Contents

1 projectTypes Theory

Built: 27 December 2018

Parent Theories: indexedLists, patternMatches

1.1 Datatypes

```
commands = PlatoonLeaderCOM platoonLeaderCom | OmniCOM omniCom

omniCom = none | omniNA

output = FormRT | RtMove | RtHalt | Complete | NoActionTaken
       | UnAuthenticated | UnAuthorized

platoonLeaderCom = formRT | rtMove | rtHalt | complete

principal = PlatoonLeader | Omni

state = MOVE_TO_ORP | FORM_RT | RT_MOVE | RT_HALT | COMPLETE
```

1.2 Theorems

[commands_distinct_clauses]

```
⊢ ∀ a′ a. PlatoonLeaderCOM a ≠ OmniCOM a′
```

[commands_one_one]

```
⊢ (∀ a a′.
     (PlatoonLeaderCOM a = PlatoonLeaderCOM a′) ⟺ (a = a′)) ∧
  ∀ a a′. (OmniCOM a = OmniCOM a′) ⟺ (a = a′)
```

[omniCom_distinct_clauses]

```
⊢ none ≠ omniNA
```

[output_distinct_clauses]

```
⊢ FormRT ≠ RtMove ∧ FormRT ≠ RtHalt ∧ FormRT ≠ Complete ∧
  FormRT ≠ NoActionTaken ∧ FormRT ≠ UnAuthenticated ∧
  FormRT ≠ UnAuthorized ∧ RtMove ≠ RtHalt ∧ RtMove ≠ Complete ∧
  RtMove ≠ NoActionTaken ∧ RtMove ≠ UnAuthenticated ∧
  RtMove ≠ UnAuthorized ∧ RtHalt ≠ Complete ∧
  RtHalt ≠ NoActionTaken ∧ RtHalt ≠ UnAuthenticated ∧
  RtHalt ≠ UnAuthorized ∧ Complete ≠ NoActionTaken ∧
  Complete ≠ UnAuthenticated ∧ Complete ≠ UnAuthorized ∧
  NoActionTaken ≠ UnAuthenticated ∧
  NoActionTaken ≠ UnAuthorized ∧ UnAuthenticated ≠ UnAuthorized
```

[platoonLeaderCom_distinct_clauses]

```
⊢ formRT ≠ rtMove ∧ formRT ≠ rtHalt ∧ formRT ≠ complete ∧
  rtMove ≠ rtHalt ∧ rtMove ≠ complete ∧ rtHalt ≠ complete
```

[principal_distinct_clauses]

```
⊢ PlatoonLeader ≠ Omni
```

[state_distinct_clauses]

```
⊢ MOVE_TO_ORP ≠ FORM_RT ∧ MOVE_TO_ORP ≠ RT_MOVE ∧
  MOVE_TO_ORP ≠ RT_HALT ∧ MOVE_TO_ORP ≠ COMPLETE ∧
  FORM_RT ≠ RT_MOVE ∧ FORM_RT ≠ RT_HALT ∧ FORM_RT ≠ COMPLETE ∧
  RT_MOVE ≠ RT_HALT ∧ RT_MOVE ≠ COMPLETE ∧ RT_HALT ≠ 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 v4.
    getOmniCOM (SOME (PlatoonLeaderCOM v4)::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)) ⇒
    ∀ 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 v146.
   getOmniCOMx
     (Name Omni says prop (SOME (PlatoonLeaderCOM v146))::
          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)) ∧
(∀ v146 xs.
   P xs ⇒
   P
     (Name Omni says prop (SOME (PlatoonLeaderCOM v146))::
          xs)) ∧
(∀ v135 v136 v68 xs.
   P xs ⇒ P (v135 meet v136 says prop v68::xs)) ∧
(∀ v137 v138 v68 xs.
   P xs ⇒ P (v137 quoting v138 says prop v68::xs)) ∧
(∀ v12 v69 xs. P xs ⇒ P (v12 says notf v69::xs)) ∧
(∀ v12 v70 v71 xs. P xs ⇒ P (v12 says (v70 andf v71)::xs)) ∧
(∀ v12 v72 v73 xs. P xs ⇒ P (v12 says (v72 orf v73)::xs)) ∧
(∀ v12 v74 v75 xs. P xs ⇒ P (v12 says (v74 impf v75)::xs)) ∧
(∀ v12 v76 v77 xs. P xs ⇒ P (v12 says (v76 eqf v77)::xs)) ∧
(∀ v12 v78 v79 xs. P xs ⇒ P (v12 says v78 says v79::xs)) ∧
(∀ v12 v80 v81 xs.
   P xs ⇒ P (v12 says v80 speaks_for v81::xs)) ∧
(∀ v12 v82 v83 xs.
   P xs ⇒ P (v12 says v82 controls v83::xs)) ∧
(∀ v12 v84 v85 v86 xs.
   P xs ⇒ P (v12 says reps v84 v85 v86::xs)) ∧
(∀ v12 v87 v88 xs. P xs ⇒ P (v12 says v87 domi v88::xs)) ∧
(∀ 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
```

[getPlatoonLeaderCOM_def]

```
⊢ (getPlatoonLeaderCOM [] = NONE) ∧
  (∀ xs cmd.
     getPlatoonLeaderCOM (SOME (PlatoonLeaderCOM cmd)::xs) =
     SOME (PlatoonLeaderCOM cmd)) ∧
  (∀ xs.
      getPlatoonLeaderCOM (NONE::xs) = getPlatoonLeaderCOM xs) ∧
   ∀ xs v5.
     getPlatoonLeaderCOM (SOME (OmniCOM v5)::xs) =
     getPlatoonLeaderCOM xs
```

[getPlatoonLeaderCOM_ind]

```
 ⊢ ∀ P.
     P [] ∧ (∀ cmd xs. P (SOME (PlatoonLeaderCOM cmd)::xs)) ∧
     (∀ xs. P xs ⇒ P (NONE::xs)) ∧
     (∀ v5 xs. P xs ⇒ P (SOME (OmniCOM v5)::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 (OmniCOM v147))::
          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 v_92 v_91 v_12.
      getPlatoonLeaderCOMx (v_12 says v_91 doms v_92::xs) =
      getPlatoonLeaderCOMx xs) ∧
   (∀ xs v_94 v_93 v_12.
      getPlatoonLeaderCOMx (v_12 says v_93 eqs v_94::xs) =
      getPlatoonLeaderCOMx xs) ∧
   (∀ xs v_96 v_95 v_12.
      getPlatoonLeaderCOMx (v_12 says v_95 eqn v_96::xs) =
      getPlatoonLeaderCOMx xs) ∧
   (∀ xs v_98 v_97 v_12.
      getPlatoonLeaderCOMx (v_12 says v_97 lte v_98::xs) =
      getPlatoonLeaderCOMx xs) ∧
   (∀ xs v_99 v_12 v100.
      getPlatoonLeaderCOMx (v_12 says v_99 lt v100::xs) =
      getPlatoonLeaderCOMx xs) ∧
   (∀ xs v_15 v_14.
      getPlatoonLeaderCOMx (v_14 speaks_for v_15::xs) =
      getPlatoonLeaderCOMx xs) ∧
   (∀ xs v_17 v_16.
      getPlatoonLeaderCOMx (v_16 controls v_17::xs) =
      getPlatoonLeaderCOMx xs) ∧
   (∀ xs v_20 v_19 v_18.
      getPlatoonLeaderCOMx (reps v_18 v_19 v_20::xs) =
      getPlatoonLeaderCOMx xs) ∧
   (∀ xs v_22 v_21.
      getPlatoonLeaderCOMx (v_21 domi v_22::xs) =
      getPlatoonLeaderCOMx xs) ∧
   (∀ xs v_24 v_23.
      getPlatoonLeaderCOMx (v_23 eqi v_24::xs) =
      getPlatoonLeaderCOMx xs) ∧
   (∀ xs v_26 v_25.
      getPlatoonLeaderCOMx (v_25 doms v_26::xs) =
      getPlatoonLeaderCOMx xs) ∧
   (∀ xs v_28 v_27.
      getPlatoonLeaderCOMx (v_27 eqs v_28::xs) =
      getPlatoonLeaderCOMx xs) ∧
   (∀ xs v_30 v_29.
      getPlatoonLeaderCOMx (v_29 eqn v_30::xs) =
      getPlatoonLeaderCOMx xs) ∧
   (∀ xs v_32 v_31.
      getPlatoonLeaderCOMx (v_31 lte v_32::xs) =
      getPlatoonLeaderCOMx xs) ∧
   ∀ xs v_34 v_33.
     getPlatoonLeaderCOMx (v_33 lt v_34::xs) =
     getPlatoonLeaderCOMx xs
```

[getPlatoonLeaderCOMx_ind]

```
 ⊢ ∀ P.
```

```
P [] ∧
(∀ cmd xs.
   P
     (Name PlatoonLeader says
      prop (SOME (PlatoonLeaderCOM cmd))::xs)) ∧
(∀ xs. P xs ⇒ P (TT::xs)) ∧ (∀ xs. P xs ⇒ P (FF::xs)) ∧
(∀ v_2 xs. P xs ⇒ P (prop v_2::xs)) ∧
(∀ v_3 xs. P xs ⇒ P (notf v_3::xs)) ∧
(∀ v_4 v_5 xs. P xs ⇒ P (v_4 andf v_5::xs)) ∧
(∀ v_6 v_7 xs. P xs ⇒ P (v_6 orf v_7::xs)) ∧
(∀ v_8 v_9 xs. P xs ⇒ P (v_8 impf v_9::xs)) ∧
(∀ v_10 v_11 xs. P xs ⇒ P (v_10 eqf v_11::xs)) ∧
(∀ v_12 xs. P xs ⇒ P (v_12 says TT::xs)) ∧
(∀ v_12 xs. P xs ⇒ P (v_12 says FF::xs)) ∧
(∀ v134 xs. P xs ⇒ P (Name v134 says prop NONE::xs)) ∧
(∀ v147 xs.
   P xs ⇒
   P
     (Name PlatoonLeader says prop (SOME (OmniCOM v147))::
          xs)) ∧
(∀ v144 xs.
   P xs ⇒ P (Name Omni says prop (SOME v144)::xs)) ∧
(∀ v135 v136 v_68 xs.
   P xs ⇒ P (v135 meet v136 says prop v_68::xs)) ∧
(∀ v137 v138 v_68 xs.
   P xs ⇒ P (v137 quoting v138 says prop v_68::xs)) ∧
(∀ v_12 v_69 xs. P xs ⇒ P (v_12 says notf v_69::xs)) ∧
(∀ v_12 v_70 v_71 xs. P xs ⇒ P (v_12 says (v_70 andf v_71)::xs)) ∧
(∀ v_12 v_72 v_73 xs. P xs ⇒ P (v_12 says (v_72 orf v_73)::xs)) ∧
(∀ v_12 v_74 v_75 xs. P xs ⇒ P (v_12 says (v_74 impf v_75)::xs)) ∧
(∀ v_12 v_76 v_77 xs. P xs ⇒ P (v_12 says (v_76 eqf v_77)::xs)) ∧
(∀ v_12 v_78 v_79 xs. P xs ⇒ P (v_12 says v_78 says v_79::xs)) ∧
(∀ v_12 v_80 v_81 xs.
   P xs ⇒ P (v_12 says v_80 speaks_for v_81::xs)) ∧
(∀ v_12 v_82 v_83 xs.
   P xs ⇒ P (v_12 says v_82 controls v_83::xs)) ∧
(∀ v_12 v_84 v_85 v_86 xs.
   P xs ⇒ P (v_12 says reps v_84 v_85 v_86::xs)) ∧
(∀ v_12 v_87 v_88 xs. P xs ⇒ P (v_12 says v_87 domi v_88::xs)) ∧
(∀ v_12 v_89 v_90 xs. P xs ⇒ P (v_12 says v_89 eqi v_90::xs)) ∧
(∀ v_12 v_91 v_92 xs. P xs ⇒ P (v_12 says v_91 doms v_92::xs)) ∧
(∀ v_12 v_93 v_94 xs. P xs ⇒ P (v_12 says v_93 eqs v_94::xs)) ∧
(∀ v_12 v_95 v_96 xs. P xs ⇒ P (v_12 says v_95 eqn v_96::xs)) ∧
(∀ v_12 v_97 v_98 xs. P xs ⇒ P (v_12 says v_97 lte v_98::xs)) ∧
(∀ v_12 v_99 v100 xs. P xs ⇒ P (v_12 says v_99 lt v100::xs)) ∧
(∀ v_14 v_15 xs. P xs ⇒ P (v_14 speaks_for v_15::xs)) ∧
(∀ v_16 v_17 xs. P xs ⇒ P (v_16 controls v_17::xs)) ∧
(∀ v_18 v_19 v_20 xs. P xs ⇒ P (reps v_18 v_19 v_20::xs)) ∧
(∀ v_21 v_22 xs. P xs ⇒ P (v_21 domi v_22::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
```

3 projectSM Theory

Built: 27 December 2018

Parent Theories: projectUtilities, ssm

3.1 Theorems

[NOut_def]

```
 ⊢ (NOut MOVE_TO_ORP (exec x) =
    if
      getPlatoonLeaderCOM x = SOME (PlatoonLeaderCOM formRT)
    then
      FormRT
    else NoActionTaken) ∧
   (NOut FORM_RT (exec x) =
    if
      getPlatoonLeaderCOM x = SOME (PlatoonLeaderCOM rtMove)
    then
      RtMove
    else NoActionTaken) ∧
   (NOut RT_MOVE (exec x) =
    if
      getPlatoonLeaderCOM x = SOME (PlatoonLeaderCOM rtHalt)
    then
      RtHalt
    else NoActionTaken) ∧
   (NOut RT_HALT (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 MOVE_TO_ORP (exec x)) ∧ (∀ x. P FORM_RT (exec x)) ∧
     (∀ x. P RT_MOVE (exec x)) ∧ (∀ x. P RT_HALT (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 MOVE_TO_ORP (exec x) =
     if
       getPlatoonLeaderCOM x = SOME (PlatoonLeaderCOM formRT)
     then
       FORM_RT
     else MOVE_TO_ORP) ∧
    (NS FORM_RT (exec x) =
     if
       getPlatoonLeaderCOM x = SOME (PlatoonLeaderCOM rtMove)
     then
       RT_MOVE
     else FORM_RT) ∧
    (NS RT_MOVE (exec x) =
     if
       getPlatoonLeaderCOM x = SOME (PlatoonLeaderCOM rtHalt)
     then
       RT_HALT
     else RT_MOVE) ∧
    (NS RT_HALT (exec x) =
     if
       getPlatoonLeaderCOM x = SOME (PlatoonLeaderCOM complete)
     then
       COMPLETE
     else RT_HALT) ∧ (NS s (trap v0) = s) ∧
    (NS s (discard v1) = s)
```

[NS_ind]

```
 ⊢ ∀P.
      (∀x. P MOVE_TO_ORP (exec x)) ∧ (∀x. P FORM_RT (exec x)) ∧
      (∀x. P RT_MOVE (exec x)) ∧ (∀x. P RT_HALT (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 = MOVE_TO_ORP then
        if
          getPlatoonLeaderCOMx x = SOME (PlatoonLeaderCOM formRT)
        then
          [Name PlatoonLeader controls
           prop (SOME (PlatoonLeaderCOM formRT))]
        else [prop NONE]
      else if s = FORM_RT then
        if
          getPlatoonLeaderCOMx x = SOME (PlatoonLeaderCOM rtMove)
        then
          [Name PlatoonLeader controls
           prop (SOME (PlatoonLeaderCOM rtMove))]
        else [prop NONE]
      else if s = RT_MOVE then
        if
          getPlatoonLeaderCOMx x = SOME (PlatoonLeaderCOM rtHalt)
        then
          [Name PlatoonLeader controls
           prop (SOME (PlatoonLeaderCOM rtHalt))]
        else [prop NONE]
      else if s = RT_HALT 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 Omni says prop (SOME (OmniCOM x))) ⟺
   T) ∧ (authentication TT ⟺ F) ∧ (authentication FF ⟺ F) ∧
  (authentication (prop v) ⟺ F) ∧
  (authentication (notf $v_1$) ⟺ F) ∧
  (authentication ($v_2$ andf $v_3$) ⟺ F) ∧
  (authentication ($v_4$ orf $v_5$) ⟺ F) ∧
  (authentication ($v_6$ impf $v_7$) ⟺ F) ∧
  (authentication ($v_8$ eqf $v_9$) ⟺ F) ∧
```

```
(authentication (Name v66 says TT) ⟺ F) ∧
(authentication (Name v66 says FF) ⟺ F) ∧
(authentication (Name v66 says prop NONE) ⟺ F) ∧
(authentication
   (Name Omni says prop (SOME (PlatoonLeaderCOM v144))) ⟺
 F) ∧
(authentication
   (Name PlatoonLeader says prop (SOME (OmniCOM v145))) ⟺
 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 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 Omni says
      prop (SOME (PlatoonLeaderCOM v144)))) ∧
(∀ v145.
   P
     (Name PlatoonLeader says
      prop (SOME (OmniCOM v145)))) ∧
(∀ 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

[FORM_RT_exec_rtMove_lemma1]

```
⊢ ∀ M Oi Os.
     CFGInterpret (M,Oi,Os)
```

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

[FORM_RT_exec_rtMove_lemma2]

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

[FORM_RT_exec_rtMove_thm]

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

[MOVE_TO_ORP_exec_formRT_lemma1]

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

[MOVE_TO_ORP_exec_formRT_lemma2]

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

[MOVE_TO_ORP_exec_formRT_thm]

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

[RT_HALT_exec_complete_lemma1]

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

[RT_HALT_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)
          RT_HALT outs)
       (CFG authentication stateAuth globalAuth ins
          (NS RT_HALT
             (exec
                (inputList
                   [Name PlatoonLeader says
                    prop (SOME (PlatoonLeaderCOM complete))])))
          (Out RT_HALT
             (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)
          RT_HALT outs) ∧
     (M,Oi,Os) satList
     propCommandList
       [Name PlatoonLeader says
        prop (SOME (PlatoonLeaderCOM complete))]
```

[RT_HALT_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)
          RT_HALT outs)
       (CFG authentication stateAuth globalAuth ins
          (NS RT_HALT (exec [SOME (PlatoonLeaderCOM complete)]))
          (Out RT_HALT
             (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)
           RT_HALT outs) ∧
      (M,Oi,Os) satList [prop (SOME (PlatoonLeaderCOM complete))]
```

[RT_MOVE_exec_rtHalt_lemma1]

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

[RT_MOVE_exec_rtHalt_lemma2]

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

[RT_MOVE_exec_rtHalt_thm]

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

Index