24}\texttt{::}xs)) \wedge$
$(\forall\, v_{25}\ v_{26}\ xs.\ P\ xs \Rightarrow P\ (v_{25}\ \texttt{doms}\ v_{26}\texttt{::}xs)) \wedge$
$(\forall\, v_{27}\ v_{28}\ xs.\ P\ xs \Rightarrow P\ (v_{27}\ \texttt{eqs}\ v_{28}\texttt{::}xs)) \wedge$
$(\forall\, v_{29}\ v_{30}\ xs.\ P\ xs \Rightarrow P\ (v_{29}\ \texttt{eqn}\ v_{30}\texttt{::}xs)) \wedge$
$(\forall\, v_{31}\ v_{32}\ xs.\ P\ xs \Rightarrow P\ (v_{31}\ \texttt{lte}\ v_{32}\texttt{::}xs)) \wedge$
$(\forall\, v_{33}\ v_{34}\ xs.\ P\ xs \Rightarrow P\ (v_{33}\ \texttt{lt}\ v_{34}\texttt{::}xs)) \Rightarrow$
$\forall\, v.\ P\ v$

[getPlatoonLeaderCOM_def]

$\vdash$ (getPlatoonLeaderCOM [] = NONE) $\wedge$
$(\forall\, xs\ cmd.$
$\quad$ getPlatoonLeaderCOM (SOME (PlatoonLeaderCOM cmd)::xs) =
$\quad$ SOME (PlatoonLeaderCOM cmd)) $\wedge$
$(\forall\, xs.$
$\quad$ getPlatoonLeaderCOM (NONE::xs) = getPlatoonLeaderCOM xs) $\wedge$
$(\forall\, xs\ v_5.$
$\quad$ getPlatoonLeaderCOM (SOME (PlatoonSergeantCOM v_5)::xs) =
$\quad$ getPlatoonLeaderCOM xs) $\wedge$
$\forall\, xs\ v_6.$
getPlatoonLeaderCOM (SOME (OmniCOM v_6)::xs) =
getPlatoonLeaderCOM xs

[getPlatoonLeaderCOM_ind]

$\vdash \forall\, P.$
P [] $\wedge$ $(\forall\, cmd\ xs.\ P$ (SOME (PlatoonLeaderCOM cmd)::xs)) $\wedge$

```
   (∀ xs. P xs ⇒ P (NONE::xs)) ∧
   (∀ v5 xs. P xs ⇒ P (SOME (PlatoonSergeantCOM v5)::xs)) ∧
   (∀ v6 xs. P xs ⇒ P (SOME (OmniCOM v6)::xs)) ⇒
   ∀ v. P v
```

[getPlatoonLeaderCOMx_def]

```
⊢ (getPlatoonLeaderCOMx [] = NONE) ∧
  (∀ xs cmd.
     getPlatoonLeaderCOMx
       (Name PlatoonLeader says
        prop (SOME (PlatoonLeaderCOM cmd))::xs) =
     SOME (PlatoonLeaderCOM cmd)) ∧
  (∀ xs.
     getPlatoonLeaderCOMx (TT::xs) = getPlatoonLeaderCOMx xs) ∧
  (∀ xs.
     getPlatoonLeaderCOMx (FF::xs) = getPlatoonLeaderCOMx xs) ∧
  (∀ xs v2.
     getPlatoonLeaderCOMx (prop v2::xs) =
     getPlatoonLeaderCOMx xs) ∧
  (∀ xs v3.
     getPlatoonLeaderCOMx (notf v3::xs) =
     getPlatoonLeaderCOMx xs) ∧
  (∀ xs v5 v4.
     getPlatoonLeaderCOMx (v4 andf v5::xs) =
     getPlatoonLeaderCOMx xs) ∧
  (∀ xs v7 v6.
     getPlatoonLeaderCOMx (v6 orf v7::xs) =
     getPlatoonLeaderCOMx xs) ∧
  (∀ xs v9 v8.
     getPlatoonLeaderCOMx (v8 impf v9::xs) =
     getPlatoonLeaderCOMx xs) ∧
  (∀ xs v11 v10.
     getPlatoonLeaderCOMx (v10 eqf v11::xs) =
     getPlatoonLeaderCOMx xs) ∧
  (∀ xs v12.
     getPlatoonLeaderCOMx (v12 says TT::xs) =
     getPlatoonLeaderCOMx xs) ∧
  (∀ xs v12.
     getPlatoonLeaderCOMx (v12 says FF::xs) =
     getPlatoonLeaderCOMx xs) ∧
  (∀ xs v134.
     getPlatoonLeaderCOMx (Name v134 says prop NONE::xs) =
     getPlatoonLeaderCOMx xs) ∧
  (∀ xs v147.
     getPlatoonLeaderCOMx
       (Name PlatoonLeader says
        prop (SOME (PlatoonSergeantCOM v147))::xs) =
     getPlatoonLeaderCOMx xs) ∧
  (∀ xs v148.
```

```
   getPlatoonLeaderCOMx
     (Name PlatoonLeader says prop (SOME (OmniCOM v148))::
          xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v144 .
   getPlatoonLeaderCOMx
     (Name PlatoonSergeant says prop (SOME v144)::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v144 .
   getPlatoonLeaderCOMx
     (Name Omni says prop (SOME v144)::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v68 v136 v135 .
   getPlatoonLeaderCOMx (v135 meet v136 says prop v68::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v68 v138 v137 .
   getPlatoonLeaderCOMx
     (v137 quoting v138 says prop v68::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v69 v12 .
   getPlatoonLeaderCOMx (v12 says notf v69::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v71 v70 v12 .
   getPlatoonLeaderCOMx (v12 says (v70 andf v71)::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v73 v72 v12 .
   getPlatoonLeaderCOMx (v12 says (v72 orf v73)::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v75 v74 v12 .
   getPlatoonLeaderCOMx (v12 says (v74 impf v75)::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v77 v76 v12 .
   getPlatoonLeaderCOMx (v12 says (v76 eqf v77)::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v79 v78 v12 .
   getPlatoonLeaderCOMx (v12 says v78 says v79::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v81 v80 v12 .
   getPlatoonLeaderCOMx (v12 says v80 speaks_for v81::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v83 v82 v12 .
   getPlatoonLeaderCOMx (v12 says v82 controls v83::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v86 v85 v84 v12 .
   getPlatoonLeaderCOMx (v12 says reps v84 v85 v86::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v88 v87 v12 .
   getPlatoonLeaderCOMx (v12 says v87 domi v88::xs) =
   getPlatoonLeaderCOMx xs) ∧
```

```
(∀ xs v90 v89 v12 .
   getPlatoonLeaderCOMx (v12 says v89 eqi v90::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v92 v91 v12 .
   getPlatoonLeaderCOMx (v12 says v91 doms v92::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v94 v93 v12 .
   getPlatoonLeaderCOMx (v12 says v93 eqs v94::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v96 v95 v12 .
   getPlatoonLeaderCOMx (v12 says v95 eqn v96::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v98 v97 v12 .
   getPlatoonLeaderCOMx (v12 says v97 lte v98::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v99 v12 v100 .
   getPlatoonLeaderCOMx (v12 says v99 lt v100::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v15 v14 .
   getPlatoonLeaderCOMx (v14 speaks_for v15::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v17 v16 .
   getPlatoonLeaderCOMx (v16 controls v17::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v20 v19 v18 .
   getPlatoonLeaderCOMx (reps v18 v19 v20::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v22 v21 .
   getPlatoonLeaderCOMx (v21 domi v22::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v24 v23 .
   getPlatoonLeaderCOMx (v23 eqi v24::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v26 v25 .
   getPlatoonLeaderCOMx (v25 doms v26::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v28 v27 .
   getPlatoonLeaderCOMx (v27 eqs v28::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v30 v29 .
   getPlatoonLeaderCOMx (v29 eqn v30::xs) =
   getPlatoonLeaderCOMx xs) ∧
(∀ xs v32 v31 .
   getPlatoonLeaderCOMx (v31 lte v32::xs) =
   getPlatoonLeaderCOMx xs) ∧
∀ xs v34 v33 .
  getPlatoonLeaderCOMx (v33 lt v34::xs) =
  getPlatoonLeaderCOMx xs
```

[getPlatoonLeaderCOMx_ind]

$\vdash \forall P.$
P [] $\wedge$
$(\forall cmd\ xs.$
P
(Name PlatoonLeader says
prop (SOME (PlatoonLeaderCOM cmd))::xs)) $\wedge$
$(\forall xs.\ P\ xs \Rightarrow P$ (TT::xs)) $\wedge$ $(\forall xs.\ P\ xs \Rightarrow P$ (FF::xs)) $\wedge$
$(\forall v_2\ xs.\ P\ xs \Rightarrow P$ (prop v_2::xs)) $\wedge$
$(\forall v_3\ xs.\ P\ xs \Rightarrow P$ (notf v_3::xs)) $\wedge$
$(\forall v_4\ v_5\ xs.\ P\ xs \Rightarrow P$ (v_4 andf v_5::xs)) $\wedge$
$(\forall v_6\ v_7\ xs.\ P\ xs \Rightarrow P$ (v_6 orf v_7::xs)) $\wedge$
$(\forall v_8\ v_9\ xs.\ P\ xs \Rightarrow P$ (v_8 impf v_9::xs)) $\wedge$
$(\forall v_{10}\ v_{11}\ xs.\ P\ xs \Rightarrow P$ (v_{10} eqf v_{11}::xs)) $\wedge$
$(\forall v_{12}\ xs.\ P\ xs \Rightarrow P$ (v_{12} says TT::xs)) $\wedge$
$(\forall v_{12}\ xs.\ P\ xs \Rightarrow P$ (v_{12} says FF::xs)) $\wedge$
$(\forall v134\ xs.\ P\ xs \Rightarrow P$ (Name $v134$ says prop NONE::xs)) $\wedge$
$(\forall v147\ xs.$
$P\ xs \Rightarrow$
P
(Name PlatoonLeader says
prop (SOME (PlatoonSergeantCOM $v147$))::xs)) $\wedge$
$(\forall v148\ xs.$
$P\ xs \Rightarrow$
P
(Name PlatoonLeader says prop (SOME (OmniCOM $v148$))::
xs)) $\wedge$
$(\forall v144\ xs.$
$P\ xs \Rightarrow$
P (Name PlatoonSergeant says prop (SOME $v144$)::xs)) $\wedge$
$(\forall v144\ xs.$
$P\ xs \Rightarrow P$ (Name Omni says prop (SOME $v144$)::xs)) $\wedge$
$(\forall v135\ v136\ v_{68}\ xs.$
$P\ xs \Rightarrow P$ ($v135$ meet $v136$ says prop v_{68}::xs)) $\wedge$
$(\forall v137\ v138\ v_{68}\ xs.$
$P\ xs \Rightarrow P$ ($v137$ quoting $v138$ says prop v_{68}::xs)) $\wedge$
$(\forall v_{12}\ v_{69}\ xs.\ P\ xs \Rightarrow P$ (v_{12} says notf v_{69}::xs)) $\wedge$
$(\forall v_{12}\ v_{70}\ v_{71}\ xs.\ P\ xs \Rightarrow P$ (v_{12} says (v_{70} andf v_{71})::xs)) $\wedge$
$(\forall v_{12}\ v_{72}\ v_{73}\ xs.\ P\ xs \Rightarrow P$ (v_{12} says (v_{72} orf v_{73})::xs)) $\wedge$
$(\forall v_{12}\ v_{74}\ v_{75}\ xs.\ P\ xs \Rightarrow P$ (v_{12} says (v_{74} impf v_{75})::xs)) $\wedge$
$(\forall v_{12}\ v_{76}\ v_{77}\ xs.\ P\ xs \Rightarrow P$ (v_{12} says (v_{76} eqf v_{77})::xs)) $\wedge$
$(\forall v_{12}\ v_{78}\ v_{79}\ xs.\ P\ xs \Rightarrow P$ (v_{12} says v_{78} says v_{79}::xs)) $\wedge$
$(\forall v_{12}\ v_{80}\ v_{81}\ xs.$
$P\ xs \Rightarrow P$ (v_{12} says v_{80} speaks_for v_{81}::xs)) $\wedge$
$(\forall v_{12}\ v_{82}\ v_{83}\ xs.$
$P\ xs \Rightarrow P$ (v_{12} says v_{82} controls v_{83}::xs)) $\wedge$
$(\forall v_{12}\ v_{84}\ v_{85}\ v_{86}\ xs.$
$P\ xs \Rightarrow P$ (v_{12} says reps v_{84} v_{85} v_{86}::xs)) $\wedge$
$(\forall v_{12}\ v_{87}\ v_{88}\ xs.\ P\ xs \Rightarrow P$ (v_{12} says v_{87} domi v_{88}::xs)) $\wedge$

```
(∀ v12 v89 v90 xs. P xs ⇒ P (v12 says v89 eqi v90::xs)) ∧
(∀ v12 v91 v92 xs. P xs ⇒ P (v12 says v91 doms v92::xs)) ∧
(∀ v12 v93 v94 xs. P xs ⇒ P (v12 says v93 eqs v94::xs)) ∧
(∀ v12 v95 v96 xs. P xs ⇒ P (v12 says v95 eqn v96::xs)) ∧
(∀ v12 v97 v98 xs. P xs ⇒ P (v12 says v97 lte v98::xs)) ∧
(∀ v12 v99 v100 xs. P xs ⇒ P (v12 says v99 lt v100::xs)) ∧
(∀ v14 v15 xs. P xs ⇒ P (v14 speaks_for v15::xs)) ∧
(∀ v16 v17 xs. P xs ⇒ P (v16 controls v17::xs)) ∧
(∀ v18 v19 v20 xs. P xs ⇒ P (reps v18 v19 v20::xs)) ∧
(∀ v21 v22 xs. P xs ⇒ P (v21 domi v22::xs)) ∧
(∀ v23 v24 xs. P xs ⇒ P (v23 eqi v24::xs)) ∧
(∀ v25 v26 xs. P xs ⇒ P (v25 doms v26::xs)) ∧
(∀ v27 v28 xs. P xs ⇒ P (v27 eqs v28::xs)) ∧
(∀ v29 v30 xs. P xs ⇒ P (v29 eqn v30::xs)) ∧
(∀ v31 v32 xs. P xs ⇒ P (v31 lte v32::xs)) ∧
(∀ v33 v34 xs. P xs ⇒ P (v33 lt v34::xs)) ⇒
∀ v. P v
```

[getPlatoonSergeantCOM_def]

```
⊢ (getPlatoonSergeantCOM [] = NONE) ∧
  (∀ xs cmd.
     getPlatoonSergeantCOM
       (SOME (PlatoonSergeantCOM cmd)::xs) =
     SOME (PlatoonSergeantCOM cmd)) ∧
  (∀ xs.
     getPlatoonSergeantCOM (NONE::xs) =
     getPlatoonSergeantCOM xs) ∧
  (∀ xs v4.
     getPlatoonSergeantCOM (SOME (PlatoonLeaderCOM v4)::xs) =
     getPlatoonSergeantCOM xs) ∧
  ∀ xs v6.
    getPlatoonSergeantCOM (SOME (OmniCOM v6)::xs) =
    getPlatoonSergeantCOM xs
```

[getPlatoonSergeantCOM_ind]

```
⊢ ∀ P.
    P [] ∧ (∀ cmd xs. P (SOME (PlatoonSergeantCOM cmd)::xs)) ∧
    (∀ xs. P xs ⇒ P (NONE::xs)) ∧
    (∀ v4 xs. P xs ⇒ P (SOME (PlatoonLeaderCOM v4)::xs)) ∧
    (∀ v6 xs. P xs ⇒ P (SOME (OmniCOM v6)::xs)) ⇒
    ∀ v. P v
```

[getPlatoonSergeantCOMx_def]

```
⊢ (getPlatoonSergeantCOMx [] = NONE) ∧
  (∀ xs cmd.
     getPlatoonSergeantCOMx
       (Name PlatoonSergeant says
        prop (SOME (PlatoonSergeantCOM cmd))::xs) =
```

```
   SOME (PlatoonSergeantCOM cmd)) ∧
(∀ xs .
   getPlatoonSergeantCOMx (TT::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs .
   getPlatoonSergeantCOMx (FF::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v2 .
   getPlatoonSergeantCOMx (prop v2::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v3 .
   getPlatoonSergeantCOMx (notf v3::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v5 v4 .
   getPlatoonSergeantCOMx (v4 andf v5::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v7 v6 .
   getPlatoonSergeantCOMx (v6 orf v7::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v9 v8 .
   getPlatoonSergeantCOMx (v8 impf v9::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v11 v10 .
   getPlatoonSergeantCOMx (v10 eqf v11::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v12 .
   getPlatoonSergeantCOMx (v12 says TT::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v12 .
   getPlatoonSergeantCOMx (v12 says FF::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v134 .
   getPlatoonSergeantCOMx (Name v134 says prop NONE::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v144 .
   getPlatoonSergeantCOMx
     (Name PlatoonLeader says prop (SOME v144)::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v146 .
   getPlatoonSergeantCOMx
     (Name PlatoonSergeant says
      prop (SOME (PlatoonLeaderCOM v146))::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v148 .
   getPlatoonSergeantCOMx
     (Name PlatoonSergeant says prop (SOME (OmniCOM v148))::
          xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v144 .
```

```
   getPlatoonSergeantCOMx
     (Name Omni says prop (SOME v144)::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v68 v136 v135.
   getPlatoonSergeantCOMx
     (v135 meet v136 says prop v68::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v68 v138 v137.
   getPlatoonSergeantCOMx
     (v137 quoting v138 says prop v68::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v69 v12.
   getPlatoonSergeantCOMx (v12 says notf v69::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v71 v70 v12.
   getPlatoonSergeantCOMx (v12 says (v70 andf v71)::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v73 v72 v12.
   getPlatoonSergeantCOMx (v12 says (v72 orf v73)::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v75 v74 v12.
   getPlatoonSergeantCOMx (v12 says (v74 impf v75)::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v77 v76 v12.
   getPlatoonSergeantCOMx (v12 says (v76 eqf v77)::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v79 v78 v12.
   getPlatoonSergeantCOMx (v12 says v78 says v79::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v81 v80 v12.
   getPlatoonSergeantCOMx (v12 says v80 speaks_for v81::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v83 v82 v12.
   getPlatoonSergeantCOMx (v12 says v82 controls v83::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v86 v85 v84 v12.
   getPlatoonSergeantCOMx (v12 says reps v84 v85 v86::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v88 v87 v12.
   getPlatoonSergeantCOMx (v12 says v87 domi v88::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v90 v89 v12.
   getPlatoonSergeantCOMx (v12 says v89 eqi v90::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v92 v91 v12.
   getPlatoonSergeantCOMx (v12 says v91 doms v92::xs) =
   getPlatoonSergeantCOMx xs) ∧
(∀ xs v94 v93 v12.
   getPlatoonSergeantCOMx (v12 says v93 eqs v94::xs) =
```

```
      getPlatoonSergeantCOMx xs) ∧
   (∀ xs v96 v95 v12.
      getPlatoonSergeantCOMx (v12 says v95 eqn v96::xs) =
      getPlatoonSergeantCOMx xs) ∧
   (∀ xs v98 v97 v12.
      getPlatoonSergeantCOMx (v12 says v97 lte v98::xs) =
      getPlatoonSergeantCOMx xs) ∧
   (∀ xs v99 v12 v100.
      getPlatoonSergeantCOMx (v12 says v99 lt v100::xs) =
      getPlatoonSergeantCOMx xs) ∧
   (∀ xs v15 v14.
      getPlatoonSergeantCOMx (v14 speaks_for v15::xs) =
      getPlatoonSergeantCOMx xs) ∧
   (∀ xs v17 v16.
      getPlatoonSergeantCOMx (v16 controls v17::xs) =
      getPlatoonSergeantCOMx xs) ∧
   (∀ xs v20 v19 v18.
      getPlatoonSergeantCOMx (reps v18 v19 v20::xs) =
      getPlatoonSergeantCOMx xs) ∧
   (∀ xs v22 v21.
      getPlatoonSergeantCOMx (v21 domi v22::xs) =
      getPlatoonSergeantCOMx xs) ∧
   (∀ xs v24 v23.
      getPlatoonSergeantCOMx (v23 eqi v24::xs) =
      getPlatoonSergeantCOMx xs) ∧
   (∀ xs v26 v25.
      getPlatoonSergeantCOMx (v25 doms v26::xs) =
      getPlatoonSergeantCOMx xs) ∧
   (∀ xs v28 v27.
      getPlatoonSergeantCOMx (v27 eqs v28::xs) =
      getPlatoonSergeantCOMx xs) ∧
   (∀ xs v30 v29.
      getPlatoonSergeantCOMx (v29 eqn v30::xs) =
      getPlatoonSergeantCOMx xs) ∧
   (∀ xs v32 v31.
      getPlatoonSergeantCOMx (v31 lte v32::xs) =
      getPlatoonSergeantCOMx xs) ∧
   ∀ xs v34 v33.
     getPlatoonSergeantCOMx (v33 lt v34::xs) =
     getPlatoonSergeantCOMx xs
```

[getPlatoonSergeantCOMx_ind]

```
⊢ ∀ P.
    P [] ∧
    (∀ cmd xs.
       P
         (Name PlatoonSergeant says
          prop (SOME (PlatoonSergeantCOM cmd))::xs)) ∧
    (∀ xs. P xs ⇒ P (TT::xs)) ∧ (∀ xs. P xs ⇒ P (FF::xs)) ∧
```

$(\forall\, v_2\ xs.\ P\ xs \Rightarrow P\ (\texttt{prop}\ v_2\texttt{::}xs)) \wedge$
$(\forall\, v_3\ xs.\ P\ xs \Rightarrow P\ (\texttt{notf}\ v_3\texttt{::}xs)) \wedge$
$(\forall\, v_4\ v_5\ xs.\ P\ xs \Rightarrow P\ (v_4\ \texttt{andf}\ v_5\texttt{::}xs)) \wedge$
$(\forall\, v_6\ v_7\ xs.\ P\ xs \Rightarrow P\ (v_6\ \texttt{orf}\ v_7\texttt{::}xs)) \wedge$
$(\forall\, v_8\ v_9\ xs.\ P\ xs \Rightarrow P\ (v_8\ \texttt{impf}\ v_9\texttt{::}xs)) \wedge$
$(\forall\, v_{10}\ v_{11}\ xs.\ P\ xs \Rightarrow P\ (v_{10}\ \texttt{eqf}\ v_{11}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says TT::}xs)) \wedge$
$(\forall\, v_{12}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says FF::}xs)) \wedge$
$(\forall\, v134\ xs.\ P\ xs \Rightarrow P\ (\texttt{Name}\ v134\ \texttt{says prop NONE::}xs)) \wedge$
$(\forall\, v144\ xs.$
$\quad P\ xs \Rightarrow$
$\quad P\ (\texttt{Name PlatoonLeader says prop (SOME}\ v144\texttt{)::}xs)) \wedge$
$(\forall\, v146\ xs.$
$\quad P\ xs \Rightarrow$
$\quad P$
$\quad\quad (\texttt{Name PlatoonSergeant says}$
$\quad\quad\ \texttt{prop (SOME (PlatoonLeaderCOM}\ v146\texttt{))::}xs)) \wedge$
$(\forall\, v148\ xs.$
$\quad P\ xs \Rightarrow$
$\quad P$
$\quad\quad (\texttt{Name PlatoonSergeant says}$
$\quad\quad\ \texttt{prop (SOME (OmniCOM}\ v148\texttt{))::}xs)) \wedge$
$(\forall\, v144\ xs.$
$\quad P\ xs \Rightarrow P\ (\texttt{Name Omni says prop (SOME}\ v144\texttt{)::}xs)) \wedge$
$(\forall\, v135\ v136\ v_{68}\ xs.$
$\quad P\ xs \Rightarrow P\ (v135\ \texttt{meet}\ v136\ \texttt{says prop}\ v_{68}\texttt{::}xs)) \wedge$
$(\forall\, v137\ v138\ v_{68}\ xs.$
$\quad P\ xs \Rightarrow P\ (v137\ \texttt{quoting}\ v138\ \texttt{says prop}\ v_{68}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{69}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says notf}\ v_{69}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{70}\ v_{71}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says (}v_{70}\ \texttt{andf}\ v_{71}\texttt{)::}xs)) \wedge$
$(\forall\, v_{12}\ v_{72}\ v_{73}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says (}v_{72}\ \texttt{orf}\ v_{73}\texttt{)::}xs)) \wedge$
$(\forall\, v_{12}\ v_{74}\ v_{75}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says (}v_{74}\ \texttt{impf}\ v_{75}\texttt{)::}xs)) \wedge$
$(\forall\, v_{12}\ v_{76}\ v_{77}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says (}v_{76}\ \texttt{eqf}\ v_{77}\texttt{)::}xs)) \wedge$
$(\forall\, v_{12}\ v_{78}\ v_{79}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{78}\ \texttt{says}\ v_{79}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{80}\ v_{81}\ xs.$
$\quad P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{80}\ \texttt{speaks\_for}\ v_{81}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{82}\ v_{83}\ xs.$
$\quad P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{82}\ \texttt{controls}\ v_{83}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{84}\ v_{85}\ v_{86}\ xs.$
$\quad P\ xs \Rightarrow P\ (v_{12}\ \texttt{says reps}\ v_{84}\ v_{85}\ v_{86}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{87}\ v_{88}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{87}\ \texttt{domi}\ v_{88}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{89}\ v_{90}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{89}\ \texttt{eqi}\ v_{90}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{91}\ v_{92}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{91}\ \texttt{doms}\ v_{92}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{93}\ v_{94}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{93}\ \texttt{eqs}\ v_{94}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{95}\ v_{96}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{95}\ \texttt{eqn}\ v_{96}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{97}\ v_{98}\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{97}\ \texttt{lte}\ v_{98}\texttt{::}xs)) \wedge$
$(\forall\, v_{12}\ v_{99}\ v100\ xs.\ P\ xs \Rightarrow P\ (v_{12}\ \texttt{says}\ v_{99}\ \texttt{lt}\ v100\texttt{::}xs)) \wedge$
$(\forall\, v_{14}\ v_{15}\ xs.\ P\ xs \Rightarrow P\ (v_{14}\ \texttt{speaks\_for}\ v_{15}\texttt{::}xs)) \wedge$
$(\forall\, v_{16}\ v_{17}\ xs.\ P\ xs \Rightarrow P\ (v_{16}\ \texttt{controls}\ v_{17}\texttt{::}xs)) \wedge$

$(\forall v_{18}\ v_{19}\ v_{20}\ xs.\ P\ xs \Rightarrow P\ (\texttt{reps}\ v_{18}\ v_{19}\ v_{20}::xs)) \wedge$
$(\forall v_{21}\ v_{22}\ xs.\ P\ xs \Rightarrow P\ (v_{21}\ \texttt{domi}\ v_{22}::xs)) \wedge$
$(\forall v_{23}\ v_{24}\ xs.\ P\ xs \Rightarrow P\ (v_{23}\ \texttt{eqi}\ v_{24}::xs)) \wedge$
$(\forall v_{25}\ v_{26}\ xs.\ P\ xs \Rightarrow P\ (v_{25}\ \texttt{doms}\ v_{26}::xs)) \wedge$
$(\forall v_{27}\ v_{28}\ xs.\ P\ xs \Rightarrow P\ (v_{27}\ \texttt{eqs}\ v_{28}::xs)) \wedge$
$(\forall v_{29}\ v_{30}\ xs.\ P\ xs \Rightarrow P\ (v_{29}\ \texttt{eqn}\ v_{30}::xs)) \wedge$
$(\forall v_{31}\ v_{32}\ xs.\ P\ xs \Rightarrow P\ (v_{31}\ \texttt{lte}\ v_{32}::xs)) \wedge$
$(\forall v_{33}\ v_{34}\ xs.\ P\ xs \Rightarrow P\ (v_{33}\ \texttt{lt}\ v_{34}::xs)) \Rightarrow$
$\forall v.\ P\ v$

3 projectSM Theory

Built: 27 December 2018
Parent Theories: projectUtilities, ssm

3.1 Theorems

[NOut_def]

```
⊢ (NOut CONDUCT_PB (exec x) =
   if
     getPlatoonLeaderCOM x = SOME (PlatoonLeaderCOM secure)
   then
     Secure
   else NoActionTaken) ∧
  (NOut SECURE (exec x) =
   if
     getPlatoonSergeantCOM x =
     SOME (PlatoonSergeantCOM actionsIn)
   then
     ActionsIn
   else NoActionTaken) ∧
  (NOut ACTIONS_IN (exec x) =
   if
     getPlatoonLeaderCOM x = SOME (PlatoonLeaderCOM withdraw)
   then
     Withdraw
   else NoActionTaken) ∧
  (NOut WITHDRAW (exec x) =
   if
     getPlatoonLeaderCOM x = SOME (PlatoonLeaderCOM complete)
   then
     Complete
   else NoActionTaken) ∧ (NOut s (trap v0) = UnAuthorized) ∧
  (NOut s (discard v1) = UnAuthenticated)
```

[NOut_ind]

```
⊢ ∀P.
    (∀x. P CONDUCT_PB (exec x)) ∧ (∀x. P SECURE (exec x)) ∧
    (∀x. P ACTIONS_IN (exec x)) ∧ (∀x. P WITHDRAW (exec x)) ∧
    (∀s v0. P s (trap v0)) ∧ (∀s v1. P s (discard v1)) ∧
    (∀v6. P COMPLETE (exec v6)) ⇒
    ∀v v1. P v v1
```

[NS_def]

```
⊢ (NS CONDUCT_PB (exec x) =
   if
     getPlatoonLeaderCOM x = SOME (PlatoonLeaderCOM secure)
   then
     SECURE
   else CONDUCT_PB) ∧
  (NS SECURE (exec x) =
   if
     getPlatoonSergeantCOM x =
     SOME (PlatoonSergeantCOM actionsIn)
   then
     ACTIONS_IN
   else SECURE) ∧
  (NS ACTIONS_IN (exec x) =
   if
     getPlatoonLeaderCOM x = SOME (PlatoonLeaderCOM withdraw)
   then
     WITHDRAW
   else ACTIONS_IN) ∧
  (NS WITHDRAW (exec x) =
   if
     getPlatoonLeaderCOM x = SOME (PlatoonLeaderCOM complete)
   then
     COMPLETE
   else WITHDRAW) ∧ (NS s (trap v0) = s) ∧
  (NS s (discard v1) = s)
```

[NS_ind]

```
⊢ ∀P.
    (∀x. P CONDUCT_PB (exec x)) ∧ (∀x. P SECURE (exec x)) ∧
    (∀x. P ACTIONS_IN (exec x)) ∧ (∀x. P WITHDRAW (exec x)) ∧
    (∀s v0. P s (trap v0)) ∧ (∀s v1. P s (discard v1)) ∧
    (∀v6. P COMPLETE (exec v6)) ⇒
    ∀v v1. P v v1
```

4 projectSecurity Theory

Built: 27 December 2018

Parent Theories: projectUtilities, ssm

4.1 Definitions

[globalAuth_def]

```
⊢ ∀x. globalAuth x = [TT]
```

[stateAuth_def]

```
⊢ ∀s x.
    stateAuth s x =
    if s = CONDUCT_PB then
      if
        getPlatoonLeaderCOMx x = SOME (PlatoonLeaderCOM secure)
      then
        [Name PlatoonLeader controls
         prop (SOME (PlatoonLeaderCOM secure))]
      else [prop NONE]
    else if s = SECURE then
      if
        getPlatoonSergeantCOMx x =
        SOME (PlatoonSergeantCOM actionsIn)
      then
        [Name PlatoonSergeant controls
         prop (SOME (PlatoonSergeantCOM actionsIn))]
      else [prop NONE]
    else if s = ACTIONS_IN then
      if
        getPlatoonLeaderCOMx x =
        SOME (PlatoonLeaderCOM withdraw)
      then
        [Name PlatoonLeader controls
         prop (SOME (PlatoonLeaderCOM withdraw))]
      else [prop NONE]
    else if s = WITHDRAW then
      if
        getPlatoonLeaderCOMx x =
        SOME (PlatoonLeaderCOM complete)
      then
        [Name PlatoonLeader controls
         prop (SOME (PlatoonLeaderCOM complete))]
      else [prop NONE]
    else [prop NONE]
```

4.2 Theorems

[authentication_def]

```
⊢ (authentication
     (Name PlatoonLeader says
      prop (SOME (PlatoonLeaderCOM x''))) ⟺ T) ∧
  (authentication
```

```
   (Name PlatoonSergeant says
    prop (SOME (PlatoonSergeantCOM x'))) ⟺ T) ∧
(authentication (Name Omni says prop (SOME (OmniCOM x))) ⟺
 T) ∧ (authentication TT ⟺ F) ∧ (authentication FF ⟺ F) ∧
(authentication (prop v) ⟺ F) ∧
(authentication (notf v1) ⟺ F) ∧
(authentication (v2 andf v3) ⟺ F) ∧
(authentication (v4 orf v5) ⟺ F) ∧
(authentication (v6 impf v7) ⟺ F) ∧
(authentication (v8 eqf v9) ⟺ F) ∧
(authentication (Name v66 says TT) ⟺ F) ∧
(authentication (Name v66 says FF) ⟺ F) ∧
(authentication (Name v66 says prop NONE) ⟺ F) ∧
(authentication
   (Name PlatoonSergeant says
    prop (SOME (PlatoonLeaderCOM v144))) ⟺ F) ∧
(authentication
   (Name Omni says prop (SOME (PlatoonLeaderCOM v144))) ⟺
 F) ∧
(authentication
   (Name PlatoonLeader says
    prop (SOME (PlatoonSergeantCOM v145))) ⟺ F) ∧
(authentication
   (Name Omni says prop (SOME (PlatoonSergeantCOM v145))) ⟺
 F) ∧
(authentication
   (Name PlatoonLeader says prop (SOME (OmniCOM v146))) ⟺
 F) ∧
(authentication
   (Name PlatoonSergeant says prop (SOME (OmniCOM v146))) ⟺
 F) ∧ (authentication (Name v66 says notf v77) ⟺ F) ∧
(authentication (Name v66 says (v78 andf v79)) ⟺ F) ∧
(authentication (Name v66 says (v80 orf v81)) ⟺ F) ∧
(authentication (Name v66 says (v82 impf v83)) ⟺ F) ∧
(authentication (Name v66 says (v84 eqf v85)) ⟺ F) ∧
(authentication (Name v66 says v86 says v87) ⟺ F) ∧
(authentication (Name v66 says v88 speaks_for v89) ⟺ F) ∧
(authentication (Name v66 says v90 controls v91) ⟺ F) ∧
(authentication (Name v66 says reps v92 v93 v94) ⟺ F) ∧
(authentication (Name v66 says v95 domi v96) ⟺ F) ∧
(authentication (Name v66 says v97 eqi v98) ⟺ F) ∧
(authentication (Name v66 says v99 doms v100) ⟺ F) ∧
(authentication (Name v66 says v101 eqs v102) ⟺ F) ∧
(authentication (Name v66 says v103 eqn v104) ⟺ F) ∧
(authentication (Name v66 says v105 lte v106) ⟺ F) ∧
(authentication (Name v66 says v107 lt v108) ⟺ F) ∧
(authentication (v67 meet v68 says v11) ⟺ F) ∧
(authentication (v69 quoting v70 says v11) ⟺ F) ∧
(authentication (v12 speaks_for v13) ⟺ F) ∧
```

```
   (authentication (v14 controls v15) ⟺ F) ∧
   (authentication (reps v16 v17 v18) ⟺ F) ∧
   (authentication (v19 domi v20) ⟺ F) ∧
   (authentication (v21 eqi v22) ⟺ F) ∧
   (authentication (v23 doms v24) ⟺ F) ∧
   (authentication (v25 eqs v26) ⟺ F) ∧
   (authentication (v27 eqn v28) ⟺ F) ∧
   (authentication (v29 lte v30) ⟺ F) ∧
   (authentication (v31 lt v32) ⟺ F)
```

[authentication_ind]

```
⊢ ∀P.
    (∀x.
       P
         (Name PlatoonLeader says
          prop (SOME (PlatoonLeaderCOM x)))) ∧
    (∀x.
       P
         (Name PlatoonSergeant says
          prop (SOME (PlatoonSergeantCOM x)))) ∧
    (∀x. P (Name Omni says prop (SOME (OmniCOM x)))) ∧ P TT ∧
    P FF ∧ (∀v. P (prop v)) ∧ (∀v1. P (notf v1)) ∧
    (∀v2 v3. P (v2 andf v3)) ∧ (∀v4 v5. P (v4 orf v5)) ∧
    (∀v6 v7. P (v6 impf v7)) ∧ (∀v8 v9. P (v8 eqf v9)) ∧
    (∀v66. P (Name v66 says TT)) ∧
    (∀v66. P (Name v66 says FF)) ∧
    (∀v66. P (Name v66 says prop NONE)) ∧
    (∀v144.
       P
         (Name PlatoonSergeant says
          prop (SOME (PlatoonLeaderCOM v144)))) ∧
    (∀v144.
       P
         (Name Omni says
          prop (SOME (PlatoonLeaderCOM v144)))) ∧
    (∀v145.
       P
         (Name PlatoonLeader says
          prop (SOME (PlatoonSergeantCOM v145)))) ∧
    (∀v145.
       P
         (Name Omni says
          prop (SOME (PlatoonSergeantCOM v145)))) ∧
    (∀v146.
       P
         (Name PlatoonLeader says
          prop (SOME (OmniCOM v146)))) ∧
    (∀v146.
       P
```

```
      (Name PlatoonSergeant says
       prop (SOME (OmniCOM v146)))) ∧
  (∀ v66 v77. P (Name v66 says notf v77)) ∧
  (∀ v66 v78 v79. P (Name v66 says (v78 andf v79))) ∧
  (∀ v66 v80 v81. P (Name v66 says (v80 orf v81))) ∧
  (∀ v66 v82 v83. P (Name v66 says (v82 impf v83))) ∧
  (∀ v66 v84 v85. P (Name v66 says (v84 eqf v85))) ∧
  (∀ v66 v86 v87. P (Name v66 says v86 says v87)) ∧
  (∀ v66 v88 v89. P (Name v66 says v88 speaks_for v89)) ∧
  (∀ v66 v90 v91. P (Name v66 says v90 controls v91)) ∧
  (∀ v66 v92 v93 v94. P (Name v66 says reps v92 v93 v94)) ∧
  (∀ v66 v95 v96. P (Name v66 says v95 domi v96)) ∧
  (∀ v66 v97 v98. P (Name v66 says v97 eqi v98)) ∧
  (∀ v66 v99 v100. P (Name v66 says v99 doms v100)) ∧
  (∀ v66 v101 v102. P (Name v66 says v101 eqs v102)) ∧
  (∀ v66 v103 v104. P (Name v66 says v103 eqn v104)) ∧
  (∀ v66 v105 v106. P (Name v66 says v105 lte v106)) ∧
  (∀ v66 v107 v108. P (Name v66 says v107 lt v108)) ∧
  (∀ v67 v68 v11. P (v67 meet v68 says v11)) ∧
  (∀ v69 v70 v11. P (v69 quoting v70 says v11)) ∧
  (∀ v12 v13. P (v12 speaks_for v13)) ∧
  (∀ v14 v15. P (v14 controls v15)) ∧
  (∀ v16 v17 v18. P (reps v16 v17 v18)) ∧
  (∀ v19 v20. P (v19 domi v20)) ∧
  (∀ v21 v22. P (v21 eqi v22)) ∧
  (∀ v23 v24. P (v23 doms v24)) ∧
  (∀ v25 v26. P (v25 eqs v26)) ∧ (∀ v27 v28. P (v27 eqn v28)) ∧
  (∀ v29 v30. P (v29 lte v30)) ∧ (∀ v31 v32. P (v31 lt v32)) ⇒
  ∀ v. P v
```

5 projectAssuranceExec Theory

Built: 27 December 2018

Parent Theories: projectSecurity

5.1 Theorems

[ACTIONS_IN_exec_withdraw_lemma1]

```
 ⊢ ∀ M Oi Os.
     CFGInterpret (M,Oi,Os)
       (CFG authentication stateAuth globalAuth
          ([Name PlatoonLeader says
            prop (SOME (PlatoonLeaderCOM withdraw))]::ins)
          ACTIONS_IN outs) ⇒
     (M,Oi,Os) satList
     propCommandList
       [Name PlatoonLeader says
        prop (SOME (PlatoonLeaderCOM withdraw))]
```

[ACTIONS_IN_exec_withdraw_lemma2]

```
⊢ ∀NS Out M Oi Os.
    TR (M,Oi,Os)
      (exec
         (inputList
            [Name PlatoonLeader says
             prop (SOME (PlatoonLeaderCOM withdraw))]))
      (CFG authentication stateAuth globalAuth
         ([Name PlatoonLeader says
           prop (SOME (PlatoonLeaderCOM withdraw))]::ins)
         ACTIONS_IN outs)
      (CFG authentication stateAuth globalAuth ins
         (NS ACTIONS_IN
            (exec
               (inputList
                  [Name PlatoonLeader says
                   prop (SOME (PlatoonLeaderCOM withdraw))])))
         (Out ACTIONS_IN
            (exec
               (inputList
                  [Name PlatoonLeader says
                   prop (SOME (PlatoonLeaderCOM withdraw))]))::
              outs)) ⟺
    authenticationTest authentication
      [Name PlatoonLeader says
       prop (SOME (PlatoonLeaderCOM withdraw))] ∧
    CFGInterpret (M,Oi,Os)
      (CFG authentication stateAuth globalAuth
         ([Name PlatoonLeader says
           prop (SOME (PlatoonLeaderCOM withdraw))]::ins)
         ACTIONS_IN outs) ∧
    (M,Oi,Os) satList
    propCommandList
      [Name PlatoonLeader says
       prop (SOME (PlatoonLeaderCOM withdraw))]
```

[ACTIONS_IN_exec_withdraw_thm]

```
⊢ ∀NS Out M Oi Os.
    TR (M,Oi,Os) (exec [SOME (PlatoonLeaderCOM withdraw)])
      (CFG authentication stateAuth globalAuth
         ([Name PlatoonLeader says
           prop (SOME (PlatoonLeaderCOM withdraw))]::ins)
         ACTIONS_IN outs)
      (CFG authentication stateAuth globalAuth ins
         (NS ACTIONS_IN
            (exec [SOME (PlatoonLeaderCOM withdraw)]))
         (Out ACTIONS_IN
            (exec [SOME (PlatoonLeaderCOM withdraw)])::
              outs)) ⟺
```

```
     authenticationTest authentication
       [Name PlatoonLeader says
        prop (SOME (PlatoonLeaderCOM withdraw))] ∧
     CFGInterpret (M,Oi,Os)
       (CFG authentication stateAuth globalAuth
          ([Name PlatoonLeader says
            prop (SOME (PlatoonLeaderCOM withdraw))]::ins)
          ACTIONS_IN outs) ∧
     (M,Oi,Os) satList [prop (SOME (PlatoonLeaderCOM withdraw))]
```

[CONDUCT_PB_exec_secure_lemma1]

```
⊢ ∀M Oi Os.
     CFGInterpret (M,Oi,Os)
       (CFG authentication stateAuth globalAuth
          ([Name PlatoonLeader says
            prop (SOME (PlatoonLeaderCOM secure))]::ins)
          CONDUCT_PB outs) ⇒
     (M,Oi,Os) satList
     propCommandList
       [Name PlatoonLeader says
        prop (SOME (PlatoonLeaderCOM secure))]
```

[CONDUCT_PB_exec_secure_lemma2]

```
⊢ ∀NS Out M Oi Os.
     TR (M,Oi,Os)
       (exec
          (inputList
             [Name PlatoonLeader says
              prop (SOME (PlatoonLeaderCOM secure))]))
       (CFG authentication stateAuth globalAuth
          ([Name PlatoonLeader says
            prop (SOME (PlatoonLeaderCOM secure))]::ins)
          CONDUCT_PB outs)
       (CFG authentication stateAuth globalAuth ins
          (NS CONDUCT_PB
             (exec
                (inputList
                   [Name PlatoonLeader says
                    prop (SOME (PlatoonLeaderCOM secure))])))
          (Out CONDUCT_PB
             (exec
                (inputList
                   [Name PlatoonLeader says
                    prop (SOME (PlatoonLeaderCOM secure))]))::
               outs)) ⟺
     authenticationTest authentication
       [Name PlatoonLeader says
        prop (SOME (PlatoonLeaderCOM secure))] ∧
     CFGInterpret (M,Oi,Os)
```

```
      (CFG authentication stateAuth globalAuth
         ([Name PlatoonLeader says
           prop (SOME (PlatoonLeaderCOM secure))]::ins)
         CONDUCT_PB outs) ∧
    (M,Oi,Os) satList
    propCommandList
      [Name PlatoonLeader says
       prop (SOME (PlatoonLeaderCOM secure))]
```

[CONDUCT_PB_exec_secure_thm]

```
⊢ ∀NS Out M Oi Os.
    TR (M,Oi,Os) (exec [SOME (PlatoonLeaderCOM secure)])
      (CFG authentication stateAuth globalAuth
         ([Name PlatoonLeader says
           prop (SOME (PlatoonLeaderCOM secure))]::ins)
         CONDUCT_PB outs)
      (CFG authentication stateAuth globalAuth ins
         (NS CONDUCT_PB
            (exec [SOME (PlatoonLeaderCOM secure)]))
         (Out CONDUCT_PB
            (exec [SOME (PlatoonLeaderCOM secure)])::outs)) ⟺
    authenticationTest authentication
      [Name PlatoonLeader says
       prop (SOME (PlatoonLeaderCOM secure))] ∧
    CFGInterpret (M,Oi,Os)
      (CFG authentication stateAuth globalAuth
         ([Name PlatoonLeader says
           prop (SOME (PlatoonLeaderCOM secure))]::ins)
         CONDUCT_PB outs) ∧
    (M,Oi,Os) satList [prop (SOME (PlatoonLeaderCOM secure))]
```

[SECURE_exec_actionsIn_lemma1]

```
⊢ ∀M Oi Os.
    CFGInterpret (M,Oi,Os)
      (CFG authentication stateAuth globalAuth
         ([Name PlatoonSergeant says
           prop (SOME (PlatoonSergeantCOM actionsIn))]::ins)
         SECURE outs) ⇒
    (M,Oi,Os) satList
    propCommandList
      [Name PlatoonSergeant says
       prop (SOME (PlatoonSergeantCOM actionsIn))]
```

[SECURE_exec_actionsIn_lemma2]

```
⊢ ∀NS Out M Oi Os.
    TR (M,Oi,Os)
      (exec
         (inputList
```

```
            [Name PlatoonSergeant says
             prop (SOME (PlatoonSergeantCOM actionsIn))]))
      (CFG authentication stateAuth globalAuth
         ([Name PlatoonSergeant says
           prop (SOME (PlatoonSergeantCOM actionsIn))]::ins)
         SECURE outs)
      (CFG authentication stateAuth globalAuth ins
         (NS SECURE
            (exec
               (inputList
                  [Name PlatoonSergeant says
                   prop
                     (SOME (PlatoonSergeantCOM actionsIn))])))
         (Out SECURE
            (exec
               (inputList
                  [Name PlatoonSergeant says
                   prop
                     (SOME (PlatoonSergeantCOM actionsIn))]))::
           outs)) ⟺
    authenticationTest authentication
      [Name PlatoonSergeant says
       prop (SOME (PlatoonSergeantCOM actionsIn))] ∧
    CFGInterpret (M,Oi,Os)
      (CFG authentication stateAuth globalAuth
         ([Name PlatoonSergeant says
           prop (SOME (PlatoonSergeantCOM actionsIn))]::ins)
         SECURE outs) ∧
    (M,Oi,Os) satList
    propCommandList
      [Name PlatoonSergeant says
       prop (SOME (PlatoonSergeantCOM actionsIn))]
```

[SECURE_exec_actionsIn_thm]

```
⊢ ∀NS Out M Oi Os.
    TR (M,Oi,Os) (exec [SOME (PlatoonSergeantCOM actionsIn)])
      (CFG authentication stateAuth globalAuth
         ([Name PlatoonSergeant says
           prop (SOME (PlatoonSergeantCOM actionsIn))]::ins)
         SECURE outs)
      (CFG authentication stateAuth globalAuth ins
         (NS SECURE
            (exec [SOME (PlatoonSergeantCOM actionsIn)]))
         (Out SECURE
            (exec [SOME (PlatoonSergeantCOM actionsIn)])::
           outs)) ⟺
    authenticationTest authentication
      [Name PlatoonSergeant says
       prop (SOME (PlatoonSergeantCOM actionsIn))] ∧
```

```
     CFGInterpret (M,Oi,Os)
       (CFG authentication stateAuth globalAuth
          ([Name PlatoonSergeant says
            prop (SOME (PlatoonSergeantCOM actionsIn))]::ins)
          SECURE outs) ∧
     (M,Oi,Os) satList
     [prop (SOME (PlatoonSergeantCOM actionsIn))]
```

[WITHDRAW_exec_complete_lemma1]

```
⊢ ∀M Oi Os.
     CFGInterpret (M,Oi,Os)
       (CFG authentication stateAuth globalAuth
          ([Name PlatoonLeader says
            prop (SOME (PlatoonLeaderCOM complete))]::ins)
          WITHDRAW outs) ⇒
     (M,Oi,Os) satList
     propCommandList
       [Name PlatoonLeader says
        prop (SOME (PlatoonLeaderCOM complete))]
```

[WITHDRAW_exec_complete_lemma2]

```
⊢ ∀NS Out M Oi Os.
     TR (M,Oi,Os)
       (exec
          (inputList
             [Name PlatoonLeader says
              prop (SOME (PlatoonLeaderCOM complete))]))
       (CFG authentication stateAuth globalAuth
          ([Name PlatoonLeader says
            prop (SOME (PlatoonLeaderCOM complete))]::ins)
          WITHDRAW outs)
       (CFG authentication stateAuth globalAuth ins
          (NS WITHDRAW
             (exec
                (inputList
                   [Name PlatoonLeader says
                    prop (SOME (PlatoonLeaderCOM complete))])))
          (Out WITHDRAW
             (exec
                (inputList
                   [Name PlatoonLeader says
                    prop (SOME (PlatoonLeaderCOM complete))]))::
               outs)) ⟺
     authenticationTest authentication
       [Name PlatoonLeader says
        prop (SOME (PlatoonLeaderCOM complete))] ∧
     CFGInterpret (M,Oi,Os)
       (CFG authentication stateAuth globalAuth
          ([Name PlatoonLeader says
```

```
          prop (SOME (PlatoonLeaderCOM complete))]::ins)
        WITHDRAW outs) ∧
    (M,Oi,Os) satList
    propCommandList
      [Name PlatoonLeader says
       prop (SOME (PlatoonLeaderCOM complete))]
```

[WITHDRAW_exec_complete_thm]

```
⊢ ∀NS Out M Oi Os.
    TR (M,Oi,Os) (exec [SOME (PlatoonLeaderCOM complete)])
      (CFG authentication stateAuth globalAuth
         ([Name PlatoonLeader says
           prop (SOME (PlatoonLeaderCOM complete))]::ins)
         WITHDRAW outs)
      (CFG authentication stateAuth globalAuth ins
         (NS WITHDRAW
            (exec [SOME (PlatoonLeaderCOM complete)]))
         (Out WITHDRAW
            (exec [SOME (PlatoonLeaderCOM complete)])::
              outs)) ⟺
    authenticationTest authentication
      [Name PlatoonLeader says
       prop (SOME (PlatoonLeaderCOM complete))] ∧
    CFGInterpret (M,Oi,Os)
      (CFG authentication stateAuth globalAuth
         ([Name PlatoonLeader says
           prop (SOME (PlatoonLeaderCOM complete))]::ins)
         WITHDRAW outs) ∧
    (M,Oi,Os) satList [prop (SOME (PlatoonLeaderCOM complete))]
```

Index