

## **Abstract**

This is the abstract for my master's thesis on Certified Security by Design (CSBD) and Access-Control Logic (ACL) because ACL is so cool and effective...because effective is cool. Here is some text for formatting.

At least 18 people have been killed and dozens trapped in the Indian city of Varanasi after a flyover collapsed, crushing vehicles beneath it. The flyover was still being built when portions of its cement structure fell on the road being used under it. Officials from the National Disaster Response Force said 18 bodies had been recovered so far. A rescue operation is continuing for those believed to still be trapped, but their number and condition is unknown. Photographs and video from the scene showed cars and a bus crushed beneath the weight of the concrete, many of which still held people inside. Local media reported that a handful of people had been successfully rescued, as seven cranes attempted to lift the concrete pillar. A large crowd also gathered at the scene. One eyewitness told reporters they were nearby when the collapse happened. "At least four cars, an auto-rickshaw and a minibus were crushed under it," they said.

India's NDTV also reported that many of those trapped are believed to be construction workers who had been building the flyover. The cause of the collapse is not yet known, and an inquiry has been ordered, NDTV added. Major collapses of buildings and other infrastructure are not uncommon in India, where the enforcement of construction standards is weaker than many Western countries. In September, 33 people died when a six-storey Mumbai building toppled and more than 20 people died in 2016 when a flyover collapsed in Kolkata. Other collapses with smaller death tolls are frequent. Varanasi is the home constituency of India's Prime Minister Narendra Modi, who said he was "extremely saddened by the loss of lives due to the collapse". "I pray that the injured recover soon. Spoke to officials and asked them to ensure all possible support to those affected," he tweeted.

Copyright

Disclaimer

Acknowledgements

# Table Of Contents

<b>Abstract</b>	<b>i</b>
<b>List of Figures</b>	<b>vi</b>
<b>List of Tables</b>	<b>vii</b>
<b>List of Acronyms</b>	<b>viii</b>
<b>Acronyms</b>	<b>viii</b>
<b>1 Introduction</b>	<b>1</b>
<b>2 Background</b>	<b>2</b>
<b>3 Systems Security Engineering</b>	<b>3</b>
3.1 NIST Special Publication 800-160 . . . . .	3
3.2 Verification & Documentation . . . . .	3
3.3 Principle of Complete Mediation . . . . .	3
3.3.1 Formal Verification Using Computer-Aided Reasoning . . . . .	3
<b>4 Certified Security by Design (CSBD) &amp; Access-Control Logic (ACL)</b>	<b>4</b>
4.1 Certified Security by Design (CSBD) . . . . .	5
4.2 Access-Control Logic (ACL) . . . . .	5
4.2.1 Principals . . . . .	5
4.2.2 Well-formed Formulas Formulas . . . . .	5
4.2.3 Kripke Structure . . . . .	5
4.2.3.1 satisfies . . . . .	5
4.2.3.2 soundness . . . . .	5
4.2.4 Well formed statements . . . . .	5
4.2.5 Inference Rules . . . . .	5
4.2.6 Complete mediation . . . . .	5
4.3 ACL in HOL . . . . .	5
4.3.1 satList . . . . .	5
4.3.2 Complete Mediation . . . . .	5
<b>5 Patrol Base Operations</b>	<b>1</b>
5.1 Motivation . . . . .	1
5.2 Ranger Handbook Description . . . . .	3
5.3 Describing The Patrol Base Operations . . . . .	3
5.4 Hierarchy of Secure State Machines . . . . .	3

5.4.1	OMNI-Level . . . . .	3
5.4.2	Escape . . . . .	3
5.4.3	Top Level . . . . .	3
5.4.4	Horizontal Slice . . . . .	3
5.4.4.1	ssmPlanPB . . . . .	3
5.4.4.2	ssmMoveToORP . . . . .	3
5.4.4.3	ssmConductORP . . . . .	3
5.4.4.4	ssmMoveToPB . . . . .	3
5.4.4.5	ssmConductPB . . . . .	3
5.4.5	Vertical Slice . . . . .	3
5.4.5.1	ssmSecureHalt . . . . .	3
5.4.5.2	ssmORPRecon . . . . .	3
5.4.5.3	ssmMoveToORP4L . . . . .	3
5.4.5.4	ssmFormRT . . . . .	3
<b>6</b>	<b>Secure State Machine Model</b>	<b>4</b>
6.1	State Machines . . . . .	5
6.1.1	Next-state Function . . . . .	5
6.1.2	Next-output Function . . . . .	5
6.1.3	Transition Commands . . . . .	5
6.2	Secure State Machines . . . . .	5
6.2.1	State Machine Versus Secure State Machine . . . . .	5
6.2.2	Transition Types . . . . .	5
6.2.3	Authentication . . . . .	5
6.2.4	Authorization . . . . .	5
6.3	Secure State Machines in HOL . . . . .	5
6.3.1	Parameterizable Secure State Machine . . . . .	5
6.3.2	Parameterization . . . . .	5
6.3.3	Configurations: five parts . . . . .	5
6.3.3.1	State Interpretation . . . . .	5
6.3.3.2	Security context . . . . .	5
6.3.3.3	Input stream . . . . .	5
6.3.3.4	State . . . . .	5
6.3.3.5	Output stream . . . . .	5
6.3.4	Authentication . . . . .	5
6.3.5	Configuration Interpretation . . . . .	5
6.3.6	Transition Definitions . . . . .	5
<b>7</b>	<b>Patrol Base Operations as Secure State Machines</b>	<b>6</b>
7.1	ssmPB: An Example from the Hierarchy . . . . .	7
7.1.1	Principals . . . . .	7
7.1.2	States . . . . .	7
7.1.3	Commands . . . . .	7
7.1.4	Next-State Function . . . . .	7
7.1.5	Next-Output Function . . . . .	7
7.1.6	Authentication . . . . .	7
7.1.7	Authorization . . . . .	7
7.1.8	Proved Theorems . . . . .	7

7.1.8.1	Platoon Leader Is Trusted on plCommands . . . . .	7
7.2	Other Variations . . . . .	7
7.2.1	ssmPlanPB: Non-sequential Transitions . . . . .	7
7.2.2	ssmConductORP: Principals Authorized for Subsets of Commands . . . . .	7
<b>8</b>	<b>Discussion</b>	<b>1</b>
8.1	Recap . . . . .	1
8.2	Mission Accomplished . . . . .	1
8.3	Stop-Gaps, Lessons Learned, & Advice . . . . .	1
8.4	Other Verifiable Theories . . . . .	1
8.4.1	Platoon Theory, Soldier Theory, Squad Theory, etc. . . . .	1
8.4.2	Soldiers in Roles . . . . .	1
<b>9</b>	<b>Future Work &amp; Implications</b>	<b>2</b>
9.1	The Devil Is in The Details . . . . .	2
9.2	Accountability Systems . . . . .	6
9.3	Applicability . . . . .	7
	<b>Appendices</b>	<b>9</b>
<b>A</b>	<b>Access Control Logic Theories: Pretty-Printed Theories</b>	<b>10</b>
<b>B</b>	<b>Secure State Machine &amp; Patrol Base Operations: Pretty-Printed Theories</b>	<b>33</b>
<b>C</b>	<b>Secure State Machine Theories: HOL Script Files</b>	<b>108</b>
C.1	ssm . . . . .	108
C.2	satList . . . . .	113
<b>D</b>	<b>Secure State Machine Theories Applied to Patrol Base Operations: HOL Script Files</b>	<b>115</b>
D.1	OMNILEvel . . . . .	115
D.2	TopLevel . . . . .	116
D.2.1	PBTypeIntegrated Theory: Type Definitions . . . . .	116
D.2.2	PBIntegratedDef Theory: Authentication & Authorization Definitions . . . . .	118
D.2.3	ssmPlanPBIntegrated Theory: Theorems . . . . .	119
D.3	Horizontal Slice . . . . .	123
D.3.1	ssmPlanPB . . . . .	123
D.3.1.1	PlanPBType Theory: Type Definitions . . . . .	123
D.3.1.2	PlanPBDef Theory: Authentication & Authorization Definitions . . . . .	123
D.3.1.3	ssmPlanPB Theory: Theorems . . . . .	123
D.3.2	ssmMoveToORP . . . . .	123
D.3.2.1	MoveToORPType Theory: Type Definitions . . . . .	123
D.3.2.2	MoveToORPDef Theory: Authentication & Authorization Definitions . . . . .	123
D.3.2.3	ssmMoveToORP Theory: Theorems . . . . .	123
D.3.3	ssmConductORP . . . . .	123

	D.3.3.1	ConductORPType Theory: Type Definitions . . . . .	123
	D.3.3.2	ConductORPDef Theory: Authentication & Authoriza- tion Definitions . . . . .	123
	D.3.3.3	ssmConductORP Theory: Theorems . . . . .	123
D.3.4	ssmMoveToPB	. . . . .	123
	D.3.4.1	MoveToPBType Theory: Type Definitions . . . . .	123
	D.3.4.2	MoveToPBDef Theory: Authentication & Authorization Definitions . . . . .	123
	D.3.4.3	ssmMoveToPB Theory: Theorems . . . . .	123
D.3.5	ssmConductPB	. . . . .	123
	D.3.5.1	ConductPBType Theory: Type Definitions . . . . .	123
	D.3.5.2	ConductPBDef Theory: Authentication & Authorization Definitions . . . . .	123
	D.3.5.3	ssmConductPB Theory: Theorems . . . . .	123
D.4	Vertical Slice	. . . . .	123
	D.4.1	ssmSecureHalt . . . . .	123
		D.4.1.1 SecureHaltType Theory: Type Definitions . . . . .	123
		D.4.1.2 SecureHaltDef Theory: Authentication & Authorization Definitions . . . . .	123
		D.4.1.3 ssmSecureHalt Theory: Theorems . . . . .	123
	D.4.2	ssmORPRecon . . . . .	123
		D.4.2.1 ORPReconType Theory: Type Definitions . . . . .	123
		D.4.2.2 ORPReconDef Theory: Authentication & Authorization Definitions . . . . .	123
		D.4.2.3 ssmORPRecon Theory: Theorems . . . . .	123
	D.4.3	ssmMoveToORP4L . . . . .	123
		D.4.3.1 MoveToORP4LType Theory: Type Definitions . . . . .	123
		D.4.3.2 MoveToORP4LDef Theory: Authentication & Authoriza- tion Definitions . . . . .	123
		D.4.3.3 ssmMoveToORP4L Theory: Theorems . . . . .	123
	D.4.4	ssmFormRT . . . . .	123
		D.4.4.1 FormRTType Theory: Type Definitions . . . . .	123
		D.4.4.2 FormRTDef Theory: Authentication & Authorization Def- initions . . . . .	123
		D.4.4.3 ssmFormRT Theory: Theorems . . . . .	123

## **E Map of The File Folder Structure 124**

## **References 125**

# List of Figures

# List of Tables



# Acronyms

**ACL** Access-Control Logic.

**CSBD** Certified Security by Design.

# Chapter 1

## Introduction

Some text here.[1]

# Chapter 2

## Background

Formal Methods

Functional Programming

Higher Order Logic (HOL) Interactive Theorem Prover

Other Interactive Theorem Provers

# Chapter 3

## Systems Security Engineering

### 3.1 NIST Special Publication 800-160

### 3.2 Verification & Documentation

### 3.3 Principle of Complete Mediation

#### 3.3.1 Formal Verification Using Computer-Aided Reasoning

# Chapter 4

## Certified Security by Design (CSBD)

&

# Access-Control Logic (ACL)

## 4.1 Certified Security by Design (CSBD)

## 4.2 Access-Control Logic (ACL)

### 4.2.1 Principals

### 4.2.2 Well-formed Formulas Formulas

### 4.2.3 Kripke Structure

#### 4.2.3.1 satisfies

#### 4.2.3.2 soundness

### 4.2.4 Well formed statements

### 4.2.5 Inference Rules

### 4.2.6 Complete mediation

## 4.3 ACL in HOL

### 4.3.1 satList

# Chapter 5

## Patrol Base Operations

This is the future works section. But, as I am typing this, it is the current working section for L<sup>A</sup>T<sub>E</sub>X. The point here is to get the margins in order. This means that there must be text of sufficient length to visually verify that the text meets LORI's standards. LORI is complying with SU standards for the senior thesis. Therefore, meeting LORI's standards is synonymous with meeting SU's standards. Resistance will only degrade you.

### 5.1 Motivation

This text deals with acronyms. This means that i'm testing where the acronym CSBD will show-up in the main document and how it will be presented in the Acronyms section.





## 5.2 Ranger Handbook Description

## 5.3 Describing The Patrol Base Operations

## 5.4 Hierarchy of Secure State Machines

### 5.4.1 OMNI-Level

### 5.4.2 Escape

### 5.4.3 Top Level

### 5.4.4 Horizontal Slice

#### 5.4.4.1 ssmPlanPB

#### 5.4.4.2 ssmMoveToORP

#### 5.4.4.3 ssmConductORP

#### 5.4.4.4 ssmMoveToPB

#### 5.4.4.5 ssmConductPB

### 5.4.5 Vertical Slice

#### 5.4.5.1 ssmSecureHalt

#### 5.4.5.2 ssmORPRecon



# Chapter 6

## Secure State Machine Model

### 6.1 State Machines

#### 6.1.1 Next-state Function

#### 6.1.2 Next-output Function

#### 6.1.3 Transition Commands

### 6.2 Secure State Machines

#### 6.2.1 State Machine Versus Secure State Machine

#### 6.2.2 Transition Types

#### 6.2.3 Authentication

#### 6.2.4 Authorization



# Chapter 7

## Patrol Base Operations as Secure State Machines

### 7.1 ssmPB: An Example from the Hierarchy

#### 7.1.1 Principals

#### 7.1.2 States

#### 7.1.3 Commands

#### 7.1.4 Next-State Function

#### 7.1.5 Next-Output Function

#### 7.1.6 Authentication

#### 7.1.7 Authorization

# Chapter 8

## Discussion

### 8.1 Recap

### 8.2 Mission Accomplished

### 8.3 Stop-Gaps, Lessons Learned, & Advice

### 8.4 Other Verifiable Theories

#### 8.4.1 Platoon Theory, Soldier Theory, Squad Theory, etc.

#### 8.4.2 Soldiers in Roles

# Chapter 9

## Future Work & Implications

This is the future works section. But, as I am typing this, it is the current working section for L<sup>A</sup>T<sub>E</sub>X. The point here is to get the margins in order. This means that there must be text of sufficient length to visually verify that the text meets LORI's standards. LORI is complying with SU standards for the senior thesis. Therefore, meeting LORI's standards is synonymous with meeting SU's standards. Resistance will only degrade you.

### 9.1 The Devil Is in The Details

Of course, there are top margins and bottom margins. This means that we'll need more text. You know, the best way to generate text is to just cut-n-paste some random stuff. Perinton, N.Y. – The FBI conducted a search of Morgan Management LLC's offices in Monroe County Monday as part of an ongoing investigation into the development company's business practices, according to Rochester area media reports.

Agents were seen carrying boxes in and out of the company's headquarters at 1080

Pittsford Victor Road in the town of Perinton, according to the reports.

An FBI spokeswoman confirmed that agents conducted "court-authorized activity at 1080 Pittsford Victor Road," the Democrat & Chronicle reported. The company's founder, developer Robert Morgan, was in the office as agents conducted the search, the newspaper said.

The newspaper reported in September that a federal investigation is focused on bank loans to Morgan's real estate portfolio, which, according to the company's website, has grown to 140 properties and more than 34,000 apartment units across 14 states since the company's founding in 1979.

The investigation is centered largely on Buffalo-region apartment complexes purchased by Morgan's companies and whether the information the company gave lenders to obtain the loans was accurate, according to the newspaper.

However, the Buffalo News reported in March that the investigation includes a look at Morgan's purchase of the Rugby Square apartment complex on Dorchester Avenue in Syracuse. One of Morgan's companies borrowed \$5.56 million to buy the apartment complex in a distress sale in 2012, then obtained a new \$9 million mortgage on the property just 10 months later after reporting a major turnaround of the complex, the newspaper said.

Morgan has said his companies have done nothing illegal to obtain financing. No charges have been filed in connection with the investigation.

According to the company's website, Morgan operates 13 apartment complexes in the Syracuse area.

Perinton, N.Y. – The FBI conducted a search of Morgan Management LLC's offices in Monroe County Monday as part of an ongoing investigation into the development



company's business practices, according to Rochester area media reports.

Agents were seen carrying boxes in and out of the company's headquarters at 1080 Pittsford Victor Road in the town of Perinton, according to the reports.

An FBI spokeswoman confirmed that agents conducted "court-authorized activity at 1080 Pittsford Victor Road," the Democrat & Chronicle reported. The company's founder, developer Robert Morgan, was in the office as agents conducted the search, the newspaper said.

The newspaper reported in September that a federal investigation is focused on bank loans to Morgan's real estate portfolio, which, according to the company's website, has grown to 140 properties and more than 34,000 apartment units across 14 states since the company's founding in 1979.

The investigation is centered largely on Buffalo-region apartment complexes purchased by Morgan's companies and whether the information the company gave lenders to obtain the loans was accurate, according to the newspaper.

However, the Buffalo News reported in March that the investigation includes a look at Morgan's purchase of the Rugby Square apartment complex on Dorchester Avenue in Syracuse. One of Morgan's companies borrowed \$5.56 million to buy the apartment complex in a distress sale in 2012, then obtained a new \$9 million mortgage on the property just 10 months later after reporting a major turnaround of the complex, the newspaper said.

Morgan has said his companies have done nothing illegal to obtain financing. No charges have been filed in connection with the investigation.

According to the company's website, Morgan operates 13 apartment complexes in the Syracuse area.

Perinton, N.Y. – The FBI conducted a search of Morgan Management LLC’s offices in Monroe County Monday as part of an ongoing investigation into the development company’s business practices, according to Rochester area media reports.

Agents were seen carrying boxes in and out of the company’s headquarters at 1080 Pittsford Victor Road in the town of Perinton, according to the reports.

An FBI spokeswoman confirmed that agents conducted ”court-authorized activity at 1080 Pittsford Victor Road,” the Democrat & Chronicle reported. The company’s founder, developer Robert Morgan, was in the office as agents conducted the search, the newspaper said.

The newspaper reported in September that a federal investigation is focused on bank loans to Morgan’s real estate portfolio, which, according to the company’s website, has grown to 140 properties and more than 34,000 apartment units across 14 states since the company’s founding in 1979.

The investigation is centered largely on Buffalo-region apartment complexes purchased by Morgan’s companies and whether the information the company gave lenders to obtain the loans was accurate, according to the newspaper.

However, the Buffalo News reported in March that the investigation includes a look at Morgan’s purchase of the Rugby Square apartment complex on Dorchester Avenue in Syracuse. One of Morgan’s companies borrowed \$5.56 million to buy the apartment complex in a distress sale in 2012, then obtained a new \$9 million mortgage on the property just 10 months later after reporting a major turnaround of the complex, the newspaper said.

Morgan has said his companies have done nothing illegal to obtain financing. No charges have been filed in connection with the investigation.

According to the company’s website, Morgan operates 13 apartment complexes in the Syracuse area.

## **9.2 Accountability Systems**

Perinton, N.Y. – The FBI conducted a search of Morgan Management LLC’s offices in Monroe County Monday as part of an ongoing investigation into the development company’s business practices, according to Rochester area media reports.

Agents were seen carrying boxes in and out of the company’s headquarters at 1080 Pittsford Victor Road in the town of Perinton, according to the reports.

An FBI spokeswoman confirmed that agents conducted ”court-authorized activity at 1080 Pittsford Victor Road,” the Democrat & Chronicle reported. The company’s founder, developer Robert Morgan, was in the office as agents conducted the search, the newspaper said.

The newspaper reported in September that a federal investigation is focused on bank loans to Morgan’s real estate portfolio, which, according to the company’s website, has grown to 140 properties and more than 34,000 apartment units across 14 states since the company’s founding in 1979.

The investigation is centered largely on Buffalo-region apartment complexes purchased by Morgan’s companies and whether the information the company gave lenders to obtain the loans was accurate, according to the newspaper.

However, the Buffalo News reported in March that the investigation includes a look at Morgan’s purchase of the Rugby Square apartment complex on Dorchester Avenue in Syracuse. One of Morgan’s companies borrowed \$5.56 million to buy the apartment

complex in a distress sale in 2012, then obtained a new \$9 million mortgage on the property just 10 months later after reporting a major turnaround of the complex, the newspaper said.

Morgan has said his companies have done nothing illegal to obtain financing. No charges have been filed in connection with the investigation.

According to the company's website, Morgan operates 13 apartment complexes in the Syracuse area.

## **9.3 Applicability**

Perinton, N.Y. – The FBI conducted a search of Morgan Management LLC's offices in Monroe County Monday as part of an ongoing investigation into the development company's business practices, according to Rochester area media reports.

Agents were seen carrying boxes in and out of the company's headquarters at 1080 Pittsford Victor Road in the town of Perinton, according to the reports.

An FBI spokeswoman confirmed that agents conducted "court-authorized activity at 1080 Pittsford Victor Road," the Democrat & Chronicle reported. The company's founder, developer Robert Morgan, was in the office as agents conducted the search, the newspaper said.

The newspaper reported in September that a federal investigation is focused on bank loans to Morgan's real estate portfolio, which, according to the company's website, has grown to 140 properties and more than 34,000 apartment units across 14 states since the company's founding in 1979.

The investigation is centered largely on Buffalo-region apartment complexes purchased by Morgan's companies and whether the information the company gave lenders to obtain the loans was accurate, according to the newspaper.

However, the Buffalo News reported in March that the investigation includes a look at Morgan's purchase of the Rugby Square apartment complex on Dorchester Avenue in Syracuse. One of Morgan's companies borrowed \$5.56 million to buy the apartment complex in a distress sale in 2012, then obtained a new \$9 million mortgage on the property just 10 months later after reporting a major turnaround of the complex, the newspaper said.

Morgan has said his companies have done nothing illegal to obtain financing. No charges have been filed in connection with the investigation.

According to the company's website, Morgan operates 13 apartment complexes in the Syracuse area.

# Appendices

# Appendix A

## Access Control Logic Theories: Pretty-Printed Theories

# Contents

<b>1</b>	<b>acfoundation Theory</b>	<b>3</b>
1.1	Datatypes . . . . .	3
1.2	Definitions . . . . .	3
1.3	Theorems . . . . .	4
<b>2</b>	<b>acsemanatics Theory</b>	<b>6</b>
2.1	Definitions . . . . .	6
2.2	Theorems . . . . .	8
<b>3</b>	<b>aclrules Theory</b>	<b>10</b>
3.1	Definitions . . . . .	11
3.2	Theorems . . . . .	11
<b>4</b>	<b>aclDrules Theory</b>	<b>17</b>
4.1	Theorems . . . . .	17





# 1 aclfoundation Theory

**Built:** 25 February 2018

**Parent Theories:** indexedLists, patternMatches

## 1.1 Datatypes

```
Form =
  TT
| FF
| prop 'aavar
| notf (('aavar, 'apn, 'il, 'sl) Form)
| (andf) (('aavar, 'apn, 'il, 'sl) Form)
      (('aavar, 'apn, 'il, 'sl) Form)
| (orf) (('aavar, 'apn, 'il, 'sl) Form)
      (('aavar, 'apn, 'il, 'sl) Form)
| (impf) (('aavar, 'apn, 'il, 'sl) Form)
      (('aavar, 'apn, 'il, 'sl) Form)
| (eqf) (('aavar, 'apn, 'il, 'sl) Form)
      (('aavar, 'apn, 'il, 'sl) Form)
| (says) ('apn Princ) (('aavar, 'apn, 'il, 'sl) Form)
| (speaks_for) ('apn Princ) ('apn Princ)
| (controls) ('apn Princ) (('aavar, 'apn, 'il, 'sl) Form)
| reps ('apn Princ) ('apn Princ)
      (('aavar, 'apn, 'il, 'sl) Form)
| (domi) (('apn, 'il) IntLevel) (('apn, 'il) IntLevel)
| (eqi) (('apn, 'il) IntLevel) (('apn, 'il) IntLevel)
| (doms) (('apn, 'sl) SecLevel) (('apn, 'sl) SecLevel)
| (eqs) (('apn, 'sl) SecLevel) (('apn, 'sl) SecLevel)
| (eqn) num num
| (lte) num num
| (lt) num num
```

```
Kripke =
  KS ('aavar -> 'aaworld -> bool)
      ('apn -> 'aaworld -> 'aaworld -> bool) ('apn -> 'il)
      ('apn -> 'sl)
```

```
Princ =
  Name 'apn
| (meet) ('apn Princ) ('apn Princ)
| (quoting) ('apn Princ) ('apn Princ) ;
```

```
IntLevel = iLab 'il | il 'apn ;
```

```
SecLevel = sLab 'sl | sl 'apn
```

## 1.2 Definitions

[imapKS\_def]

$$\vdash \forall \text{Intp } Jfn \text{ ilmap } slmap. \\ \text{imapKS } (KS \text{ Intp } Jfn \text{ ilmap } slmap) = \text{ilmap}$$

[intpKS\_def]

$$\vdash \forall \text{Intp } Jfn \text{ ilmap } slmap. \\ \text{intpKS } (KS \text{ Intp } Jfn \text{ ilmap } slmap) = \text{Intp}$$

[jKS\_def]

$$\vdash \forall \text{Intp } Jfn \text{ ilmap } slmap. \text{jKS } (KS \text{ Intp } Jfn \text{ ilmap } slmap) = Jfn$$

[O1\_def]

$$\vdash O1 = PO \text{ one\_weakorder}$$

[one\_weakorder\_def]

$$\vdash \forall x \ y. \text{one\_weakorder } x \ y \iff T$$

[po\_TY\_DEF]

$$\vdash \exists rep. \text{TYPE\_DEFINITION WeakOrder } rep$$

[po\_tybij]

$$\vdash (\forall a. PO \text{ (repPO } a) = a) \wedge \\ \forall r. \text{WeakOrder } r \iff (\text{repPO } (PO \ r) = r)$$

[prod\_PO\_def]

$$\vdash \forall PO_1 \ PO_2. \\ \text{prod\_PO } PO_1 \ PO_2 = PO \text{ (RPROD } (\text{repPO } PO_1) \ (\text{repPO } PO_2))$$

[smapKS\_def]

$$\vdash \forall \text{Intp } Jfn \text{ ilmap } slmap. \\ \text{smapKS } (KS \text{ Intp } Jfn \text{ ilmap } slmap) = \text{slmap}$$

[Subset\_PO\_def]

$$\vdash \text{Subset\_PO} = PO \ (\subseteq)$$

### 1.3 Theorems

[abs\_po11]

$$\vdash \forall r \ r'. \\ \text{WeakOrder } r \Rightarrow \text{WeakOrder } r' \Rightarrow ((PO \ r = PO \ r') \iff (r = r'))$$

[absPO\_fn\_onto]

$$\vdash \forall a. \exists r. (a = PO \ r) \wedge \text{WeakOrder } r$$

[antisym\_prod\_antisym]

$\vdash \forall r\ s.$   
 $\text{antisymmetric } r \wedge \text{antisymmetric } s \Rightarrow$   
 $\text{antisymmetric } (\text{RPROD } r\ s)$

[EQ\_WeakOrder]

$\vdash \text{WeakOrder } (=)$

[KS\_bij]

$\vdash \forall M. M = \text{KS } (\text{intpKS } M) (\text{jKS } M) (\text{imapKS } M) (\text{smmapKS } M)$

[one\_weakorder\_WO]

$\vdash \text{WeakOrder one\_weakorder}$

[onto\_po]

$\vdash \forall r. \text{WeakOrder } r \iff \exists a. r = \text{repPO } a$

[po\_bij]

$\vdash (\forall a. \text{PO } (\text{repPO } a) = a) \wedge$   
 $\forall r. \text{WeakOrder } r \iff (\text{repPO } (\text{PO } r) = r)$

[PO\_repPO]

$\vdash \forall a. \text{PO } (\text{repPO } a) = a$

[refl\_prod\_refl]

$\vdash \forall r\ s. \text{reflexive } r \wedge \text{reflexive } s \Rightarrow \text{reflexive } (\text{RPROD } r\ s)$

[repPO\_iPO\_partial\_order]

$\vdash (\forall x. \text{repPO } iPO\ x\ x) \wedge$   
 $(\forall x\ y. \text{repPO } iPO\ x\ y \wedge \text{repPO } iPO\ y\ x \Rightarrow (x = y)) \wedge$   
 $\forall x\ y\ z. \text{repPO } iPO\ x\ y \wedge \text{repPO } iPO\ y\ z \Rightarrow \text{repPO } iPO\ x\ z$

[repPO\_01]

$\vdash \text{repPO } 01 = \text{one\_weakorder}$

[repPO\_prod\_PO]

$\vdash \forall po_1\ po_2.$   
 $\text{repPO } (\text{prod\_PO } po_1\ po_2) = \text{RPROD } (\text{repPO } po_1) (\text{repPO } po_2)$

[repPO\_Subset\_PO]

$\vdash \text{repPO } \text{Subset\_PO} = (\subseteq)$

[RPROD\_THM]

$\vdash \forall r\ s\ a\ b.$   
 $\text{RPROD } r\ s\ a\ b \iff r\ (\text{FST } a)\ (\text{FST } b) \wedge s\ (\text{SND } a)\ (\text{SND } b)$

[SUBSET\_WO]

$\vdash \text{WeakOrder } (\subseteq)$

[trans\_prod\_trans]

$\vdash \forall r s. \text{transitive } r \wedge \text{transitive } s \Rightarrow \text{transitive } (\text{RPROD } r s)$

[WeakOrder\_Exists]

$\vdash \exists R. \text{WeakOrder } R$

[WO\_prod\_WO]

$\vdash \forall r s. \text{WeakOrder } r \wedge \text{WeakOrder } s \Rightarrow \text{WeakOrder } (\text{RPROD } r s)$

[WO\_repPO]

$\vdash \forall r. \text{WeakOrder } r \iff (\text{repPO } (\text{PO } r) = r)$

## 2 aclsemanatics Theory

**Built:** 25 February 2018

**Parent Theories:** acelfoundation

### 2.1 Definitions

[Efn\_def]

$\vdash (\forall Oi Os M. \text{Efn } Oi Os M \text{ TT} = \mathcal{U}(:'v)) \wedge$   
 $(\forall Oi Os M. \text{Efn } Oi Os M \text{ FF} = \{\}) \wedge$   
 $(\forall Oi Os M p. \text{Efn } Oi Os M (\text{prop } p) = \text{intpKS } M p) \wedge$   
 $(\forall Oi Os M f.$   
 $\quad \text{Efn } Oi Os M (\text{notf } f) = \mathcal{U}(:'v) \text{ DIFF Efn } Oi Os M f) \wedge$   
 $(\forall Oi Os M f_1 f_2.$   
 $\quad \text{Efn } Oi Os M (f_1 \text{ andf } f_2) =$   
 $\quad \text{Efn } Oi Os M f_1 \cap \text{Efn } Oi Os M f_2) \wedge$   
 $(\forall Oi Os M f_1 f_2.$   
 $\quad \text{Efn } Oi Os M (f_1 \text{ orf } f_2) =$   
 $\quad \text{Efn } Oi Os M f_1 \cup \text{Efn } Oi Os M f_2) \wedge$   
 $(\forall Oi Os M f_1 f_2.$   
 $\quad \text{Efn } Oi Os M (f_1 \text{ impf } f_2) =$   
 $\quad \mathcal{U}(:'v) \text{ DIFF Efn } Oi Os M f_1 \cup \text{Efn } Oi Os M f_2) \wedge$   
 $(\forall Oi Os M f_1 f_2.$   
 $\quad \text{Efn } Oi Os M (f_1 \text{ eqf } f_2) =$   
 $\quad (\mathcal{U}(:'v) \text{ DIFF Efn } Oi Os M f_1 \cup \text{Efn } Oi Os M f_2) \cap$   
 $\quad (\mathcal{U}(:'v) \text{ DIFF Efn } Oi Os M f_2 \cup \text{Efn } Oi Os M f_1)) \wedge$   
 $(\forall Oi Os M P f.$   
 $\quad \text{Efn } Oi Os M (P \text{ says } f) =$   
 $\quad \{w \mid \text{Jext } (\text{jKS } M) P w \subseteq \text{Efn } Oi Os M f\}) \wedge$   
 $(\forall Oi Os M P Q.$   
 $\quad \text{Efn } Oi Os M (P \text{ speaks\_for } Q) =$

```

if Jext (jKS M) Q RSUBSET Jext (jKS M) P then  $\mathcal{U}(:,v)$ 
else  $\{\}$   $\wedge$ 
 $(\forall Oi Os M P f.$ 
  Efn Oi Os M (P controls f) =
   $\mathcal{U}(:,v)$  DIFF  $\{w \mid \text{Jext (jKS M) } P \ w \subseteq \text{Efn Oi Os M } f\} \cup$ 
  Efn Oi Os M f)  $\wedge$ 
 $(\forall Oi Os M P Q f.$ 
  Efn Oi Os M (reps P Q f) =
   $\mathcal{U}(:,v)$  DIFF
   $\{w \mid \text{Jext (jKS M) (P quoting Q) } w \subseteq \text{Efn Oi Os M } f\} \cup$ 
   $\{w \mid \text{Jext (jKS M) } Q \ w \subseteq \text{Efn Oi Os M } f\}) \wedge$ 
 $(\forall Oi Os M intl_1 intl_2.$ 
  Efn Oi Os M ( $intl_1$  domi  $intl_2$ ) =
  if repP0 Oi (Lifn M  $intl_2$ ) (Lifn M  $intl_1$ ) then  $\mathcal{U}(:,v)$ 
  else  $\{\}$   $\wedge$ 
 $(\forall Oi Os M intl_2 intl_1.$ 
  Efn Oi Os M ( $intl_2$  eqi  $intl_1$ ) =
  (if repP0 Oi (Lifn M  $intl_2$ ) (Lifn M  $intl_1$ ) then  $\mathcal{U}(:,v)$ 
  else  $\{\}) \cap$ 
  (if repP0 Oi (Lifn M  $intl_1$ ) (Lifn M  $intl_2$ ) then  $\mathcal{U}(:,v)$ 
  else  $\{\}) \wedge$ 
 $(\forall Oi Os M secl_1 secl_2.$ 
  Efn Oi Os M ( $secl_1$  doms  $secl_2$ ) =
  if repP0 Os (Lsfm M  $secl_2$ ) (Lsfm M  $secl_1$ ) then  $\mathcal{U}(:,v)$ 
  else  $\{\}$   $\wedge$ 
 $(\forall Oi Os M secl_2 secl_1.$ 
  Efn Oi Os M ( $secl_2$  eqs  $secl_1$ ) =
  (if repP0 Os (Lsfm M  $secl_2$ ) (Lsfm M  $secl_1$ ) then  $\mathcal{U}(:,v)$ 
  else  $\{\}) \cap$ 
  (if repP0 Os (Lsfm M  $secl_1$ ) (Lsfm M  $secl_2$ ) then  $\mathcal{U}(:,v)$ 
  else  $\{\}) \wedge$ 
 $(\forall Oi Os M numExp_1 numExp_2.$ 
  Efn Oi Os M ( $numExp_1$  eqn  $numExp_2$ ) =
  if  $numExp_1 = numExp_2$  then  $\mathcal{U}(:,v)$  else  $\{\}$   $\wedge$ 
 $(\forall Oi Os M numExp_1 numExp_2.$ 
  Efn Oi Os M ( $numExp_1$  lte  $numExp_2$ ) =
  if  $numExp_1 \leq numExp_2$  then  $\mathcal{U}(:,v)$  else  $\{\}$   $\wedge$ 
 $\forall Oi Os M numExp_1 numExp_2.$ 
  Efn Oi Os M ( $numExp_1$  lt  $numExp_2$ ) =
  if  $numExp_1 < numExp_2$  then  $\mathcal{U}(:,v)$  else  $\{\}$ 

```

**[Jext\_def]**

```

 $\vdash (\forall J s. \text{Jext } J (\text{Name } s) = J s) \wedge$ 
 $(\forall J P_1 P_2.$ 
   $\text{Jext } J (P_1 \text{ meet } P_2) = \text{Jext } J P_1 \text{ RUNION } \text{Jext } J P_2) \wedge$ 
 $\forall J P_1 P_2. \text{Jext } J (P_1 \text{ quoting } P_2) = \text{Jext } J P_2 \text{ } 0 \text{Jext } J P_1$ 

```

**[Lifn\_def]**

```

 $\vdash (\forall M l. \text{Lifn } M (\text{iLab } l) = l) \wedge$ 
 $\forall M \text{ name}. \text{Lifn } M (\text{il name}) = \text{imapKS } M \text{ name}$ 

```

[Lsfn\_def]

$$\vdash (\forall M \ l. \text{Lsfn } M \ (\text{sLab } l) = l) \wedge \\ \forall M \ \text{name}. \text{Lsfn } M \ (\text{sl } \text{name}) = \text{smapKS } M \ \text{name}$$

## 2.2 Theorems

[andf\_def]

$$\vdash \forall Oi \ Os \ M \ f_1 \ f_2. \\ \text{Efn } Oi \ Os \ M \ (f_1 \ \text{andf } f_2) = \text{Efn } Oi \ Os \ M \ f_1 \cap \text{Efn } Oi \ Os \ M \ f_2$$

[controls\_def]

$$\vdash \forall Oi \ Os \ M \ P \ f. \\ \text{Efn } Oi \ Os \ M \ (P \ \text{controls } f) = \\ \mathcal{U}(:, 'v) \text{ DIFF } \{w \mid \text{Jext } (\text{jKS } M) \ P \ w \subseteq \text{Efn } Oi \ Os \ M \ f\} \cup \\ \text{Efn } Oi \ Os \ M \ f$$

[controls\_says]

$$\vdash \forall M \ P \ f. \\ \text{Efn } Oi \ Os \ M \ (P \ \text{controls } f) = \text{Efn } Oi \ Os \ M \ (P \ \text{says } f \ \text{impf } f)$$

[domi\_def]

$$\vdash \forall Oi \ Os \ M \ \text{intl}_1 \ \text{intl}_2. \\ \text{Efn } Oi \ Os \ M \ (\text{intl}_1 \ \text{domi } \text{intl}_2) = \\ \text{if repP0 } Oi \ (\text{Lifn } M \ \text{intl}_2) \ (\text{Lifn } M \ \text{intl}_1) \ \text{then } \mathcal{U}(:, 'v) \\ \text{else } \{\}$$

[doms\_def]

$$\vdash \forall Oi \ Os \ M \ \text{secl}_1 \ \text{secl}_2. \\ \text{Efn } Oi \ Os \ M \ (\text{secl}_1 \ \text{doms } \text{secl}_2) = \\ \text{if repP0 } Os \ (\text{Lsfn } M \ \text{secl}_2) \ (\text{Lsfn } M \ \text{secl}_1) \ \text{then } \mathcal{U}(:, 'v) \\ \text{else } \{\}$$

[eqf\_def]

$$\vdash \forall Oi \ Os \ M \ f_1 \ f_2. \\ \text{Efn } Oi \ Os \ M \ (f_1 \ \text{eqf } f_2) = \\ (\mathcal{U}(:, 'v) \text{ DIFF } \text{Efn } Oi \ Os \ M \ f_1 \cup \text{Efn } Oi \ Os \ M \ f_2) \cap \\ (\mathcal{U}(:, 'v) \text{ DIFF } \text{Efn } Oi \ Os \ M \ f_2 \cup \text{Efn } Oi \ Os \ M \ f_1)$$

[eqf\_impf]

$$\vdash \forall M \ f_1 \ f_2. \\ \text{Efn } Oi \ Os \ M \ (f_1 \ \text{eqf } f_2) = \\ \text{Efn } Oi \ Os \ M \ ((f_1 \ \text{impf } f_2) \ \text{andf } (f_2 \ \text{impf } f_1))$$

**[eqi\_def]**

$\vdash \forall Oi\ Os\ M\ intl_2\ intl_1.$   
 $\text{Efn } Oi\ Os\ M\ (intl_2\ \text{eqi}\ intl_1) =$   
 $(\text{if repP0 } Oi\ (\text{Lifn } M\ intl_2)\ (\text{Lifn } M\ intl_1)\ \text{then } \mathcal{U}(:, 'v)$   
 $\quad \text{else } \{\}) \cap$   
 $\text{if repP0 } Oi\ (\text{Lifn } M\ intl_1)\ (\text{Lifn } M\ intl_2)\ \text{then } \mathcal{U}(:, 'v)$   
 $\quad \text{else } \{\}$

**[eqi\_domi]**

$\vdash \forall M\ intL_1\ intL_2.$   
 $\text{Efn } Oi\ Os\ M\ (intL_1\ \text{eqi}\ intL_2) =$   
 $\text{Efn } Oi\ Os\ M\ (intL_2\ \text{domi}\ intL_1\ \text{andf}\ intL_1\ \text{domi}\ intL_2)$

**[eqn\_def]**

$\vdash \forall Oi\ Os\ M\ numExp_1\ numExp_2.$   
 $\text{Efn } Oi\ Os\ M\ (numExp_1\ \text{eqn}\ numExp_2) =$   
 $\text{if } numExp_1 = numExp_2\ \text{then } \mathcal{U}(:, 'v)\ \text{else } \{\}$

**[eqs\_def]**

$\vdash \forall Oi\ Os\ M\ secl_2\ secl_1.$   
 $\text{Efn } Oi\ Os\ M\ (secl_2\ \text{eqs}\ secl_1) =$   
 $(\text{if repP0 } Os\ (\text{Lsfm } M\ secl_2)\ (\text{Lsfm } M\ secl_1)\ \text{then } \mathcal{U}(:, 'v)$   
 $\quad \text{else } \{\}) \cap$   
 $\text{if repP0 } Os\ (\text{Lsfm } M\ secl_1)\ (\text{Lsfm } M\ secl_2)\ \text{then } \mathcal{U}(:, 'v)$   
 $\quad \text{else } \{\}$

**[eqs\_doms]**

$\vdash \forall M\ secL_1\ secL_2.$   
 $\text{Efn } Oi\ Os\ M\ (secL_1\ \text{eqs}\ secL_2) =$   
 $\text{Efn } Oi\ Os\ M\ (secL_2\ \text{doms}\ secL_1\ \text{andf}\ secL_1\ \text{doms}\ secL_2)$

**[FF\_def]**

$\vdash \forall Oi\ Os\ M. \text{Efn } Oi\ Os\ M\ \text{FF} = \{\}$

**[impf\_def]**

$\vdash \forall Oi\ Os\ M\ f_1\ f_2.$   
 $\text{Efn } Oi\ Os\ M\ (f_1\ \text{impf}\ f_2) =$   
 $\mathcal{U}(:, 'v)\ \text{DIFF}\ \text{Efn } Oi\ Os\ M\ f_1 \cup \text{Efn } Oi\ Os\ M\ f_2$

**[lt\_def]**

$\vdash \forall Oi\ Os\ M\ numExp_1\ numExp_2.$   
 $\text{Efn } Oi\ Os\ M\ (numExp_1\ \text{lt}\ numExp_2) =$   
 $\text{if } numExp_1 < numExp_2\ \text{then } \mathcal{U}(:, 'v)\ \text{else } \{\}$

**[lte\_def]**

$\vdash \forall Oi\ Os\ M\ numExp_1\ numExp_2.$   
 $\text{Efn } Oi\ Os\ M\ (numExp_1\ \text{lte}\ numExp_2) =$   
 $\text{if } numExp_1 \leq numExp_2\ \text{then } \mathcal{U}(:, 'v)\ \text{else } \{\}$



[meet\_def]

$$\vdash \forall J P_1 P_2. \text{Jext } J (P_1 \text{ meet } P_2) = \text{Jext } J P_1 \text{ RUNION } \text{Jext } J P_2$$

[name\_def]

$$\vdash \forall J s. \text{Jext } J (\text{Name } s) = J s$$

[notf\_def]

$$\vdash \forall Oi Os M f. \text{Efn } Oi Os M (\text{notf } f) = \mathcal{U}(:'v) \text{ DIFF } \text{Efn } Oi Os M f$$

[orf\_def]

$$\vdash \forall Oi Os M f_1 f_2. \\ \text{Efn } Oi Os M (f_1 \text{ orf } f_2) = \text{Efn } Oi Os M f_1 \cup \text{Efn } Oi Os M f_2$$

[prop\_def]

$$\vdash \forall Oi Os M p. \text{Efn } Oi Os M (\text{prop } p) = \text{intpKS } M p$$

[quoting\_def]

$$\vdash \forall J P_1 P_2. \text{Jext } J (P_1 \text{ quoting } P_2) = \text{Jext } J P_2 \text{ } 0 \text{ Jext } J P_1$$

[reps\_def]

$$\vdash \forall Oi Os M P Q f. \\ \text{Efn } Oi Os M (\text{reps } P Q f) = \\ \mathcal{U}(:'v) \text{ DIFF} \\ \{w \mid \text{Jext } (\text{jKS } M) (P \text{ quoting } Q) w \subseteq \text{Efn } Oi Os M f\} \cup \\ \{w \mid \text{Jext } (\text{jKS } M) Q w \subseteq \text{Efn } Oi Os M f\}$$

[says\_def]

$$\vdash \forall Oi Os M P f. \\ \text{Efn } Oi Os M (P \text{ says } f) = \\ \{w \mid \text{Jext } (\text{jKS } M) P w \subseteq \text{Efn } Oi Os M f\}$$

[speaks\_for\_def]

$$\vdash \forall Oi Os M P Q. \\ \text{Efn } Oi Os M (P \text{ speaks\_for } Q) = \\ \text{if } \text{Jext } (\text{jKS } M) Q \text{ RSUBSET } \text{Jext } (\text{jKS } M) P \text{ then } \mathcal{U}(:'v) \\ \text{else } \{\}$$

[TT\_def]

$$\vdash \forall Oi Os M. \text{Efn } Oi Os M \text{ TT} = \mathcal{U}(:'v)$$

### 3 aclrules Theory

**Built:** 25 February 2018

**Parent Theories:** aclsemantics

### 3.1 Definitions

[sat\_def]

$$\vdash \forall M \ Oi \ Os \ f. (M, Oi, Os) \text{ sat } f \iff (\text{Efn } Oi \ Os \ M \ f = \mathcal{U}(:'world))$$

### 3.2 Theorems

[And\_Says]

$$\vdash \forall M \ Oi \ Os \ P \ Q \ f. \\ (M, Oi, Os) \text{ sat } P \text{ meet } Q \text{ says } f \text{ eqf } P \text{ says } f \text{ andf } Q \text{ says } f$$

[And\_Says\_Eq]

$$\vdash (M, Oi, Os) \text{ sat } P \text{ meet } Q \text{ says } f \iff \\ (M, Oi, Os) \text{ sat } P \text{ says } f \text{ andf } Q \text{ says } f$$

[and\_says\_lemma]

$$\vdash \forall M \ Oi \ Os \ P \ Q \ f. \\ (M, Oi, Os) \text{ sat } P \text{ meet } Q \text{ says } f \text{ impf } P \text{ says } f \text{ andf } Q \text{ says } f$$

[Controls\_Eq]

$$\vdash \forall M \ Oi \ Os \ P \ f. \\ (M, Oi, Os) \text{ sat } P \text{ controls } f \iff (M, Oi, Os) \text{ sat } P \text{ says } f \text{ impf } f$$

[DIFF\_UNIV\_SUBSET]

$$\vdash (\mathcal{U}(:'a) \text{ DIFF } s \cup t = \mathcal{U}(:'a)) \iff s \subseteq t$$

[domi\_antisymmetric]

$$\vdash \forall M \ Oi \ Os \ l_1 \ l_2. \\ (M, Oi, Os) \text{ sat } l_1 \text{ domi } l_2 \Rightarrow \\ (M, Oi, Os) \text{ sat } l_2 \text{ domi } l_1 \Rightarrow \\ (M, Oi, Os) \text{ sat } l_1 \text{ eqi } l_2$$

[domi\_reflexive]

$$\vdash \forall M \ Oi \ Os \ l. (M, Oi, Os) \text{ sat } l \text{ domi } l$$

[domi\_transitive]

$$\vdash \forall M \ Oi \ Os \ l_1 \ l_2 \ l_3. \\ (M, Oi, Os) \text{ sat } l_1 \text{ domi } l_2 \Rightarrow \\ (M, Oi, Os) \text{ sat } l_2 \text{ domi } l_3 \Rightarrow \\ (M, Oi, Os) \text{ sat } l_1 \text{ domi } l_3$$

[doms\_antisymmetric]

$$\vdash \forall M \ Oi \ Os \ l_1 \ l_2. \\ (M, Oi, Os) \text{ sat } l_1 \text{ doms } l_2 \Rightarrow \\ (M, Oi, Os) \text{ sat } l_2 \text{ doms } l_1 \Rightarrow \\ (M, Oi, Os) \text{ sat } l_1 \text{ eqs } l_2$$

[doms\_reflexive]

$$\vdash \forall M \ Oi \ Os \ l. (M, Oi, Os) \text{ sat } l \text{ doms } l$$

[doms\_transitive]

$$\begin{aligned} \vdash \forall M \ Oi \ Os \ l_1 \ l_2 \ l_3. \\ (M, Oi, Os) \text{ sat } l_1 \text{ doms } l_2 \Rightarrow \\ (M, Oi, Os) \text{ sat } l_2 \text{ doms } l_3 \Rightarrow \\ (M, Oi, Os) \text{ sat } l_1 \text{ doms } l_3 \end{aligned}$$

[eqf\_and\_impf]

$$\begin{aligned} \vdash \forall M \ Oi \ Os \ f_1 \ f_2. \\ (M, Oi, Os) \text{ sat } f_1 \text{ eqf } f_2 \iff \\ (M, Oi, Os) \text{ sat } (f_1 \text{ impf } f_2) \text{ andf } (f_2 \text{ impf } f_1) \end{aligned}$$

[eqf\_andf1]

$$\begin{aligned} \vdash \forall M \ Oi \ Os \ f \ f' \ g. \\ (M, Oi, Os) \text{ sat } f \text{ eqf } f' \Rightarrow \\ (M, Oi, Os) \text{ sat } f \text{ andf } g \Rightarrow \\ (M, Oi, Os) \text{ sat } f' \text{ andf } g \end{aligned}$$

[eqf\_andf2]

$$\begin{aligned} \vdash \forall M \ Oi \ Os \ f \ f' \ g. \\ (M, Oi, Os) \text{ sat } f \text{ eqf } f' \Rightarrow \\ (M, Oi, Os) \text{ sat } g \text{ andf } f \Rightarrow \\ (M, Oi, Os) \text{ sat } g \text{ andf } f' \end{aligned}$$

[eqf\_controls]

$$\begin{aligned} \vdash \forall M \ Oi \ Os \ P \ f \ f'. \\ (M, Oi, Os) \text{ sat } f \text{ eqf } f' \Rightarrow \\ (M, Oi, Os) \text{ sat } P \text{ controls } f \Rightarrow \\ (M, Oi, Os) \text{ sat } P \text{ controls } f' \end{aligned}$$

[eqf\_eq]

$$\begin{aligned} \vdash (\text{Efn } Oi \ Os \ M \ (f_1 \text{ eqf } f_2) = \mathcal{U}(:'b)) \iff \\ (\text{Efn } Oi \ Os \ M \ f_1 = \text{Efn } Oi \ Os \ M \ f_2) \end{aligned}$$

[eqf\_eqf1]

$$\begin{aligned} \vdash \forall M \ Oi \ Os \ f \ f' \ g. \\ (M, Oi, Os) \text{ sat } f \text{ eqf } f' \Rightarrow \\ (M, Oi, Os) \text{ sat } f \text{ eqf } g \Rightarrow \\ (M, Oi, Os) \text{ sat } f' \text{ eqf } g \end{aligned}$$

[eqf\_eqf2]

$$\begin{aligned} \vdash \forall M \ Oi \ Os \ f \ f' \ g. \\ (M, Oi, Os) \text{ sat } f \text{ eqf } f' \Rightarrow \\ (M, Oi, Os) \text{ sat } g \text{ eqf } f \Rightarrow \\ (M, Oi, Os) \text{ sat } g \text{ eqf } f' \end{aligned}$$

**[eqf\_impf1]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ f \ f' \ g. \\ &\quad (M, Oi, Os) \text{ sat } f \text{ eqf } f' \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } f \text{ impf } g \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } f' \text{ impf } g \end{aligned}$$
**[eqf\_impf2]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ f \ f' \ g. \\ &\quad (M, Oi, Os) \text{ sat } f \text{ eqf } f' \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } g \text{ impf } f \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } g \text{ impf } f' \end{aligned}$$
**[eqf\_notf]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ f \ f'. \\ &\quad (M, Oi, Os) \text{ sat } f \text{ eqf } f' \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat notf } f \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat notf } f' \end{aligned}$$
**[eqf\_orf1]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ f \ f' \ g. \\ &\quad (M, Oi, Os) \text{ sat } f \text{ eqf } f' \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } f \text{ orf } g \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } f' \text{ orf } g \end{aligned}$$
**[eqf\_orf2]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ f \ f' \ g. \\ &\quad (M, Oi, Os) \text{ sat } f \text{ eqf } f' \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } g \text{ orf } f \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } g \text{ orf } f' \end{aligned}$$
**[eqf\_reps]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ P \ Q \ f \ f'. \\ &\quad (M, Oi, Os) \text{ sat } f \text{ eqf } f' \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat reps } P \ Q \ f \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat reps } P \ Q \ f' \end{aligned}$$
**[eqf\_sat]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ f_1 \ f_2. \\ &\quad (M, Oi, Os) \text{ sat } f_1 \text{ eqf } f_2 \Rightarrow \\ &\quad ((M, Oi, Os) \text{ sat } f_1 \iff (M, Oi, Os) \text{ sat } f_2) \end{aligned}$$
**[eqf\_says]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ P \ f \ f'. \\ &\quad (M, Oi, Os) \text{ sat } f \text{ eqf } f' \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } P \text{ says } f \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } P \text{ says } f' \end{aligned}$$

**[eqi\_Eq]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ l_1 \ l_2. \\ &\quad (M, Oi, Os) \text{ sat } l_1 \text{ eqi } l_2 \iff \\ &\quad (M, Oi, Os) \text{ sat } l_2 \text{ domi } l_1 \text{ andf } l_1 \text{ domi } l_2 \end{aligned}$$
**[eqs\_Eq]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ l_1 \ l_2. \\ &\quad (M, Oi, Os) \text{ sat } l_1 \text{ eqs } l_2 \iff \\ &\quad (M, Oi, Os) \text{ sat } l_2 \text{ doms } l_1 \text{ andf } l_1 \text{ doms } l_2 \end{aligned}$$
**[Idemp\_Speaks\_For]**

$$\vdash \forall M \ Oi \ Os \ P. (M, Oi, Os) \text{ sat } P \text{ speaks\_for } P$$
**[Image\_cmp]**

$$\vdash \forall R_1 \ R_2 \ R_3 \ u. (R_1 \ 0 \ R_2) \ u \subseteq R_3 \iff R_2 \ u \subseteq \{y \mid R_1 \ y \subseteq R_3\}$$
**[Image\_SUBSET]**

$$\vdash \forall R_1 \ R_2. R_2 \text{ RSUBSET } R_1 \Rightarrow \forall w. R_2 \ w \subseteq R_1 \ w$$
**[Image\_UNION]**

$$\vdash \forall R_1 \ R_2 \ w. (R_1 \text{ RUNION } R_2) \ w = R_1 \ w \cup R_2 \ w$$
**[INTER\_EQ\_UNIV]**

$$\vdash (s \cap t = \mathcal{U}(:, 'a)) \iff (s = \mathcal{U}(:, 'a)) \wedge (t = \mathcal{U}(:, 'a))$$
**[Modus\_Ponens]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ f_1 \ f_2. \\ &\quad (M, Oi, Os) \text{ sat } f_1 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } f_1 \text{ impf } f_2 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } f_2 \end{aligned}$$
**[Mono\_speaks\_for]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ P \ P' \ Q \ Q'. \\ &\quad (M, Oi, Os) \text{ sat } P \text{ speaks\_for } P' \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } Q \text{ speaks\_for } Q' \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } P \text{ quoting } Q \text{ speaks\_for } P' \text{ quoting } Q' \end{aligned}$$
**[MP\_Says]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ P \ f_1 \ f_2. \\ &\quad (M, Oi, Os) \text{ sat } \\ &\quad P \text{ says } (f_1 \text{ impf } f_2) \text{ impf } P \text{ says } f_1 \text{ impf } P \text{ says } f_2 \end{aligned}$$
**[Quoting]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ P \ Q \ f. \\ &\quad (M, Oi, Os) \text{ sat } P \text{ quoting } Q \text{ says } f \text{ eqf } P \text{ says } Q \text{ says } f \end{aligned}$$

**[Quoting\_Eq]**

$$\vdash \forall M \ Oi \ Os \ P \ Q \ f. \\ (M, Oi, Os) \text{ sat } P \text{ quoting } Q \text{ says } f \iff \\ (M, Oi, Os) \text{ sat } P \text{ says } Q \text{ says } f$$
**[reps\_def\_lemma]**

$$\vdash \forall M \ Oi \ Os \ P \ Q \ f. \\ \text{Efn } Oi \ Os \ M \ (\text{reps } P \ Q \ f) = \\ \text{Efn } Oi \ Os \ M \ (P \text{ quoting } Q \text{ says } f \text{ impf } Q \text{ says } f)$$
**[Reps\_Eq]**

$$\vdash \forall M \ Oi \ Os \ P \ Q \ f. \\ (M, Oi, Os) \text{ sat reps } P \ Q \ f \iff \\ (M, Oi, Os) \text{ sat } P \text{ quoting } Q \text{ says } f \text{ impf } Q \text{ says } f$$
**[sat\_allworld]**

$$\vdash \forall M \ f. (M, Oi, Os) \text{ sat } f \iff \forall w. w \in \text{Efn } Oi \ Os \ M \ f$$
**[sat\_andf\_eq\_and\_sat]**

$$\vdash (M, Oi, Os) \text{ sat } f_1 \text{ andf } f_2 \iff \\ (M, Oi, Os) \text{ sat } f_1 \wedge (M, Oi, Os) \text{ sat } f_2$$
**[sat\_TT]**

$$\vdash (M, Oi, Os) \text{ sat TT}$$
**[Says]**

$$\vdash \forall M \ Oi \ Os \ P \ f. (M, Oi, Os) \text{ sat } f \Rightarrow (M, Oi, Os) \text{ sat } P \text{ says } f$$
**[says\_and\_lemma]**

$$\vdash \forall M \ Oi \ Os \ P \ Q \ f. \\ (M, Oi, Os) \text{ sat } P \text{ says } f \text{ andf } Q \text{ says } f \text{ impf } P \text{ meet } Q \text{ says } f$$
**[Speaks\_For]**

$$\vdash \forall M \ Oi \ Os \ P \ Q \ f. \\ (M, Oi, Os) \text{ sat } P \text{ speaks\_for } Q \text{ impf } P \text{ says } f \text{ impf } Q \text{ says } f$$
**[speaks\_for\_SUBSET]**

$$\vdash \forall R_3 \ R_2 \ R_1. \\ R_2 \text{ RSUBSET } R_1 \Rightarrow \forall w. \{w \mid R_1 \ w \subseteq R_3\} \subseteq \{w \mid R_2 \ w \subseteq R_3\}$$
**[SUBSET\_Image\_SUBSET]**

$$\vdash \forall R_1 \ R_2 \ R_3. \\ (\forall w_1. R_2 \ w_1 \subseteq R_1 \ w_1) \Rightarrow \\ \forall w. \{w \mid R_1 \ w \subseteq R_3\} \subseteq \{w \mid R_2 \ w \subseteq R_3\}$$

**[Trans\_Speaks\_For]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ P \ Q \ R. \\ &\quad (M, Oi, Os) \text{ sat } P \text{ speaks\_for } Q \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } Q \text{ speaks\_for } R \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } P \text{ speaks\_for } R \end{aligned}$$
**[UNIV\_DIFF\_SUBSET]**

$$\vdash \forall R_1 \ R_2. \ R_1 \subseteq R_2 \Rightarrow (\mathcal{U}(:'a) \text{ DIFF } R_1 \cup R_2 = \mathcal{U}(:'a))$$
**[world\_and]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ f_1 \ f_2 \ w. \\ &\quad w \in \text{Efn } Oi \ Os \ M \ (f_1 \text{ andf } f_2) \iff \\ &\quad w \in \text{Efn } Oi \ Os \ M \ f_1 \wedge w \in \text{Efn } Oi \ Os \ M \ f_2 \end{aligned}$$
**[world\_eq]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ f_1 \ f_2 \ w. \\ &\quad w \in \text{Efn } Oi \ Os \ M \ (f_1 \text{ eqf } f_2) \iff \\ &\quad (w \in \text{Efn } Oi \ Os \ M \ f_1 \iff w \in \text{Efn } Oi \ Os \ M \ f_2) \end{aligned}$$
**[world\_eqn]**

$$\vdash \forall M \ Oi \ Os \ n_1 \ n_2 \ w. \ w \in \text{Efn } Oi \ Os \ m \ (n_1 \text{ eqn } n_2) \iff (n_1 = n_2)$$
**[world\_F]**

$$\vdash \forall M \ Oi \ Os \ w. \ w \notin \text{Efn } Oi \ Os \ M \text{ FF}$$
**[world\_imp]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ f_1 \ f_2 \ w. \\ &\quad w \in \text{Efn } Oi \ Os \ M \ (f_1 \text{ impf } f_2) \iff \\ &\quad w \in \text{Efn } Oi \ Os \ M \ f_1 \Rightarrow w \in \text{Efn } Oi \ Os \ M \ f_2 \end{aligned}$$
**[world\_lt]**

$$\vdash \forall M \ Oi \ Os \ n_1 \ n_2 \ w. \ w \in \text{Efn } Oi \ Os \ m \ (n_1 \text{ lt } n_2) \iff n_1 < n_2$$
**[world\_lte]**

$$\vdash \forall M \ Oi \ Os \ n_1 \ n_2 \ w. \ w \in \text{Efn } Oi \ Os \ m \ (n_1 \text{ lte } n_2) \iff n_1 \leq n_2$$
**[world\_not]**

$$\vdash \forall M \ Oi \ Os \ f \ w. \ w \in \text{Efn } Oi \ Os \ M \ (\text{notf } f) \iff w \notin \text{Efn } Oi \ Os \ M \ f$$
**[world\_or]**

$$\begin{aligned} &\vdash \forall M \ f_1 \ f_2 \ w. \\ &\quad w \in \text{Efn } Oi \ Os \ M \ (f_1 \text{ orf } f_2) \iff \\ &\quad w \in \text{Efn } Oi \ Os \ M \ f_1 \vee w \in \text{Efn } Oi \ Os \ M \ f_2 \end{aligned}$$
**[world\_says]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ P \ f \ w. \\ &\quad w \in \text{Efn } Oi \ Os \ M \ (P \text{ says } f) \iff \\ &\quad \forall v. v \in \text{Jext } (\text{jKS } M) \ P \ w \Rightarrow v \in \text{Efn } Oi \ Os \ M \ f \end{aligned}$$
**[world\_T]**

$$\vdash \forall M \ Oi \ Os \ w. \ w \in \text{Efn } Oi \ Os \ M \text{ TT}$$

## 4 aclDrules Theory

**Built:** 25 February 2018

**Parent Theories:** acldrules

### 4.1 Theorems

#### [Conjunction]

$$\begin{aligned} \vdash \forall M \ Oi \ Os \ f_1 \ f_2. \\ (M, Oi, Os) \text{ sat } f_1 \Rightarrow \\ (M, Oi, Os) \text{ sat } f_2 \Rightarrow \\ (M, Oi, Os) \text{ sat } f_1 \text{ andf } f_2 \end{aligned}$$

#### [Controls]

$$\begin{aligned} \vdash \forall M \ Oi \ Os \ P \ f. \\ (M, Oi, Os) \text{ sat } P \text{ says } f \Rightarrow \\ (M, Oi, Os) \text{ sat } P \text{ controls } f \Rightarrow \\ (M, Oi, Os) \text{ sat } f \end{aligned}$$

#### [Derived\_Controls]

$$\begin{aligned} \vdash \forall M \ Oi \ Os \ P \ Q \ f. \\ (M, Oi, Os) \text{ sat } P \text{ speaks\_for } Q \Rightarrow \\ (M, Oi, Os) \text{ sat } Q \text{ controls } f \Rightarrow \\ (M, Oi, Os) \text{ sat } P \text{ controls } f \end{aligned}$$

#### [Derived\_Speaks\_For]

$$\begin{aligned} \vdash \forall M \ Oi \ Os \ P \ Q \ f. \\ (M, Oi, Os) \text{ sat } P \text{ speaks\_for } Q \Rightarrow \\ (M, Oi, Os) \text{ sat } P \text{ says } f \Rightarrow \\ (M, Oi, Os) \text{ sat } Q \text{ says } f \end{aligned}$$

#### [Disjunction1]

$$\vdash \forall M \ Oi \ Os \ f_1 \ f_2. (M, Oi, Os) \text{ sat } f_1 \Rightarrow (M, Oi, Os) \text{ sat } f_1 \text{ orf } f_2$$

#### [Disjunction2]

$$\vdash \forall M \ Oi \ Os \ f_1 \ f_2. (M, Oi, Os) \text{ sat } f_2 \Rightarrow (M, Oi, Os) \text{ sat } f_1 \text{ orf } f_2$$

#### [Disjunctive\_Syllogism]

$$\begin{aligned} \vdash \forall M \ Oi \ Os \ f_1 \ f_2. \\ (M, Oi, Os) \text{ sat } f_1 \text{ orf } f_2 \Rightarrow \\ (M, Oi, Os) \text{ sat notf } f_1 \Rightarrow \\ (M, Oi, Os) \text{ sat } f_2 \end{aligned}$$

#### [Double\_Negation]

$$\vdash \forall M \ Oi \ Os \ f. (M, Oi, Os) \text{ sat notf (notf } f) \Rightarrow (M, Oi, Os) \text{ sat } f$$



**[eqn\_eqn]**

$$\begin{aligned} &\vdash (M, Oi, Os) \text{ sat } c_1 \text{ eqn } n_1 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } c_2 \text{ eqn } n_2 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } n_1 \text{ eqn } n_2 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } c_1 \text{ eqn } c_2 \end{aligned}$$
**[eqn\_lt]**

$$\begin{aligned} &\vdash (M, Oi, Os) \text{ sat } c_1 \text{ eqn } n_1 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } c_2 \text{ eqn } n_2 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } n_1 \text{ lt } n_2 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } c_1 \text{ lt } c_2 \end{aligned}$$
**[eqn\_lte]**

$$\begin{aligned} &\vdash (M, Oi, Os) \text{ sat } c_1 \text{ eqn } n_1 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } c_2 \text{ eqn } n_2 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } n_1 \text{ lte } n_2 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } c_1 \text{ lte } c_2 \end{aligned}$$
**[Hypothetical\_Syllogism]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ f_1 \ f_2 \ f_3. \\ &\quad (M, Oi, Os) \text{ sat } f_1 \text{ impf } f_2 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } f_2 \text{ impf } f_3 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } f_1 \text{ impf } f_3 \end{aligned}$$
**[il\_domi]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ P \ Q \ l_1 \ l_2. \\ &\quad (M, Oi, Os) \text{ sat il } P \text{ eqi } l_1 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat il } Q \text{ eqi } l_2 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } l_2 \text{ domi } l_1 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat il } Q \text{ domi il } P \end{aligned}$$
**[INTER\_EQ\_UNIV]**

$$\vdash \forall s_1 \ s_2. (s_1 \cap s_2 = \mathcal{U}(:'a)) \iff (s_1 = \mathcal{U}(:'a)) \wedge (s_2 = \mathcal{U}(:'a))$$
**[Modus\_Tollens]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ f_1 \ f_2. \\ &\quad (M, Oi, Os) \text{ sat } f_1 \text{ impf } f_2 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat notf } f_2 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat notf } f_1 \end{aligned}$$
**[Rep\_Controls\_Eq]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ A \ B \ f. \\ &\quad (M, Oi, Os) \text{ sat reps } A \ B \ f \iff \\ &\quad (M, Oi, Os) \text{ sat } A \text{ controls } B \text{ says } f \end{aligned}$$

**[Rep\_Says]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ P \ Q \ f. \\ &\quad (M, Oi, Os) \text{ sat } \text{reps } P \ Q \ f \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } P \text{ quoting } Q \text{ says } f \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } Q \text{ says } f \end{aligned}$$
**[Reps]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ P \ Q \ f. \\ &\quad (M, Oi, Os) \text{ sat } \text{reps } P \ Q \ f \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } P \text{ quoting } Q \text{ says } f \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } Q \text{ controls } f \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } f \end{aligned}$$
**[Says\_Simplification1]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ P \ f_1 \ f_2. \\ &\quad (M, Oi, Os) \text{ sat } P \text{ says } (f_1 \text{ andf } f_2) \Rightarrow (M, Oi, Os) \text{ sat } P \text{ says } f_1 \end{aligned}$$
**[Says\_Simplification2]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ P \ f_1 \ f_2. \\ &\quad (M, Oi, Os) \text{ sat } P \text{ says } (f_1 \text{ andf } f_2) \Rightarrow (M, Oi, Os) \text{ sat } P \text{ says } f_2 \end{aligned}$$
**[Simplification1]**

$$\vdash \forall M \ Oi \ Os \ f_1 \ f_2. (M, Oi, Os) \text{ sat } f_1 \text{ andf } f_2 \Rightarrow (M, Oi, Os) \text{ sat } f_1$$
**[Simplification2]**

$$\vdash \forall M \ Oi \ Os \ f_1 \ f_2. (M, Oi, Os) \text{ sat } f_1 \text{ andf } f_2 \Rightarrow (M, Oi, Os) \text{ sat } f_2$$
**[sl\_doms]**

$$\begin{aligned} &\vdash \forall M \ Oi \ Os \ P \ Q \ l_1 \ l_2. \\ &\quad (M, Oi, Os) \text{ sat } \text{sl } P \text{ eqs } l_1 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } \text{sl } Q \text{ eqs } l_2 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } l_2 \text{ doms } l_1 \Rightarrow \\ &\quad (M, Oi, Os) \text{ sat } \text{sl } Q \text{ doms } \text{sl } P \end{aligned}$$



## Index

### **aclDrules Theory**, 17

- Theorems, 17
  - Conjunction, 17
  - Controls, 17
  - Derived\_Controls, 17
  - Derived\_Speaks\_For, 17
  - Disjunction1, 17
  - Disjunction2, 17
  - Disjunctive\_Syllogism, 17
  - Double\_Negation, 17
  - eqn\_eqn, 18
  - eqn\_lt, 18
  - eqn\_lte, 18
  - Hypothetical\_Syllogism, 18
  - il\_domi, 18
  - INTER\_EQ\_UNIV, 18
  - Modus\_Tollens, 18
  - Rep\_Controls\_Eq, 18
  - Rep\_Says, 19
  - Reps, 19
  - Says\_Simplification1, 19
  - Says\_Simplification2, 19
  - Simplification1, 19
  - Simplification2, 19
  - sl\_doms, 19

### **aclfoundation Theory**, 3

- Datatypes, 3
- Definitions, 3
  - imapKS\_def, 4
  - intpKS\_def, 4
  - jKS\_def, 4
  - O1\_def, 4
  - one\_weakorder\_def, 4
  - po\_TY\_DEF, 4
  - po\_tybij, 4
  - prod\_PO\_def, 4
  - smapKS\_def, 4
  - Subset\_PO\_def, 4
- Theorems, 4
  - abs\_po11, 4

- absPO\_fn\_onto, 4
- antisym\_prod\_antisym, 5
- EQ\_WeakOrder, 5
- KS\_bij, 5
- one\_weakorder\_WO, 5
- onto\_po, 5
- po\_bij, 5
- PO\_repPO, 5
- refl\_prod\_refl, 5
- repPO\_iPO\_partial\_order, 5
- repPO\_O1, 5
- repPO\_prod\_PO, 5
- repPO\_Subset\_PO, 5
- RPROD\_THM, 5
- SUBSET\_WO, 6
- trans\_prod\_trans, 6
- WeakOrder\_Exists, 6
- WO\_prod\_WO, 6
- WO\_repPO, 6

### **aclrules Theory**, 10

- Definitions, 11
  - sat\_def, 11
- Theorems, 11
  - And\_Says, 11
  - And\_Says\_Eq, 11
  - and\_says\_lemma, 11
  - Controls\_Eq, 11
  - DIFF\_UNIV\_SUBSET, 11
  - domi\_antisymmetric, 11
  - domi\_reflexive, 11
  - domi\_transitive, 11
  - doms\_antisymmetric, 11
  - doms\_reflexive, 12
  - doms\_transitive, 12
  - eqf\_and\_impf, 12
  - eqf\_andf1, 12
  - eqf\_andf2, 12
  - eqf\_controls, 12
  - eqf\_eq, 12
  - eqf\_eqf1, 12

- eqf\_eqf2, 12
- eqf\_impf1, 13
- eqf\_impf2, 13
- eqf\_notf, 13
- eqf\_orf1, 13
- eqf\_orf2, 13
- eqf\_reps, 13
- eqf\_sat, 13
- eqf\_says, 13
- eqi\_Eq, 14
- eqs\_Eq, 14
- Idemp\_Speaks\_For, 14
- Image\_cmp, 14
- Image\_SUBSET, 14
- Image\_UNION, 14
- INTER\_EQ\_UNIV, 14
- Modus\_Ponens, 14
- Mono\_speaks\_for, 14
- MP\_Says, 14
- Quoting, 14
- Quoting\_Eq, 15
- reps\_def\_lemma, 15
- Reps\_Eq, 15
- sat\_allworld, 15
- sat\_andf\_eq\_and\_sat, 15
- sat\_TT, 15
- Says, 15
- says\_and\_lemma, 15
- Speaks\_For, 15
- speaks\_for\_SUBSET, 15
- SUBSET\_Image\_SUBSET, 15
- Trans\_Speaks\_For, 16
- UNIV\_DIFF\_SUBSET, 16
- world\_and, 16
- world\_eq, 16
- world\_eqn, 16
- world\_F, 16
- world\_imp, 16
- world\_lt, 16
- world\_lte, 16
- world\_not, 16
- world\_or, 16
- world\_says, 16

- world\_T, 16
- ac semantics Theory**, 6
  - Definitions, 6
    - Efn\_def, 6
    - Jext\_def, 7
    - Lifn\_def, 7
    - Lsfm\_def, 8
  - Theorems, 8
    - andf\_def, 8
    - controls\_def, 8
    - controls\_says, 8
    - domi\_def, 8
    - doms\_def, 8
    - eqf\_def, 8
    - eqf\_impf, 8
    - eqi\_def, 9
    - eqi\_domi, 9
    - eqn\_def, 9
    - eqs\_def, 9
    - eqs\_doms, 9
    - FF\_def, 9
    - impf\_def, 9
    - lt\_def, 9
    - lte\_def, 9
    - meet\_def, 10
    - name\_def, 10
    - notf\_def, 10
    - orf\_def, 10
    - prop\_def, 10
    - quoting\_def, 10
    - reps\_def, 10
    - says\_def, 10
    - speaks\_for\_def, 10
    - TT\_def, 10

## Appendix B

### Secure State Machine & Patrol Base Operations: Pretty-Printed Theories

# Contents

<b>1</b>	<b>OMNITYPE Theory</b>	<b>3</b>
1.1	Datatypes . . . . .	3
1.2	Theorems . . . . .	3
<b>2</b>	<b>ssm11 Theory</b>	<b>4</b>
2.1	Datatypes . . . . .	4
2.2	Definitions . . . . .	4
2.3	Theorems . . . . .	5
<b>3</b>	<b>ssm Theory</b>	<b>11</b>
3.1	Datatypes . . . . .	11
3.2	Definitions . . . . .	12
3.3	Theorems . . . . .	13
<b>4</b>	<b>satList Theory</b>	<b>21</b>
4.1	Definitions . . . . .	21
4.2	Theorems . . . . .	21
<b>5</b>	<b>ssmPB Theory</b>	<b>21</b>
5.1	Definitions . . . . .	21
5.2	Theorems . . . . .	22
<b>6</b>	<b>PBTypeIntegrated Theory</b>	<b>26</b>
6.1	Datatypes . . . . .	26
6.2	Theorems . . . . .	27
<b>7</b>	<b>PBIntegratedDef Theory</b>	<b>28</b>
7.1	Definitions . . . . .	28
7.2	Theorems . . . . .	28
<b>8</b>	<b>ssmConductORP Theory</b>	<b>33</b>
8.1	Definitions . . . . .	33
8.2	Theorems . . . . .	33
<b>9</b>	<b>ConductORPType Theory</b>	<b>38</b>
9.1	Datatypes . . . . .	38
9.2	Theorems . . . . .	39
<b>10</b>	<b>ssmConductPB Theory</b>	<b>39</b>
10.1	Definitions . . . . .	40
10.2	Theorems . . . . .	40

<b>11 ConductPBType Theory</b>	<b>45</b>
11.1 Datatypes . . . . .	45
11.2 Theorems . . . . .	45
<b>12 ssmMoveToORP Theory</b>	<b>46</b>
12.1 Definitions . . . . .	46
12.2 Theorems . . . . .	46
<b>13 MoveToORPType Theory</b>	<b>51</b>
13.1 Datatypes . . . . .	51
13.2 Theorems . . . . .	51
<b>14 ssmMoveToPB Theory</b>	<b>52</b>
14.1 Definitions . . . . .	52
14.2 Theorems . . . . .	52
<b>15 MoveToPBType Theory</b>	<b>56</b>
15.1 Datatypes . . . . .	56
15.2 Theorems . . . . .	56
<b>16 ssmPlanPB Theory</b>	<b>57</b>
16.1 Theorems . . . . .	57
<b>17 PlanPBType Theory</b>	<b>67</b>
17.1 Datatypes . . . . .	67
17.2 Theorems . . . . .	68



# 1 OMNIType Theory

**Built:** 13 May 2018

**Parent Theories:** indexedLists, patternMatches

## 1.1 Datatypes

```
command = ESCc escCommand | SLc 'slCommand

escCommand = returnToBase | changeMission | resupply
             | reactToContact

escOutput = ReturnToBase | ChangeMission | Resupply
           | ReactToContact

escState = RTB | CM | RESUPPLY | RTC

output = ESCo escOutput | SLo 'slOutput

principal = SR 'stateRole

state = ESCs escState | SLs 'slState
```

## 1.2 Theorems

[command\_distinct\_clauses]

$\vdash \forall a' a. \text{ESCc } a \neq \text{SLc } a'$

[command\_one\_one]

$\vdash (\forall a a'. (\text{ESCc } a = \text{ESCc } a') \iff (a = a')) \wedge$   
 $\quad \forall a a'. (\text{SLc } a = \text{SLc } a') \iff (a = a')$

[escCommand\_distinct\_clauses]

$\vdash \text{returnToBase} \neq \text{changeMission} \wedge \text{returnToBase} \neq \text{resupply} \wedge$   
 $\quad \text{returnToBase} \neq \text{reactToContact} \wedge \text{changeMission} \neq \text{resupply} \wedge$   
 $\quad \text{changeMission} \neq \text{reactToContact} \wedge \text{resupply} \neq \text{reactToContact}$

[escOutput\_distinct\_clauses]

$\vdash \text{ReturnToBase} \neq \text{ChangeMission} \wedge \text{ReturnToBase} \neq \text{Resupply} \wedge$   
 $\quad \text{ReturnToBase} \neq \text{ReactToContact} \wedge \text{ChangeMission} \neq \text{Resupply} \wedge$   
 $\quad \text{ChangeMission} \neq \text{ReactToContact} \wedge \text{Resupply} \neq \text{ReactToContact}$

[escState\_distinct\_clauses]

$\vdash \text{RTB} \neq \text{CM} \wedge \text{RTB} \neq \text{RESUPPLY} \wedge \text{RTB} \neq \text{RTC} \wedge \text{CM} \neq \text{RESUPPLY} \wedge$   
 $\quad \text{CM} \neq \text{RTC} \wedge \text{RESUPPLY} \neq \text{RTC}$

[output\_distinct\_clauses]

$\vdash \forall a' a. \text{ESCo } a \neq \text{SLo } a'$

[output\_one\_one]

$\vdash (\forall a a'. (\text{ESCo } a = \text{ESCo } a') \iff (a = a')) \wedge$   
 $\quad \forall a a'. (\text{SLo } a = \text{SLo } a') \iff (a = a')$

[principal\_one\_one]

$\vdash \forall a a'. (\text{SR } a = \text{SR } a') \iff (a = a')$

[state\_distinct\_clauses]

$\vdash \forall a' a. \text{ESCs } a \neq \text{SLs } a'$

[state\_one\_one]

$\vdash (\forall a a'. (\text{ESCs } a = \text{ESCs } a') \iff (a = a')) \wedge$   
 $\quad \forall a a'. (\text{SLs } a = \text{SLs } a') \iff (a = a')$

## 2 ssm11 Theory

**Built:** 13 May 2018

**Parent Theories:** satList

### 2.1 Datatypes

```
configuration =
  CFG (('command order, 'principal, 'd, 'e) Form -> bool)
      ('state -> ('command order, 'principal, 'd, 'e) Form)
      (('command order, 'principal, 'd, 'e) Form list)
      (('command order, 'principal, 'd, 'e) Form list) 'state
      ('output list)

order = SOME 'command | NONE

trType = discard 'command | trap 'command | exec 'command
```

### 2.2 Definitions

[TR\_def]

$\vdash \text{TR} =$   
 $\quad (\lambda a_0 a_1 a_2 a_3.$   
 $\quad \quad \forall TR'.$   
 $\quad \quad (\forall a_0 a_1 a_2 a_3.$   
 $\quad \quad \quad (\exists \text{authenticationTest } P \text{ NS } M \text{ Oi } Os \text{ Out } s$   
 $\quad \quad \quad \quad \text{securityContext stateInterp cmd ins outs.}$   
 $\quad \quad \quad (a_0 = (M, Oi, Os)) \wedge (a_1 = \text{exec cmd}) \wedge$   
 $\quad \quad \quad (a_2 =$

```

CFG authenticationTest stateInterp
  securityContext (P says prop (SOME cmd)::ins) s
  outs) ∧
(a3 =
  CFG authenticationTest stateInterp
    securityContext ins (NS s (exec cmd))
    (Out s (exec cmd)::outs)) ∧
authenticationTest (P says prop (SOME cmd)) ∧
CFGInterpret (M, Oi, Os)
  (CFG authenticationTest stateInterp
    securityContext (P says prop (SOME cmd)::ins)
    s outs)) ∨
(∃ authenticationTest P NS M Oi Os Out s
  securityContext stateInterp cmd ins outs.
  (a0 = (M, Oi, Os)) ∧ (a1 = trap cmd) ∧
  (a2 =
    CFG authenticationTest stateInterp
      securityContext (P says prop (SOME cmd)::ins) s
      outs) ∧
  (a3 =
    CFG authenticationTest stateInterp
      securityContext ins (NS s (trap cmd))
      (Out s (trap cmd)::outs)) ∧
  authenticationTest (P says prop (SOME cmd)) ∧
  CFGInterpret (M, Oi, Os)
    (CFG authenticationTest stateInterp
      securityContext (P says prop (SOME cmd)::ins)
      s outs)) ∨
(∃ authenticationTest NS M Oi Os Out s securityContext
  stateInterp cmd x ins outs.
  (a0 = (M, Oi, Os)) ∧ (a1 = discard cmd) ∧
  (a2 =
    CFG authenticationTest stateInterp
      securityContext (x::ins) s outs) ∧
  (a3 =
    CFG authenticationTest stateInterp
      securityContext ins (NS s (discard cmd))
      (Out s (discard cmd)::outs)) ∧
  ¬authenticationTest x) ⇒
  TR' a0 a1 a2 a3) ⇒
  TR' a0 a1 a2 a3)

```

## 2.3 Theorems

[CFGInterpret\_def]

```

⊢ CFGInterpret (M, Oi, Os)
  (CFG authenticationTest stateInterp securityContext
    (input::ins) state outputStream) ⇔

```

$$(M, Oi, Os) \text{ satList } securityContext \wedge (M, Oi, Os) \text{ sat } input \wedge \\ (M, Oi, Os) \text{ sat } stateInterp \ state$$

[CFGInterpret\_ind]

$$\vdash \forall P. \\ (\forall M \ Oi \ Os \ authenticationTest \ stateInterp \ securityContext \\ input \ ins \ state \ outputStream. \\ P \ (M, Oi, Os) \\ (CFG \ authenticationTest \ stateInterp \ securityContext \\ (input :: ins) \ state \ outputStream)) \wedge \\ (\forall v_{15} \ v_{10} \ v_{11} \ v_{12} \ v_{13} \ v_{14}. \\ P \ v_{15} \ (CFG \ v_{10} \ v_{11} \ v_{12} \ [] \ v_{13} \ v_{14})) \Rightarrow \\ \forall v \ v_1 \ v_2 \ v_3. \ P \ (v, v_1, v_2) \ v_3$$

[configuration\_one\_one]

$$\vdash \forall a_0 \ a_1 \ a_2 \ a_3 \ a_4 \ a_5 \ a'_0 \ a'_1 \ a'_2 \ a'_3 \ a'_4 \ a'_5. \\ (CFG \ a_0 \ a_1 \ a_2 \ a_3 \ a_4 \ a_5 = CFG \ a'_0 \ a'_1 \ a'_2 \ a'_3 \ a'_4 \ a'_5) \iff \\ (a_0 = a'_0) \wedge (a_1 = a'_1) \wedge (a_2 = a'_2) \wedge (a_3 = a'_3) \wedge \\ (a_4 = a'_4) \wedge (a_5 = a'_5)$$

[order\_distinct\_clauses]

$$\vdash \forall a. \text{ SOME } a \neq \text{ NONE}$$

[order\_one\_one]

$$\vdash \forall a \ a'. \ (\text{SOME } a = \text{SOME } a') \iff (a = a')$$

[TR\_cases]

$$\vdash \forall a_0 \ a_1 \ a_2 \ a_3. \\ \text{TR } a_0 \ a_1 \ a_2 \ a_3 \iff \\ (\exists authenticationTest \ P \ NS \ M \ Oi \ Os \ Out \ s \ securityContext \\ stateInterp \ cmd \ ins \ outs. \\ (a_0 = (M, Oi, Os)) \wedge (a_1 = \text{exec } cmd) \wedge \\ (a_2 = \\ CFG \ authenticationTest \ stateInterp \ securityContext \\ (P \ \text{says prop } (\text{SOME } cmd) :: ins) \ s \ outs) \wedge \\ (a_3 = \\ CFG \ authenticationTest \ stateInterp \ securityContext \ ins \\ (NS \ s \ (\text{exec } cmd)) \ (Out \ s \ (\text{exec } cmd) :: outs)) \wedge \\ authenticationTest \ (P \ \text{says prop } (\text{SOME } cmd)) \wedge \\ CFGInterpret \ (M, Oi, Os) \\ (CFG \ authenticationTest \ stateInterp \ securityContext \\ (P \ \text{says prop } (\text{SOME } cmd) :: ins) \ s \ outs)) \vee \\ (\exists authenticationTest \ P \ NS \ M \ Oi \ Os \ Out \ s \ securityContext \\ stateInterp \ cmd \ ins \ outs. \\ (a_0 = (M, Oi, Os)) \wedge (a_1 = \text{trap } cmd) \wedge \\ (a_2 = \\ CFG \ authenticationTest \ stateInterp \ securityContext \\ (P \ \text{says prop } (\text{SOME } cmd) :: ins) \ s \ outs) \wedge$$

$$\begin{aligned}
& (a_3 = \\
& \quad \text{CFG authenticationTest stateInterp securityContext ins} \\
& \quad \quad (\text{NS } s \text{ (trap cmd)}) (\text{Out } s \text{ (trap cmd)::outs})) \wedge \\
& \quad \text{authenticationTest } (P \text{ says prop (SOME cmd)}) \wedge \\
& \quad \text{CFGInterpret } (M, Oi, Os) \\
& \quad \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad \quad (P \text{ says prop (SOME cmd)::ins) } s \text{ outs})) \vee \\
& \exists \text{ authenticationTest NS } M \text{ Oi Os Out } s \text{ securityContext} \\
& \quad \text{stateInterp cmd } x \text{ ins outs.} \\
& (a_0 = (M, Oi, Os)) \wedge (a_1 = \text{discard cmd}) \wedge \\
& (a_2 = \\
& \quad \text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad (x::ins) s \text{ outs}) \wedge \\
& (a_3 = \\
& \quad \text{CFG authenticationTest stateInterp securityContext ins} \\
& \quad \quad (\text{NS } s \text{ (discard cmd)}) (\text{Out } s \text{ (discard cmd)::outs})) \wedge \\
& \neg \text{authenticationTest } x
\end{aligned}$$

[TR\_discard\_cmd\_rule]

$$\begin{aligned}
& \vdash \text{TR } (M, Oi, Os) \text{ (discard cmd)} \\
& \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad (x::ins) s \text{ outs}) \\
& \quad (\text{CFG authenticationTest stateInterp securityContext ins} \\
& \quad \quad \quad (\text{NS } s \text{ (discard cmd)}) (\text{Out } s \text{ (discard cmd)::outs})) \iff \\
& \neg \text{authenticationTest } x
\end{aligned}$$

[TR\_EQ\_rules\_thm]

$$\begin{aligned}
& \vdash (\text{TR } (M, Oi, Os) \text{ (exec cmd)}) \\
& \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad (P \text{ says prop (SOME cmd)::ins) } s \text{ outs}) \\
& \quad (\text{CFG authenticationTest stateInterp securityContext ins} \\
& \quad \quad \quad (\text{NS } s \text{ (exec cmd)}) (\text{Out } s \text{ (exec cmd)::outs})) \iff \\
& \text{authenticationTest } (P \text{ says prop (SOME cmd)}) \wedge \\
& \text{CFGInterpret } (M, Oi, Os) \\
& \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad (P \text{ says prop (SOME cmd)::ins) } s \text{ outs})) \wedge \\
& (\text{TR } (M, Oi, Os) \text{ (trap cmd)}) \\
& \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad (P \text{ says prop (SOME cmd)::ins) } s \text{ outs}) \\
& \quad (\text{CFG authenticationTest stateInterp securityContext ins} \\
& \quad \quad \quad (\text{NS } s \text{ (trap cmd)}) (\text{Out } s \text{ (trap cmd)::outs})) \iff \\
& \text{authenticationTest } (P \text{ says prop (SOME cmd)}) \wedge \\
& \text{CFGInterpret } (M, Oi, Os) \\
& \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad (P \text{ says prop (SOME cmd)::ins) } s \text{ outs})) \wedge \\
& (\text{TR } (M, Oi, Os) \text{ (discard cmd)}) \\
& \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad (x::ins) s \text{ outs}) \\
& \quad (\text{CFG authenticationTest stateInterp securityContext ins}
\end{aligned}$$

$$(NS\ s\ (\text{discard}\ cmd))\ (Out\ s\ (\text{discard}\ cmd)::outs)) \iff \neg authenticationTest\ x)$$

[TR\_exec\_cmd\_rule]

$$\begin{aligned} &\vdash \forall authenticationTest\ securityContext\ stateInterp\ P\ cmd\ ins\ s\ outs. \\ &\quad (\forall M\ Oi\ Os. \\ &\quad \quad CFGInterpret\ (M, Oi, Os) \\ &\quad \quad \quad (CFG\ authenticationTest\ stateInterp\ securityContext \\ &\quad \quad \quad \quad (P\ \text{says}\ \text{prop}\ (SOME\ cmd)::ins)\ s\ outs) \Rightarrow \\ &\quad \quad \quad (M, Oi, Os)\ \text{sat}\ \text{prop}\ (SOME\ cmd)) \Rightarrow \\ &\quad \forall NS\ Out\ M\ Oi\ Os. \\ &\quad TR\ (M, Oi, Os)\ (\text{exec}\ cmd) \\ &\quad \quad (CFG\ authenticationTest\ stateInterp\ securityContext \\ &\quad \quad \quad (P\ \text{says}\ \text{prop}\ (SOME\ cmd)::ins)\ s\ outs) \\ &\quad \quad (CFG\ authenticationTest\ stateInterp\ securityContext\ ins \\ &\quad \quad \quad (NS\ s\ (\text{exec}\ cmd))\ (Out\ s\ (\text{exec}\ cmd)::outs)) \iff \\ &\quad authenticationTest\ (P\ \text{says}\ \text{prop}\ (SOME\ cmd)) \wedge \\ &\quad CFGInterpret\ (M, Oi, Os) \\ &\quad \quad (CFG\ authenticationTest\ stateInterp\ securityContext \\ &\quad \quad \quad (P\ \text{says}\ \text{prop}\ (SOME\ cmd)::ins)\ s\ outs) \wedge \\ &\quad (M, Oi, Os)\ \text{sat}\ \text{prop}\ (SOME\ cmd)) \end{aligned}$$

[TR\_ind]

$$\begin{aligned} &\vdash \forall TR'. \\ &\quad (\forall authenticationTest\ P\ NS\ M\ Oi\ Os\ Out\ s\ securityContext \\ &\quad \quad stateInterp\ cmd\ ins\ outs. \\ &\quad \quad authenticationTest\ (P\ \text{says}\ \text{prop}\ (SOME\ cmd)) \wedge \\ &\quad \quad CFGInterpret\ (M, Oi, Os) \\ &\quad \quad \quad (CFG\ authenticationTest\ stateInterp\ securityContext \\ &\quad \quad \quad \quad (P\ \text{says}\ \text{prop}\ (SOME\ cmd)::ins)\ s\ outs) \Rightarrow \\ &\quad \quad TR'\ (M, Oi, Os)\ (\text{exec}\ cmd) \\ &\quad \quad \quad (CFG\ authenticationTest\ stateInterp\ securityContext \\ &\quad \quad \quad \quad (P\ \text{says}\ \text{prop}\ (SOME\ cmd)::ins)\ s\ outs) \\ &\quad \quad \quad (CFG\ authenticationTest\ stateInterp\ securityContext \\ &\quad \quad \quad \quad \quad ins\ (NS\ s\ (\text{exec}\ cmd))\ (Out\ s\ (\text{exec}\ cmd)::outs))) \wedge \\ &\quad (\forall authenticationTest\ P\ NS\ M\ Oi\ Os\ Out\ s\ securityContext \\ &\quad \quad stateInterp\ cmd\ ins\ outs. \\ &\quad \quad authenticationTest\ (P\ \text{says}\ \text{prop}\ (SOME\ cmd)) \wedge \\ &\quad \quad CFGInterpret\ (M, Oi, Os) \\ &\quad \quad \quad (CFG\ authenticationTest\ stateInterp\ securityContext \\ &\quad \quad \quad \quad (P\ \text{says}\ \text{prop}\ (SOME\ cmd)::ins)\ s\ outs) \Rightarrow \\ &\quad \quad TR'\ (M, Oi, Os)\ (\text{trap}\ cmd) \\ &\quad \quad \quad (CFG\ authenticationTest\ stateInterp\ securityContext \\ &\quad \quad \quad \quad (P\ \text{says}\ \text{prop}\ (SOME\ cmd)::ins)\ s\ outs) \\ &\quad \quad \quad (CFG\ authenticationTest\ stateInterp\ securityContext \\ &\quad \quad \quad \quad \quad ins\ (NS\ s\ (\text{trap}\ cmd))\ (Out\ s\ (\text{trap}\ cmd)::outs))) \wedge \\ &\quad (\forall authenticationTest\ NS\ M\ Oi\ Os\ Out\ s\ securityContext \\ &\quad \quad stateInterp\ cmd\ x\ ins\ outs. \end{aligned}$$

$$\begin{aligned}
& \neg \text{authenticationTest } x \Rightarrow \\
& \text{TR}' (M, Oi, Os) (\text{discard } cmd) \\
& \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad (x :: ins) s outs) \\
& \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad ins (NS s (\text{discard } cmd))) \\
& \quad (\text{Out } s (\text{discard } cmd) :: outs))) \Rightarrow \\
& \forall a_0 a_1 a_2 a_3. \text{TR } a_0 a_1 a_2 a_3 \Rightarrow \text{TR}' a_0 a_1 a_2 a_3
\end{aligned}$$

## [TR\_rules]

$$\begin{aligned}
& \vdash (\forall \text{authenticationTest } P \text{ NS } M \text{ Oi } Os \text{ Out } s \text{ securityContext} \\
& \quad \text{stateInterp } cmd \text{ ins } outs. \\
& \quad \text{authenticationTest } (P \text{ says prop (SOME } cmd)) \wedge \\
& \quad \text{CFGInterpret } (M, Oi, Os) \\
& \quad \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad \quad (P \text{ says prop (SOME } cmd) :: ins) s outs) \Rightarrow \\
& \quad \text{TR } (M, Oi, Os) (\text{exec } cmd) \\
& \quad \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad \quad (P \text{ says prop (SOME } cmd) :: ins) s outs) \\
& \quad \quad (\text{CFG authenticationTest stateInterp securityContext ins} \\
& \quad \quad \quad (NS s (\text{exec } cmd)) (\text{Out } s (\text{exec } cmd) :: outs))) \wedge \\
& (\forall \text{authenticationTest } P \text{ NS } M \text{ Oi } Os \text{ Out } s \text{ securityContext} \\
& \quad \text{stateInterp } cmd \text{ ins } outs. \\
& \quad \text{authenticationTest } (P \text{ says prop (SOME } cmd)) \wedge \\
& \quad \text{CFGInterpret } (M, Oi, Os) \\
& \quad \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad \quad (P \text{ says prop (SOME } cmd) :: ins) s outs) \Rightarrow \\
& \quad \text{TR } (M, Oi, Os) (\text{trap } cmd) \\
& \quad \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad \quad (P \text{ says prop (SOME } cmd) :: ins) s outs) \\
& \quad \quad (\text{CFG authenticationTest stateInterp securityContext ins} \\
& \quad \quad \quad (NS s (\text{trap } cmd)) (\text{Out } s (\text{trap } cmd) :: outs))) \wedge \\
& \forall \text{authenticationTest } NS \text{ M } Oi \text{ Os } Out \text{ s securityContext} \\
& \quad \text{stateInterp } cmd \text{ x ins } outs. \\
& \neg \text{authenticationTest } x \Rightarrow \\
& \text{TR } (M, Oi, Os) (\text{discard } cmd) \\
& \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad (x :: ins) s outs) \\
& \quad (\text{CFG authenticationTest stateInterp securityContext ins} \\
& \quad \quad (NS s (\text{discard } cmd)) (\text{Out } s (\text{discard } cmd) :: outs)))
\end{aligned}$$

## [TR\_strongind]

$$\begin{aligned}
& \vdash \forall \text{TR}'. \\
& \quad (\forall \text{authenticationTest } P \text{ NS } M \text{ Oi } Os \text{ Out } s \text{ securityContext} \\
& \quad \quad \text{stateInterp } cmd \text{ ins } outs. \\
& \quad \quad \text{authenticationTest } (P \text{ says prop (SOME } cmd)) \wedge \\
& \quad \quad \text{CFGInterpret } (M, Oi, Os) \\
& \quad \quad \quad (\text{CFG authenticationTest stateInterp securityContext} \\
& \quad \quad \quad \quad (P \text{ says prop (SOME } cmd) :: ins) s outs) \Rightarrow
\end{aligned}$$

$$\begin{aligned}
& TR' (M, Oi, Os) (\text{exec } cmd) \\
& \quad (CFG \text{ authenticationTest stateInterp securityContext} \\
& \quad \quad (P \text{ says prop (SOME cmd)::ins) } s \text{ outs}) \\
& \quad (CFG \text{ authenticationTest stateInterp securityContext} \\
& \quad \quad \text{ins (NS s (exec cmd)) (Out s (exec cmd)::outs))) \wedge \\
& (\forall \text{ authenticationTest } P \text{ NS } M \text{ Oi } Os \text{ Out } s \text{ securityContext} \\
& \quad \text{stateInterp cmd ins outs.} \\
& \text{authenticationTest (P says prop (SOME cmd))} \wedge \\
& \text{CFGInterpret (M, Oi, Os)} \\
& \quad (CFG \text{ authenticationTest stateInterp securityContext} \\
& \quad \quad (P \text{ says prop (SOME cmd)::ins) } s \text{ outs}) \Rightarrow \\
& TR' (M, Oi, Os) (\text{trap } cmd) \\
& \quad (CFG \text{ authenticationTest stateInterp securityContext} \\
& \quad \quad (P \text{ says prop (SOME cmd)::ins) } s \text{ outs}) \\
& \quad (CFG \text{ authenticationTest stateInterp securityContext} \\
& \quad \quad \text{ins (NS s (trap cmd)) (Out s (trap cmd)::outs))) \wedge \\
& (\forall \text{ authenticationTest NS } M \text{ Oi } Os \text{ Out } s \text{ securityContext} \\
& \quad \text{stateInterp cmd } x \text{ ins outs.} \\
& \neg \text{authenticationTest } x \Rightarrow \\
& TR' (M, Oi, Os) (\text{discard } cmd) \\
& \quad (CFG \text{ authenticationTest stateInterp securityContext} \\
& \quad \quad (x::ins) s \text{ outs}) \\
& \quad (CFG \text{ authenticationTest stateInterp securityContext} \\
& \quad \quad \text{ins (NS s (discard cmd))} \\
& \quad \quad \quad (\text{Out s (discard cmd)::outs}))) \Rightarrow \\
& \forall a_0 \ a_1 \ a_2 \ a_3. \text{ TR } a_0 \ a_1 \ a_2 \ a_3 \Rightarrow TR' a_0 \ a_1 \ a_2 \ a_3
\end{aligned}$$

[TR\_trap\_cmd\_rule]

$$\begin{aligned}
& \vdash \forall \text{ authenticationTest stateInterp securityContext } P \text{ cmd ins } s \\
& \quad \text{outs.} \\
& (\forall M \text{ Oi } Os. \\
& \quad \text{CFGInterpret (M, Oi, Os)} \\
& \quad \quad (CFG \text{ authenticationTest stateInterp securityContext} \\
& \quad \quad \quad (P \text{ says prop (SOME cmd)::ins) } s \text{ outs}) \Rightarrow \\
& \quad \quad (M, Oi, Os) \text{ sat prop NONE}) \Rightarrow \\
& \forall NS \text{ Out } M \text{ Oi } Os. \\
& \text{TR (M, Oi, Os) (trap cmd)} \\
& \quad (CFG \text{ authenticationTest stateInterp securityContext} \\
& \quad \quad (P \text{ says prop (SOME cmd)::ins) } s \text{ outs}) \\
& \quad (CFG \text{ authenticationTest stateInterp securityContext ins} \\
& \quad \quad \quad (\text{NS s (trap cmd)) (Out s (trap cmd)::outs})) \iff \\
& \text{authenticationTest (P says prop (SOME cmd))} \wedge \\
& \text{CFGInterpret (M, Oi, Os)} \\
& \quad (CFG \text{ authenticationTest stateInterp securityContext} \\
& \quad \quad (P \text{ says prop (SOME cmd)::ins) } s \text{ outs}) \wedge \\
& (M, Oi, Os) \text{ sat prop NONE}
\end{aligned}$$

[TRrule0]

$$\begin{aligned}
& \vdash \text{TR (M, Oi, Os) (exec cmd)} \\
& \quad (CFG \text{ authenticationTest stateInterp securityContext}
\end{aligned}$$



---

```

(P says prop (SOME cmd)::ins) s outs)
(CFG authenticationTest stateInterp securityContext ins
 (NS s (exec cmd)) (Out s (exec cmd)::outs))  $\iff$ 
authenticationTest (P says prop (SOME cmd))  $\wedge$ 
CFGInterpret (M, Oi, Os)
 (CFG authenticationTest stateInterp securityContext
  (P says prop (SOME cmd)::ins) s outs)

```

[TRrule1]

```

 $\vdash$  TR (M, Oi, Os) (trap cmd)
  (CFG authenticationTest stateInterp securityContext
   (P says prop (SOME cmd)::ins) s outs)
  (CFG authenticationTest stateInterp securityContext ins
   (NS s (trap cmd)) (Out s (trap cmd)::outs))  $\iff$ 
authenticationTest (P says prop (SOME cmd))  $\wedge$ 
CFGInterpret (M, Oi, Os)
  (CFG authenticationTest stateInterp securityContext
   (P says prop (SOME cmd)::ins) s outs)

```

[trType\_distinct\_clauses]

```

 $\vdash (\forall a' a. \text{discard } a \neq \text{trap } a') \wedge (\forall a' a. \text{discard } a \neq \text{exec } a') \wedge$ 
 $\forall a' a. \text{trap } a \neq \text{exec } a'$ 

```

[trType\_one\_one]

```

 $\vdash (\forall a a'. (\text{discard } a = \text{discard } a') \iff (a = a')) \wedge$ 
 $(\forall a a'. (\text{trap } a = \text{trap } a') \iff (a = a')) \wedge$ 
 $\forall a a'. (\text{exec } a = \text{exec } a') \iff (a = a')$ 

```

### 3 ssm Theory

**Built:** 13 May 2018

**Parent Theories:** satList

#### 3.1 Datatypes

```

configuration =
  CFG (('command option, 'principal, 'd, 'e) Form -> bool)
    ('state ->
      ('command option, 'principal, 'd, 'e) Form list ->
        ('command option, 'principal, 'd, 'e) Form list)
      (('command option, 'principal, 'd, 'e) Form list ->
        ('command option, 'principal, 'd, 'e) Form list)
      (('command option, 'principal, 'd, 'e) Form list list)
      'state ('output list)

trType = discard 'cmdlist | trap 'cmdlist | exec 'cmdlist

```

### 3.2 Definitions

[authenticationTest\_def]

$$\vdash \forall \text{elementTest } x. \\ \text{authenticationTest } \text{elementTest } x \iff \\ \text{FOLDR } (\lambda p \ q. \ p \wedge \ q) \ \text{T} \ (\text{MAP } \text{elementTest } x)$$

[commandList\_def]

$$\vdash \forall x. \text{commandList } x = \text{MAP } \text{extractCommand } x$$

[inputList\_def]

$$\vdash \forall xs. \text{inputList } xs = \text{MAP } \text{extractInput } xs$$

[propCommandList\_def]

$$\vdash \forall x. \text{propCommandList } x = \text{MAP } \text{extractPropCommand } x$$

[TR\_def]

$$\vdash \text{TR} = \\ (\lambda a_0 \ a_1 \ a_2 \ a_3. \\ \forall TR'. \\ (\forall a_0 \ a_1 \ a_2 \ a_3. \\ (\exists \text{elementTest } NS \ M \ Oi \ Os \ Out \ s \ \text{context } \text{stateInterp } x \\ \text{ins } \text{outs}. \\ (a_0 = (M, Oi, Os)) \wedge (a_1 = \text{exec } (\text{inputList } x)) \wedge \\ (a_2 = \\ \text{CFG } \text{elementTest } \text{stateInterp } \text{context } (x::\text{ins}) \ s \\ \text{outs}) \wedge \\ (a_3 = \\ \text{CFG } \text{elementTest } \text{stateInterp } \text{context } \text{ins} \\ (NS \ s \ (\text{exec } (\text{inputList } x))) \\ (Out \ s \ (\text{exec } (\text{inputList } x)::\text{outs})) \wedge \\ \text{authenticationTest } \text{elementTest } x \wedge \\ \text{CFGInterpret } (M, Oi, Os) \\ (\text{CFG } \text{elementTest } \text{stateInterp } \text{context } (x::\text{ins}) \ s \\ \text{outs})) \vee \\ (\exists \text{elementTest } NS \ M \ Oi \ Os \ Out \ s \ \text{context } \text{stateInterp } x \\ \text{ins } \text{outs}. \\ (a_0 = (M, Oi, Os)) \wedge (a_1 = \text{trap } (\text{inputList } x)) \wedge \\ (a_2 = \\ \text{CFG } \text{elementTest } \text{stateInterp } \text{context } (x::\text{ins}) \ s \\ \text{outs}) \wedge \\ (a_3 = \\ \text{CFG } \text{elementTest } \text{stateInterp } \text{context } \text{ins} \\ (NS \ s \ (\text{trap } (\text{inputList } x))) \\ (Out \ s \ (\text{trap } (\text{inputList } x)::\text{outs})) \wedge \\ \text{authenticationTest } \text{elementTest } x \wedge \\ \text{CFGInterpret } (M, Oi, Os) \\ (\text{CFG } \text{elementTest } \text{stateInterp } \text{context } (x::\text{ins}) \ s$$

$$\begin{aligned}
& \text{outs})) \vee \\
& (\exists \text{elementTest } NS \ M \ Oi \ Os \ Out \ s \ \text{context } stateInterp \ x \\
& \quad \text{ins } outs. \\
& \quad (a_0 = (M, Oi, Os)) \wedge (a_1 = \text{discard } (\text{inputList } x)) \wedge \\
& \quad (a_2 = \\
& \quad \quad \text{CFG } \text{elementTest } stateInterp \ \text{context } (x::ins) \ s \\
& \quad \quad \text{outs}) \wedge \\
& \quad (a_3 = \\
& \quad \quad \text{CFG } \text{elementTest } stateInterp \ \text{context } ins \\
& \quad \quad (NS \ s \ (\text{discard } (\text{inputList } x))) \\
& \quad \quad (Out \ s \ (\text{discard } (\text{inputList } x))::outs)) \wedge \\
& \quad \neg \text{authenticationTest } \text{elementTest } x) \Rightarrow \\
& TR' \ a_0 \ a_1 \ a_2 \ a_3) \Rightarrow \\
& TR' \ a_0 \ a_1 \ a_2 \ a_3)
\end{aligned}$$

### 3.3 Theorems

[CFGInterpret\_def]

$$\begin{aligned}
& \vdash \text{CFGInterpret } (M, Oi, Os) \\
& \quad (\text{CFG } \text{elementTest } stateInterp \ \text{context } (x::ins) \ state \\
& \quad \quad \text{outStream}) \iff \\
& \quad (M, Oi, Os) \text{ satList } \text{context } x \wedge (M, Oi, Os) \text{ satList } x \wedge \\
& \quad (M, Oi, Os) \text{ satList } stateInterp \ state \ x
\end{aligned}$$

[CFGInterpret\_ind]

$$\begin{aligned}
& \vdash \forall P. \\
& \quad (\forall M \ Oi \ Os \ \text{elementTest } stateInterp \ \text{context } x \ \text{ins } state \\
& \quad \quad \text{outStream}. \\
& \quad \quad P \ (M, Oi, Os) \\
& \quad \quad (\text{CFG } \text{elementTest } stateInterp \ \text{context } (x::ins) \ state \\
& \quad \quad \quad \text{outStream})) \wedge \\
& \quad (\forall v_{15} \ v_{10} \ v_{11} \ v_{12} \ v_{13} \ v_{14}. \\
& \quad \quad P \ v_{15} \ (\text{CFG } v_{10} \ v_{11} \ v_{12} \ [] \ v_{13} \ v_{14})) \Rightarrow \\
& \quad \forall v \ v_1 \ v_2 \ v_3. \ P \ (v, v_1, v_2) \ v_3
\end{aligned}$$

[configuration\_one\_one]

$$\begin{aligned}
& \vdash \forall a_0 \ a_1 \ a_2 \ a_3 \ a_4 \ a_5 \ a'_0 \ a'_1 \ a'_2 \ a'_3 \ a'_4 \ a'_5. \\
& \quad (\text{CFG } a_0 \ a_1 \ a_2 \ a_3 \ a_4 \ a_5 = \text{CFG } a'_0 \ a'_1 \ a'_2 \ a'_3 \ a'_4 \ a'_5) \iff \\
& \quad (a_0 = a'_0) \wedge (a_1 = a'_1) \wedge (a_2 = a'_2) \wedge (a_3 = a'_3) \wedge \\
& \quad (a_4 = a'_4) \wedge (a_5 = a'_5)
\end{aligned}$$

[extractCommand\_def]

$$\vdash \text{extractCommand } (P \ \text{says prop } (\text{SOME } cmd)) = cmd$$

[extractCommand\_ind]

$$\begin{aligned}
& \vdash \forall P'. \\
& \quad (\forall P \ cmd. \ P' \ (P \ \text{says prop } (\text{SOME } cmd))) \wedge P' \ \text{TT} \wedge P' \ \text{FF} \wedge \\
& \quad (\forall v_1. \ P' \ (\text{prop } v_1)) \wedge (\forall v_3. \ P' \ (\text{notf } v_3)) \wedge
\end{aligned}$$

$$\begin{aligned}
& (\forall v_6 v_7. P' (v_6 \text{ andf } v_7)) \wedge (\forall v_{10} v_{11}. P' (v_{10} \text{ orf } v_{11})) \wedge \\
& (\forall v_{14} v_{15}. P' (v_{14} \text{ impf } v_{15})) \wedge \\
& (\forall v_{18} v_{19}. P' (v_{18} \text{ eqf } v_{19})) \wedge (\forall v_{129}. P' (v_{129} \text{ says TT})) \wedge \\
& (\forall v_{130}. P' (v_{130} \text{ says FF})) \wedge \\
& (\forall v_{132}. P' (v_{132} \text{ says prop NONE})) \wedge \\
& (\forall v_{133} v_{66}. P' (v_{133} \text{ says notf } v_{66})) \wedge \\
& (\forall v_{134} v_{69} v_{70}. P' (v_{134} \text{ says } (v_{69} \text{ andf } v_{70}))) \wedge \\
& (\forall v_{135} v_{73} v_{74}. P' (v_{135} \text{ says } (v_{73} \text{ orf } v_{74}))) \wedge \\
& (\forall v_{136} v_{77} v_{78}. P' (v_{136} \text{ says } (v_{77} \text{ impf } v_{78}))) \wedge \\
& (\forall v_{137} v_{81} v_{82}. P' (v_{137} \text{ says } (v_{81} \text{ eqf } v_{82}))) \wedge \\
& (\forall v_{138} v_{85} v_{86}. P' (v_{138} \text{ says } v_{85} \text{ says } v_{86})) \wedge \\
& (\forall v_{139} v_{89} v_{90}. P' (v_{139} \text{ says } v_{89} \text{ speaks\_for } v_{90})) \wedge \\
& (\forall v_{140} v_{93} v_{94}. P' (v_{140} \text{ says } v_{93} \text{ controls } v_{94})) \wedge \\
& (\forall v_{141} v_{98} v_{99} v_{100}. P' (v_{141} \text{ says reps } v_{98} v_{99} v_{100})) \wedge \\
& (\forall v_{142} v_{103} v_{104}. P' (v_{142} \text{ says } v_{103} \text{ domi } v_{104})) \wedge \\
& (\forall v_{143} v_{107} v_{108}. P' (v_{143} \text{ says } v_{107} \text{ eqi } v_{108})) \wedge \\
& (\forall v_{144} v_{111} v_{112}. P' (v_{144} \text{ says } v_{111} \text{ doms } v_{112})) \wedge \\
& (\forall v_{145} v_{115} v_{116}. P' (v_{145} \text{ says } v_{115} \text{ eqs } v_{116})) \wedge \\
& (\forall v_{146} v_{119} v_{120}. P' (v_{146} \text{ says } v_{119} \text{ eqn } v_{120})) \wedge \\
& (\forall v_{147} v_{123} v_{124}. P' (v_{147} \text{ says } v_{123} \text{ lte } v_{124})) \wedge \\
& (\forall v_{148} v_{127} v_{128}. P' (v_{148} \text{ says } v_{127} \text{ lt } v_{128})) \wedge \\
& (\forall v_{24} v_{25}. P' (v_{24} \text{ speaks\_for } v_{25})) \wedge \\
& (\forall v_{28} v_{29}. P' (v_{28} \text{ controls } v_{29})) \wedge \\
& (\forall v_{33} v_{34} v_{35}. P' (\text{reps } v_{33} v_{34} v_{35})) \wedge \\
& (\forall v_{38} v_{39}. P' (v_{38} \text{ domi } v_{39})) \wedge \\
& (\forall v_{42} v_{43}. P' (v_{42} \text{ eqi } v_{43})) \wedge \\
& (\forall v_{46} v_{47}. P' (v_{46} \text{ doms } v_{47})) \wedge \\
& (\forall v_{50} v_{51}. P' (v_{50} \text{ eqs } v_{51})) \wedge \\
& (\forall v_{54} v_{55}. P' (v_{54} \text{ eqn } v_{55})) \wedge \\
& (\forall v_{58} v_{59}. P' (v_{58} \text{ lte } v_{59})) \wedge \\
& (\forall v_{62} v_{63}. P' (v_{62} \text{ lt } v_{63})) \Rightarrow \\
& \forall v. P' v
\end{aligned}$$

[extractInput\_def]

$\vdash \text{extractInput } (P \text{ says prop } x) = x$

[extractInput\_ind]

$\vdash \forall P'.$

$$\begin{aligned}
& (\forall P x. P' (P \text{ says prop } x)) \wedge P' \text{ TT} \wedge P' \text{ FF} \wedge \\
& (\forall v_1. P' (\text{prop } v_1)) \wedge (\forall v_3. P' (\text{notf } v_3)) \wedge \\
& (\forall v_6 v_7. P' (v_6 \text{ andf } v_7)) \wedge (\forall v_{10} v_{11}. P' (v_{10} \text{ orf } v_{11})) \wedge \\
& (\forall v_{14} v_{15}. P' (v_{14} \text{ impf } v_{15})) \wedge \\
& (\forall v_{18} v_{19}. P' (v_{18} \text{ eqf } v_{19})) \wedge (\forall v_{129}. P' (v_{129} \text{ says TT})) \wedge \\
& (\forall v_{130}. P' (v_{130} \text{ says FF})) \wedge \\
& (\forall v_{131} v_{66}. P' (v_{131} \text{ says notf } v_{66})) \wedge \\
& (\forall v_{132} v_{69} v_{70}. P' (v_{132} \text{ says } (v_{69} \text{ andf } v_{70}))) \wedge \\
& (\forall v_{133} v_{73} v_{74}. P' (v_{133} \text{ says } (v_{73} \text{ orf } v_{74}))) \wedge \\
& (\forall v_{134} v_{77} v_{78}. P' (v_{134} \text{ says } (v_{77} \text{ impf } v_{78}))) \wedge \\
& (\forall v_{135} v_{81} v_{82}. P' (v_{135} \text{ says } (v_{81} \text{ eqf } v_{82}))) \wedge
\end{aligned}$$

$$\begin{aligned}
& (\forall v136 \ v85 \ v86. \ P' \ (v136 \ \text{says} \ v85 \ \text{says} \ v86)) \wedge \\
& (\forall v137 \ v89 \ v90. \ P' \ (v137 \ \text{says} \ v89 \ \text{speaks\_for} \ v90)) \wedge \\
& (\forall v138 \ v93 \ v94. \ P' \ (v138 \ \text{says} \ v93 \ \text{controls} \ v94)) \wedge \\
& (\forall v139 \ v98 \ v99 \ v100. \ P' \ (v139 \ \text{says} \ \text{reps} \ v98 \ v99 \ v100)) \wedge \\
& (\forall v140 \ v103 \ v104. \ P' \ (v140 \ \text{says} \ v103 \ \text{domi} \ v104)) \wedge \\
& (\forall v141 \ v107 \ v108. \ P' \ (v141 \ \text{says} \ v107 \ \text{eqi} \ v108)) \wedge \\
& (\forall v142 \ v111 \ v112. \ P' \ (v142 \ \text{says} \ v111 \ \text{doms} \ v112)) \wedge \\
& (\forall v143 \ v115 \ v116. \ P' \ (v143 \ \text{says} \ v115 \ \text{eqs} \ v116)) \wedge \\
& (\forall v144 \ v119 \ v120. \ P' \ (v144 \ \text{says} \ v119 \ \text{eqn} \ v120)) \wedge \\
& (\forall v145 \ v123 \ v124. \ P' \ (v145 \ \text{says} \ v123 \ \text{lte} \ v124)) \wedge \\
& (\forall v146 \ v127 \ v128. \ P' \ (v146 \ \text{says} \ v127 \ \text{lt} \ v128)) \wedge \\
& (\forall v24 \ v25. \ P' \ (v24 \ \text{speaks\_for} \ v25)) \wedge \\
& (\forall v28 \ v29. \ P' \ (v28 \ \text{controls} \ v29)) \wedge \\
& (\forall v33 \ v34 \ v35. \ P' \ (\text{reps} \ v33 \ v34 \ v35)) \wedge \\
& (\forall v38 \ v39. \ P' \ (v38 \ \text{domi} \ v39)) \wedge \\
& (\forall v42 \ v43. \ P' \ (v42 \ \text{eqi} \ v43)) \wedge \\
& (\forall v46 \ v47. \ P' \ (v46 \ \text{doms} \ v47)) \wedge \\
& (\forall v50 \ v51. \ P' \ (v50 \ \text{eqs} \ v51)) \wedge \\
& (\forall v54 \ v55. \ P' \ (v54 \ \text{eqn} \ v55)) \wedge \\
& (\forall v58 \ v59. \ P' \ (v58 \ \text{lte} \ v59)) \wedge \\
& (\forall v62 \ v63. \ P' \ (v62 \ \text{lt} \ v63)) \Rightarrow \\
& \forall v. \ P' \ v
\end{aligned}$$

[extractPropCommand\_def]

$$\vdash \text{extractPropCommand} \ (P \ \text{says} \ \text{prop} \ (\text{SOME} \ \text{cmd})) = \text{prop} \ (\text{SOME} \ \text{cmd})$$

[extractPropCommand\_ind]

$$\begin{aligned}
& \vdash \forall P'. \\
& \quad (\forall P \ \text{cmd}. \ P' \ (P \ \text{says} \ \text{prop} \ (\text{SOME} \ \text{cmd}))) \wedge P' \ \text{TT} \wedge P' \ \text{FF} \wedge \\
& \quad (\forall v_1. \ P' \ (\text{prop} \ v_1)) \wedge (\forall v_3. \ P' \ (\text{notf} \ v_3)) \wedge \\
& \quad (\forall v_6 \ v_7. \ P' \ (v_6 \ \text{andf} \ v_7)) \wedge (\forall v_{10} \ v_{11}. \ P' \ (v_{10} \ \text{orf} \ v_{11})) \wedge \\
& \quad (\forall v_{14} \ v_{15}. \ P' \ (v_{14} \ \text{impf} \ v_{15})) \wedge \\
& \quad (\forall v_{18} \ v_{19}. \ P' \ (v_{18} \ \text{eqf} \ v_{19})) \wedge (\forall v_{129}. \ P' \ (v_{129} \ \text{says} \ \text{TT})) \wedge \\
& \quad (\forall v_{130}. \ P' \ (v_{130} \ \text{says} \ \text{FF})) \wedge \\
& \quad (\forall v_{132}. \ P' \ (v_{132} \ \text{says} \ \text{prop} \ \text{NONE})) \wedge \\
& \quad (\forall v_{133} \ v_{66}. \ P' \ (v_{133} \ \text{says} \ \text{notf} \ v_{66})) \wedge \\
& \quad (\forall v_{134} \ v_{69} \ v_{70}. \ P' \ (v_{134} \ \text{says} \ (v_{69} \ \text{andf} \ v_{70}))) \wedge \\
& \quad (\forall v_{135} \ v_{73} \ v_{74}. \ P' \ (v_{135} \ \text{says} \ (v_{73} \ \text{orf} \ v_{74}))) \wedge \\
& \quad (\forall v_{136} \ v_{77} \ v_{78}. \ P' \ (v_{136} \ \text{says} \ (v_{77} \ \text{impf} \ v_{78}))) \wedge \\
& \quad (\forall v_{137} \ v_{81} \ v_{82}. \ P' \ (v_{137} \ \text{says} \ (v_{81} \ \text{eqf} \ v_{82}))) \wedge \\
& \quad (\forall v_{138} \ v_{85} \ v_{86}. \ P' \ (v_{138} \ \text{says} \ v_{85} \ \text{says} \ v_{86})) \wedge \\
& \quad (\forall v_{139} \ v_{89} \ v_{90}. \ P' \ (v_{139} \ \text{says} \ v_{89} \ \text{speaks\_for} \ v_{90})) \wedge \\
& \quad (\forall v_{140} \ v_{93} \ v_{94}. \ P' \ (v_{140} \ \text{says} \ v_{93} \ \text{controls} \ v_{94})) \wedge \\
& \quad (\forall v_{141} \ v_{98} \ v_{99} \ v_{100}. \ P' \ (v_{141} \ \text{says} \ \text{reps} \ v_{98} \ v_{99} \ v_{100})) \wedge \\
& \quad (\forall v_{142} \ v_{103} \ v_{104}. \ P' \ (v_{142} \ \text{says} \ v_{103} \ \text{domi} \ v_{104})) \wedge \\
& \quad (\forall v_{143} \ v_{107} \ v_{108}. \ P' \ (v_{143} \ \text{says} \ v_{107} \ \text{eqi} \ v_{108})) \wedge \\
& \quad (\forall v_{144} \ v_{111} \ v_{112}. \ P' \ (v_{144} \ \text{says} \ v_{111} \ \text{doms} \ v_{112})) \wedge \\
& \quad (\forall v_{145} \ v_{115} \ v_{116}. \ P' \ (v_{145} \ \text{says} \ v_{115} \ \text{eqs} \ v_{116})) \wedge \\
& \quad (\forall v_{146} \ v_{119} \ v_{120}. \ P' \ (v_{146} \ \text{says} \ v_{119} \ \text{eqn} \ v_{120})) \wedge
\end{aligned}$$

$$\begin{aligned}
& (\forall v_{147} v_{123} v_{124}. P' (v_{147} \text{ says } v_{123} \text{ lte } v_{124})) \wedge \\
& (\forall v_{148} v_{127} v_{128}. P' (v_{148} \text{ says } v_{127} \text{ lt } v_{128})) \wedge \\
& (\forall v_{24} v_{25}. P' (v_{24} \text{ speaks\_for } v_{25})) \wedge \\
& (\forall v_{28} v_{29}. P' (v_{28} \text{ controls } v_{29})) \wedge \\
& (\forall v_{33} v_{34} v_{35}. P' (\text{reps } v_{33} v_{34} v_{35})) \wedge \\
& (\forall v_{38} v_{39}. P' (v_{38} \text{ domi } v_{39})) \wedge \\
& (\forall v_{42} v_{43}. P' (v_{42} \text{ eqi } v_{43})) \wedge \\
& (\forall v_{46} v_{47}. P' (v_{46} \text{ doms } v_{47})) \wedge \\
& (\forall v_{50} v_{51}. P' (v_{50} \text{ eqs } v_{51})) \wedge \\
& (\forall v_{54} v_{55}. P' (v_{54} \text{ eqn } v_{55})) \wedge \\
& (\forall v_{58} v_{59}. P' (v_{58} \text{ lte } v_{59})) \wedge \\
& (\forall v_{62} v_{63}. P' (v_{62} \text{ lt } v_{63})) \Rightarrow \\
& \forall v. P' v
\end{aligned}$$

[TR\_cases]

$$\begin{aligned}
& \vdash \forall a_0 a_1 a_2 a_3. \\
& \text{TR } a_0 a_1 a_2 a_3 \iff \\
& (\exists \text{elementTest } NS \ M \ Oi \ Os \ Out \ s \ context \ stateInterp \ x \ ins \\
& \quad outs. \\
& \quad (a_0 = (M, Oi, Os)) \wedge (a_1 = \text{exec } (\text{inputList } x)) \wedge \\
& \quad (a_2 = \\
& \quad \quad \text{CFG elementTest stateInterp context } (x::ins) \ s \ outs) \wedge \\
& \quad (a_3 = \\
& \quad \quad \text{CFG elementTest stateInterp context } ins \\
& \quad \quad \quad (NS \ s \ (\text{exec } (\text{inputList } x))) \\
& \quad \quad \quad (Out \ s \ (\text{exec } (\text{inputList } x))::outs)) \wedge \\
& \quad \text{authenticationTest elementTest } x \wedge \\
& \quad \text{CFGInterpret } (M, Oi, Os) \\
& \quad \quad (\text{CFG elementTest stateInterp context } (x::ins) \ s \\
& \quad \quad \quad outs)) \vee \\
& (\exists \text{elementTest } NS \ M \ Oi \ Os \ Out \ s \ context \ stateInterp \ x \ ins \\
& \quad outs. \\
& \quad (a_0 = (M, Oi, Os)) \wedge (a_1 = \text{trap } (\text{inputList } x)) \wedge \\
& \quad (a_2 = \\
& \quad \quad \text{CFG elementTest stateInterp context } (x::ins) \ s \ outs) \wedge \\
& \quad (a_3 = \\
& \quad \quad \text{CFG elementTest stateInterp context } ins \\
& \quad \quad \quad (NS \ s \ (\text{trap } (\text{inputList } x))) \\
& \quad \quad \quad (Out \ s \ (\text{trap } (\text{inputList } x))::outs)) \wedge \\
& \quad \text{authenticationTest elementTest } x \wedge \\
& \quad \text{CFGInterpret } (M, Oi, Os) \\
& \quad \quad (\text{CFG elementTest stateInterp context } (x::ins) \ s \\
& \quad \quad \quad outs)) \vee \\
& \exists \text{elementTest } NS \ M \ Oi \ Os \ Out \ s \ context \ stateInterp \ x \ ins \\
& \quad outs. \\
& \quad (a_0 = (M, Oi, Os)) \wedge (a_1 = \text{discard } (\text{inputList } x)) \wedge \\
& \quad (a_2 = \\
& \quad \quad \text{CFG elementTest stateInterp context } (x::ins) \ s \ outs) \wedge \\
& \quad (a_3 =
\end{aligned}$$

CFG elementTest stateInterp context ins  
 (NS s (discard (inputList x)))  
 (Out s (discard (inputList x))::outs))  $\wedge$   
 $\neg$ authenticationTest elementTest x

[TR\_discard\_cmd\_rule]

$\vdash$  TR (M, Oi, Os) (discard (inputList x))  
 (CFG elementTest stateInterp context (x::ins) s outs)  
 (CFG elementTest stateInterp context ins  
 (NS s (discard (inputList x)))  
 (Out s (discard (inputList x))::outs))  $\iff$   
 $\neg$ authenticationTest elementTest x

[TR\_EQ\_rules\_thm]

$\vdash$  (TR (M, Oi, Os) (exec (inputList x))  
 (CFG elementTest stateInterp context (x::ins) s outs)  
 (CFG elementTest stateInterp context ins  
 (NS s (exec (inputList x)))  
 (Out s (exec (inputList x))::outs))  $\iff$   
 authenticationTest elementTest x  $\wedge$   
 CFGInterpret (M, Oi, Os)  
 (CFG elementTest stateInterp context (x::ins) s outs))  $\wedge$   
 (TR (M, Oi, Os) (trap (inputList x))  
 (CFG elementTest stateInterp context (x::ins) s outs)  
 (CFG elementTest stateInterp context ins  
 (NS s (trap (inputList x)))  
 (Out s (trap (inputList x))::outs))  $\iff$   
 authenticationTest elementTest x  $\wedge$   
 CFGInterpret (M, Oi, Os)  
 (CFG elementTest stateInterp context (x::ins) s outs))  $\wedge$   
 (TR (M, Oi, Os) (discard (inputList x))  
 (CFG elementTest stateInterp context (x::ins) s outs)  
 (CFG elementTest stateInterp context ins  
 (NS s (discard (inputList x)))  
 (Out s (discard (inputList x))::outs))  $\iff$   
 $\neg$ authenticationTest elementTest x)

[TR\_exec\_cmd\_rule]

$\vdash \forall$  elementTest context stateInterp x ins s outs.  
 ( $\forall$  M Oi Os.  
 CFGInterpret (M, Oi, Os)  
 (CFG elementTest stateInterp context (x::ins) s  
 outs)  $\Rightarrow$   
 (M, Oi, Os) satList propCommandList x)  $\Rightarrow$   
 $\forall$  NS Out M Oi Os.  
 TR (M, Oi, Os) (exec (inputList x))  
 (CFG elementTest stateInterp context (x::ins) s outs)  
 (CFG elementTest stateInterp context ins

$$\begin{aligned}
& (NS \ s \ (\text{exec} \ (\text{inputList} \ x))) \\
& (\text{Out} \ s \ (\text{exec} \ (\text{inputList} \ x))::\text{outs})) \iff \\
& \text{authenticationTest} \ \text{elementTest} \ x \wedge \\
& \text{CFGInterpret} \ (M, Oi, Os) \\
& \quad (\text{CFG} \ \text{elementTest} \ \text{stateInterp} \ \text{context} \ (x::\text{ins}) \ s \ \text{outs}) \wedge \\
& (M, Oi, Os) \ \text{satList} \ \text{propCommandList} \ x
\end{aligned}$$

[TR\_ind]

$\vdash \forall TR'.$

$$\begin{aligned}
& (\forall \text{elementTest} \ NS \ M \ Oi \ Os \ Out \ s \ \text{context} \ \text{stateInterp} \ x \ \text{ins} \\
& \quad \text{outs}. \\
& \text{authenticationTest} \ \text{elementTest} \ x \wedge \\
& \text{CFGInterpret} \ (M, Oi, Os) \\
& \quad (\text{CFG} \ \text{elementTest} \ \text{stateInterp} \ \text{context} \ (x::\text{ins}) \ s \\
& \quad \text{outs}) \Rightarrow \\
& TR' \ (M, Oi, Os) \ (\text{exec} \ (\text{inputList} \ x)) \\
& \quad (\text{CFG} \ \text{elementTest} \ \text{stateInterp} \ \text{context} \ (x::\text{ins}) \ s \ \text{outs}) \\
& \quad (\text{CFG} \ \text{elementTest} \ \text{stateInterp} \ \text{context} \ \text{ins} \\
& \quad \quad (NS \ s \ (\text{exec} \ (\text{inputList} \ x))) \\
& \quad \quad (\text{Out} \ s \ (\text{exec} \ (\text{inputList} \ x))::\text{outs}))) \wedge \\
& (\forall \text{elementTest} \ NS \ M \ Oi \ Os \ Out \ s \ \text{context} \ \text{stateInterp} \ x \ \text{ins} \\
& \quad \text{outs}. \\
& \text{authenticationTest} \ \text{elementTest} \ x \wedge \\
& \text{CFGInterpret} \ (M, Oi, Os) \\
& \quad (\text{CFG} \ \text{elementTest} \ \text{stateInterp} \ \text{context} \ (x::\text{ins}) \ s \\
& \quad \text{outs}) \Rightarrow \\
& TR' \ (M, Oi, Os) \ (\text{trap} \ (\text{inputList} \ x)) \\
& \quad (\text{CFG} \ \text{elementTest} \ \text{stateInterp} \ \text{context} \ (x::\text{ins}) \ s \ \text{outs}) \\
& \quad (\text{CFG} \ \text{elementTest} \ \text{stateInterp} \ \text{context} \ \text{ins} \\
& \quad \quad (NS \ s \ (\text{trap} \ (\text{inputList} \ x))) \\
& \quad \quad (\text{Out} \ s \ (\text{trap} \ (\text{inputList} \ x))::\text{outs}))) \wedge \\
& (\forall \text{elementTest} \ NS \ M \ Oi \ Os \ Out \ s \ \text{context} \ \text{stateInterp} \ x \ \text{ins} \\
& \quad \text{outs}. \\
& \neg \text{authenticationTest} \ \text{elementTest} \ x \Rightarrow \\
& TR' \ (M, Oi, Os) \ (\text{discard} \ (\text{inputList} \ x)) \\
& \quad (\text{CFG} \ \text{elementTest} \ \text{stateInterp} \ \text{context} \ (x::\text{ins}) \ s \ \text{outs}) \\
& \quad (\text{CFG} \ \text{elementTest} \ \text{stateInterp} \ \text{context} \ \text{ins} \\
& \quad \quad (NS \ s \ (\text{discard} \ (\text{inputList} \ x))) \\
& \quad \quad (\text{Out} \ s \ (\text{discard} \ (\text{inputList} \ x))::\text{outs}))) \Rightarrow \\
& \forall a_0 \ a_1 \ a_2 \ a_3. \ TR \ a_0 \ a_1 \ a_2 \ a_3 \Rightarrow TR' \ a_0 \ a_1 \ a_2 \ a_3
\end{aligned}$$

[TR\_rules]

$$\begin{aligned}
& \vdash (\forall \text{elementTest} \ NS \ M \ Oi \ Os \ Out \ s \ \text{context} \ \text{stateInterp} \ x \ \text{ins} \\
& \quad \text{outs}. \\
& \text{authenticationTest} \ \text{elementTest} \ x \wedge \\
& \text{CFGInterpret} \ (M, Oi, Os) \\
& \quad (\text{CFG} \ \text{elementTest} \ \text{stateInterp} \ \text{context} \ (x::\text{ins}) \ s \ \text{outs}) \Rightarrow \\
& TR \ (M, Oi, Os) \ (\text{exec} \ (\text{inputList} \ x)) \\
& \quad (\text{CFG} \ \text{elementTest} \ \text{stateInterp} \ \text{context} \ (x::\text{ins}) \ s \ \text{outs})
\end{aligned}$$



$(\text{CFG } \text{elementTest } \text{stateInterp } \text{context } \text{ins}$   
 $\quad (\text{NS } s \text{ (exec (inputList } x)))$   
 $\quad (\text{Out } s \text{ (exec (inputList } x))::\text{outs}))) \wedge$   
 $(\forall \text{elementTest } \text{NS } M \text{ } Oi \text{ } Os \text{ } \text{Out } s \text{ context } \text{stateInterp } x \text{ ins}$   
 $\quad \text{outs.}$   
 $\text{authenticationTest } \text{elementTest } x \wedge$   
 $\text{CFGInterpret } (M, Oi, Os)$   
 $\quad (\text{CFG } \text{elementTest } \text{stateInterp } \text{context } (x::\text{ins}) \text{ } s \text{ } \text{outs}) \Rightarrow$   
 $\text{TR } (M, Oi, Os) \text{ (trap (inputList } x))$   
 $\quad (\text{CFG } \text{elementTest } \text{stateInterp } \text{context } (x::\text{ins}) \text{ } s \text{ } \text{outs})$   
 $\quad (\text{CFG } \text{elementTest } \text{stateInterp } \text{context } \text{ins}$   
 $\quad \quad (\text{NS } s \text{ (trap (inputList } x)))$   
 $\quad \quad (\text{Out } s \text{ (trap (inputList } x))::\text{outs}))) \wedge$   
 $\forall \text{elementTest } \text{NS } M \text{ } Oi \text{ } Os \text{ } \text{Out } s \text{ context } \text{stateInterp } x \text{ ins } \text{outs.}$   
 $\neg \text{authenticationTest } \text{elementTest } x \Rightarrow$   
 $\text{TR } (M, Oi, Os) \text{ (discard (inputList } x))$   
 $\quad (\text{CFG } \text{elementTest } \text{stateInterp } \text{context } (x::\text{ins}) \text{ } s \text{ } \text{outs})$   
 $\quad (\text{CFG } \text{elementTest } \text{stateInterp } \text{context } \text{ins}$   
 $\quad \quad (\text{NS } s \text{ (discard (inputList } x)))$   
 $\quad \quad (\text{Out } s \text{ (discard (inputList } x))::\text{outs}))$

[TR\_strongind]

$\vdash \forall \text{TR'.$   
 $(\forall \text{elementTest } \text{NS } M \text{ } Oi \text{ } Os \text{ } \text{Out } s \text{ context } \text{stateInterp } x \text{ ins}$   
 $\quad \text{outs.}$   
 $\text{authenticationTest } \text{elementTest } x \wedge$   
 $\text{CFGInterpret } (M, Oi, Os)$   
 $\quad (\text{CFG } \text{elementTest } \text{stateInterp } \text{context } (x::\text{ins}) \text{ } s$   
 $\quad \quad \text{outs}) \Rightarrow$   
 $\text{TR' } (M, Oi, Os) \text{ (exec (inputList } x))$   
 $\quad (\text{CFG } \text{elementTest } \text{stateInterp } \text{context } (x::\text{ins}) \text{ } s \text{ } \text{outs})$   
 $\quad (\text{CFG } \text{elementTest } \text{stateInterp } \text{context } \text{ins}$   
 $\quad \quad (\text{NS } s \text{ (exec (inputList } x)))$   
 $\quad \quad (\text{Out } s \text{ (exec (inputList } x))::\text{outs}))) \wedge$   
 $(\forall \text{elementTest } \text{NS } M \text{ } Oi \text{ } Os \text{ } \text{Out } s \text{ context } \text{stateInterp } x \text{ ins}$   
 $\quad \text{outs.}$   
 $\text{authenticationTest } \text{elementTest } x \wedge$   
 $\text{CFGInterpret } (M, Oi, Os)$   
 $\quad (\text{CFG } \text{elementTest } \text{stateInterp } \text{context } (x::\text{ins}) \text{ } s$   
 $\quad \quad \text{outs}) \Rightarrow$   
 $\text{TR' } (M, Oi, Os) \text{ (trap (inputList } x))$   
 $\quad (\text{CFG } \text{elementTest } \text{stateInterp } \text{context } (x::\text{ins}) \text{ } s \text{ } \text{outs})$   
 $\quad (\text{CFG } \text{elementTest } \text{stateInterp } \text{context } \text{ins}$   
 $\quad \quad (\text{NS } s \text{ (trap (inputList } x)))$   
 $\quad \quad (\text{Out } s \text{ (trap (inputList } x))::\text{outs}))) \wedge$   
 $(\forall \text{elementTest } \text{NS } M \text{ } Oi \text{ } Os \text{ } \text{Out } s \text{ context } \text{stateInterp } x \text{ ins}$   
 $\quad \text{outs.}$   
 $\neg \text{authenticationTest } \text{elementTest } x \Rightarrow$   
 $\text{TR' } (M, Oi, Os) \text{ (discard (inputList } x))$

$$\begin{aligned}
& (\text{CFG elementTest stateInterp context } (x::\text{ins}) \text{ s outs}) \\
& (\text{CFG elementTest stateInterp context ins} \\
& \quad (\text{NS s (discard (inputList x))}) \\
& \quad (\text{Out s (discard (inputList x))::outs})) \Rightarrow \\
& \forall a_0 \ a_1 \ a_2 \ a_3. \text{ TR } a_0 \ a_1 \ a_2 \ a_3 \Rightarrow \text{TR}' a_0 \ a_1 \ a_2 \ a_3
\end{aligned}$$

[TR\_trap\_cmd\_rule]

$$\begin{aligned}
& \vdash \forall \text{elementTest context stateInterp } x \text{ ins s outs.} \\
& \quad (\forall M \ Oi \ Os. \\
& \quad \quad \text{CFGInterpret } (M, Oi, Os) \\
& \quad \quad (\text{CFG elementTest stateInterp context } (x::\text{ins}) \text{ s} \\
& \quad \quad \quad \text{outs}) \Rightarrow \\
& \quad \quad (M, Oi, Os) \text{ sat prop NONE}) \Rightarrow \\
& \quad \forall \text{NS Out } M \ Oi \ Os. \\
& \quad \text{TR } (M, Oi, Os) (\text{trap (inputList x)}) \\
& \quad (\text{CFG elementTest stateInterp context } (x::\text{ins}) \text{ s outs}) \\
& \quad (\text{CFG elementTest stateInterp context ins} \\
& \quad \quad (\text{NS s (trap (inputList x))}) \\
& \quad \quad (\text{Out s (trap (inputList x))::outs})) \iff \\
& \quad \text{authenticationTest elementTest } x \wedge \\
& \quad \text{CFGInterpret } (M, Oi, Os) \\
& \quad \quad (\text{CFG elementTest stateInterp context } (x::\text{ins}) \text{ s outs}) \wedge \\
& \quad \quad (M, Oi, Os) \text{ sat prop NONE}
\end{aligned}$$

[TRrule0]

$$\begin{aligned}
& \vdash \text{TR } (M, Oi, Os) (\text{exec (inputList x)}) \\
& \quad (\text{CFG elementTest stateInterp context } (x::\text{ins}) \text{ s outs}) \\
& \quad (\text{CFG elementTest stateInterp context ins} \\
& \quad \quad (\text{NS s (exec (inputList x))}) \\
& \quad \quad (\text{Out s (exec (inputList x))::outs})) \iff \\
& \quad \text{authenticationTest elementTest } x \wedge \\
& \quad \text{CFGInterpret } (M, Oi, Os) \\
& \quad \quad (\text{CFG elementTest stateInterp context } (x::\text{ins}) \text{ s outs})
\end{aligned}$$

[TRrule1]

$$\begin{aligned}
& \vdash \text{TR } (M, Oi, Os) (\text{trap (inputList x)}) \\
& \quad (\text{CFG elementTest stateInterp context } (x::\text{ins}) \text{ s outs}) \\
& \quad (\text{CFG elementTest stateInterp context ins} \\
& \quad \quad (\text{NS s (trap (inputList x))}) \\
& \quad \quad (\text{Out s (trap (inputList x))::outs})) \iff \\
& \quad \text{authenticationTest elementTest } x \wedge \\
& \quad \text{CFGInterpret } (M, Oi, Os) \\
& \quad \quad (\text{CFG elementTest stateInterp context } (x::\text{ins}) \text{ s outs})
\end{aligned}$$

[trType\_distinct\_clauses]

$$\begin{aligned}
& \vdash (\forall a' \ a. \text{discard } a \neq \text{trap } a') \wedge (\forall a' \ a. \text{discard } a \neq \text{exec } a') \wedge \\
& \quad \forall a' \ a. \text{trap } a \neq \text{exec } a'
\end{aligned}$$

[trType\_one\_one]

$$\vdash (\forall a \ a'. (\text{discard } a = \text{discard } a') \iff (a = a')) \wedge$$

$$(\forall a \ a'. (\text{trap } a = \text{trap } a') \iff (a = a')) \wedge$$

$$\forall a \ a'. (\text{exec } a = \text{exec } a') \iff (a = a')$$

## 4 satList Theory

**Built:** 13 May 2018

**Parent Theories:** aclRules

### 4.1 Definitions

[satList\_def]

$$\vdash \forall M \ Oi \ Os \ formList.$$

$$(M, Oi, Os) \text{ satList } formList \iff$$

$$\text{FOLDR } (\lambda x \ y. x \wedge y) \ T \ (\text{MAP } (\lambda f. (M, Oi, Os) \text{ sat } f) \ formList)$$

### 4.2 Theorems

[satList\_conj]

$$\vdash \forall l_1 \ l_2 \ M \ Oi \ Os.$$

$$(M, Oi, Os) \text{ satList } l_1 \wedge (M, Oi, Os) \text{ satList } l_2 \iff$$

$$(M, Oi, Os) \text{ satList } (l_1 ++ l_2)$$

[satList\_CONS]

$$\vdash \forall h \ t \ M \ Oi \ Os.$$

$$(M, Oi, Os) \text{ satList } (h :: t) \iff$$

$$(M, Oi, Os) \text{ sat } h \wedge (M, Oi, Os) \text{ satList } t$$

[satList\_nil]

$$\vdash (M, Oi, Os) \text{ satList } []$$

## 5 ssmPB Theory

**Built:** 13 May 2018

**Parent Theories:** PBType, ssm11, OMNIType

### 5.1 Definitions

[secContext\_def]

$$\vdash \forall cmd.$$

$$\text{secContext } cmd =$$

$$[\text{Name PlatoonLeader controls prop (SOME (SLc } cmd))]$$

[ssmPBStateInterp\_def]

$$\vdash \forall state. \text{ssmPBStateInterp } state = \text{TT}$$

## 5.2 Theorems

[authenticationTest\_cmd\_reject\_lemma]

$\vdash \forall cmd. \neg \text{authenticationTest} (\text{prop } (\text{SOME } cmd))$

[authenticationTest\_def]

$\vdash (\text{authenticationTest } (\text{Name PlatoonLeader says prop } cmd) \iff$   
 $T) \wedge (\text{authenticationTest } TT \iff F) \wedge$   
 $(\text{authenticationTest } FF \iff F) \wedge$   
 $(\text{authenticationTest } (\text{prop } v) \iff F) \wedge$   
 $(\text{authenticationTest } (\text{notf } v_1) \iff F) \wedge$   
 $(\text{authenticationTest } (v_2 \text{ andf } v_3) \iff F) \wedge$   
 $(\text{authenticationTest } (v_4 \text{ orf } v_5) \iff F) \wedge$   
 $(\text{authenticationTest } (v_6 \text{ impf } v_7) \iff F) \wedge$   
 $(\text{authenticationTest } (v_8 \text{ eqf } v_9) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } TT) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } FF) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{133} \text{ meet } v_{134} \text{ says prop } v_{66}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{135} \text{ quoting } v_{136} \text{ says prop } v_{66}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says notf } v_{67}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } (v_{68} \text{ andf } v_{69})) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } (v_{70} \text{ orf } v_{71})) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } (v_{72} \text{ impf } v_{73})) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } (v_{74} \text{ eqf } v_{75})) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } v_{76} \text{ says } v_{77}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } v_{78} \text{ speaks\_for } v_{79}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } v_{80} \text{ controls } v_{81}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says reps } v_{82} \ v_{83} \ v_{84}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } v_{85} \text{ domi } v_{86}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } v_{87} \text{ eqi } v_{88}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } v_{89} \text{ doms } v_{90}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } v_{91} \text{ eqs } v_{92}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } v_{93} \text{ eqn } v_{94}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } v_{95} \text{ lte } v_{96}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{10} \text{ says } v_{97} \text{ lt } v_{98}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{12} \text{ speaks\_for } v_{13}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{14} \text{ controls } v_{15}) \iff F) \wedge$   
 $(\text{authenticationTest } (\text{reps } v_{16} \ v_{17} \ v_{18}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{19} \text{ domi } v_{20}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{21} \text{ eqi } v_{22}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{23} \text{ doms } v_{24}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{25} \text{ eqs } v_{26}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{27} \text{ eqn } v_{28}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{29} \text{ lte } v_{30}) \iff F) \wedge$   
 $(\text{authenticationTest } (v_{31} \text{ lt } v_{32}) \iff F)$

[authenticationTest\_ind]

$\vdash \forall P.$   
 $(\forall cmd. P (\text{Name PlatoonLeader says prop } cmd)) \wedge P \ TT \wedge$

$$\begin{aligned}
& P \text{ FF} \wedge (\forall v. P (\text{prop } v)) \wedge (\forall v_1. P (\text{notf } v_1)) \wedge \\
& (\forall v_2 v_3. P (v_2 \text{ andf } v_3)) \wedge (\forall v_4 v_5. P (v_4 \text{ orf } v_5)) \wedge \\
& (\forall v_6 v_7. P (v_6 \text{ impf } v_7)) \wedge (\forall v_8 v_9. P (v_8 \text{ eqf } v_9)) \wedge \\
& (\forall v_{10}. P (v_{10} \text{ says TT})) \wedge (\forall v_{10}. P (v_{10} \text{ says FF})) \wedge \\
& (\forall v_{133} v_{134} v_{66}. P (v_{133} \text{ meet } v_{134} \text{ says prop } v_{66})) \wedge \\
& (\forall v_{135} v_{136} v_{66}. P (v_{135} \text{ quoting } v_{136} \text{ says prop } v_{66})) \wedge \\
& (\forall v_{10} v_{67}. P (v_{10} \text{ says notf } v_{67})) \wedge \\
& (\forall v_{10} v_{68} v_{69}. P (v_{10} \text{ says } (v_{68} \text{ andf } v_{69}))) \wedge \\
& (\forall v_{10} v_{70} v_{71}. P (v_{10} \text{ says } (v_{70} \text{ orf } v_{71}))) \wedge \\
& (\forall v_{10} v_{72} v_{73}. P (v_{10} \text{ says } (v_{72} \text{ impf } v_{73}))) \wedge \\
& (\forall v_{10} v_{74} v_{75}. P (v_{10} \text{ says } (v_{74} \text{ eqf } v_{75}))) \wedge \\
& (\forall v_{10} v_{76} v_{77}. P (v_{10} \text{ says } v_{76} \text{ says } v_{77})) \wedge \\
& (\forall v_{10} v_{78} v_{79}. P (v_{10} \text{ says } v_{78} \text{ speaks\_for } v_{79})) \wedge \\
& (\forall v_{10} v_{80} v_{81}. P (v_{10} \text{ says } v_{80} \text{ controls } v_{81})) \wedge \\
& (\forall v_{10} v_{82} v_{83} v_{84}. P (v_{10} \text{ says reps } v_{82} v_{83} v_{84})) \wedge \\
& (\forall v_{10} v_{85} v_{86}. P (v_{10} \text{ says } v_{85} \text{ domi } v_{86})) \wedge \\
& (\forall v_{10} v_{87} v_{88}. P (v_{10} \text{ says } v_{87} \text{ eqi } v_{88})) \wedge \\
& (\forall v_{10} v_{89} v_{90}. P (v_{10} \text{ says } v_{89} \text{ doms } v_{90})) \wedge \\
& (\forall v_{10} v_{91} v_{92}. P (v_{10} \text{ says } v_{91} \text{ eqs } v_{92})) \wedge \\
& (\forall v_{10} v_{93} v_{94}. P (v_{10} \text{ says } v_{93} \text{ eqn } v_{94})) \wedge \\
& (\forall v_{10} v_{95} v_{96}. P (v_{10} \text{ says } v_{95} \text{ lte } v_{96})) \wedge \\
& (\forall v_{10} v_{97} v_{98}. P (v_{10} \text{ says } v_{97} \text{ lt } v_{98})) \wedge \\
& (\forall v_{12} v_{13}. P (v_{12} \text{ speaks\_for } v_{13})) \wedge \\
& (\forall v_{14} v_{15}. P (v_{14} \text{ controls } v_{15})) \wedge \\
& (\forall v_{16} v_{17} v_{18}. P (\text{reps } v_{16} v_{17} v_{18})) \wedge \\
& (\forall v_{19} v_{20}. P (v_{19} \text{ domi } v_{20})) \wedge \\
& (\forall v_{21} v_{22}. P (v_{21} \text{ eqi } v_{22})) \wedge \\
& (\forall v_{23} v_{24}. P (v_{23} \text{ doms } v_{24})) \wedge \\
& (\forall v_{25} v_{26}. P (v_{25} \text{ eqs } v_{26})) \wedge (\forall v_{27} v_{28}. P (v_{27} \text{ eqn } v_{28})) \wedge \\
& (\forall v_{29} v_{30}. P (v_{29} \text{ lte } v_{30})) \wedge (\forall v_{31} v_{32}. P (v_{31} \text{ lt } v_{32})) \Rightarrow \\
& \forall v. P v
\end{aligned}$$

[PBNS\_def]

$$\begin{aligned}
& \vdash (\text{PBNS PLAN\_PB (exec (SLc crossLD))} = \text{MOVE\_TO\_ORP}) \wedge \\
& (\text{PBNS PLAN\_PB (exec (SLc incomplete))} = \text{PLAN\_PB}) \wedge \\
& (\text{PBNS MOVE\_TO\_ORP (exec (SLc conductorORP))} = \text{CONDUCT\_ORP}) \wedge \\
& (\text{PBNS MOVE\_TO\_ORP (exec (SLc incomplete))} = \text{MOVE\_TO\_ORP}) \wedge \\
& (\text{PBNS CONDUCT\_ORP (exec (SLc moveToPB))} = \text{MOVE\_TO\_PB}) \wedge \\
& (\text{PBNS CONDUCT\_ORP (exec (SLc incomplete))} = \text{CONDUCT\_ORP}) \wedge \\
& (\text{PBNS MOVE\_TO\_PB (exec (SLc conductPB))} = \text{CONDUCT\_PB}) \wedge \\
& (\text{PBNS MOVE\_TO\_PB (exec (SLc incomplete))} = \text{MOVE\_TO\_PB}) \wedge \\
& (\text{PBNS CONDUCT\_PB (exec (SLc completePB))} = \text{COMPLETE\_PB}) \wedge \\
& (\text{PBNS CONDUCT\_PB (exec (SLc incomplete))} = \text{CONDUCT\_PB}) \wedge \\
& (\text{PBNS } s \text{ (trap (SLc cmd))} = s) \wedge \\
& (\text{PBNS } s \text{ (discard (SLc cmd))} = s)
\end{aligned}$$

[PBNS\_ind]

$$\begin{aligned}
& \vdash \forall P. \\
& P \text{ PLAN\_PB (exec (SLc crossLD))} \wedge
\end{aligned}$$

$$\begin{aligned}
& P \text{ PLAN\_PB } (\text{exec } (\text{SLc incomplete})) \wedge \\
& P \text{ MOVE\_TO\_ORP } (\text{exec } (\text{SLc conductORP})) \wedge \\
& P \text{ MOVE\_TO\_ORP } (\text{exec } (\text{SLc incomplete})) \wedge \\
& P \text{ CONDUCT\_ORP } (\text{exec } (\text{SLc moveToPB})) \wedge \\
& P \text{ CONDUCT\_ORP } (\text{exec } (\text{SLc incomplete})) \wedge \\
& P \text{ MOVE\_TO\_PB } (\text{exec } (\text{SLc conductPB})) \wedge \\
& P \text{ MOVE\_TO\_PB } (\text{exec } (\text{SLc incomplete})) \wedge \\
& P \text{ CONDUCT\_PB } (\text{exec } (\text{SLc completePB})) \wedge \\
& P \text{ CONDUCT\_PB } (\text{exec } (\text{SLc incomplete})) \wedge \\
& (\forall s \text{ cmd. } P \text{ s } (\text{trap } (\text{SLc cmd}))) \wedge \\
& (\forall s \text{ cmd. } P \text{ s } (\text{discard } (\text{SLc cmd}))) \wedge \\
& (\forall s \text{ v}_6. P \text{ s } (\text{discard } (\text{ESCc v}_6))) \wedge \\
& (\forall s \text{ v}_9. P \text{ s } (\text{trap } (\text{ESCc v}_9))) \wedge \\
& (\forall v_{12}. P \text{ PLAN\_PB } (\text{exec } (\text{ESCc v}_{12}))) \wedge \\
& P \text{ PLAN\_PB } (\text{exec } (\text{SLc conductORP})) \wedge \\
& P \text{ PLAN\_PB } (\text{exec } (\text{SLc moveToPB})) \wedge \\
& P \text{ PLAN\_PB } (\text{exec } (\text{SLc conductPB})) \wedge \\
& P \text{ PLAN\_PB } (\text{exec } (\text{SLc completePB})) \wedge \\
& (\forall v_{15}. P \text{ MOVE\_TO\_ORP } (\text{exec } (\text{ESCc v}_{15}))) \wedge \\
& P \text{ MOVE\_TO\_ORP } (\text{exec } (\text{SLc crossLD})) \wedge \\
& P \text{ MOVE\_TO\_ORP } (\text{exec } (\text{SLc moveToPB})) \wedge \\
& P \text{ MOVE\_TO\_ORP } (\text{exec } (\text{SLc conductPB})) \wedge \\
& P \text{ MOVE\_TO\_ORP } (\text{exec } (\text{SLc completePB})) \wedge \\
& (\forall v_{18}. P \text{ CONDUCT\_ORP } (\text{exec } (\text{ESCc v}_{18}))) \wedge \\
& P \text{ CONDUCT\_ORP } (\text{exec } (\text{SLc crossLD})) \wedge \\
& P \text{ CONDUCT\_ORP } (\text{exec } (\text{SLc conductORP})) \wedge \\
& P \text{ CONDUCT\_ORP } (\text{exec } (\text{SLc conductPB})) \wedge \\
& P \text{ CONDUCT\_ORP } (\text{exec } (\text{SLc completePB})) \wedge \\
& (\forall v_{21}. P \text{ MOVE\_TO\_PB } (\text{exec } (\text{ESCc v}_{21}))) \wedge \\
& P \text{ MOVE\_TO\_PB } (\text{exec } (\text{SLc crossLD})) \wedge \\
& P \text{ MOVE\_TO\_PB } (\text{exec } (\text{SLc conductORP})) \wedge \\
& P \text{ MOVE\_TO\_PB } (\text{exec } (\text{SLc moveToPB})) \wedge \\
& P \text{ MOVE\_TO\_PB } (\text{exec } (\text{SLc completePB})) \wedge \\
& (\forall v_{24}. P \text{ CONDUCT\_PB } (\text{exec } (\text{ESCc v}_{24}))) \wedge \\
& P \text{ CONDUCT\_PB } (\text{exec } (\text{SLc crossLD})) \wedge \\
& P \text{ CONDUCT\_PB } (\text{exec } (\text{SLc conductORP})) \wedge \\
& P \text{ CONDUCT\_PB } (\text{exec } (\text{SLc moveToPB})) \wedge \\
& P \text{ CONDUCT\_PB } (\text{exec } (\text{SLc conductPB})) \wedge \\
& (\forall v_{26}. P \text{ COMPLETE\_PB } (\text{exec } v_{26})) \Rightarrow \\
& \forall v \text{ v}_1. P \text{ v } v_1
\end{aligned}$$

[PBOut\_def]

$$\begin{aligned}
& \vdash (\text{PBOut PLAN\_PB } (\text{exec } (\text{SLc crossLD})) = \text{MoveToORP}) \wedge \\
& (\text{PBOut PLAN\_PB } (\text{exec } (\text{SLc incomplete})) = \text{PlanPB}) \wedge \\
& (\text{PBOut MOVE\_TO\_ORP } (\text{exec } (\text{SLc conductORP})) = \text{ConductORP}) \wedge \\
& (\text{PBOut MOVE\_TO\_ORP } (\text{exec } (\text{SLc incomplete})) = \text{MoveToORP}) \wedge \\
& (\text{PBOut CONDUCT\_ORP } (\text{exec } (\text{SLc moveToPB})) = \text{MoveToPB}) \wedge \\
& (\text{PBOut CONDUCT\_ORP } (\text{exec } (\text{SLc incomplete})) = \text{ConductORP}) \wedge \\
& (\text{PBOut MOVE\_TO\_PB } (\text{exec } (\text{SLc conductPB})) = \text{ConductPB}) \wedge
\end{aligned}$$

$(\text{PBOut MOVE\_TO\_PB (exec (SLc incomplete))} = \text{MoveToPB}) \wedge$   
 $(\text{PBOut CONDUCT\_PB (exec (SLc completePB))} = \text{CompletePB}) \wedge$   
 $(\text{PBOut CONDUCT\_PB (exec (SLc incomplete))} = \text{ConductPB}) \wedge$   
 $(\text{PBOut } s \text{ (trap (SLc cmd))} = \text{unAuthorized}) \wedge$   
 $(\text{PBOut } s \text{ (discard (SLc cmd))} = \text{unAuthenticated})$

[PBOut\_ind]

$\vdash \forall P.$

$P \text{ PLAN\_PB (exec (SLc crossLD))} \wedge$   
 $P \text{ PLAN\_PB (exec (SLc incomplete))} \wedge$   
 $P \text{ MOVE\_TO\_ORP (exec (SLc conductORP))} \wedge$   
 $P \text{ MOVE\_TO\_ORP (exec (SLc incomplete))} \wedge$   
 $P \text{ CONDUCT\_ORP (exec (SLc moveToPB))} \wedge$   
 $P \text{ CONDUCT\_ORP (exec (SLc incomplete))} \wedge$   
 $P \text{ MOVE\_TO\_PB (exec (SLc conductPB))} \wedge$   
 $P \text{ MOVE\_TO\_PB (exec (SLc incomplete))} \wedge$   
 $P \text{ CONDUCT\_PB (exec (SLc completePB))} \wedge$   
 $P \text{ CONDUCT\_PB (exec (SLc incomplete))} \wedge$   
 $(\forall s \text{ cmd. } P \text{ } s \text{ (trap (SLc cmd))}) \wedge$   
 $(\forall s \text{ cmd. } P \text{ } s \text{ (discard (SLc cmd))}) \wedge$   
 $(\forall s \text{ } v_6. P \text{ } s \text{ (discard (ESCc } v_6))}) \wedge$   
 $(\forall s \text{ } v_9. P \text{ } s \text{ (trap (ESCc } v_9))}) \wedge$   
 $(\forall v_{12}. P \text{ PLAN\_PB (exec (ESCc } v_{12}))}) \wedge$   
 $P \text{ PLAN\_PB (exec (SLc conductORP))} \wedge$   
 $P \text{ PLAN\_PB (exec (SLc moveToPB))} \wedge$   
 $P \text{ PLAN\_PB (exec (SLc conductPB))} \wedge$   
 $P \text{ PLAN\_PB (exec (SLc completePB))} \wedge$   
 $(\forall v_{15}. P \text{ MOVE\_TO\_ORP (exec (ESCc } v_{15}))}) \wedge$   
 $P \text{ MOVE\_TO\_ORP (exec (SLc crossLD))} \wedge$   
 $P \text{ MOVE\_TO\_ORP (exec (SLc moveToPB))} \wedge$   
 $P \text{ MOVE\_TO\_ORP (exec (SLc conductPB))} \wedge$   
 $P \text{ MOVE\_TO\_ORP (exec (SLc completePB))} \wedge$   
 $(\forall v_{18}. P \text{ CONDUCT\_ORP (exec (ESCc } v_{18}))}) \wedge$   
 $P \text{ CONDUCT\_ORP (exec (SLc crossLD))} \wedge$   
 $P \text{ CONDUCT\_ORP (exec (SLc conductORP))} \wedge$   
 $P \text{ CONDUCT\_ORP (exec (SLc conductPB))} \wedge$   
 $P \text{ CONDUCT\_ORP (exec (SLc completePB))} \wedge$   
 $(\forall v_{21}. P \text{ MOVE\_TO\_PB (exec (ESCc } v_{21}))}) \wedge$   
 $P \text{ MOVE\_TO\_PB (exec (SLc crossLD))} \wedge$   
 $P \text{ MOVE\_TO\_PB (exec (SLc conductORP))} \wedge$   
 $P \text{ MOVE\_TO\_PB (exec (SLc moveToPB))} \wedge$   
 $P \text{ MOVE\_TO\_PB (exec (SLc completePB))} \wedge$   
 $(\forall v_{24}. P \text{ CONDUCT\_PB (exec (ESCc } v_{24}))}) \wedge$   
 $P \text{ CONDUCT\_PB (exec (SLc crossLD))} \wedge$   
 $P \text{ CONDUCT\_PB (exec (SLc conductORP))} \wedge$   
 $P \text{ CONDUCT\_PB (exec (SLc moveToPB))} \wedge$   
 $P \text{ CONDUCT\_PB (exec (SLc conductPB))} \wedge$   
 $(\forall v_{26}. P \text{ COMPLETE\_PB (exec } v_{26})) \Rightarrow$   
 $\forall v \text{ } v_1. P \text{ } v \text{ } v_1$

[PlatoonLeader\_exec\_slCommand\_justified\_thm]

```

⊢ ∀ NS Out M Oi Os.
  TR (M, Oi, Os) (exec (SLc slCommand))
    (CFG authenticationTest ssmPBStateInterp
      (secContext slCommand)
      (Name PlatoonLeader says prop (SOME (SLc slCommand))::
        ins) s outs)
    (CFG authenticationTest ssmPBStateInterp
      (secContext slCommand) ins
      (NS s (exec (SLc slCommand))))
    (Out s (exec (SLc slCommand))::outs)) ⇔
authenticationTest
  (Name PlatoonLeader says prop (SOME (SLc slCommand))) ∧
CFGInterpret (M, Oi, Os)
  (CFG authenticationTest ssmPBStateInterp
    (secContext slCommand)
    (Name PlatoonLeader says prop (SOME (SLc slCommand))::
      ins) s outs) ∧
  (M, Oi, Os) sat prop (SOME (SLc slCommand))

```

[PlatoonLeader\_slCommand\_lemma]

```

⊢ CFGInterpret (M, Oi, Os)
  (CFG authenticationTest ssmPBStateInterp
    (secContext slCommand)
    (Name PlatoonLeader says prop (SOME (SLc slCommand))::
      ins) s outs) ⇒
  (M, Oi, Os) sat prop (SOME (SLc slCommand))

```

## 6 PBTypeIntegrated Theory

**Built:** 13 May 2018

**Parent Theories:** OMNIType

### 6.1 Datatypes

```

omniCommand = ssmPlanPBComplete | ssmMoveToORPComplete
              | ssmConductORPComplete | ssmMoveToPBComplete
              | ssmConductPBComplete | invalidOmniCommand

```

```

plCommand = crossLD | conductORP | moveToPB | conductPB
            | completePB | incomplete

```

```

slCommand = PL PBTypeIntegrated$plCommand | OMNI omniCommand

```

```

slOutput = PlanPB | MoveToORP | ConductORP | MoveToPB
           | ConductPB | CompletePB | unAuthenticated
           | unAuthorized

```



$$slState = \text{PLAN\_PB} \mid \text{MOVE\_TO\_ORP} \mid \text{CONDUCT\_ORP} \mid \text{MOVE\_TO\_PB} \\ \mid \text{CONDUCT\_PB} \mid \text{COMPLETE\_PB}$$

$$stateRole = \text{PlatoonLeader} \mid \text{Omni}$$

## 6.2 Theorems

[omniCommand\_distinct\_clauses]

$$\begin{aligned} \vdash & \text{ssmPlanPBComplete} \neq \text{ssmMoveToORPComplete} \wedge \\ & \text{ssmPlanPBComplete} \neq \text{ssmConductORPComplete} \wedge \\ & \text{ssmPlanPBComplete} \neq \text{ssmMoveToPBComplete} \wedge \\ & \text{ssmPlanPBComplete} \neq \text{ssmConductPBComplete} \wedge \\ & \text{ssmPlanPBComplete} \neq \text{invalidOmniCommand} \wedge \\ & \text{ssmMoveToORPComplete} \neq \text{ssmConductORPComplete} \wedge \\ & \text{ssmMoveToORPComplete} \neq \text{ssmMoveToPBComplete} \wedge \\ & \text{ssmMoveToORPComplete} \neq \text{ssmConductPBComplete} \wedge \\ & \text{ssmMoveToORPComplete} \neq \text{invalidOmniCommand} \wedge \\ & \text{ssmConductORPComplete} \neq \text{ssmMoveToPBComplete} \wedge \\ & \text{ssmConductORPComplete} \neq \text{ssmConductPBComplete} \wedge \\ & \text{ssmConductORPComplete} \neq \text{invalidOmniCommand} \wedge \\ & \text{ssmMoveToPBComplete} \neq \text{ssmConductPBComplete} \wedge \\ & \text{ssmMoveToPBComplete} \neq \text{invalidOmniCommand} \wedge \\ & \text{ssmConductPBComplete} \neq \text{invalidOmniCommand} \end{aligned}$$

[plCommand\_distinct\_clauses]

$$\begin{aligned} \vdash & \text{crossLD} \neq \text{conductORP} \wedge \text{crossLD} \neq \text{moveToPB} \wedge \\ & \text{crossLD} \neq \text{conductPB} \wedge \text{crossLD} \neq \text{completePB} \wedge \\ & \text{crossLD} \neq \text{incomplete} \wedge \text{conductORP} \neq \text{moveToPB} \wedge \\ & \text{conductORP} \neq \text{conductPB} \wedge \text{conductORP} \neq \text{completePB} \wedge \\ & \text{conductORP} \neq \text{incomplete} \wedge \text{moveToPB} \neq \text{conductPB} \wedge \\ & \text{moveToPB} \neq \text{completePB} \wedge \text{moveToPB} \neq \text{incomplete} \wedge \\ & \text{conductPB} \neq \text{completePB} \wedge \text{conductPB} \neq \text{incomplete} \wedge \\ & \text{completePB} \neq \text{incomplete} \end{aligned}$$

[slCommand\_distinct\_clauses]

$$\vdash \forall a' a. \text{PL } a \neq \text{OMNI } a'$$

[slCommand\_one\_one]

$$\begin{aligned} \vdash & (\forall a a'. (\text{PL } a = \text{PL } a') \iff (a = a')) \wedge \\ & \forall a a'. (\text{OMNI } a = \text{OMNI } a') \iff (a = a') \end{aligned}$$

[slOutput\_distinct\_clauses]

$$\begin{aligned} \vdash & \text{PlanPB} \neq \text{MoveToORP} \wedge \text{PlanPB} \neq \text{ConductORP} \wedge \\ & \text{PlanPB} \neq \text{MoveToPB} \wedge \text{PlanPB} \neq \text{ConductPB} \wedge \\ & \text{PlanPB} \neq \text{CompletePB} \wedge \text{PlanPB} \neq \text{unAuthenticated} \wedge \\ & \text{PlanPB} \neq \text{unAuthorized} \wedge \text{MoveToORP} \neq \text{ConductORP} \wedge \\ & \text{MoveToORP} \neq \text{MoveToPB} \wedge \text{MoveToORP} \neq \text{ConductPB} \wedge \\ & \text{MoveToORP} \neq \text{CompletePB} \wedge \text{MoveToORP} \neq \text{unAuthenticated} \wedge \end{aligned}$$

```

MoveToORP ≠ unauthorized ∧ ConductORP ≠ MoveToPB ∧
ConductORP ≠ ConductPB ∧ ConductORP ≠ CompletePB ∧
ConductORP ≠ unAuthenticated ∧ ConductORP ≠ unauthorized ∧
MoveToPB ≠ ConductPB ∧ MoveToPB ≠ CompletePB ∧
MoveToPB ≠ unAuthenticated ∧ MoveToPB ≠ unauthorized ∧
ConductPB ≠ CompletePB ∧ ConductPB ≠ unAuthenticated ∧
ConductPB ≠ unauthorized ∧ CompletePB ≠ unAuthenticated ∧
CompletePB ≠ unauthorized ∧ unAuthenticated ≠ unauthorized

```

[slState\_distinct\_clauses]

```

⊢ PLAN_PB ≠ MOVE_TO_ORP ∧ PLAN_PB ≠ CONDUCT_ORP ∧
  PLAN_PB ≠ MOVE_TO_PB ∧ PLAN_PB ≠ CONDUCT_PB ∧
  PLAN_PB ≠ COMPLETE_PB ∧ MOVE_TO_ORP ≠ CONDUCT_ORP ∧
  MOVE_TO_ORP ≠ MOVE_TO_PB ∧ MOVE_TO_ORP ≠ CONDUCT_PB ∧
  MOVE_TO_ORP ≠ COMPLETE_PB ∧ CONDUCT_ORP ≠ MOVE_TO_PB ∧
  CONDUCT_ORP ≠ CONDUCT_PB ∧ CONDUCT_ORP ≠ COMPLETE_PB ∧
  MOVE_TO_PB ≠ CONDUCT_PB ∧ MOVE_TO_PB ≠ COMPLETE_PB ∧
  CONDUCT_PB ≠ COMPLETE_PB

```

[stateRole\_distinct\_clauses]

```

⊢ PlatoonLeader ≠ Omni

```

## 7 PBIntegratedDef Theory

**Built:** 13 May 2018

**Parent Theories:** PBTypeIntegrated, aclfoundation

### 7.1 Definitions

[secAuthorization\_def]

```

⊢ ∀ xs. secAuthorization xs = secHelper (getOmniCommand xs)

```

[secHelper\_def]

```

⊢ ∀ cmd.
  secHelper cmd =
    [Name Omni controls prop (SOME (SLc (OMNI cmd)))]

```

### 7.2 Theorems

[getOmniCommand\_def]

```

⊢ (getOmniCommand [] = invalidOmniCommand) ∧
  (∀ xs cmd.
    getOmniCommand
      (Name Omni controls prop (SOME (SLc (OMNI cmd))))::xs =
      cmd) ∧
  (∀ xs. getOmniCommand (TT::xs) = getOmniCommand xs) ∧

```

---

```

(∀ xs. getOmniCommand (FF::xs) = getOmniCommand xs) ∧
(∀ xs v2. getOmniCommand (prop v2::xs) = getOmniCommand xs) ∧
(∀ xs v3. getOmniCommand (notf v3::xs) = getOmniCommand xs) ∧
(∀ xs v5 v4.
  getOmniCommand (v4 andf v5::xs) = getOmniCommand xs) ∧
(∀ xs v7 v6.
  getOmniCommand (v6 orf v7::xs) = getOmniCommand xs) ∧
(∀ xs v9 v8.
  getOmniCommand (v8 impf v9::xs) = getOmniCommand xs) ∧
(∀ xs v11 v10.
  getOmniCommand (v10 eqf v11::xs) = getOmniCommand xs) ∧
(∀ xs v13 v12.
  getOmniCommand (v12 says v13::xs) = getOmniCommand xs) ∧
(∀ xs v15 v14.
  getOmniCommand (v14 speaks_for v15::xs) =
  getOmniCommand xs) ∧
(∀ xs v16.
  getOmniCommand (v16 controls TT::xs) =
  getOmniCommand xs) ∧
(∀ xs v16.
  getOmniCommand (v16 controls FF::xs) =
  getOmniCommand xs) ∧
(∀ xs v134.
  getOmniCommand (Name v134 controls prop NONE::xs) =
  getOmniCommand xs) ∧
(∀ xs v144.
  getOmniCommand
    (Name PlatoonLeader controls prop (SOME v144)::xs) =
  getOmniCommand xs) ∧
(∀ xs v146.
  getOmniCommand
    (Name Omni controls prop (SOME (ESCc v146))::xs) =
  getOmniCommand xs) ∧
(∀ xs v150.
  getOmniCommand
    (Name Omni controls prop (SOME (SLc (PL v150)))::xs) =
  getOmniCommand xs) ∧
(∀ xs v68 v136 v135.
  getOmniCommand (v135 meet v136 controls prop v68::xs) =
  getOmniCommand xs) ∧
(∀ xs v68 v138 v137.
  getOmniCommand (v137 quoting v138 controls prop v68::xs) =
  getOmniCommand xs) ∧
(∀ xs v69 v16.
  getOmniCommand (v16 controls notf v69::xs) =
  getOmniCommand xs) ∧
(∀ xs v71 v70 v16.
  getOmniCommand (v16 controls (v70 andf v71)::xs) =
  getOmniCommand xs) ∧

```

---

---

```

(∀ xs v73 v72 v16.
  getOmniCommand (v16 controls (v72 orf v73)::xs) =
  getOmniCommand xs) ∧
(∀ xs v75 v74 v16.
  getOmniCommand (v16 controls (v74 impf v75)::xs) =
  getOmniCommand xs) ∧
(∀ xs v77 v76 v16.
  getOmniCommand (v16 controls (v76 eqf v77)::xs) =
  getOmniCommand xs) ∧
(∀ xs v79 v78 v16.
  getOmniCommand (v16 controls v78 says v79::xs) =
  getOmniCommand xs) ∧
(∀ xs v81 v80 v16.
  getOmniCommand (v16 controls v80 speaks_for v81::xs) =
  getOmniCommand xs) ∧
(∀ xs v83 v82 v16.
  getOmniCommand (v16 controls v82 controls v83::xs) =
  getOmniCommand xs) ∧
(∀ xs v86 v85 v84 v16.
  getOmniCommand (v16 controls reps v84 v85 v86::xs) =
  getOmniCommand xs) ∧
(∀ xs v88 v87 v16.
  getOmniCommand (v16 controls v87 domi v88::xs) =
  getOmniCommand xs) ∧
(∀ xs v90 v89 v16.
  getOmniCommand (v16 controls v89 eqi v90::xs) =
  getOmniCommand xs) ∧
(∀ xs v92 v91 v16.
  getOmniCommand (v16 controls v91 doms v92::xs) =
  getOmniCommand xs) ∧
(∀ xs v94 v93 v16.
  getOmniCommand (v16 controls v93 eqs v94::xs) =
  getOmniCommand xs) ∧
(∀ xs v96 v95 v16.
  getOmniCommand (v16 controls v95 eqn v96::xs) =
  getOmniCommand xs) ∧
(∀ xs v98 v97 v16.
  getOmniCommand (v16 controls v97 lte v98::xs) =
  getOmniCommand xs) ∧
(∀ xs v99 v16 v100.
  getOmniCommand (v16 controls v99 lt v100::xs) =
  getOmniCommand xs) ∧
(∀ xs v20 v19 v18.
  getOmniCommand (reps v18 v19 v20::xs) =
  getOmniCommand xs) ∧
(∀ xs v22 v21.
  getOmniCommand (v21 domi v22::xs) = getOmniCommand xs) ∧
(∀ xs v24 v23.
  getOmniCommand (v23 eqi v24::xs) = getOmniCommand xs) ∧

```

---

$(\forall xs \ v_{26} \ v_{25}.$   
 $\quad \text{getOmniCommand } (v_{25} \text{ doms } v_{26}::xs) = \text{getOmniCommand } xs) \wedge$   
 $(\forall xs \ v_{28} \ v_{27}.$   
 $\quad \text{getOmniCommand } (v_{27} \text{ eqs } v_{28}::xs) = \text{getOmniCommand } xs) \wedge$   
 $(\forall xs \ v_{30} \ v_{29}.$   
 $\quad \text{getOmniCommand } (v_{29} \text{ eqn } v_{30}::xs) = \text{getOmniCommand } xs) \wedge$   
 $(\forall xs \ v_{32} \ v_{31}.$   
 $\quad \text{getOmniCommand } (v_{31} \text{ lte } v_{32}::xs) = \text{getOmniCommand } xs) \wedge$   
 $\forall xs \ v_{34} \ v_{33}.$   
 $\quad \text{getOmniCommand } (v_{33} \text{ lt } v_{34}::xs) = \text{getOmniCommand } xs$

[getOmniCommand\_ind]

$\vdash \forall P.$   
 $\quad P \ \square \ \wedge$   
 $\quad (\forall cmd \ xs.$   
 $\quad \quad P$   
 $\quad \quad (\text{Name Omni controls prop (SOME (SLc (OMNI cmd))))}::$   
 $\quad \quad \quad xs)) \wedge (\forall xs. P \ xs \Rightarrow P \ (\text{TT}::xs)) \wedge$   
 $\quad (\forall xs. P \ xs \Rightarrow P \ (\text{FF}::xs)) \wedge$   
 $\quad (\forall v_2 \ xs. P \ xs \Rightarrow P \ (\text{prop } v_2::xs)) \wedge$   
 $\quad (\forall v_3 \ xs. P \ xs \Rightarrow P \ (\text{notf } v_3::xs)) \wedge$   
 $\quad (\forall v_4 \ v_5 \ xs. P \ xs \Rightarrow P \ (v_4 \ \text{andf } v_5::xs)) \wedge$   
 $\quad (\forall v_6 \ v_7 \ xs. P \ xs \Rightarrow P \ (v_6 \ \text{orf } v_7::xs)) \wedge$   
 $\quad (\forall v_8 \ v_9 \ xs. P \ xs \Rightarrow P \ (v_8 \ \text{impf } v_9::xs)) \wedge$   
 $\quad (\forall v_{10} \ v_{11} \ xs. P \ xs \Rightarrow P \ (v_{10} \ \text{eqf } v_{11}::xs)) \wedge$   
 $\quad (\forall v_{12} \ v_{13} \ xs. P \ xs \Rightarrow P \ (v_{12} \ \text{says } v_{13}::xs)) \wedge$   
 $\quad (\forall v_{14} \ v_{15} \ xs. P \ xs \Rightarrow P \ (v_{14} \ \text{speaks\_for } v_{15}::xs)) \wedge$   
 $\quad (\forall v_{16} \ xs. P \ xs \Rightarrow P \ (v_{16} \ \text{controls TT}::xs)) \wedge$   
 $\quad (\forall v_{16} \ xs. P \ xs \Rightarrow P \ (v_{16} \ \text{controls FF}::xs)) \wedge$   
 $\quad (\forall v_{134} \ xs. P \ xs \Rightarrow P \ (\text{Name } v_{134} \ \text{controls prop NONE}::xs)) \wedge$   
 $\quad (\forall v_{144} \ xs.$   
 $\quad \quad P \ xs \Rightarrow$   
 $\quad \quad P \ (\text{Name PlatoonLeader controls prop (SOME } v_{144})::xs)) \wedge$   
 $\quad (\forall v_{146} \ xs.$   
 $\quad \quad P \ xs \Rightarrow$   
 $\quad \quad P \ (\text{Name Omni controls prop (SOME (ESCc } v_{146}))::xs)) \wedge$   
 $\quad (\forall v_{150} \ xs.$   
 $\quad \quad P \ xs \Rightarrow$   
 $\quad \quad P$   
 $\quad \quad (\text{Name Omni controls prop (SOME (SLc (PL } v_{150}))))::$   
 $\quad \quad \quad xs)) \wedge$   
 $\quad (\forall v_{135} \ v_{136} \ v_{68} \ xs.$   
 $\quad \quad P \ xs \Rightarrow P \ (v_{135} \ \text{meet } v_{136} \ \text{controls prop } v_{68}::xs)) \wedge$   
 $\quad (\forall v_{137} \ v_{138} \ v_{68} \ xs.$   
 $\quad \quad P \ xs \Rightarrow P \ (v_{137} \ \text{quoting } v_{138} \ \text{controls prop } v_{68}::xs)) \wedge$   
 $\quad (\forall v_{16} \ v_{69} \ xs. P \ xs \Rightarrow P \ (v_{16} \ \text{controls notf } v_{69}::xs)) \wedge$   
 $\quad (\forall v_{16} \ v_{70} \ v_{71} \ xs.$   
 $\quad \quad P \ xs \Rightarrow P \ (v_{16} \ \text{controls } (v_{70} \ \text{andf } v_{71})::xs)) \wedge$   
 $\quad (\forall v_{16} \ v_{72} \ v_{73} \ xs.$

$$\begin{aligned}
& P \text{ } xs \Rightarrow P \text{ } (v_{16} \text{ controls } (v_{72} \text{ orf } v_{73})::xs)) \wedge \\
& (\forall v_{16} \text{ } v_{74} \text{ } v_{75} \text{ } xs. \\
& \quad P \text{ } xs \Rightarrow P \text{ } (v_{16} \text{ controls } (v_{74} \text{ impf } v_{75})::xs)) \wedge \\
& (\forall v_{16} \text{ } v_{76} \text{ } v_{77} \text{ } xs. \\
& \quad P \text{ } xs \Rightarrow P \text{ } (v_{16} \text{ controls } (v_{76} \text{ eqf } v_{77})::xs)) \wedge \\
& (\forall v_{16} \text{ } v_{78} \text{ } v_{79} \text{ } xs. \\
& \quad P \text{ } xs \Rightarrow P \text{ } (v_{16} \text{ controls } v_{78} \text{ says } v_{79}::xs)) \wedge \\
& (\forall v_{16} \text{ } v_{80} \text{ } v_{81} \text{ } xs. \\
& \quad P \text{ } xs \Rightarrow P \text{ } (v_{16} \text{ controls } v_{80} \text{ speaks\_for } v_{81}::xs)) \wedge \\
& (\forall v_{16} \text{ } v_{82} \text{ } v_{83} \text{ } xs. \\
& \quad P \text{ } xs \Rightarrow P \text{ } (v_{16} \text{ controls } v_{82} \text{ controls } v_{83}::xs)) \wedge \\
& (\forall v_{16} \text{ } v_{84} \text{ } v_{85} \text{ } v_{86} \text{ } xs. \\
& \quad P \text{ } xs \Rightarrow P \text{ } (v_{16} \text{ controls reps } v_{84} \text{ } v_{85} \text{ } v_{86}::xs)) \wedge \\
& (\forall v_{16} \text{ } v_{87} \text{ } v_{88} \text{ } xs. \\
& \quad P \text{ } xs \Rightarrow P \text{ } (v_{16} \text{ controls } v_{87} \text{ domi } v_{88}::xs)) \wedge \\
& (\forall v_{16} \text{ } v_{89} \text{ } v_{90} \text{ } xs. \\
& \quad P \text{ } xs \Rightarrow P \text{ } (v_{16} \text{ controls } v_{89} \text{ eqi } v_{90}::xs)) \wedge \\
& (\forall v_{16} \text{ } v_{91} \text{ } v_{92} \text{ } xs. \\
& \quad P \text{ } xs \Rightarrow P \text{ } (v_{16} \text{ controls } v_{91} \text{ doms } v_{92}::xs)) \wedge \\
& (\forall v_{16} \text{ } v_{93} \text{ } v_{94} \text{ } xs. \\
& \quad P \text{ } xs \Rightarrow P \text{ } (v_{16} \text{ controls } v_{93} \text{ eqs } v_{94}::xs)) \wedge \\
& (\forall v_{16} \text{ } v_{95} \text{ } v_{96} \text{ } xs. \\
& \quad P \text{ } xs \Rightarrow P \text{ } (v_{16} \text{ controls } v_{95} \text{ eqn } v_{96}::xs)) \wedge \\
& (\forall v_{16} \text{ } v_{97} \text{ } v_{98} \text{ } xs. \\
& \quad P \text{ } xs \Rightarrow P \text{ } (v_{16} \text{ controls } v_{97} \text{ lte } v_{98}::xs)) \wedge \\
& (\forall v_{16} \text{ } v_{99} \text{ } v_{100} \text{ } xs. \\
& \quad P \text{ } xs \Rightarrow P \text{ } (v_{16} \text{ controls } v_{99} \text{ lt } v_{100}::xs)) \wedge \\
& (\forall v_{18} \text{ } v_{19} \text{ } v_{20} \text{ } xs. P \text{ } xs \Rightarrow P \text{ } (\text{reps } v_{18} \text{ } v_{19} \text{ } v_{20}::xs)) \wedge \\
& (\forall v_{21} \text{ } v_{22} \text{ } xs. P \text{ } xs \Rightarrow P \text{ } (v_{21} \text{ domi } v_{22}::xs)) \wedge \\
& (\forall v_{23} \text{ } v_{24} \text{ } xs. P \text{ } xs \Rightarrow P \text{ } (v_{23} \text{ eqi } v_{24}::xs)) \wedge \\
& (\forall v_{25} \text{ } v_{26} \text{ } xs. P \text{ } xs \Rightarrow P \text{ } (v_{25} \text{ doms } v_{26}::xs)) \wedge \\
& (\forall v_{27} \text{ } v_{28} \text{ } xs. P \text{ } xs \Rightarrow P \text{ } (v_{27} \text{ eqs } v_{28}::xs)) \wedge \\
& (\forall v_{29} \text{ } v_{30} \text{ } xs. P \text{ } xs \Rightarrow P \text{ } (v_{29} \text{ eqn } v_{30}::xs)) \wedge \\
& (\forall v_{31} \text{ } v_{32} \text{ } xs. P \text{ } xs \Rightarrow P \text{ } (v_{31} \text{ lte } v_{32}::xs)) \wedge \\
& (\forall v_{33} \text{ } v_{34} \text{ } xs. P \text{ } xs \Rightarrow P \text{ } (v_{33} \text{ lt } v_{34}::xs)) \Rightarrow \\
& \forall v. P \text{ } v
\end{aligned}$$

[secContext\_def]

$$\begin{aligned}
& \vdash (\text{secContext PLAN\_PB } (x::xs) = \\
& \quad [\text{prop } (\text{SOME } (\text{SLc } (\text{OMNI ssmPlanPBComplete}))) \text{ impf } \\
& \quad \text{Name PlatoonLeader controls} \\
& \quad \text{prop } (\text{SOME } (\text{SLc } (\text{PL crossLD})))]) \wedge \\
& (\text{secContext MOVE\_TO\_ORP } (x::xs) = \\
& \quad [\text{prop } (\text{SOME } (\text{SLc } (\text{OMNI ssmMoveToORPComplete}))) \text{ impf } \\
& \quad \text{Name PlatoonLeader controls} \\
& \quad \text{prop } (\text{SOME } (\text{SLc } (\text{PL conductORP})))]) \wedge \\
& (\text{secContext CONDUCT\_ORP } (x::xs) = \\
& \quad [\text{prop } (\text{SOME } (\text{SLc } (\text{OMNI ssmConductORPComplete}))) \text{ impf } \\
& \quad \text{Name PlatoonLeader controls}
\end{aligned}$$

```

    prop (SOME (SLc (PL moveToPB)))))) ∧
(secContext MOVE_TO_PB (x::xs) =
  [prop (SOME (SLc (OMNI ssmMoveToPBComplete))) impf
    Name PlatoonLeader controls
    prop (SOME (SLc (PL conductPB)))))) ∧
(secContext CONDUCT_PB (x::xs) =
  [prop (SOME (SLc (OMNI ssmConductPBComplete))) impf
    Name PlatoonLeader controls
    prop (SOME (SLc (PL completePB))))])

```

[secContext\_ind]

```

⊢ ∀ P.
  (∀ x xs. P PLAN_PB (x::xs)) ∧
  (∀ x xs. P MOVE_TO_ORP (x::xs)) ∧
  (∀ x xs. P CONDUCT_ORP (x::xs)) ∧
  (∀ x xs. P MOVE_TO_PB (x::xs)) ∧
  (∀ x xs. P CONDUCT_PB (x::xs)) ∧ (∀ v4. P v4 []) ∧
  (∀ v5 v6. P COMPLETE_PB (v5::v6)) ⇒
  ∀ v v1. P v v1

```

## 8 ssmConductORP Theory

**Built:** 13 May 2018

**Parent Theories:** ConductORPType, ssm11, OMNITYPE

### 8.1 Definitions

[secContextConductORP\_def]

```

⊢ ∀ plcnd psgcmd incomplete.
  secContextConductORP plcnd psgcmd incomplete =
  [Name PlatoonLeader controls prop (SOME (SLc (PL plcnd)));
   Name PlatoonSergeant controls
   prop (SOME (SLc (PSG psgcmd)));
   Name PlatoonLeader says
   prop (SOME (SLc (PSG psgcmd))) impf prop NONE;
   Name PlatoonSergeant says
   prop (SOME (SLc (PL plcnd))) impf prop NONE]

```

[ssmConductORPStateInterp\_def]

```

⊢ ∀ slState. ssmConductORPStateInterp slState = TT

```

### 8.2 Theorems

[authTestConductORP\_cmd\_reject\_lemma]

```

⊢ ∀ cmd. ¬authTestConductORP (prop (SOME cmd))

```

[authTestConductORP\_def]

$$\begin{aligned}
&\vdash (\text{authTestConductORP } (\text{Name PlatoonLeader says prop } cmd) \iff \\
&\quad T) \wedge \\
&(\text{authTestConductORP } (\text{Name PlatoonSergeant says prop } cmd) \iff \\
&\quad T) \wedge (\text{authTestConductORP } TT \iff F) \wedge \\
&(\text{authTestConductORP } FF \iff F) \wedge \\
&(\text{authTestConductORP } (\text{prop } v) \iff F) \wedge \\
&(\text{authTestConductORP } (\text{notf } v_1) \iff F) \wedge \\
&(\text{authTestConductORP } (v_2 \text{ andf } v_3) \iff F) \wedge \\
&(\text{authTestConductORP } (v_4 \text{ orf } v_5) \iff F) \wedge \\
&(\text{authTestConductORP } (v_6 \text{ impf } v_7) \iff F) \wedge \\
&(\text{authTestConductORP } (v_8 \text{ eqf } v_9) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } TT) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } FF) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{133} \text{ meet } v_{134} \text{ says prop } v_{66}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{135} \text{ quoting } v_{136} \text{ says prop } v_{66}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says notf } v_{67}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } (v_{68} \text{ andf } v_{69})) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } (v_{70} \text{ orf } v_{71})) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } (v_{72} \text{ impf } v_{73})) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } (v_{74} \text{ eqf } v_{75})) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } v_{76} \text{ says } v_{77}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } v_{78} \text{ speaks\_for } v_{79}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } v_{80} \text{ controls } v_{81}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says reps } v_{82} \ v_{83} \ v_{84}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } v_{85} \text{ domi } v_{86}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } v_{87} \text{ eqi } v_{88}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } v_{89} \text{ doms } v_{90}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } v_{91} \text{ eqs } v_{92}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } v_{93} \text{ eqn } v_{94}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } v_{95} \text{ lte } v_{96}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{10} \text{ says } v_{97} \text{ lt } v_{98}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{12} \text{ speaks\_for } v_{13}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{14} \text{ controls } v_{15}) \iff F) \wedge \\
&(\text{authTestConductORP } (\text{reps } v_{16} \ v_{17} \ v_{18}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{19} \text{ domi } v_{20}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{21} \text{ eqi } v_{22}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{23} \text{ doms } v_{24}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{25} \text{ eqs } v_{26}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{27} \text{ eqn } v_{28}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{29} \text{ lte } v_{30}) \iff F) \wedge \\
&(\text{authTestConductORP } (v_{31} \text{ lt } v_{32}) \iff F)
\end{aligned}$$

[authTestConductORP\_ind]

$$\begin{aligned}
&\vdash \forall P. \\
&\quad (\forall cmd. P (\text{Name PlatoonLeader says prop } cmd)) \wedge \\
&\quad (\forall cmd. P (\text{Name PlatoonSergeant says prop } cmd)) \wedge P \ TT \wedge \\
&\quad P \ FF \wedge (\forall v. P (\text{prop } v)) \wedge (\forall v_1. P (\text{notf } v_1)) \wedge \\
&\quad (\forall v_2 \ v_3. P (v_2 \text{ andf } v_3)) \wedge (\forall v_4 \ v_5. P (v_4 \text{ orf } v_5)) \wedge
\end{aligned}$$



$$\begin{aligned}
& (\forall v_6 v_7. P (v_6 \text{ impf } v_7)) \wedge (\forall v_8 v_9. P (v_8 \text{ eqf } v_9)) \wedge \\
& (\forall v_{10}. P (v_{10} \text{ says TT})) \wedge (\forall v_{10}. P (v_{10} \text{ says FF})) \wedge \\
& (\forall v_{133} v_{134} v_{66}. P (v_{133} \text{ meet } v_{134} \text{ says prop } v_{66})) \wedge \\
& (\forall v_{135} v_{136} v_{66}. P (v_{135} \text{ quoting } v_{136} \text{ says prop } v_{66})) \wedge \\
& (\forall v_{10} v_{67}. P (v_{10} \text{ says notf } v_{67})) \wedge \\
& (\forall v_{10} v_{68} v_{69}. P (v_{10} \text{ says } (v_{68} \text{ andf } v_{69}))) \wedge \\
& (\forall v_{10} v_{70} v_{71}. P (v_{10} \text{ says } (v_{70} \text{ orf } v_{71}))) \wedge \\
& (\forall v_{10} v_{72} v_{73}. P (v_{10} \text{ says } (v_{72} \text{ impf } v_{73}))) \wedge \\
& (\forall v_{10} v_{74} v_{75}. P (v_{10} \text{ says } (v_{74} \text{ eqf } v_{75}))) \wedge \\
& (\forall v_{10} v_{76} v_{77}. P (v_{10} \text{ says } v_{76} \text{ says } v_{77})) \wedge \\
& (\forall v_{10} v_{78} v_{79}. P (v_{10} \text{ says } v_{78} \text{ speaks\_for } v_{79})) \wedge \\
& (\forall v_{10} v_{80} v_{81}. P (v_{10} \text{ says } v_{80} \text{ controls } v_{81})) \wedge \\
& (\forall v_{10} v_{82} v_{83} v_{84}. P (v_{10} \text{ says reps } v_{82} v_{83} v_{84})) \wedge \\
& (\forall v_{10} v_{85} v_{86}. P (v_{10} \text{ says } v_{85} \text{ domi } v_{86})) \wedge \\
& (\forall v_{10} v_{87} v_{88}. P (v_{10} \text{ says } v_{87} \text{ eqi } v_{88})) \wedge \\
& (\forall v_{10} v_{89} v_{90}. P (v_{10} \text{ says } v_{89} \text{ doms } v_{90})) \wedge \\
& (\forall v_{10} v_{91} v_{92}. P (v_{10} \text{ says } v_{91} \text{ eqs } v_{92})) \wedge \\
& (\forall v_{10} v_{93} v_{94}. P (v_{10} \text{ says } v_{93} \text{ eqn } v_{94})) \wedge \\
& (\forall v_{10} v_{95} v_{96}. P (v_{10} \text{ says } v_{95} \text{ lte } v_{96})) \wedge \\
& (\forall v_{10} v_{97} v_{98}. P (v_{10} \text{ says } v_{97} \text{ lt } v_{98})) \wedge \\
& (\forall v_{12} v_{13}. P (v_{12} \text{ speaks\_for } v_{13})) \wedge \\
& (\forall v_{14} v_{15}. P (v_{14} \text{ controls } v_{15})) \wedge \\
& (\forall v_{16} v_{17} v_{18}. P (\text{reps } v_{16} v_{17} v_{18})) \wedge \\
& (\forall v_{19} v_{20}. P (v_{19} \text{ domi } v_{20})) \wedge \\
& (\forall v_{21} v_{22}. P (v_{21} \text{ eqi } v_{22})) \wedge \\
& (\forall v_{23} v_{24}. P (v_{23} \text{ doms } v_{24})) \wedge \\
& (\forall v_{25} v_{26}. P (v_{25} \text{ eqs } v_{26})) \wedge (\forall v_{27} v_{28}. P (v_{27} \text{ eqn } v_{28})) \wedge \\
& (\forall v_{29} v_{30}. P (v_{29} \text{ lte } v_{30})) \wedge (\forall v_{31} v_{32}. P (v_{31} \text{ lt } v_{32})) \Rightarrow \\
& \forall v. P v
\end{aligned}$$

[conductORPNS\_def]

$$\begin{aligned}
& \vdash (\text{conductORPNS CONDUCT_ORP (exec (PL secure))} = \text{SECURE}) \wedge \\
& (\text{conductORPNS CONDUCT_ORP (exec (PL plIncomplete))} = \\
& \quad \text{CONDUCT_ORP}) \wedge \\
& (\text{conductORPNS SECURE (exec (PSG actionsIn))} = \text{ACTIONS\_IN}) \wedge \\
& (\text{conductORPNS SECURE (exec (PSG psgIncomplete))} = \text{SECURE}) \wedge \\
& (\text{conductORPNS ACTIONS\_IN (exec (PL withdraw))} = \text{WITHDRAW}) \wedge \\
& (\text{conductORPNS ACTIONS\_IN (exec (PL plIncomplete))} = \\
& \quad \text{ACTIONS\_IN}) \wedge \\
& (\text{conductORPNS WITHDRAW (exec (PL complete))} = \text{COMPLETE}) \wedge \\
& (\text{conductORPNS WITHDRAW (exec (PL plIncomplete))} = \text{WITHDRAW}) \wedge \\
& (\text{conductORPNS } s \text{ (trap (PL cmd'))} = s) \wedge \\
& (\text{conductORPNS } s \text{ (trap (PSG cmd))} = s) \wedge \\
& (\text{conductORPNS } s \text{ (discard (PL cmd'))} = s) \wedge \\
& (\text{conductORPNS } s \text{ (discard (PSG cmd))} = s)
\end{aligned}$$

[conductORPNS\_ind]

$$\begin{aligned}
& \vdash \forall P. \\
& \quad P \text{ CONDUCT\_ORP (exec (PL secure))} \wedge
\end{aligned}$$

$P \text{ CONDUCT\_ORP (exec (PL plIncomplete))} \wedge$   
 $P \text{ SECURE (exec (PSG actionsIn))} \wedge$   
 $P \text{ SECURE (exec (PSG psgIncomplete))} \wedge$   
 $P \text{ ACTIONS\_IN (exec (PL withdraw))} \wedge$   
 $P \text{ ACTIONS\_IN (exec (PL plIncomplete))} \wedge$   
 $P \text{ WITHDRAW (exec (PL complete))} \wedge$   
 $P \text{ WITHDRAW (exec (PL plIncomplete))} \wedge$   
 $(\forall s \text{ cmd. } P \text{ s (trap (PL cmd))}) \wedge$   
 $(\forall s \text{ cmd. } P \text{ s (trap (PSG cmd))}) \wedge$   
 $(\forall s \text{ cmd. } P \text{ s (discard (PL cmd))}) \wedge$   
 $(\forall s \text{ cmd. } P \text{ s (discard (PSG cmd))}) \wedge$   
 $P \text{ CONDUCT\_ORP (exec (PL withdraw))} \wedge$   
 $P \text{ CONDUCT\_ORP (exec (PL complete))} \wedge$   
 $(\forall v_{11}. P \text{ CONDUCT\_ORP (exec (PSG } v_{11})) \wedge$   
 $(\forall v_{13}. P \text{ SECURE (exec (PL } v_{13})) \wedge$   
 $P \text{ ACTIONS\_IN (exec (PL secure))} \wedge$   
 $P \text{ ACTIONS\_IN (exec (PL complete))} \wedge$   
 $(\forall v_{17}. P \text{ ACTIONS\_IN (exec (PSG } v_{17})) \wedge$   
 $P \text{ WITHDRAW (exec (PL secure))} \wedge$   
 $P \text{ WITHDRAW (exec (PL withdraw))} \wedge$   
 $(\forall v_{20}. P \text{ WITHDRAW (exec (PSG } v_{20})) \wedge$   
 $(\forall v_{21}. P \text{ COMPLETE (exec } v_{21})) \Rightarrow$   
 $\forall v \text{ v}_1. P \text{ v v}_1$

#### [conductORPOut\_def]

$\vdash (\text{conductORPOut CONDUCT\_ORP (exec (PL secure))} = \text{Secure}) \wedge$   
 $(\text{conductORPOut CONDUCT\_ORP (exec (PL plIncomplete))} =$   
 $\text{ConductORP}) \wedge$   
 $(\text{conductORPOut SECURE (exec (PSG actionsIn))} = \text{ActionsIn}) \wedge$   
 $(\text{conductORPOut SECURE (exec (PSG psgIncomplete))} = \text{Secure}) \wedge$   
 $(\text{conductORPOut ACTIONS\_IN (exec (PL withdraw))} = \text{Withdraw}) \wedge$   
 $(\text{conductORPOut ACTIONS\_IN (exec (PL plIncomplete))} =$   
 $\text{ActionsIn}) \wedge$   
 $(\text{conductORPOut WITHDRAW (exec (PL complete))} = \text{Complete}) \wedge$   
 $(\text{conductORPOut WITHDRAW (exec (PL plIncomplete))} =$   
 $\text{Withdraw}) \wedge$   
 $(\text{conductORPOut s (trap (PL cmd'))} = \text{unAuthorized}) \wedge$   
 $(\text{conductORPOut s (trap (PSG cmd))} = \text{unAuthorized}) \wedge$   
 $(\text{conductORPOut s (discard (PL cmd'))} = \text{unAuthenticated}) \wedge$   
 $(\text{conductORPOut s (discard (PSG cmd))} = \text{unAuthenticated})$

#### [conductORPOut\_ind]

$\vdash \forall P.$   
 $P \text{ CONDUCT\_ORP (exec (PL secure))} \wedge$   
 $P \text{ CONDUCT\_ORP (exec (PL plIncomplete))} \wedge$   
 $P \text{ SECURE (exec (PSG actionsIn))} \wedge$   
 $P \text{ SECURE (exec (PSG psgIncomplete))} \wedge$   
 $P \text{ ACTIONS\_IN (exec (PL withdraw))} \wedge$   
 $P \text{ ACTIONS\_IN (exec (PL plIncomplete))} \wedge$

$$\begin{aligned}
& P \text{ WITHDRAW } (\text{exec } (\text{PL complete})) \wedge \\
& P \text{ WITHDRAW } (\text{exec } (\text{PL plIncomplete})) \wedge \\
& (\forall s \text{ cmd. } P \ s \ (\text{trap } (\text{PL cmd}))) \wedge \\
& (\forall s \text{ cmd. } P \ s \ (\text{trap } (\text{PSG cmd}))) \wedge \\
& (\forall s \text{ cmd. } P \ s \ (\text{discard } (\text{PL cmd}))) \wedge \\
& (\forall s \text{ cmd. } P \ s \ (\text{discard } (\text{PSG cmd}))) \wedge \\
& P \text{ CONDUCT\_ORP } (\text{exec } (\text{PL withdraw})) \wedge \\
& P \text{ CONDUCT\_ORP } (\text{exec } (\text{PL complete})) \wedge \\
& (\forall v_{11}. P \text{ CONDUCT\_ORP } (\text{exec } (\text{PSG } v_{11}))) \wedge \\
& (\forall v_{13}. P \text{ SECURE } (\text{exec } (\text{PL } v_{13}))) \wedge \\
& P \text{ ACTIONS\_IN } (\text{exec } (\text{PL secure})) \wedge \\
& P \text{ ACTIONS\_IN } (\text{exec } (\text{PL complete})) \wedge \\
& (\forall v_{17}. P \text{ ACTIONS\_IN } (\text{exec } (\text{PSG } v_{17}))) \wedge \\
& P \text{ WITHDRAW } (\text{exec } (\text{PL secure})) \wedge \\
& P \text{ WITHDRAW } (\text{exec } (\text{PL withdraw})) \wedge \\
& (\forall v_{20}. P \text{ WITHDRAW } (\text{exec } (\text{PSG } v_{20}))) \wedge \\
& (\forall v_{21}. P \text{ COMPLETE } (\text{exec } v_{21})) \Rightarrow \\
& \forall v \ v_1. P \ v \ v_1
\end{aligned}$$

[PlatoonLeader\_exec\_plCommand\_justified\_thm]

$$\begin{aligned}
& \vdash \forall NS \text{ Out } M \ Oi \ Os. \\
& \text{TR } (M, Oi, Os) \ (\text{exec } (\text{SLc } (\text{PL } plCommand))) \\
& \quad (\text{CFG authTestConductORP ssmConductORPStateInterp} \\
& \quad \quad (\text{secContextConductORP } plCommand \ psgCommand \ incomplete) \\
& \quad \quad (\text{Name PlatoonLeader says} \\
& \quad \quad \quad \text{prop } (\text{SOME } (\text{SLc } (\text{PL } plCommand)))::ins) \ s \ outs) \\
& \quad \quad (\text{CFG authTestConductORP ssmConductORPStateInterp} \\
& \quad \quad \quad (\text{secContextConductORP } plCommand \ psgCommand \ incomplete) \\
& \quad \quad \quad ins \ (NS \ s \ (\text{exec } (\text{SLc } (\text{PL } plCommand)))) \\
& \quad \quad \quad (\text{Out } s \ (\text{exec } (\text{SLc } (\text{PL } plCommand)))::outs)) \iff \\
& \text{authTestConductORP} \\
& \quad (\text{Name PlatoonLeader says} \\
& \quad \quad \text{prop } (\text{SOME } (\text{SLc } (\text{PL } plCommand)))) \wedge \\
& \text{CFGInterpret } (M, Oi, Os) \\
& \quad (\text{CFG authTestConductORP ssmConductORPStateInterp} \\
& \quad \quad (\text{secContextConductORP } plCommand \ psgCommand \ incomplete) \\
& \quad \quad (\text{Name PlatoonLeader says} \\
& \quad \quad \quad \text{prop } (\text{SOME } (\text{SLc } (\text{PL } plCommand)))::ins) \ s \ outs) \wedge \\
& \quad (M, Oi, Os) \text{ sat } \text{prop } (\text{SOME } (\text{SLc } (\text{PL } plCommand)))
\end{aligned}$$

[PlatoonLeader\_plCommand\_lemma]

$$\begin{aligned}
& \vdash \text{CFGInterpret } (M, Oi, Os) \\
& \quad (\text{CFG authTestConductORP ssmConductORPStateInterp} \\
& \quad \quad (\text{secContextConductORP } plCommand \ psgCommand \ incomplete) \\
& \quad \quad (\text{Name PlatoonLeader says} \\
& \quad \quad \quad \text{prop } (\text{SOME } (\text{SLc } (\text{PL } plCommand)))::ins) \ s \ outs) \Rightarrow \\
& \quad (M, Oi, Os) \text{ sat } \text{prop } (\text{SOME } (\text{SLc } (\text{PL } plCommand)))
\end{aligned}$$

[PlatoonSergeant\_exec\_psgCommand\_justified\_thm]

```

⊢ ∀ NS Out M Oi Os.
  TR (M, Oi, Os) (exec (SLc (PSG psgCommand)))
    (CFG authTestConductORP ssmConductORPStateInterp
      (secContextConductORP plCommand psgCommand incomplete)
      (Name PlatoonSergeant says
        prop (SOME (SLc (PSG psgCommand)))::ins) s outs)
    (CFG authTestConductORP ssmConductORPStateInterp
      (secContextConductORP plCommand psgCommand incomplete)
      ins (NS s (exec (SLc (PSG psgCommand))))
      (Out s (exec (SLc (PSG psgCommand)))::outs)) ⇔⇒
  authTestConductORP
    (Name PlatoonSergeant says
      prop (SOME (SLc (PSG psgCommand)))) ∧
  CFGInterpret (M, Oi, Os)
    (CFG authTestConductORP ssmConductORPStateInterp
      (secContextConductORP plCommand psgCommand incomplete)
      (Name PlatoonSergeant says
        prop (SOME (SLc (PSG psgCommand)))::ins) s outs) ∧
    (M, Oi, Os) sat prop (SOME (SLc (PSG psgCommand)))

```

[PlatoonSergeant\_psgCommand\_lemma]

```

⊢ CFGInterpret (M, Oi, Os)
  (CFG authTestConductORP ssmConductORPStateInterp
    (secContextConductORP plCommand psgCommand incomplete)
    (Name PlatoonSergeant says
      prop (SOME (SLc (PSG psgCommand)))::ins) s outs) ⇒
  (M, Oi, Os) sat prop (SOME (SLc (PSG psgCommand)))

```

## 9 ConductORPType Theory

**Built:** 13 May 2018

**Parent Theories:** indexedLists, patternMatches

### 9.1 Datatypes

```

plCommand = secure | withdraw | complete | plIncomplete
psgCommand = actionsIn | psgIncomplete
slCommand =
  PL ConductORPType$plCommand
  | PSG ConductORPType$psgCommand
slOutput = ConductORP | Secure | ActionsIn | Withdraw | Complete
           | unAuthenticated | unAuthorized
slState = CONDUCT_ORP | SECURE | ACTIONS_IN | WITHDRAW
          | COMPLETE
stateRole = PlatoonLeader | PlatoonSergeant

```

## 9.2 Theorems

[plCommand\_distinct\_clauses]

$$\vdash \text{secure} \neq \text{withdraw} \wedge \text{secure} \neq \text{complete} \wedge \\ \text{secure} \neq \text{plIncomplete} \wedge \text{withdraw} \neq \text{complete} \wedge \\ \text{withdraw} \neq \text{plIncomplete} \wedge \text{complete} \neq \text{plIncomplete}$$

[psgCommand\_distinct\_clauses]

$$\vdash \text{actionsIn} \neq \text{psgIncomplete}$$

[slCommand\_distinct\_clauses]

$$\vdash \forall a' a. \text{PL } a \neq \text{PSG } a'$$

[slCommand\_one\_one]

$$\vdash (\forall a a'. (\text{PL } a = \text{PL } a') \iff (a = a')) \wedge \\ \forall a a'. (\text{PSG } a = \text{PSG } a') \iff (a = a')$$

[slOutput\_distinct\_clauses]

$$\vdash \text{ConductORP} \neq \text{Secure} \wedge \text{ConductORP} \neq \text{ActionsIn} \wedge \\ \text{ConductORP} \neq \text{Withdraw} \wedge \text{ConductORP} \neq \text{Complete} \wedge \\ \text{ConductORP} \neq \text{unAuthenticated} \wedge \text{ConductORP} \neq \text{unAuthorized} \wedge \\ \text{Secure} \neq \text{ActionsIn} \wedge \text{Secure} \neq \text{Withdraw} \wedge \text{Secure} \neq \text{Complete} \wedge \\ \text{Secure} \neq \text{unAuthenticated} \wedge \text{Secure} \neq \text{unAuthorized} \wedge \\ \text{ActionsIn} \neq \text{Withdraw} \wedge \text{ActionsIn} \neq \text{Complete} \wedge \\ \text{ActionsIn} \neq \text{unAuthenticated} \wedge \text{ActionsIn} \neq \text{unAuthorized} \wedge \\ \text{Withdraw} \neq \text{Complete} \wedge \text{Withdraw} \neq \text{unAuthenticated} \wedge \\ \text{Withdraw} \neq \text{unAuthorized} \wedge \text{Complete} \neq \text{unAuthenticated} \wedge \\ \text{Complete} \neq \text{unAuthorized} \wedge \text{unAuthenticated} \neq \text{unAuthorized}$$

[slRole\_distinct\_clauses]

$$\vdash \text{PlatoonLeader} \neq \text{PlatoonSergeant}$$

[slState\_distinct\_clauses]

$$\vdash \text{CONDUCT\_ORP} \neq \text{SECURE} \wedge \text{CONDUCT\_ORP} \neq \text{ACTIONS\_IN} \wedge \\ \text{CONDUCT\_ORP} \neq \text{WITHDRAW} \wedge \text{CONDUCT\_ORP} \neq \text{COMPLETE} \wedge \\ \text{SECURE} \neq \text{ACTIONS\_IN} \wedge \text{SECURE} \neq \text{WITHDRAW} \wedge \text{SECURE} \neq \text{COMPLETE} \wedge \\ \text{ACTIONS\_IN} \neq \text{WITHDRAW} \wedge \text{ACTIONS\_IN} \neq \text{COMPLETE} \wedge \\ \text{WITHDRAW} \neq \text{COMPLETE}$$

## 10 ssmConductPB Theory

**Built:** 13 May 2018

**Parent Theories:** ConductPBType, ssm11, OMNIType

## 10.1 Definitions

[secContextConductPB\_def]

```

⊢ ∀ plcmd psgcmd incomplete.
  secContextConductPB plcmd psgcmd incomplete =
  [Name PlatoonLeader controls prop (SOME (SLc (PL plcmd)))];
  Name PlatoonSergeant controls
  prop (SOME (SLc (PSG psgcmd)));
  Name PlatoonLeader says
  prop (SOME (SLc (PSG psgcmd))) impf prop NONE;
  Name PlatoonSergeant says
  prop (SOME (SLc (PL plcmd))) impf prop NONE]

```

[ssmConductPBStateInterp\_def]

```

⊢ ∀ slState. ssmConductPBStateInterp slState = TT

```

## 10.2 Theorems

[authTestConductPB\_cmd\_reject\_lemma]

```

⊢ ∀ cmd. ¬authTestConductPB (prop (SOME cmd))

```

[authTestConductPB\_def]

```

⊢ (authTestConductPB (Name PlatoonLeader says prop cmd) ⇔ T) ∧
  (authTestConductPB (Name PlatoonSergeant says prop cmd) ⇔
  T) ∧ (authTestConductPB TT ⇔ F) ∧
  (authTestConductPB FF ⇔ F) ∧
  (authTestConductPB (prop v) ⇔ F) ∧
  (authTestConductPB (notf v1) ⇔ F) ∧
  (authTestConductPB (v2 andf v3) ⇔ F) ∧
  (authTestConductPB (v4 orf v5) ⇔ F) ∧
  (authTestConductPB (v6 impf v7) ⇔ F) ∧
  (authTestConductPB (v8 eqf v9) ⇔ F) ∧
  (authTestConductPB (v10 says TT) ⇔ F) ∧
  (authTestConductPB (v10 says FF) ⇔ F) ∧
  (authTestConductPB (v133 meet v134 says prop v66) ⇔ F) ∧
  (authTestConductPB (v135 quoting v136 says prop v66) ⇔ F) ∧
  (authTestConductPB (v10 says notf v67) ⇔ F) ∧
  (authTestConductPB (v10 says (v68 andf v69)) ⇔ F) ∧
  (authTestConductPB (v10 says (v70 orf v71)) ⇔ F) ∧
  (authTestConductPB (v10 says (v72 impf v73)) ⇔ F) ∧
  (authTestConductPB (v10 says (v74 eqf v75)) ⇔ F) ∧
  (authTestConductPB (v10 says v76 says v77) ⇔ F) ∧
  (authTestConductPB (v10 says v78 speaks_for v79) ⇔ F) ∧
  (authTestConductPB (v10 says v80 controls v81) ⇔ F) ∧
  (authTestConductPB (v10 says reps v82 v83 v84) ⇔ F) ∧
  (authTestConductPB (v10 says v85 domi v86) ⇔ F) ∧
  (authTestConductPB (v10 says v87 eqi v88) ⇔ F) ∧
  (authTestConductPB (v10 says v89 doms v90) ⇔ F) ∧

```

$(\text{authTestConductPB } (v_{10} \text{ says } v_{91} \text{ eqs } v_{92}) \iff F) \wedge$   
 $(\text{authTestConductPB } (v_{10} \text{ says } v_{93} \text{ eqn } v_{94}) \iff F) \wedge$   
 $(\text{authTestConductPB } (v_{10} \text{ says } v_{95} \text{ lte } v_{96}) \iff F) \wedge$   
 $(\text{authTestConductPB } (v_{10} \text{ says } v_{97} \text{ lt } v_{98}) \iff F) \wedge$   
 $(\text{authTestConductPB } (v_{12} \text{ speaks\_for } v_{13}) \iff F) \wedge$   
 $(\text{authTestConductPB } (v_{14} \text{ controls } v_{15}) \iff F) \wedge$   
 $(\text{authTestConductPB } (\text{reps } v_{16} \ v_{17} \ v_{18}) \iff F) \wedge$   
 $(\text{authTestConductPB } (v_{19} \text{ domi } v_{20}) \iff F) \wedge$   
 $(\text{authTestConductPB } (v_{21} \text{ eqi } v_{22}) \iff F) \wedge$   
 $(\text{authTestConductPB } (v_{23} \text{ doms } v_{24}) \iff F) \wedge$   
 $(\text{authTestConductPB } (v_{25} \text{ eqs } v_{26}) \iff F) \wedge$   
 $(\text{authTestConductPB } (v_{27} \text{ eqn } v_{28}) \iff F) \wedge$   
 $(\text{authTestConductPB } (v_{29} \text{ lte } v_{30}) \iff F) \wedge$   
 $(\text{authTestConductPB } (v_{31} \text{ lt } v_{32}) \iff F)$

$[\text{authTestConductPB\_ind}]$

$\vdash \forall P.$

$(\forall \text{cmd}. P (\text{Name PlatoonLeader says prop cmd})) \wedge$   
 $(\forall \text{cmd}. P (\text{Name PlatoonSergeant says prop cmd})) \wedge P \text{ TT} \wedge$   
 $P \text{ FF} \wedge (\forall v. P (\text{prop } v)) \wedge (\forall v_1. P (\text{notf } v_1)) \wedge$   
 $(\forall v_2 \ v_3. P (v_2 \text{ andf } v_3)) \wedge (\forall v_4 \ v_5. P (v_4 \text{ orf } v_5)) \wedge$   
 $(\forall v_6 \ v_7. P (v_6 \text{ impf } v_7)) \wedge (\forall v_8 \ v_9. P (v_8 \text{ eqf } v_9)) \wedge$   
 $(\forall v_{10}. P (v_{10} \text{ says TT})) \wedge (\forall v_{10}. P (v_{10} \text{ says FF})) \wedge$   
 $(\forall v_{133} \ v_{134} \ v_{66}. P (v_{133} \text{ meet } v_{134} \text{ says prop } v_{66})) \wedge$   
 $(\forall v_{135} \ v_{136} \ v_{66}. P (v_{135} \text{ quoting } v_{136} \text{ says prop } v_{66})) \wedge$   
 $(\forall v_{10} \ v_{67}. P (v_{10} \text{ says notf } v_{67})) \wedge$   
 $(\forall v_{10} \ v_{68} \ v_{69}. P (v_{10} \text{ says } (v_{68} \text{ andf } v_{69}))) \wedge$   
 $(\forall v_{10} \ v_{70} \ v_{71}. P (v_{10} \text{ says } (v_{70} \text{ orf } v_{71}))) \wedge$   
 $(\forall v_{10} \ v_{72} \ v_{73}. P (v_{10} \text{ says } (v_{72} \text{ impf } v_{73}))) \wedge$   
 $(\forall v_{10} \ v_{74} \ v_{75}. P (v_{10} \text{ says } (v_{74} \text{ eqf } v_{75}))) \wedge$   
 $(\forall v_{10} \ v_{76} \ v_{77}. P (v_{10} \text{ says } v_{76} \text{ says } v_{77})) \wedge$   
 $(\forall v_{10} \ v_{78} \ v_{79}. P (v_{10} \text{ says } v_{78} \text{ speaks\_for } v_{79})) \wedge$   
 $(\forall v_{10} \ v_{80} \ v_{81}. P (v_{10} \text{ says } v_{80} \text{ controls } v_{81})) \wedge$   
 $(\forall v_{10} \ v_{82} \ v_{83} \ v_{84}. P (v_{10} \text{ says reps } v_{82} \ v_{83} \ v_{84})) \wedge$   
 $(\forall v_{10} \ v_{85} \ v_{86}. P (v_{10} \text{ says } v_{85} \text{ domi } v_{86})) \wedge$   
 $(\forall v_{10} \ v_{87} \ v_{88}. P (v_{10} \text{ says } v_{87} \text{ eqi } v_{88})) \wedge$   
 $(\forall v_{10} \ v_{89} \ v_{90}. P (v_{10} \text{ says } v_{89} \text{ doms } v_{90})) \wedge$   
 $(\forall v_{10} \ v_{91} \ v_{92}. P (v_{10} \text{ says } v_{91} \text{ eqs } v_{92})) \wedge$   
 $(\forall v_{10} \ v_{93} \ v_{94}. P (v_{10} \text{ says } v_{93} \text{ eqn } v_{94})) \wedge$   
 $(\forall v_{10} \ v_{95} \ v_{96}. P (v_{10} \text{ says } v_{95} \text{ lte } v_{96})) \wedge$   
 $(\forall v_{10} \ v_{97} \ v_{98}. P (v_{10} \text{ says } v_{97} \text{ lt } v_{98})) \wedge$   
 $(\forall v_{12} \ v_{13}. P (v_{12} \text{ speaks\_for } v_{13})) \wedge$   
 $(\forall v_{14} \ v_{15}. P (v_{14} \text{ controls } v_{15})) \wedge$   
 $(\forall v_{16} \ v_{17} \ v_{18}. P (\text{reps } v_{16} \ v_{17} \ v_{18})) \wedge$   
 $(\forall v_{19} \ v_{20}. P (v_{19} \text{ domi } v_{20})) \wedge$   
 $(\forall v_{21} \ v_{22}. P (v_{21} \text{ eqi } v_{22})) \wedge$   
 $(\forall v_{23} \ v_{24}. P (v_{23} \text{ doms } v_{24})) \wedge$   
 $(\forall v_{25} \ v_{26}. P (v_{25} \text{ eqs } v_{26})) \wedge (\forall v_{27} \ v_{28}. P (v_{27} \text{ eqn } v_{28})) \wedge$   
 $(\forall v_{29} \ v_{30}. P (v_{29} \text{ lte } v_{30})) \wedge (\forall v_{31} \ v_{32}. P (v_{31} \text{ lt } v_{32})) \Rightarrow$

$$\forall v. P \ v$$

[conductPBNS\_def]

$$\begin{aligned} \vdash & (\text{conductPBNS CONDUCT\_PB (exec (PL securePB))} = \text{SECURE\_PB}) \wedge \\ & (\text{conductPBNS CONDUCT\_PB (exec (PL plIncompletePB))} = \\ & \quad \text{CONDUCT\_PB}) \wedge \\ & (\text{conductPBNS SECURE\_PB (exec (PSG actionsInPB))} = \\ & \quad \text{ACTIONS\_IN\_PB}) \wedge \\ & (\text{conductPBNS SECURE\_PB (exec (PSG psgIncompletePB))} = \\ & \quad \text{SECURE\_PB}) \wedge \\ & (\text{conductPBNS ACTIONS\_IN\_PB (exec (PL withdrawPB))} = \\ & \quad \text{WITHDRAW\_PB}) \wedge \\ & (\text{conductPBNS ACTIONS\_IN\_PB (exec (PL plIncompletePB))} = \\ & \quad \text{ACTIONS\_IN\_PB}) \wedge \\ & (\text{conductPBNS WITHDRAW\_PB (exec (PL completePB))} = \\ & \quad \text{COMPLETE\_PB}) \wedge \\ & (\text{conductPBNS WITHDRAW\_PB (exec (PL plIncompletePB))} = \\ & \quad \text{WITHDRAW\_PB}) \wedge (\text{conductPBNS } s \text{ (trap (PL cmd'))} = s) \wedge \\ & (\text{conductPBNS } s \text{ (trap (PSG cmd))} = s) \wedge \\ & (\text{conductPBNS } s \text{ (discard (PL cmd'))} = s) \wedge \\ & (\text{conductPBNS } s \text{ (discard (PSG cmd))} = s) \end{aligned}$$

[conductPBNS\_ind]

$$\begin{aligned} \vdash & \forall P. \\ & P \text{ CONDUCT\_PB (exec (PL securePB))} \wedge \\ & P \text{ CONDUCT\_PB (exec (PL plIncompletePB))} \wedge \\ & P \text{ SECURE\_PB (exec (PSG actionsInPB))} \wedge \\ & P \text{ SECURE\_PB (exec (PSG psgIncompletePB))} \wedge \\ & P \text{ ACTIONS\_IN\_PB (exec (PL withdrawPB))} \wedge \\ & P \text{ ACTIONS\_IN\_PB (exec (PL plIncompletePB))} \wedge \\ & P \text{ WITHDRAW\_PB (exec (PL completePB))} \wedge \\ & P \text{ WITHDRAW\_PB (exec (PL plIncompletePB))} \wedge \\ & (\forall s \text{ cmd. } P \ s \text{ (trap (PL cmd))}) \wedge \\ & (\forall s \text{ cmd. } P \ s \text{ (trap (PSG cmd))}) \wedge \\ & (\forall s \text{ cmd. } P \ s \text{ (discard (PL cmd))}) \wedge \\ & (\forall s \text{ cmd. } P \ s \text{ (discard (PSG cmd))}) \wedge \\ & P \text{ CONDUCT\_PB (exec (PL withdrawPB))} \wedge \\ & P \text{ CONDUCT\_PB (exec (PL completePB))} \wedge \\ & (\forall v_{11}. P \text{ CONDUCT\_PB (exec (PSG } v_{11})) \wedge \\ & (\forall v_{13}. P \text{ SECURE\_PB (exec (PL } v_{13})) \wedge \\ & P \text{ ACTIONS\_IN\_PB (exec (PL securePB))} \wedge \\ & P \text{ ACTIONS\_IN\_PB (exec (PL completePB))} \wedge \\ & (\forall v_{17}. P \text{ ACTIONS\_IN\_PB (exec (PSG } v_{17})) \wedge \\ & P \text{ WITHDRAW\_PB (exec (PL securePB))} \wedge \\ & P \text{ WITHDRAW\_PB (exec (PL withdrawPB))} \wedge \\ & (\forall v_{20}. P \text{ WITHDRAW\_PB (exec (PSG } v_{20})) \wedge \\ & (\forall v_{21}. P \text{ COMPLETE\_PB (exec } v_{21})) \Rightarrow \\ & \forall v \ v_1. P \ v \ v_1 \end{aligned}$$



**[conductPBOut\_def]**

$$\begin{aligned}
&\vdash (\text{conductPBOut CONDUCT\_PB (exec (PL securePB))} = \text{ConductPB}) \wedge \\
&\quad (\text{conductPBOut CONDUCT\_PB (exec (PL plIncompletePB))} = \\
&\quad \quad \text{ConductPB}) \wedge \\
&\quad (\text{conductPBOut SECURE\_PB (exec (PSG actionsInPB))} = \\
&\quad \quad \text{SecurePB}) \wedge \\
&\quad (\text{conductPBOut SECURE\_PB (exec (PSG psgIncompletePB))} = \\
&\quad \quad \text{SecurePB}) \wedge \\
&\quad (\text{conductPBOut ACTIONS\_IN\_PB (exec (PL withdrawPB))} = \\
&\quad \quad \text{ActionsInPB}) \wedge \\
&\quad (\text{conductPBOut ACTIONS\_IN\_PB (exec (PL plIncompletePB))} = \\
&\quad \quad \text{ActionsInPB}) \wedge \\
&\quad (\text{conductPBOut WITHDRAW\_PB (exec (PL completePB))} = \\
&\quad \quad \text{WithdrawPB}) \wedge \\
&\quad (\text{conductPBOut WITHDRAW\_PB (exec (PL plIncompletePB))} = \\
&\quad \quad \text{WithdrawPB}) \wedge \\
&\quad (\text{conductPBOut } s \text{ (trap (PL cmd'))} = \text{unAuthorized}) \wedge \\
&\quad (\text{conductPBOut } s \text{ (trap (PSG cmd))} = \text{unAuthorized}) \wedge \\
&\quad (\text{conductPBOut } s \text{ (discard (PL cmd'))} = \text{unAuthenticated}) \wedge \\
&\quad (\text{conductPBOut } s \text{ (discard (PSG cmd))} = \text{unAuthenticated})
\end{aligned}$$
**[conductPBOut\_ind]**

$$\begin{aligned}
&\vdash \forall P. \\
&\quad P \text{ CONDUCT\_PB (exec (PL securePB))} \wedge \\
&\quad P \text{ CONDUCT\_PB (exec (PL plIncompletePB))} \wedge \\
&\quad P \text{ SECURE\_PB (exec (PSG actionsInPB))} \wedge \\
&\quad P \text{ SECURE\_PB (exec (PSG psgIncompletePB))} \wedge \\
&\quad P \text{ ACTIONS\_IN\_PB (exec (PL withdrawPB))} \wedge \\
&\quad P \text{ ACTIONS\_IN\_PB (exec (PL plIncompletePB))} \wedge \\
&\quad P \text{ WITHDRAW\_PB (exec (PL completePB))} \wedge \\
&\quad P \text{ WITHDRAW\_PB (exec (PL plIncompletePB))} \wedge \\
&\quad (\forall s \text{ cmd. } P \text{ } s \text{ (trap (PL cmd))}) \wedge \\
&\quad (\forall s \text{ cmd. } P \text{ } s \text{ (trap (PSG cmd))}) \wedge \\
&\quad (\forall s \text{ cmd. } P \text{ } s \text{ (discard (PL cmd))}) \wedge \\
&\quad (\forall s \text{ cmd. } P \text{ } s \text{ (discard (PSG cmd))}) \wedge \\
&\quad P \text{ CONDUCT\_PB (exec (PL withdrawPB))} \wedge \\
&\quad P \text{ CONDUCT\_PB (exec (PL completePB))} \wedge \\
&\quad (\forall v_{11}. P \text{ CONDUCT\_PB (exec (PSG } v_{11})) \wedge \\
&\quad (\forall v_{13}. P \text{ SECURE\_PB (exec (PL } v_{13})) \wedge \\
&\quad P \text{ ACTIONS\_IN\_PB (exec (PL securePB))} \wedge \\
&\quad P \text{ ACTIONS\_IN\_PB (exec (PL completePB))} \wedge \\
&\quad (\forall v_{17}. P \text{ ACTIONS\_IN\_PB (exec (PSG } v_{17})) \wedge \\
&\quad P \text{ WITHDRAW\_PB (exec (PL securePB))} \wedge \\
&\quad P \text{ WITHDRAW\_PB (exec (PL withdrawPB))} \wedge \\
&\quad (\forall v_{20}. P \text{ WITHDRAW\_PB (exec (PSG } v_{20})) \wedge \\
&\quad (\forall v_{21}. P \text{ COMPLETE\_PB (exec } v_{21})) \Rightarrow \\
&\quad \forall v \text{ } v_1. P \text{ } v \text{ } v_1
\end{aligned}$$

**[PlatoonLeader\_exec\_plCommandPB\_justified\_thm]**

$\vdash \forall NS \text{ Out } M \text{ } Oi \text{ } Os.$   
 TR  $(M, Oi, Os)$  (exec (SLc (PL  $plCommand$ )))  
 (CFG authTestConductPB ssmConductPBStateInterp  
 (secContextConductPB  $plCommand$   $psgCommand$  incomplete)  
 (Name PlatoonLeader says  
 prop (SOME (SLc (PL  $plCommand$ )))::ins)  $s$  outs)  
 (CFG authTestConductPB ssmConductPBStateInterp  
 (secContextConductPB  $plCommand$   $psgCommand$  incomplete)  
 ins (NS  $s$  (exec (SLc (PL  $plCommand$ ))))  
 (Out  $s$  (exec (SLc (PL  $plCommand$ )))::outs))  $\iff$   
 authTestConductPB  
 (Name PlatoonLeader says  
 prop (SOME (SLc (PL  $plCommand$ ))))  $\wedge$   
 CFGInterpret  $(M, Oi, Os)$   
 (CFG authTestConductPB ssmConductPBStateInterp  
 (secContextConductPB  $plCommand$   $psgCommand$  incomplete)  
 (Name PlatoonLeader says  
 prop (SOME (SLc (PL  $plCommand$ )))::ins)  $s$  outs)  $\wedge$   
 $(M, Oi, Os)$  sat prop (SOME (SLc (PL  $plCommand$ )))

**[PlatoonLeader\_plCommandPB\_lemma]**

$\vdash$  CFGInterpret  $(M, Oi, Os)$   
 (CFG authTestConductPB ssmConductPBStateInterp  
 (secContextConductPB  $plCommand$   $psgCommand$  incomplete)  
 (Name PlatoonLeader says  
 prop (SOME (SLc (PL  $plCommand$ )))::ins)  $s$  outs)  $\Rightarrow$   
 $(M, Oi, Os)$  sat prop (SOME (SLc (PL  $plCommand$ )))

**[PlatoonSergeant\_exec\_psgCommandPB\_justified\_thm]**

$\vdash \forall NS \text{ Out } M \text{ } Oi \text{ } Os.$   
 TR  $(M, Oi, Os)$  (exec (SLc (PSG  $psgCommand$ )))  
 (CFG authTestConductPB ssmConductPBStateInterp  
 (secContextConductPB  $plCommand$   $psgCommand$  incomplete)  
 (Name PlatoonSergeant says  
 prop (SOME (SLc (PSG  $psgCommand$ )))::ins)  $s$  outs)  
 (CFG authTestConductPB ssmConductPBStateInterp  
 (secContextConductPB  $plCommand$   $psgCommand$  incomplete)  
 ins (NS  $s$  (exec (SLc (PSG  $psgCommand$ ))))  
 (Out  $s$  (exec (SLc (PSG  $psgCommand$ )))::outs))  $\iff$   
 authTestConductPB  
 (Name PlatoonSergeant says  
 prop (SOME (SLc (PSG  $psgCommand$ ))))  $\wedge$   
 CFGInterpret  $(M, Oi, Os)$   
 (CFG authTestConductPB ssmConductPBStateInterp  
 (secContextConductPB  $plCommand$   $psgCommand$  incomplete)  
 (Name PlatoonSergeant says  
 prop (SOME (SLc (PSG  $psgCommand$ )))::ins)  $s$  outs)  $\wedge$   
 $(M, Oi, Os)$  sat prop (SOME (SLc (PSG  $psgCommand$ )))

[PlatoonSergeant\_psgCommandPB\_lemma]

```

⊢ CFGInterpret (M, Oi, Os)
  (CFG authTestConductPB ssmConductPBStateInterp
    (secContextConductPB plCommand psgCommand incomplete)
    (Name PlatoonSergeant says
      prop (SOME (SLc (PSG psgCommand)))::ins) s outs) ⇒
    (M, Oi, Os) sat prop (SOME (SLc (PSG psgCommand)))

```

## 11 ConductPBType Theory

**Built:** 13 May 2018

**Parent Theories:** indexedLists, patternMatches

### 11.1 Datatypes

```

plCommandPB = securePB | withdrawPB | completePB
              | plIncompletePB

```

```

psgCommandPB = actionsInPB | psgIncompletePB

```

```

slCommand = PL plCommandPB | PSG psgCommandPB

```

```

slOutput = ConductPB | SecurePB | ActionsInPB | WithdrawPB
           | CompletePB | unAuthenticated | unAuthorized

```

```

slState = CONDUCT_PB | SECURE_PB | ACTIONS_IN_PB | WITHDRAW_PB
          | COMPLETE_PB

```

```

stateRole = PlatoonLeader | PlatoonSergeant

```

### 11.2 Theorems

[plCommandPB\_distinct\_clauses]

```

⊢ securePB ≠ withdrawPB ∧ securePB ≠ completePB ∧
  securePB ≠ plIncompletePB ∧ withdrawPB ≠ completePB ∧
  withdrawPB ≠ plIncompletePB ∧ completePB ≠ plIncompletePB

```

[psgCommandPB\_distinct\_clauses]

```

⊢ actionsInPB ≠ psgIncompletePB

```

[slCommand\_distinct\_clauses]

```

⊢ ∀ a' a. PL a ≠ PSG a'

```

[slCommand\_one\_one]

```

⊢ (∀ a a'. (PL a = PL a') ⇔ (a = a')) ∧
  (∀ a a'. (PSG a = PSG a') ⇔ (a = a'))

```

[slOutput\_distinct\_clauses]

$$\begin{aligned}
&\vdash \text{ConductPB} \neq \text{SecurePB} \wedge \text{ConductPB} \neq \text{ActionsInPB} \wedge \\
&\quad \text{ConductPB} \neq \text{WithdrawPB} \wedge \text{ConductPB} \neq \text{CompletePB} \wedge \\
&\quad \text{ConductPB} \neq \text{unAuthenticated} \wedge \text{ConductPB} \neq \text{unAuthorized} \wedge \\
&\quad \text{SecurePB} \neq \text{ActionsInPB} \wedge \text{SecurePB} \neq \text{WithdrawPB} \wedge \\
&\quad \text{SecurePB} \neq \text{CompletePB} \wedge \text{SecurePB} \neq \text{unAuthenticated} \wedge \\
&\quad \text{SecurePB} \neq \text{unAuthorized} \wedge \text{ActionsInPB} \neq \text{WithdrawPB} \wedge \\
&\quad \text{ActionsInPB} \neq \text{CompletePB} \wedge \text{ActionsInPB} \neq \text{unAuthenticated} \wedge \\
&\quad \text{ActionsInPB} \neq \text{unAuthorized} \wedge \text{WithdrawPB} \neq \text{CompletePB} \wedge \\
&\quad \text{WithdrawPB} \neq \text{unAuthenticated} \wedge \text{WithdrawPB} \neq \text{unAuthorized} \wedge \\
&\quad \text{CompletePB} \neq \text{unAuthenticated} \wedge \text{CompletePB} \neq \text{unAuthorized} \wedge \\
&\quad \text{unAuthenticated} \neq \text{unAuthorized}
\end{aligned}$$

[slRole\_distinct\_clauses]

$$\vdash \text{PlatoonLeader} \neq \text{PlatoonSergeant}$$

[slState\_distinct\_clauses]

$$\begin{aligned}
&\vdash \text{CONDUCT\_PB} \neq \text{SECURE\_PB} \wedge \text{CONDUCT\_PB} \neq \text{ACTIONS\_IN\_PB} \wedge \\
&\quad \text{CONDUCT\_PB} \neq \text{WITHDRAW\_PB} \wedge \text{CONDUCT\_PB} \neq \text{COMPLETE\_PB} \wedge \\
&\quad \text{SECURE\_PB} \neq \text{ACTIONS\_IN\_PB} \wedge \text{SECURE\_PB} \neq \text{WITHDRAW\_PB} \wedge \\
&\quad \text{SECURE\_PB} \neq \text{COMPLETE\_PB} \wedge \text{ACTIONS\_IN\_PB} \neq \text{WITHDRAW\_PB} \wedge \\
&\quad \text{ACTIONS\_IN\_PB} \neq \text{COMPLETE\_PB} \wedge \text{WITHDRAW\_PB} \neq \text{COMPLETE\_PB}
\end{aligned}$$

## 12 ssmMoveToORP Theory

**Built:** 13 May 2018

**Parent Theories:** MoveToORPType, ssm11, OMNIType

### 12.1 Definitions

[secContextMoveToORP\_def]

$$\begin{aligned}
&\vdash \forall cmd. \\
&\quad \text{secContextMoveToORP } cmd = \\
&\quad [\text{Name PlatoonLeader controls prop (SOME (SLc cmd))}]
\end{aligned}$$

[ssmMoveToORPStateInterp\_def]

$$\vdash \forall state. \text{ssmMoveToORPStateInterp } state = \text{TT}$$

### 12.2 Theorems

[authTestMoveToORP\_cmd\_reject\_lemma]

$$\vdash \forall cmd. \neg \text{authTestMoveToORP (prop (SOME cmd))}$$

**[authTestMoveToORP\_def]**

$$\begin{aligned}
&\vdash (\text{authTestMoveToORP } (\text{Name PlatoonLeader says prop cmd}) \iff T) \wedge \\
&\quad (\text{authTestMoveToORP TT} \iff F) \wedge (\text{authTestMoveToORP FF} \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (\text{prop } v) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (\text{notf } v_1) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_2 \text{ andf } v_3) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_4 \text{ orf } v_5) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_6 \text{ impf } v_7) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_8 \text{ eqf } v_9) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says TT}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says FF}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{133} \text{ meet } v_{134} \text{ says prop } v_{66}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{135} \text{ quoting } v_{136} \text{ says prop } v_{66}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says notf } v_{67}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says } (v_{68} \text{ andf } v_{69})) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says } (v_{70} \text{ orf } v_{71})) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says } (v_{72} \text{ impf } v_{73})) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says } (v_{74} \text{ eqf } v_{75})) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says } v_{76} \text{ says } v_{77}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says } v_{78} \text{ speaks\_for } v_{79}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says } v_{80} \text{ controls } v_{81}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says reps } v_{82} \ v_{83} \ v_{84}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says } v_{85} \text{ domi } v_{86}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says } v_{87} \text{ eqi } v_{88}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says } v_{89} \text{ doms } v_{90}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says } v_{91} \text{ eqs } v_{92}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says } v_{93} \text{ eqn } v_{94}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says } v_{95} \text{ lte } v_{96}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{10} \text{ says } v_{97} \text{ lt } v_{98}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{12} \text{ speaks\_for } v_{13}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{14} \text{ controls } v_{15}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (\text{reps } v_{16} \ v_{17} \ v_{18}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{19} \text{ domi } v_{20}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{21} \text{ eqi } v_{22}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{23} \text{ doms } v_{24}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{25} \text{ eqs } v_{26}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{27} \text{ eqn } v_{28}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{29} \text{ lte } v_{30}) \iff F) \wedge \\
&\quad (\text{authTestMoveToORP } (v_{31} \text{ lt } v_{32}) \iff F)
\end{aligned}$$
**[authTestMoveToORP\_ind]**

$$\begin{aligned}
&\vdash \forall P. \\
&\quad (\forall \text{cmd}. P (\text{Name PlatoonLeader says prop cmd})) \wedge P \text{ TT} \wedge \\
&\quad P \text{ FF} \wedge (\forall v. P (\text{prop } v)) \wedge (\forall v_1. P (\text{notf } v_1)) \wedge \\
&\quad (\forall v_2 \ v_3. P (v_2 \text{ andf } v_3)) \wedge (\forall v_4 \ v_5. P (v_4 \text{ orf } v_5)) \wedge \\
&\quad (\forall v_6 \ v_7. P (v_6 \text{ impf } v_7)) \wedge (\forall v_8 \ v_9. P (v_8 \text{ eqf } v_9)) \wedge \\
&\quad (\forall v_{10}. P (v_{10} \text{ says TT})) \wedge (\forall v_{10}. P (v_{10} \text{ says FF})) \wedge \\
&\quad (\forall v_{133} \ v_{134} \ v_{66}. P (v_{133} \text{ meet } v_{134} \text{ says prop } v_{66})) \wedge \\
&\quad (\forall v_{135} \ v_{136} \ v_{66}. P (v_{135} \text{ quoting } v_{136} \text{ says prop } v_{66})) \wedge
\end{aligned}$$

$$\begin{aligned}
& (\forall v_{10} v_{67}. P (v_{10} \text{ says notf } v_{67})) \wedge \\
& (\forall v_{10} v_{68} v_{69}. P (v_{10} \text{ says } (v_{68} \text{ andf } v_{69}))) \wedge \\
& (\forall v_{10} v_{70} v_{71}. P (v_{10} \text{ says } (v_{70} \text{ orf } v_{71}))) \wedge \\
& (\forall v_{10} v_{72} v_{73}. P (v_{10} \text{ says } (v_{72} \text{ impf } v_{73}))) \wedge \\
& (\forall v_{10} v_{74} v_{75}. P (v_{10} \text{ says } (v_{74} \text{ eqf } v_{75}))) \wedge \\
& (\forall v_{10} v_{76} v_{77}. P (v_{10} \text{ says } v_{76} \text{ says } v_{77})) \wedge \\
& (\forall v_{10} v_{78} v_{79}. P (v_{10} \text{ says } v_{78} \text{ speaks\_for } v_{79})) \wedge \\
& (\forall v_{10} v_{80} v_{81}. P (v_{10} \text{ says } v_{80} \text{ controls } v_{81})) \wedge \\
& (\forall v_{10} v_{82} v_{83} v_{84}. P (v_{10} \text{ says reps } v_{82} v_{83} v_{84})) \wedge \\
& (\forall v_{10} v_{85} v_{86}. P (v_{10} \text{ says } v_{85} \text{ domi } v_{86})) \wedge \\
& (\forall v_{10} v_{87} v_{88}. P (v_{10} \text{ says } v_{87} \text{ eqi } v_{88})) \wedge \\
& (\forall v_{10} v_{89} v_{90}. P (v_{10} \text{ says } v_{89} \text{ doms } v_{90})) \wedge \\
& (\forall v_{10} v_{91} v_{92}. P (v_{10} \text{ says } v_{91} \text{ eqs } v_{92})) \wedge \\
& (\forall v_{10} v_{93} v_{94}. P (v_{10} \text{ says } v_{93} \text{ eqn } v_{94})) \wedge \\
& (\forall v_{10} v_{95} v_{96}. P (v_{10} \text{ says } v_{95} \text{ lte } v_{96})) \wedge \\
& (\forall v_{10} v_{97} v_{98}. P (v_{10} \text{ says } v_{97} \text{ lt } v_{98})) \wedge \\
& (\forall v_{12} v_{13}. P (v_{12} \text{ speaks\_for } v_{13})) \wedge \\
& (\forall v_{14} v_{15}. P (v_{14} \text{ controls } v_{15})) \wedge \\
& (\forall v_{16} v_{17} v_{18}. P (\text{reps } v_{16} v_{17} v_{18})) \wedge \\
& (\forall v_{19} v_{20}. P (v_{19} \text{ domi } v_{20})) \wedge \\
& (\forall v_{21} v_{22}. P (v_{21} \text{ eqi } v_{22})) \wedge \\
& (\forall v_{23} v_{24}. P (v_{23} \text{ doms } v_{24})) \wedge \\
& (\forall v_{25} v_{26}. P (v_{25} \text{ eqs } v_{26})) \wedge (\forall v_{27} v_{28}. P (v_{27} \text{ eqn } v_{28})) \wedge \\
& (\forall v_{29} v_{30}. P (v_{29} \text{ lte } v_{30})) \wedge (\forall v_{31} v_{32}. P (v_{31} \text{ lt } v_{32})) \Rightarrow \\
& \forall v. P v
\end{aligned}$$

[moveToORPNS\_def]

$$\begin{aligned}
& \vdash (\text{moveToORPNS MOVE\_TO\_ORP (exec (SLc pltForm))} = \text{PLT\_FORM}) \wedge \\
& (\text{moveToORPNS MOVE\_TO\_ORP (exec (SLc incomplete))} = \\
& \quad \text{MOVE\_TO\_ORP}) \wedge \\
& (\text{moveToORPNS PLT\_FORM (exec (SLc pltMove))} = \text{PLT\_MOVE}) \wedge \\
& (\text{moveToORPNS PLT\_FORM (exec (SLc incomplete))} = \text{PLT\_FORM}) \wedge \\
& (\text{moveToORPNS PLT\_MOVE (exec (SLc pltSecureHalt))} = \\
& \quad \text{PLT\_SECURE\_HALT}) \wedge \\
& (\text{moveToORPNS PLT\_MOVE (exec (SLc incomplete))} = \text{PLT\_MOVE}) \wedge \\
& (\text{moveToORPNS PLT\_SECURE\_HALT (exec (SLc complete))} = \\
& \quad \text{COMPLETE}) \wedge \\
& (\text{moveToORPNS PLT\_SECURE\_HALT (exec (SLc incomplete))} = \\
& \quad \text{PLT\_SECURE\_HALT}) \wedge (\text{moveToORPNS } s \text{ (trap (SLc cmd))} = s) \wedge \\
& (\text{moveToORPNS } s \text{ (discard (SLc cmd))} = s)
\end{aligned}$$

[moveToORPNS\_ind]

$$\begin{aligned}
& \vdash \forall P. \\
& \quad P \text{ MOVE\_TO\_ORP (exec (SLc pltForm))} \wedge \\
& \quad P \text{ MOVE\_TO\_ORP (exec (SLc incomplete))} \wedge \\
& \quad P \text{ PLT\_FORM (exec (SLc pltMove))} \wedge \\
& \quad P \text{ PLT\_FORM (exec (SLc incomplete))} \wedge \\
& \quad P \text{ PLT\_MOVE (exec (SLc pltSecureHalt))} \wedge \\
& \quad P \text{ PLT\_MOVE (exec (SLc incomplete))} \wedge
\end{aligned}$$

$$\begin{aligned}
& P \text{ PLT\_SECURE\_HALT (exec (SLc complete))} \wedge \\
& P \text{ PLT\_SECURE\_HALT (exec (SLc incomplete))} \wedge \\
& (\forall s \text{ cmd. } P \text{ s (trap (SLc cmd))}) \wedge \\
& (\forall s \text{ cmd. } P \text{ s (discard (SLc cmd))}) \wedge \\
& (\forall s \text{ v}_6. P \text{ s (discard (ESCc v}_6\text{))}) \wedge \\
& (\forall s \text{ v}_9. P \text{ s (trap (ESCc v}_9\text{))}) \wedge \\
& (\forall v_{12}. P \text{ MOVE\_TO\_ORP (exec (ESCc v}_{12}\text{))}) \wedge \\
& P \text{ MOVE\_TO\_ORP (exec (SLc pltMove))} \wedge \\
& P \text{ MOVE\_TO\_ORP (exec (SLc pltSecureHalt))} \wedge \\
& P \text{ MOVE\_TO\_ORP (exec (SLc complete))} \wedge \\
& (\forall v_{15}. P \text{ PLT\_FORM (exec (ESCc v}_{15}\text{))}) \wedge \\
& P \text{ PLT\_FORM (exec (SLc pltForm))} \wedge \\
& P \text{ PLT\_FORM (exec (SLc pltSecureHalt))} \wedge \\
& P \text{ PLT\_FORM (exec (SLc complete))} \wedge \\
& (\forall v_{18}. P \text{ PLT\_MOVE (exec (ESCc v}_{18}\text{))}) \wedge \\
& P \text{ PLT\_MOVE (exec (SLc pltForm))} \wedge \\
& P \text{ PLT\_MOVE (exec (SLc pltMove))} \wedge \\
& P \text{ PLT\_MOVE (exec (SLc complete))} \wedge \\
& (\forall v_{21}. P \text{ PLT\_SECURE\_HALT (exec (ESCc v}_{21}\text{))}) \wedge \\
& P \text{ PLT\_SECURE\_HALT (exec (SLc pltForm))} \wedge \\
& P \text{ PLT\_SECURE\_HALT (exec (SLc pltMove))} \wedge \\
& P \text{ PLT\_SECURE\_HALT (exec (SLc pltSecureHalt))} \wedge \\
& (\forall v_{23}. P \text{ COMPLETE (exec v}_{23}\text{)}) \Rightarrow \\
& \forall v \text{ v}_1. P \text{ v v}_1
\end{aligned}$$

[moveToORPOut\_def]

$$\begin{aligned}
& \vdash (\text{moveToORPOut MOVE\_TO\_ORP (exec (SLc pltForm))} = \text{PLTForm}) \wedge \\
& (\text{moveToORPOut MOVE\_TO\_ORP (exec (SLc incomplete))} = \\
& \quad \text{MoveToORP}) \wedge \\
& (\text{moveToORPOut PLT\_FORM (exec (SLc pltMove))} = \text{PLTMove}) \wedge \\
& (\text{moveToORPOut PLT\_FORM (exec (SLc incomplete))} = \text{PLTForm}) \wedge \\
& (\text{moveToORPOut PLT\_MOVE (exec (SLc pltSecureHalt))} = \\
& \quad \text{PLTSecureHalt}) \wedge \\
& (\text{moveToORPOut PLT\_MOVE (exec (SLc incomplete))} = \text{PLTMove}) \wedge \\
& (\text{moveToORPOut PLT\_SECURE\_HALT (exec (SLc complete))} = \\
& \quad \text{Complete}) \wedge \\
& (\text{moveToORPOut PLT\_SECURE\_HALT (exec (SLc incomplete))} = \\
& \quad \text{PLTSecureHalt}) \wedge \\
& (\text{moveToORPOut s (trap (SLc cmd))} = \text{unAuthorized}) \wedge \\
& (\text{moveToORPOut s (discard (SLc cmd))} = \text{unAuthenticated})
\end{aligned}$$

[moveToORPOut\_ind]

$$\begin{aligned}
& \vdash \forall P. \\
& \quad P \text{ MOVE\_TO\_ORP (exec (SLc pltForm))} \wedge \\
& \quad P \text{ MOVE\_TO\_ORP (exec (SLc incomplete))} \wedge \\
& \quad P \text{ PLT\_FORM (exec (SLc pltMove))} \wedge \\
& \quad P \text{ PLT\_FORM (exec (SLc incomplete))} \wedge \\
& \quad P \text{ PLT\_MOVE (exec (SLc pltSecureHalt))} \wedge \\
& \quad P \text{ PLT\_MOVE (exec (SLc incomplete))} \wedge
\end{aligned}$$

$$\begin{aligned}
& P \text{ PLT\_SECURE\_HALT } (\text{exec } (\text{SLc complete})) \wedge \\
& P \text{ PLT\_SECURE\_HALT } (\text{exec } (\text{SLc incomplete})) \wedge \\
& (\forall s \text{ cmd. } P \ s \ (\text{trap } (\text{SLc cmd}))) \wedge \\
& (\forall s \text{ cmd. } P \ s \ (\text{discard } (\text{SLc cmd}))) \wedge \\
& (\forall s \ v_6. \ P \ s \ (\text{discard } (\text{ESCc } v_6))) \wedge \\
& (\forall s \ v_9. \ P \ s \ (\text{trap } (\text{ESCc } v_9))) \wedge \\
& (\forall v_{12}. \ P \ \text{MOVE\_TO\_ORP } (\text{exec } (\text{ESCc } v_{12}))) \wedge \\
& P \ \text{MOVE\_TO\_ORP } (\text{exec } (\text{SLc pltMove})) \wedge \\
& P \ \text{MOVE\_TO\_ORP } (\text{exec } (\text{SLc pltSecureHalt})) \wedge \\
& P \ \text{MOVE\_TO\_ORP } (\text{exec } (\text{SLc complete})) \wedge \\
& (\forall v_{15}. \ P \ \text{PLT\_FORM } (\text{exec } (\text{ESCc } v_{15}))) \wedge \\
& P \ \text{PLT\_FORM } (\text{exec } (\text{SLc pltForm})) \wedge \\
& P \ \text{PLT\_FORM } (\text{exec } (\text{SLc pltSecureHalt})) \wedge \\
& P \ \text{PLT\_FORM } (\text{exec } (\text{SLc complete})) \wedge \\
& (\forall v_{18}. \ P \ \text{PLT\_MOVE } (\text{exec } (\text{ESCc } v_{18}))) \wedge \\
& P \ \text{PLT\_MOVE } (\text{exec } (\text{SLc pltForm})) \wedge \\
& P \ \text{PLT\_MOVE } (\text{exec } (\text{SLc pltMove})) \wedge \\
& P \ \text{PLT\_MOVE } (\text{exec } (\text{SLc complete})) \wedge \\
& (\forall v_{21}. \ P \ \text{PLT\_SECURE\_HALT } (\text{exec } (\text{ESCc } v_{21}))) \wedge \\
& P \ \text{PLT\_SECURE\_HALT } (\text{exec } (\text{SLc pltForm})) \wedge \\
& P \ \text{PLT\_SECURE\_HALT } (\text{exec } (\text{SLc pltMove})) \wedge \\
& P \ \text{PLT\_SECURE\_HALT } (\text{exec } (\text{SLc pltSecureHalt})) \wedge \\
& (\forall v_{23}. \ P \ \text{COMPLETE } (\text{exec } v_{23})) \Rightarrow \\
& \forall v \ v_1. \ P \ v \ v_1
\end{aligned}$$

[PlatoonLeader\_exec\_slCommand\_justified\_thm]

$$\begin{aligned}
& \vdash \forall NS \ Out \ M \ Oi \ Os. \\
& \quad \text{TR } (M, Oi, Os) \ (\text{exec } (\text{SLc slCommand})) \\
& \quad (\text{CFG authTestMoveToORP ssmMoveToORPStateInterp} \\
& \quad \quad (\text{secContextMoveToORP slCommand}) \\
& \quad \quad (\text{Name PlatoonLeader says prop (SOME (SLc slCommand))} :: \\
& \quad \quad \quad \text{ins}) \ s \ \text{outs}) \\
& \quad (\text{CFG authTestMoveToORP ssmMoveToORPStateInterp} \\
& \quad \quad (\text{secContextMoveToORP slCommand}) \ \text{ins} \\
& \quad \quad (NS \ s \ (\text{exec } (\text{SLc slCommand}))) \\
& \quad \quad (\text{Out } s \ (\text{exec } (\text{SLc slCommand})) :: \text{outs})) \iff \\
& \text{authTestMoveToORP} \\
& \quad (\text{Name PlatoonLeader says prop (SOME (SLc slCommand))}) \wedge \\
& \text{CFGInterpret } (M, Oi, Os) \\
& \quad (\text{CFG authTestMoveToORP ssmMoveToORPStateInterp} \\
& \quad \quad (\text{secContextMoveToORP slCommand}) \\
& \quad \quad (\text{Name PlatoonLeader says prop (SOME (SLc slCommand))} :: \\
& \quad \quad \quad \text{ins}) \ s \ \text{outs}) \wedge \\
& (M, Oi, Os) \ \text{sat prop (SOME (SLc slCommand))}
\end{aligned}$$

[PlatoonLeader\_slCommand\_lemma]

$$\begin{aligned}
& \vdash \text{CFGInterpret } (M, Oi, Os) \\
& \quad (\text{CFG authTestMoveToORP ssmMoveToORPStateInterp} \\
& \quad \quad (\text{secContextMoveToORP slCommand})
\end{aligned}$$



(Name PlatoonLeader says prop (SOME (SLc slCommand)))::  
 ins) s outs)  $\Rightarrow$   
 (M, Oi, Os) sat prop (SOME (SLc slCommand))

## 13 MoveToORPType Theory

**Built:** 13 May 2018

**Parent Theories:** indexedLists, patternMatches

### 13.1 Datatypes

slCommand = pltForm | pltMove | pltSecureHalt | complete  
 | incomplete  
 slOutput = MoveToORP | PLTForm | PLTMove | PLTSecureHalt  
 | Complete | unauthorized | unauthenticated  
 slState = MOVE\_TO\_ORP | PLT\_FORM | PLT\_MOVE | PLT\_SECURE\_HALT  
 | COMPLETE  
 stateRole = PlatoonLeader

### 13.2 Theorems

[slCommand\_distinct\_clauses]

$\vdash$  pltForm  $\neq$  pltMove  $\wedge$  pltForm  $\neq$  pltSecureHalt  $\wedge$   
 pltForm  $\neq$  complete  $\wedge$  pltForm  $\neq$  incomplete  $\wedge$   
 pltMove  $\neq$  pltSecureHalt  $\wedge$  pltMove  $\neq$  complete  $\wedge$   
 pltMove  $\neq$  incomplete  $\wedge$  pltSecureHalt  $\neq$  complete  $\wedge$   
 pltSecureHalt  $\neq$  incomplete  $\wedge$  complete  $\neq$  incomplete

[slOutput\_distinct\_clauses]

$\vdash$  MoveToORP  $\neq$  PLTForm  $\wedge$  MoveToORP  $\neq$  PLTMove  $\wedge$   
 MoveToORP  $\neq$  PLTSecureHalt  $\wedge$  MoveToORP  $\neq$  Complete  $\wedge$   
 MoveToORP  $\neq$  unauthorized  $\wedge$  MoveToORP  $\neq$  unauthenticated  $\wedge$   
 PLTForm  $\neq$  PLTMove  $\wedge$  PLTForm  $\neq$  PLTSecureHalt  $\wedge$   
 PLTForm  $\neq$  Complete  $\wedge$  PLTForm  $\neq$  unauthorized  $\wedge$   
 PLTForm  $\neq$  unauthenticated  $\wedge$  PLTMove  $\neq$  PLTSecureHalt  $\wedge$   
 PLTMove  $\neq$  Complete  $\wedge$  PLTMove  $\neq$  unauthorized  $\wedge$   
 PLTMove  $\neq$  unauthenticated  $\wedge$  PLTSecureHalt  $\neq$  Complete  $\wedge$   
 PLTSecureHalt  $\neq$  unauthorized  $\wedge$   
 PLTSecureHalt  $\neq$  unauthenticated  $\wedge$  Complete  $\neq$  unauthorized  $\wedge$   
 Complete  $\neq$  unauthenticated  $\wedge$  unauthorized  $\neq$  unauthenticated

[slState\_distinct\_clauses]

$\vdash$  MOVE\_TO\_ORP  $\neq$  PLT\_FORM  $\wedge$  MOVE\_TO\_ORP  $\neq$  PLT\_MOVE  $\wedge$   
 MOVE\_TO\_ORP  $\neq$  PLT\_SECURE\_HALT  $\wedge$  MOVE\_TO\_ORP  $\neq$  COMPLETE  $\wedge$   
 PLT\_FORM  $\neq$  PLT\_MOVE  $\wedge$  PLT\_FORM  $\neq$  PLT\_SECURE\_HALT  $\wedge$   
 PLT\_FORM  $\neq$  COMPLETE  $\wedge$  PLT\_MOVE  $\neq$  PLT\_SECURE\_HALT  $\wedge$   
 PLT\_MOVE  $\neq$  COMPLETE  $\wedge$  PLT\_SECURE\_HALT  $\neq$  COMPLETE

## 14 ssmMoveToPB Theory

**Built:** 13 May 2018

**Parent Theories:** MoveToPBType, ssm11, OMNIType

### 14.1 Definitions

[secContextMoveToPB\_def]

$$\vdash \forall cmd. \\ \text{secContextMoveToPB } cmd = \\ [\text{Name PlatoonLeader controls prop (SOME (SLc cmd))}]$$

[ssmMoveToPBStateInterp\_def]

$$\vdash \forall state. \text{ssmMoveToPBStateInterp } state = \text{TT}$$

### 14.2 Theorems

[authTestMoveToPB\_cmd\_reject\_lemma]

$$\vdash \forall cmd. \neg \text{authTestMoveToPB (prop (SOME cmd))}$$

[authTestMoveToPB\_def]

$$\vdash (\text{authTestMoveToPB (Name PlatoonLeader says prop cmd)} \iff \text{T}) \wedge \\ (\text{authTestMoveToPB TT} \iff \text{F}) \wedge (\text{authTestMoveToPB FF} \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (prop } v) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (notf } v_1) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_2 \text{ andf } v_3) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_4 \text{ orf } v_5) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_6 \text{ impf } v_7) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_8 \text{ eqf } v_9) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says TT) } \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says FF) } \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{133} \text{ meet } v_{134} \text{ says prop } v_{66}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{135} \text{ quoting } v_{136} \text{ says prop } v_{66}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says notf } v_{67}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says (} v_{68} \text{ andf } v_{69}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says (} v_{70} \text{ orf } v_{71}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says (} v_{72} \text{ impf } v_{73}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says (} v_{74} \text{ eqf } v_{75}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says } v_{76} \text{ says } v_{77}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says } v_{78} \text{ speaks_for } v_{79}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says } v_{80} \text{ controls } v_{81}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says reps } v_{82} \text{ } v_{83} \text{ } v_{84}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says } v_{85} \text{ domi } v_{86}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says } v_{87} \text{ eqi } v_{88}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says } v_{89} \text{ doms } v_{90}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says } v_{91} \text{ eqs } v_{92}) \iff \text{F}) \wedge \\ (\text{authTestMoveToPB (} v_{10} \text{ says } v_{93} \text{ eqn } v_{94}) \iff \text{F}) \wedge$$

$(\text{authTestMoveToPB } (v_{10} \text{ says } v_{95} \text{ lte } v_{96}) \iff F) \wedge$   
 $(\text{authTestMoveToPB } (v_{10} \text{ says } v_{97} \text{ lt } v_{98}) \iff F) \wedge$   
 $(\text{authTestMoveToPB } (v_{12} \text{ speaks\_for } v_{13}) \iff F) \wedge$   
 $(\text{authTestMoveToPB } (v_{14} \text{ controls } v_{15}) \iff F) \wedge$   
 $(\text{authTestMoveToPB } (\text{reps } v_{16} \ v_{17} \ v_{18}) \iff F) \wedge$   
 $(\text{authTestMoveToPB } (v_{19} \text{ domi } v_{20}) \iff F) \wedge$   
 $(\text{authTestMoveToPB } (v_{21} \text{ eqi } v_{22}) \iff F) \wedge$   
 $(\text{authTestMoveToPB } (v_{23} \text{ doms } v_{24}) \iff F) \wedge$   
 $(\text{authTestMoveToPB } (v_{25} \text{ eqs } v_{26}) \iff F) \wedge$   
 $(\text{authTestMoveToPB } (v_{27} \text{ eqn } v_{28}) \iff F) \wedge$   
 $(\text{authTestMoveToPB } (v_{29} \text{ lte } v_{30}) \iff F) \wedge$   
 $(\text{authTestMoveToPB } (v_{31} \text{ lt } v_{32}) \iff F)$

[authTestMoveToPB\_ind]

$\vdash \forall P.$

$(\forall \text{cmd}. P (\text{Name PlatoonLeader says prop cmd})) \wedge P \text{ TT} \wedge$   
 $P \text{ FF} \wedge (\forall v. P (\text{prop } v)) \wedge (\forall v_1. P (\text{notf } v_1)) \wedge$   
 $(\forall v_2 \ v_3. P (v_2 \text{ andf } v_3)) \wedge (\forall v_4 \ v_5. P (v_4 \text{ orf } v_5)) \wedge$   
 $(\forall v_6 \ v_7. P (v_6 \text{ impf } v_7)) \wedge (\forall v_8 \ v_9. P (v_8 \text{ eqf } v_9)) \wedge$   
 $(\forall v_{10}. P (v_{10} \text{ says TT})) \wedge (\forall v_{10}. P (v_{10} \text{ says FF})) \wedge$   
 $(\forall v_{133} \ v_{134} \ v_{66}. P (v_{133} \text{ meet } v_{134} \text{ says prop } v_{66})) \wedge$   
 $(\forall v_{135} \ v_{136} \ v_{66}. P (v_{135} \text{ quoting } v_{136} \text{ says prop } v_{66})) \wedge$   
 $(\forall v_{10} \ v_{67}. P (v_{10} \text{ says notf } v_{67})) \wedge$   
 $(\forall v_{10} \ v_{68} \ v_{69}. P (v_{10} \text{ says } (v_{68} \text{ andf } v_{69}))) \wedge$   
 $(\forall v_{10} \ v_{70} \ v_{71}. P (v_{10} \text{ says } (v_{70} \text{ orf } v_{71}))) \wedge$   
 $(\forall v_{10} \ v_{72} \ v_{73}. P (v_{10} \text{ says } (v_{72} \text{ impf } v_{73}))) \wedge$   
 $(\forall v_{10} \ v_{74} \ v_{75}. P (v_{10} \text{ says } (v_{74} \text{ eqf } v_{75}))) \wedge$   
 $(\forall v_{10} \ v_{76} \ v_{77}. P (v_{10} \text{ says } v_{76} \text{ says } v_{77})) \wedge$   
 $(\forall v_{10} \ v_{78} \ v_{79}. P (v_{10} \text{ says } v_{78} \text{ speaks\_for } v_{79})) \wedge$   
 $(\forall v_{10} \ v_{80} \ v_{81}. P (v_{10} \text{ says } v_{80} \text{ controls } v_{81})) \wedge$   
 $(\forall v_{10} \ v_{82} \ v_{83} \ v_{84}. P (v_{10} \text{ says reps } v_{82} \ v_{83} \ v_{84})) \wedge$   
 $(\forall v_{10} \ v_{85} \ v_{86}. P (v_{10} \text{ says } v_{85} \text{ domi } v_{86})) \wedge$   
 $(\forall v_{10} \ v_{87} \ v_{88}. P (v_{10} \text{ says } v_{87} \text{ eqi } v_{88})) \wedge$   
 $(\forall v_{10} \ v_{89} \ v_{90}. P (v_{10} \text{ says } v_{89} \text{ doms } v_{90})) \wedge$   
 $(\forall v_{10} \ v_{91} \ v_{92}. P (v_{10} \text{ says } v_{91} \text{ eqs } v_{92})) \wedge$   
 $(\forall v_{10} \ v_{93} \ v_{94}. P (v_{10} \text{ says } v_{93} \text{ eqn } v_{94})) \wedge$   
 $(\forall v_{10} \ v_{95} \ v_{96}. P (v_{10} \text{ says } v_{95} \text{ lte } v_{96})) \wedge$   
 $(\forall v_{10} \ v_{97} \ v_{98}. P (v_{10} \text{ says } v_{97} \text{ lt } v_{98})) \wedge$   
 $(\forall v_{12} \ v_{13}. P (v_{12} \text{ speaks\_for } v_{13})) \wedge$   
 $(\forall v_{14} \ v_{15}. P (v_{14} \text{ controls } v_{15})) \wedge$   
 $(\forall v_{16} \ v_{17} \ v_{18}. P (\text{reps } v_{16} \ v_{17} \ v_{18})) \wedge$   
 $(\forall v_{19} \ v_{20}. P (v_{19} \text{ domi } v_{20})) \wedge$   
 $(\forall v_{21} \ v_{22}. P (v_{21} \text{ eqi } v_{22})) \wedge$   
 $(\forall v_{23} \ v_{24}. P (v_{23} \text{ doms } v_{24})) \wedge$   
 $(\forall v_{25} \ v_{26}. P (v_{25} \text{ eqs } v_{26})) \wedge (\forall v_{27} \ v_{28}. P (v_{27} \text{ eqn } v_{28})) \wedge$   
 $(\forall v_{29} \ v_{30}. P (v_{29} \text{ lte } v_{30})) \wedge (\forall v_{31} \ v_{32}. P (v_{31} \text{ lt } v_{32})) \Rightarrow$   
 $\forall v. P \ v$

[moveToPBNS\_def]

$$\begin{aligned}
&\vdash (\text{moveToPBNS MOVE\_TO\_PB (exec (SLc pltForm))} = \text{PLT\_FORM}) \wedge \\
&\quad (\text{moveToPBNS MOVE\_TO\_PB (exec (SLc incomplete))} = \\
&\quad \text{MOVE\_TO\_PB}) \wedge \\
&\quad (\text{moveToPBNS PLT\_FORM (exec (SLc pltMove))} = \text{PLT\_MOVE}) \wedge \\
&\quad (\text{moveToPBNS PLT\_FORM (exec (SLc incomplete))} = \text{PLT\_FORM}) \wedge \\
&\quad (\text{moveToPBNS PLT\_MOVE (exec (SLc pltHalt))} = \text{PLT\_HALT}) \wedge \\
&\quad (\text{moveToPBNS PLT\_MOVE (exec (SLc incomplete))} = \text{PLT\_MOVE}) \wedge \\
&\quad (\text{moveToPBNS PLT\_HALT (exec (SLc complete))} = \text{COMPLETE}) \wedge \\
&\quad (\text{moveToPBNS PLT\_HALT (exec (SLc incomplete))} = \text{PLT\_HALT}) \wedge \\
&\quad (\text{moveToPBNS } s \text{ (trap (SLc cmd))} = s) \wedge \\
&\quad (\text{moveToPBNS } s \text{ (discard (SLc cmd))} = s)
\end{aligned}$$

[moveToPBNS\_ind]

$$\begin{aligned}
&\vdash \forall P. \\
&\quad P \text{ MOVE\_TO\_PB (exec (SLc pltForm))} \wedge \\
&\quad P \text{ MOVE\_TO\_PB (exec (SLc incomplete))} \wedge \\
&\quad P \text{ PLT\_FORM (exec (SLc pltMove))} \wedge \\
&\quad P \text{ PLT\_FORM (exec (SLc incomplete))} \wedge \\
&\quad P \text{ PLT\_MOVE (exec (SLc pltHalt))} \wedge \\
&\quad P \text{ PLT\_MOVE (exec (SLc incomplete))} \wedge \\
&\quad P \text{ PLT\_HALT (exec (SLc complete))} \wedge \\
&\quad P \text{ PLT\_HALT (exec (SLc incomplete))} \wedge \\
&\quad (\forall s \text{ cmd. } P \text{ } s \text{ (trap (SLc cmd))}) \wedge \\
&\quad (\forall s \text{ cmd. } P \text{ } s \text{ (discard (SLc cmd))}) \wedge \\
&\quad (\forall s \text{ } v_6. P \text{ } s \text{ (discard (ESCc } v_6))) \wedge \\
&\quad (\forall s \text{ } v_9. P \text{ } s \text{ (trap (ESCc } v_9))) \wedge \\
&\quad (\forall v_{12}. P \text{ MOVE\_TO\_PB (exec (ESCc } v_{12}))) \wedge \\
&\quad P \text{ MOVE\_TO\_PB (exec (SLc pltMove))} \wedge \\
&\quad P \text{ MOVE\_TO\_PB (exec (SLc pltHalt))} \wedge \\
&\quad P \text{ MOVE\_TO\_PB (exec (SLc complete))} \wedge \\
&\quad (\forall v_{15}. P \text{ PLT\_FORM (exec (ESCc } v_{15}))) \wedge \\
&\quad P \text{ PLT\_FORM (exec (SLc pltForm))} \wedge \\
&\quad P \text{ PLT\_FORM (exec (SLc pltHalt))} \wedge \\
&\quad P \text{ PLT\_FORM (exec (SLc complete))} \wedge \\
&\quad (\forall v_{18}. P \text{ PLT\_MOVE (exec (ESCc } v_{18}))) \wedge \\
&\quad P \text{ PLT\_MOVE (exec (SLc pltForm))} \wedge \\
&\quad P \text{ PLT\_MOVE (exec (SLc pltMove))} \wedge \\
&\quad P \text{ PLT\_MOVE (exec (SLc complete))} \wedge \\
&\quad (\forall v_{21}. P \text{ PLT\_HALT (exec (ESCc } v_{21}))) \wedge \\
&\quad P \text{ PLT\_HALT (exec (SLc pltForm))} \wedge \\
&\quad P \text{ PLT\_HALT (exec (SLc pltMove))} \wedge \\
&\quad P \text{ PLT\_HALT (exec (SLc pltHalt))} \wedge \\
&\quad (\forall v_{23}. P \text{ COMPLETE (exec } v_{23})) \Rightarrow \\
&\quad \forall v \text{ } v_1. P \text{ } v \text{ } v_1
\end{aligned}$$

[moveToPBOut\_def]

$$\begin{aligned}
&\vdash (\text{moveToPBOut MOVE\_TO\_PB (exec (SLc pltForm))} = \text{PLTForm}) \wedge \\
&\quad (\text{moveToPBOut MOVE\_TO\_PB (exec (SLc incomplete))} = \text{MoveToPB}) \wedge \\
&\quad (\text{moveToPBOut PLT\_FORM (exec (SLc pltMove))} = \text{PLTMove}) \wedge
\end{aligned}$$

$(\text{moveToPBOut PLT\_FORM (exec (SLc incomplete))} = \text{PLTForm}) \wedge$   
 $(\text{moveToPBOut PLT\_MOVE (exec (SLc pltHalt))} = \text{PLTHalt}) \wedge$   
 $(\text{moveToPBOut PLT\_MOVE (exec (SLc incomplete))} = \text{PLTMove}) \wedge$   
 $(\text{moveToPBOut PLT\_HALT (exec (SLc complete))} = \text{Complete}) \wedge$   
 $(\text{moveToPBOut PLT\_HALT (exec (SLc incomplete))} = \text{PLTHalt}) \wedge$   
 $(\text{moveToPBOut } s \text{ (trap (SLc cmd))} = \text{unAuthorized}) \wedge$   
 $(\text{moveToPBOut } s \text{ (discard (SLc cmd))} = \text{unAuthenticated})$

[moveToPBOut\_ind]

$\vdash \forall P.$   
 $P \text{ MOVE\_TO\_PB (exec (SLc pltForm))} \wedge$   
 $P \text{ MOVE\_TO\_PB (exec (SLc incomplete))} \wedge$   
 $P \text{ PLT\_FORM (exec (SLc pltMove))} \wedge$   
 $P \text{ PLT\_FORM (exec (SLc incomplete))} \wedge$   
 $P \text{ PLT\_MOVE (exec (SLc pltHalt))} \wedge$   
 $P \text{ PLT\_MOVE (exec (SLc incomplete))} \wedge$   
 $P \text{ PLT\_HALT (exec (SLc complete))} \wedge$   
 $P \text{ PLT\_HALT (exec (SLc incomplete))} \wedge$   
 $(\forall s \text{ cmd. } P \text{ } s \text{ (trap (SLc cmd))}) \wedge$   
 $(\forall s \text{ cmd. } P \text{ } s \text{ (discard (SLc cmd))}) \wedge$   
 $(\forall s \text{ } v_6. P \text{ } s \text{ (discard (ESCc } v_6))) \wedge$   
 $(\forall s \text{ } v_9. P \text{ } s \text{ (trap (ESCc } v_9))) \wedge$   
 $(\forall v_{12}. P \text{ MOVE\_TO\_PB (exec (ESCc } v_{12}))) \wedge$   
 $P \text{ MOVE\_TO\_PB (exec (SLc pltMove))} \wedge$   
 $P \text{ MOVE\_TO\_PB (exec (SLc pltHalt))} \wedge$   
 $P \text{ MOVE\_TO\_PB (exec (SLc complete))} \wedge$   
 $(\forall v_{15}. P \text{ PLT\_FORM (exec (ESCc } v_{15}))) \wedge$   
 $P \text{ PLT\_FORM (exec (SLc pltForm))} \wedge$   
 $P \text{ PLT\_FORM (exec (SLc pltHalt))} \wedge$   
 $P \text{ PLT\_FORM (exec (SLc complete))} \wedge$   
 $(\forall v_{18}. P \text{ PLT\_MOVE (exec (ESCc } v_{18}))) \wedge$   
 $P \text{ PLT\_MOVE (exec (SLc pltForm))} \wedge$   
 $P \text{ PLT\_MOVE (exec (SLc pltMove))} \wedge$   
 $P \text{ PLT\_MOVE (exec (SLc complete))} \wedge$   
 $(\forall v_{21}. P \text{ PLT\_HALT (exec (ESCc } v_{21}))) \wedge$   
 $P \text{ PLT\_HALT (exec (SLc pltForm))} \wedge$   
 $P \text{ PLT\_HALT (exec (SLc pltMove))} \wedge$   
 $P \text{ PLT\_HALT (exec (SLc pltHalt))} \wedge$   
 $(\forall v_{23}. P \text{ COMPLETE (exec } v_{23})) \Rightarrow$   
 $\forall v \text{ } v_1. P \text{ } v \text{ } v_1$

[PlatoonLeader\_exec\_slCommand\_justified\_thm]

$\vdash \forall NS \text{ Out } M \text{ } O_i \text{ } O_s.$   
 $\text{TR } (M, O_i, O_s) \text{ (exec (SLc slCommand))}$   
 $(\text{CFG authTestMoveToPB ssmMoveToPBStateInterp}$   
 $\quad (\text{secContextMoveToPB slCommand})$   
 $\quad (\text{Name PlatoonLeader says prop (SOME (SLc slCommand))} ::$   
 $\quad \quad \text{ins) } s \text{ outs})$   
 $\quad (\text{CFG authTestMoveToPB ssmMoveToPBStateInterp}$

```

      (secContextMoveToPB slCommand) ins
      (NS s (exec (SLc slCommand)))
      (Out s (exec (SLc slCommand))::outs))  $\iff$ 
authTestMoveToPB
  (Name PlatoonLeader says prop (SOME (SLc slCommand)))  $\wedge$ 
CFGInterpret (M, Oi, Os)
  (CFG authTestMoveToPB ssmMoveToPBStateInterp
    (secContextMoveToPB slCommand)
    (Name PlatoonLeader says prop (SOME (SLc slCommand))::
      ins) s outs)  $\wedge$ 
  (M, Oi, Os) sat prop (SOME (SLc slCommand))

```

[PlatoonLeader\_slCommand\_lemma]

```

 $\vdash$  CFGInterpret (M, Oi, Os)
  (CFG authTestMoveToPB ssmMoveToPBStateInterp
    (secContextMoveToPB slCommand)
    (Name PlatoonLeader says prop (SOME (SLc slCommand))::
      ins) s outs)  $\Rightarrow$ 
  (M, Oi, Os) sat prop (SOME (SLc slCommand))

```

## 15 MoveToPBType Theory

**Built:** 13 May 2018

**Parent Theories:** indexedLists, patternMatches

### 15.1 Datatypes

*slCommand* = pltForm | pltMove | pltHalt | complete | incomplete

*slOutput* = MoveToPB | PLTForm | PLTMove | PLTHalt | Complete  
 | unauthorized | unAuthenticated

*slState* = MOVE\_TO\_PB | PLT\_FORM | PLT\_MOVE | PLT\_HALT | COMPLETE

*stateRole* = PlatoonLeader

### 15.2 Theorems

[slCommand\_distinct\_clauses]

```

 $\vdash$  pltForm  $\neq$  pltMove  $\wedge$  pltForm  $\neq$  pltHalt  $\wedge$  pltForm  $\neq$  complete  $\wedge$ 
  pltForm  $\neq$  incomplete  $\wedge$  pltMove  $\neq$  pltHalt  $\wedge$ 
  pltMove  $\neq$  complete  $\wedge$  pltMove  $\neq$  incomplete  $\wedge$ 
  pltHalt  $\neq$  complete  $\wedge$  pltHalt  $\neq$  incomplete  $\wedge$ 
  complete  $\neq$  incomplete

```

**[slOutput\_distinct\_clauses]**

$\vdash \text{MoveToPB} \neq \text{PLTForm} \wedge \text{MoveToPB} \neq \text{PLTMove} \wedge$   
 $\text{MoveToPB} \neq \text{PLTHalt} \wedge \text{MoveToPB} \neq \text{Complete} \wedge$   
 $\text{MoveToPB} \neq \text{unAuthorized} \wedge \text{MoveToPB} \neq \text{unAuthenticated} \wedge$   
 $\text{PLTForm} \neq \text{PLTMove} \wedge \text{PLTForm} \neq \text{PLTHalt} \wedge \text{PLTForm} \neq \text{Complete} \wedge$   
 $\text{PLTForm} \neq \text{unAuthorized} \wedge \text{PLTForm} \neq \text{unAuthenticated} \wedge$   
 $\text{PLTMove} \neq \text{PLTHalt} \wedge \text{PLTMove} \neq \text{Complete} \wedge$   
 $\text{PLTMove} \neq \text{unAuthorized} \wedge \text{PLTMove} \neq \text{unAuthenticated} \wedge$   
 $\text{PLTHalt} \neq \text{Complete} \wedge \text{PLTHalt} \neq \text{unAuthorized} \wedge$   
 $\text{PLTHalt} \neq \text{unAuthenticated} \wedge \text{Complete} \neq \text{unAuthorized} \wedge$   
 $\text{Complete} \neq \text{unAuthenticated} \wedge \text{unAuthorized} \neq \text{unAuthenticated}$

**[slState\_distinct\_clauses]**

$\vdash \text{MOVE\_TO\_PB} \neq \text{PLT\_FORM} \wedge \text{MOVE\_TO\_PB} \neq \text{PLT\_MOVE} \wedge$   
 $\text{MOVE\_TO\_PB} \neq \text{PLT\_HALT} \wedge \text{MOVE\_TO\_PB} \neq \text{COMPLETE} \wedge$   
 $\text{PLT\_FORM} \neq \text{PLT\_MOVE} \wedge \text{PLT\_FORM} \neq \text{PLT\_HALT} \wedge$   
 $\text{PLT\_FORM} \neq \text{COMPLETE} \wedge \text{PLT\_MOVE} \neq \text{PLT\_HALT} \wedge$   
 $\text{PLT\_MOVE} \neq \text{COMPLETE} \wedge \text{PLT\_HALT} \neq \text{COMPLETE}$

## 16 ssmPlanPB Theory

**Built:** 13 May 2018

**Parent Theories:** PlanPBDef, ssm

### 16.1 Theorems

**[inputOK\_def]**

$\vdash (\text{inputOK} (\text{Name PlatoonLeader says prop } cmd) \iff T) \wedge$   
 $(\text{inputOK} (\text{Name PlatoonSergeant says prop } cmd) \iff T) \wedge$   
 $(\text{inputOK TT} \iff F) \wedge (\text{inputOK FF} \iff F) \wedge$   
 $(\text{inputOK} (\text{prop } v) \iff F) \wedge (\text{inputOK} (\text{notf } v_1) \iff F) \wedge$   
 $(\text{inputOK} (v_2 \text{ andf } v_3) \iff F) \wedge (\text{inputOK} (v_4 \text{ orf } v_5) \iff F) \wedge$   
 $(\text{inputOK} (v_6 \text{ impf } v_7) \iff F) \wedge (\text{inputOK} (v_8 \text{ eqf } v_9) \iff F) \wedge$   
 $(\text{inputOK} (v_{10} \text{ says TT}) \iff F) \wedge (\text{inputOK} (v_{10} \text{ says FF}) \iff F) \wedge$   
 $(\text{inputOK} (v_{133} \text{ meet } v_{134} \text{ says prop } v_{66}) \iff F) \wedge$   
 $(\text{inputOK} (v_{135} \text{ quoting } v_{136} \text{ says prop } v_{66}) \iff F) \wedge$   
 $(\text{inputOK} (v_{10} \text{ says notf } v_{67}) \iff F) \wedge$   
 $(\text{inputOK} (v_{10} \text{ says } (v_{68} \text{ andf } v_{69})) \iff F) \wedge$   
 $(\text{inputOK} (v_{10} \text{ says } (v_{70} \text{ orf } v_{71})) \iff F) \wedge$   
 $(\text{inputOK} (v_{10} \text{ says } (v_{72} \text{ impf } v_{73})) \iff F) \wedge$   
 $(\text{inputOK} (v_{10} \text{ says } (v_{74} \text{ eqf } v_{75})) \iff F) \wedge$   
 $(\text{inputOK} (v_{10} \text{ says } v_{76} \text{ says } v_{77}) \iff F) \wedge$   
 $(\text{inputOK} (v_{10} \text{ says } v_{78} \text{ speaks\_for } v_{79}) \iff F) \wedge$   
 $(\text{inputOK} (v_{10} \text{ says } v_{80} \text{ controls } v_{81}) \iff F) \wedge$   
 $(\text{inputOK} (v_{10} \text{ says reps } v_{82} v_{83} v_{84}) \iff F) \wedge$   
 $(\text{inputOK} (v_{10} \text{ says } v_{85} \text{ domi } v_{86}) \iff F) \wedge$   
 $(\text{inputOK} (v_{10} \text{ says } v_{87} \text{ eqi } v_{88}) \iff F) \wedge$

$(\text{inputOK } (v_{10} \text{ says } v_{89} \text{ doms } v_{90}) \iff F) \wedge$   
 $(\text{inputOK } (v_{10} \text{ says } v_{91} \text{ eqs } v_{92}) \iff F) \wedge$   
 $(\text{inputOK } (v_{10} \text{ says } v_{93} \text{ eqn } v_{94}) \iff F) \wedge$   
 $(\text{inputOK } (v_{10} \text{ says } v_{95} \text{ lte } v_{96}) \iff F) \wedge$   
 $(\text{inputOK } (v_{10} \text{ says } v_{97} \text{ lt } v_{98}) \iff F) \wedge$   
 $(\text{inputOK } (v_{12} \text{ speaks\_for } v_{13}) \iff F) \wedge$   
 $(\text{inputOK } (v_{14} \text{ controls } v_{15}) \iff F) \wedge$   
 $(\text{inputOK } (\text{reps } v_{16} \ v_{17} \ v_{18}) \iff F) \wedge$   
 $(\text{inputOK } (v_{19} \text{ domi } v_{20}) \iff F) \wedge$   
 $(\text{inputOK } (v_{21} \text{ eqi } v_{22}) \iff F) \wedge$   
 $(\text{inputOK } (v_{23} \text{ doms } v_{24}) \iff F) \wedge$   
 $(\text{inputOK } (v_{25} \text{ eqs } v_{26}) \iff F) \wedge (\text{inputOK } (v_{27} \text{ eqn } v_{28}) \iff F) \wedge$   
 $(\text{inputOK } (v_{29} \text{ lte } v_{30}) \iff F) \wedge (\text{inputOK } (v_{31} \text{ lt } v_{32}) \iff F)$

[inputOK\_ind]

$\vdash \forall P.$

$(\forall \text{cmd}. P (\text{Name PlatoonLeader says prop cmd})) \wedge$   
 $(\forall \text{cmd}. P (\text{Name PlatoonSergeant says prop cmd})) \wedge P \text{ TT} \wedge$   
 $P \text{ FF} \wedge (\forall v. P (\text{prop } v)) \wedge (\forall v_1. P (\text{notf } v_1)) \wedge$   
 $(\forall v_2 \ v_3. P (v_2 \text{ andf } v_3)) \wedge (\forall v_4 \ v_5. P (v_4 \text{ orf } v_5)) \wedge$   
 $(\forall v_6 \ v_7. P (v_6 \text{ impf } v_7)) \wedge (\forall v_8 \ v_9. P (v_8 \text{ eqf } v_9)) \wedge$   
 $(\forall v_{10}. P (v_{10} \text{ says TT})) \wedge (\forall v_{10}. P (v_{10} \text{ says FF})) \wedge$   
 $(\forall v_{133} \ v_{134} \ v_{66}. P (v_{133} \text{ meet } v_{134} \text{ says prop } v_{66})) \wedge$   
 $(\forall v_{135} \ v_{136} \ v_{66}. P (v_{135} \text{ quoting } v_{136} \text{ says prop } v_{66})) \wedge$   
 $(\forall v_{10} \ v_{67}. P (v_{10} \text{ says notf } v_{67})) \wedge$   
 $(\forall v_{10} \ v_{68} \ v_{69}. P (v_{10} \text{ says } (v_{68} \text{ andf } v_{69}))) \wedge$   
 $(\forall v_{10} \ v_{70} \ v_{71}. P (v_{10} \text{ says } (v_{70} \text{ orf } v_{71}))) \wedge$   
 $(\forall v_{10} \ v_{72} \ v_{73}. P (v_{10} \text{ says } (v_{72} \text{ impf } v_{73}))) \wedge$   
 $(\forall v_{10} \ v_{74} \ v_{75}. P (v_{10} \text{ says } (v_{74} \text{ eqf } v_{75}))) \wedge$   
 $(\forall v_{10} \ v_{76} \ v_{77}. P (v_{10} \text{ says } v_{76} \text{ says } v_{77})) \wedge$   
 $(\forall v_{10} \ v_{78} \ v_{79}. P (v_{10} \text{ says } v_{78} \text{ speaks\_for } v_{79})) \wedge$   
 $(\forall v_{10} \ v_{80} \ v_{81}. P (v_{10} \text{ says } v_{80} \text{ controls } v_{81})) \wedge$   
 $(\forall v_{10} \ v_{82} \ v_{83} \ v_{84}. P (v_{10} \text{ says reps } v_{82} \ v_{83} \ v_{84})) \wedge$   
 $(\forall v_{10} \ v_{85} \ v_{86}. P (v_{10} \text{ says } v_{85} \text{ domi } v_{86})) \wedge$   
 $(\forall v_{10} \ v_{87} \ v_{88}. P (v_{10} \text{ says } v_{87} \text{ eqi } v_{88})) \wedge$   
 $(\forall v_{10} \ v_{89} \ v_{90}. P (v_{10} \text{ says } v_{89} \text{ doms } v_{90})) \wedge$   
 $(\forall v_{10} \ v_{91} \ v_{92}. P (v_{10} \text{ says } v_{91} \text{ eqs } v_{92})) \wedge$   
 $(\forall v_{10} \ v_{93} \ v_{94}. P (v_{10} \text{ says } v_{93} \text{ eqn } v_{94})) \wedge$   
 $(\forall v_{10} \ v_{95} \ v_{96}. P (v_{10} \text{ says } v_{95} \text{ lte } v_{96})) \wedge$   
 $(\forall v_{10} \ v_{97} \ v_{98}. P (v_{10} \text{ says } v_{97} \text{ lt } v_{98})) \wedge$   
 $(\forall v_{12} \ v_{13}. P (v_{12} \text{ speaks\_for } v_{13})) \wedge$   
 $(\forall v_{14} \ v_{15}. P (v_{14} \text{ controls } v_{15})) \wedge$   
 $(\forall v_{16} \ v_{17} \ v_{18}. P (\text{reps } v_{16} \ v_{17} \ v_{18})) \wedge$   
 $(\forall v_{19} \ v_{20}. P (v_{19} \text{ domi } v_{20})) \wedge$   
 $(\forall v_{21} \ v_{22}. P (v_{21} \text{ eqi } v_{22})) \wedge$   
 $(\forall v_{23} \ v_{24}. P (v_{23} \text{ doms } v_{24})) \wedge$   
 $(\forall v_{25} \ v_{26}. P (v_{25} \text{ eqs } v_{26})) \wedge (\forall v_{27} \ v_{28}. P (v_{27} \text{ eqn } v_{28})) \wedge$   
 $(\forall v_{29} \ v_{30}. P (v_{29} \text{ lte } v_{30})) \wedge (\forall v_{31} \ v_{32}. P (v_{31} \text{ lt } v_{32})) \Rightarrow$   
 $\forall v. P \ v$



**[planPBNS\_def]**

```

⊢ (planPBNS WARNO (exec x) =
  if
    (getRecon x = [SOME (SLc (PL recon))]) ∧
    (getTenativePlan x = [SOME (SLc (PL tentativePlan))]) ∧
    (getReport x = [SOME (SLc (PL report1))]) ∧
    (getInitMove x = [SOME (SLc (PSG initiateMovement))])
  then
    REPORT1
  else WARNO) ∧
(planPBNS PLAN_PB (exec x) =
  if getPlCom x = receiveMission then RECEIVE_MISSION
  else PLAN_PB) ∧
(planPBNS RECEIVE_MISSION (exec x) =
  if getPlCom x = warno then WARNO else RECEIVE_MISSION) ∧
(planPBNS REPORT1 (exec x) =
  if getPlCom x = completePlan then COMPLETE_PLAN
  else REPORT1) ∧
(planPBNS COMPLETE_PLAN (exec x) =
  if getPlCom x = opoid then OPOID else COMPLETE_PLAN) ∧
(planPBNS OPOID (exec x) =
  if getPlCom x = supervise then SUPERVISE else OPOID) ∧
(planPBNS SUPERVISE (exec x) =
  if getPlCom x = report2 then REPORT2 else SUPERVISE) ∧
(planPBNS REPORT2 (exec x) =
  if getPlCom x = complete then COMPLETE else REPORT2) ∧
(planPBNS s (trap v0) = s) ∧ (planPBNS s (discard v1) = s)

```

**[planPBNS\_ind]**

```

⊢ ∀ P.
  (∀ x. P WARNO (exec x)) ∧ (∀ x. P PLAN_PB (exec x)) ∧
  (∀ x. P RECEIVE_MISSION (exec x)) ∧
  (∀ x. P REPORT1 (exec x)) ∧ (∀ x. P COMPLETE_PLAN (exec x)) ∧
  (∀ x. P OPOID (exec x)) ∧ (∀ x. P SUPERVISE (exec x)) ∧
  (∀ x. P REPORT2 (exec x)) ∧ (∀ s v0. P s (trap v0)) ∧
  (∀ s v1. P s (discard v1)) ∧
  (∀ v6. P TENTATIVE_PLAN (exec v6)) ∧
  (∀ v7. P INITIATE_MOVEMENT (exec v7)) ∧
  (∀ v8. P RECON (exec v8)) ∧ (∀ v9. P COMPLETE (exec v9)) ⇒
  ∀ v v1. P v v1

```

**[planPBOut\_def]**

```

⊢ (planPBOut WARNO (exec x) =
  if
    (getRecon x = [SOME (SLc (PL recon))]) ∧
    (getTenativePlan x = [SOME (SLc (PL tentativePlan))]) ∧
    (getReport x = [SOME (SLc (PL report1))]) ∧
    (getInitMove x = [SOME (SLc (PSG initiateMovement))])
  then
    REPORT1
  else WARNO)

```

```

then
  Report1
  else unauthorized)  $\wedge$ 
(planPBOut PLAN_PB (exec  $x$ ) =
  if getPlCom  $x$  = receiveMission then ReceiveMission
  else unauthorized)  $\wedge$ 
(planPBOut RECEIVE_MISSION (exec  $x$ ) =
  if getPlCom  $x$  = warno then Warno else unauthorized)  $\wedge$ 
(planPBOut REPORT1 (exec  $x$ ) =
  if getPlCom  $x$  = completePlan then CompletePlan
  else unauthorized)  $\wedge$ 
(planPBOut COMPLETE_PLAN (exec  $x$ ) =
  if getPlCom  $x$  = opoid then Opoid else unauthorized)  $\wedge$ 
(planPBOut OPOID (exec  $x$ ) =
  if getPlCom  $x$  = supervise then Supervise
  else unauthorized)  $\wedge$ 
(planPBOut SUPERVISE (exec  $x$ ) =
  if getPlCom  $x$  = report2 then Report2 else unauthorized)  $\wedge$ 
(planPBOut REPORT2 (exec  $x$ ) =
  if getPlCom  $x$  = complete then Complete else unauthorized)  $\wedge$ 
(planPBOut  $s$  (trap  $v_0$ ) = unauthorized)  $\wedge$ 
(planPBOut  $s$  (discard  $v_1$ ) = unAuthenticated)

```

[planPBOut\_ind]

```

 $\vdash \forall P.$ 
  ( $\forall x. P$  WARNO (exec  $x$ ))  $\wedge$  ( $\forall x. P$  PLAN_PB (exec  $x$ ))  $\wedge$ 
  ( $\forall x. P$  RECEIVE_MISSION (exec  $x$ ))  $\wedge$ 
  ( $\forall x. P$  REPORT1 (exec  $x$ ))  $\wedge$  ( $\forall x. P$  COMPLETE_PLAN (exec  $x$ ))  $\wedge$ 
  ( $\forall x. P$  OPOID (exec  $x$ ))  $\wedge$  ( $\forall x. P$  SUPERVISE (exec  $x$ ))  $\wedge$ 
  ( $\forall x. P$  REPORT2 (exec  $x$ ))  $\wedge$  ( $\forall s v_0. P s$  (trap  $v_0$ ))  $\wedge$ 
  ( $\forall s v_1. P s$  (discard  $v_1$ ))  $\wedge$ 
  ( $\forall v_6. P$  TENTATIVE_PLAN (exec  $v_6$ ))  $\wedge$ 
  ( $\forall v_7. P$  INITIATE_MOVEMENT (exec  $v_7$ ))  $\wedge$ 
  ( $\forall v_8. P$  RECON (exec  $v_8$ ))  $\wedge$  ( $\forall v_9. P$  COMPLETE (exec  $v_9$ ))  $\Rightarrow$ 
   $\forall v v_1. P v v_1$ 

```

[PlatoonLeader\_notWARNO\_notreport1\_exec\_plCommand\_justified\_lemma]

```

 $\vdash s \neq \text{WARNO} \Rightarrow$ 
   $plCommand \neq \text{invalidPlCommand} \Rightarrow$ 
   $plCommand \neq \text{report1} \Rightarrow$ 
   $\forall NS \text{ Out } M \text{ } O_i \text{ } O_s.$ 
    TR ( $M, O_i, O_s$ )
      (exec
        (inputList
          [Name PlatoonLeader says
            prop (SOME (SLc (PL  $plCommand$ ))))]))
      (CFG inputOK secContext secContextNull
        ([Name PlatoonLeader says
          prop (SOME (SLc (PL  $plCommand$ )))]::ins)  $s$  outs)

```

```

(CFG inputOK secContext secContextNull ins
  (NS s
    (exec
      (inputList
        [Name PlatoonLeader says
          prop (SOME (SLc (PL plCommand))))]))
  (Out s
    (exec
      (inputList
        [Name PlatoonLeader says
          prop (SOME (SLc (PL plCommand))))]))::
    outs))  $\iff$ 
authenticationTest inputOK
  [Name PlatoonLeader says
    prop (SOME (SLc (PL plCommand)))]  $\wedge$ 
CFGInterpret (M, Oi, Os)
  (CFG inputOK secContext secContextNull
    ([Name PlatoonLeader says
      prop (SOME (SLc (PL plCommand)))]::ins) s outs)  $\wedge$ 
  (M, Oi, Os) satList
  propCommandList
  [Name PlatoonLeader says
    prop (SOME (SLc (PL plCommand)))]

```

[PlatoonLeader\_notWARNO\_notreport1\_exec\_plCommand\_justified\_thm]

```

 $\vdash s \neq \text{WARNO} \Rightarrow$ 
  plCommand  $\neq$  invalidPlCommand  $\Rightarrow$ 
  plCommand  $\neq$  report1  $\Rightarrow$ 
 $\forall NS \text{ Out } M \text{ Oi } Os.$ 
  TR (M, Oi, Os) (exec [SOME (SLc (PL plCommand))])
  (CFG inputOK secContext secContextNull
    ([Name PlatoonLeader says
      prop (SOME (SLc (PL plCommand)))]::ins) s outs)
  (CFG inputOK secContext secContextNull ins
    (NS s (exec [SOME (SLc (PL plCommand))]))
    (Out s (exec [SOME (SLc (PL plCommand)))]::outs))  $\iff$ 
authenticationTest inputOK
  [Name PlatoonLeader says
    prop (SOME (SLc (PL plCommand)))]  $\wedge$ 
CFGInterpret (M, Oi, Os)
  (CFG inputOK secContext secContextNull
    ([Name PlatoonLeader says
      prop (SOME (SLc (PL plCommand)))]::ins) s outs)  $\wedge$ 
  (M, Oi, Os) satList [prop (SOME (SLc (PL plCommand)))]

```

[PlatoonLeader\_notWARNO\_notreport1\_exec\_plCommand\_lemma]

```

 $\vdash s \neq \text{WARNO} \Rightarrow$ 
  plCommand  $\neq$  invalidPlCommand  $\Rightarrow$ 
  plCommand  $\neq$  report1  $\Rightarrow$ 

```

$\forall M \text{ } Oi \text{ } Os.$   
 CFGInterpret  $(M, Oi, Os)$   
 (CFG inputOK secContext secContextNull  
 ([Name PlatoonLeader says  
 prop (SOME (SLc (PL  $plCommand$ ))))] $::ins$ )  $s$   $outs$ )  $\Rightarrow$   
 $(M, Oi, Os)$  satList  
 propCommandList  
 [Name PlatoonLeader says  
 prop (SOME (SLc (PL  $plCommand$ )))]

[PlatoonLeader\_psgCommand\_notDiscard\_thm]

$\vdash \forall NS \text{ } Out \text{ } M \text{ } Oi \text{ } Os.$   
 $\neg$ TR  $(M, Oi, Os)$   
 (discard  
 (inputList  
 [Name PlatoonLeader says  
 prop (SOME (SLc (PSG  $psgCommand$ ))))]))  
 (CFG inputOK secContext secContextNull  
 ([Name PlatoonLeader says  
 prop (SOME (SLc (PSG  $psgCommand$ ))))] $::ins$ )  $s$   $outs$ )  
 (CFG inputOK secContext secContextNull  $ins$   
 (NS  $s$   
 (discard  
 (inputList  
 [Name PlatoonLeader says  
 prop (SOME (SLc (PSG  $psgCommand$ ))))]))))  
 (Out  $s$   
 (discard  
 (inputList  
 [Name PlatoonLeader says  
 prop (SOME (SLc (PSG  $psgCommand$ ))))]))] $::$   
 $outs$ ))

[PlatoonLeader\_trap\_psgCommand\_justified\_lemma]

$\vdash \forall NS \text{ } Out \text{ } M \text{ } Oi \text{ } Os.$   
 TR  $(M, Oi, Os)$   
 (trap  
 (inputList  
 [Name PlatoonLeader says  
 prop (SOME (SLc (PSG  $psgCommand$ ))))]))  
 (CFG inputOK secContext secContextNull  
 ([Name PlatoonLeader says  
 prop (SOME (SLc (PSG  $psgCommand$ ))))] $::ins$ )  $s$   $outs$ )  
 (CFG inputOK secContext secContextNull  $ins$   
 (NS  $s$   
 (trap  
 (inputList  
 [Name PlatoonLeader says  
 prop (SOME (SLc (PSG  $psgCommand$ ))))]))))

```

      (Out s
        (trap
          (inputList
            [Name PlatoonLeader says
              prop (SOME (SLc (PSG psgCommand))))]))::
        outs))  $\iff$ 
authenticationTest inputOK
  [Name PlatoonLeader says
    prop (SOME (SLc (PSG psgCommand)))]  $\wedge$ 
CFGInterpret (M, Oi, Os)
  (CFG inputOK secContext secContextNull
    ([Name PlatoonLeader says
      prop (SOME (SLc (PSG psgCommand)))]::ins) s outs)  $\wedge$ 
(M, Oi, Os) sat prop NONE

```

[PlatoonLeader\_trap\_psgCommand\_lemma]

```

 $\vdash \forall M \text{ } Oi \text{ } Os.$ 
CFGInterpret (M, Oi, Os)
  (CFG inputOK secContext secContextNull
    ([Name PlatoonLeader says
      prop (SOME (SLc (PSG psgCommand)))]::ins) s outs)  $\Rightarrow$ 
(M, Oi, Os) sat prop NONE

```

[PlatoonLeader\_WARNO\_exec\_report1\_justified\_lemma]

```

 $\vdash \forall NS \text{ } Out \text{ } M \text{ } Oi \text{ } Os.$ 
TR (M, Oi, Os)
  (exec
    (inputList
      [Name PlatoonLeader says
        prop (SOME (SLc (PL recon)));
        Name PlatoonLeader says
        prop (SOME (SLc (PL tentativePlan)));
        Name PlatoonSergeant says
        prop (SOME (SLc (PSG initiateMovement)));
        Name PlatoonLeader says
        prop (SOME (SLc (PL report1)))]))
    (CFG inputOK secContext secContextNull
      ([Name PlatoonLeader says
        prop (SOME (SLc (PL recon)));
        Name PlatoonLeader says
        prop (SOME (SLc (PL tentativePlan)));
        Name PlatoonSergeant says
        prop (SOME (SLc (PSG initiateMovement)));
        Name PlatoonLeader says
        prop (SOME (SLc (PL report1)))]::ins) WARNO outs)
    (CFG inputOK secContext secContextNull ins
      (NS WARNO
        (exec
          (inputList

```

```

      [Name PlatoonLeader says
      prop (SOME (SLc (PL recon)));
      Name PlatoonLeader says
      prop (SOME (SLc (PL tentativePlan)));
      Name PlatoonSergeant says
      prop (SOME (SLc (PSG initiateMovement)));
      Name PlatoonLeader says
      prop (SOME (SLc (PL report1)))))])))
(Out WARNO
  (exec
    (inputList
      [Name PlatoonLeader says
      prop (SOME (SLc (PL recon)));
      Name PlatoonLeader says
      prop (SOME (SLc (PL tentativePlan)));
      Name PlatoonSergeant says
      prop (SOME (SLc (PSG initiateMovement)));
      Name PlatoonLeader says
      prop (SOME (SLc (PL report1)))))]::outs))  $\iff$ 
authenticationTest inputOK
  [Name PlatoonLeader says prop (SOME (SLc (PL recon)));
  Name PlatoonLeader says
  prop (SOME (SLc (PL tentativePlan)));
  Name PlatoonSergeant says
  prop (SOME (SLc (PSG initiateMovement)));
  Name PlatoonLeader says
  prop (SOME (SLc (PL report1)))]  $\wedge$ 
CFGInterpret (M, Oi, Os)
  (CFG inputOK secContext secContextNull
    ([Name PlatoonLeader says
    prop (SOME (SLc (PL recon)));
    Name PlatoonLeader says
    prop (SOME (SLc (PL tentativePlan)));
    Name PlatoonSergeant says
    prop (SOME (SLc (PSG initiateMovement)));
    Name PlatoonLeader says
    prop (SOME (SLc (PL report1)))]::ins) WARNO outs)  $\wedge$ 
(M, Oi, Os) satList
propCommandList
  [Name PlatoonLeader says prop (SOME (SLc (PL recon)));
  Name PlatoonLeader says
  prop (SOME (SLc (PL tentativePlan)));
  Name PlatoonSergeant says
  prop (SOME (SLc (PSG initiateMovement)));
  Name PlatoonLeader says prop (SOME (SLc (PL report1)))]

```

[PlatoonLeader\_WARNO\_exec\_report1\_justified\_thm]

$\vdash \forall NS \text{ Out } M \text{ Oi } Os.$   
 TR (M, Oi, Os)

```

(exec
  [SOME (SLc (PL recon)); SOME (SLc (PL tentativePlan));
   SOME (SLc (PSG initiateMovement));
   SOME (SLc (PL report1))])
(CFG inputOK secContext secContextNull
  ([Name PlatoonLeader says
    prop (SOME (SLc (PL recon)));
    Name PlatoonLeader says
    prop (SOME (SLc (PL tentativePlan)));
    Name PlatoonSergeant says
    prop (SOME (SLc (PSG initiateMovement)));
    Name PlatoonLeader says
    prop (SOME (SLc (PL report1)))]::ins) WARNO outs)
(CFG inputOK secContext secContextNull ins
  (NS WARNO
    (exec
      [SOME (SLc (PL recon));
       SOME (SLc (PL tentativePlan));
       SOME (SLc (PSG initiateMovement));
       SOME (SLc (PL report1))])
    (Out WARNO
      (exec
        [SOME (SLc (PL recon));
         SOME (SLc (PL tentativePlan));
         SOME (SLc (PSG initiateMovement));
         SOME (SLc (PL report1)))]::outs))  $\iff$ 
authenticationTest inputOK
  [Name PlatoonLeader says prop (SOME (SLc (PL recon)));
   Name PlatoonLeader says
   prop (SOME (SLc (PL tentativePlan)));
   Name PlatoonSergeant says
   prop (SOME (SLc (PSG initiateMovement)));
   Name PlatoonLeader says
   prop (SOME (SLc (PL report1)))]  $\wedge$ 
CFGInterpret (M, Oi, Os)
  (CFG inputOK secContext secContextNull
    ([Name PlatoonLeader says
      prop (SOME (SLc (PL recon)));
      Name PlatoonLeader says
      prop (SOME (SLc (PL tentativePlan)));
      Name PlatoonSergeant says
      prop (SOME (SLc (PSG initiateMovement)));
      Name PlatoonLeader says
      prop (SOME (SLc (PL report1)))]::ins) WARNO outs)  $\wedge$ 
  (M, Oi, Os) satList
  [prop (SOME (SLc (PL recon)));
   prop (SOME (SLc (PL tentativePlan)));
   prop (SOME (SLc (PSG initiateMovement)));
   prop (SOME (SLc (PL report1)))]

```

**[PlatoonLeader\_WARNO\_exec\_report1\_lemma]**

$\vdash \forall M \ O_i \ O_s.$   
 CFGInterpret  $(M, O_i, O_s)$   
 (CFG inputOK secContext secContextNull  
 ([Name PlatoonLeader says  
 prop (SOME (SLc (PL recon)));  
 Name PlatoonLeader says  
 prop (SOME (SLc (PL tentativePlan)));  
 Name PlatoonSergeant says  
 prop (SOME (SLc (PSG initiateMovement)));  
 Name PlatoonLeader says  
 prop (SOME (SLc (PL report1)))]::ins) WARNO outs)  $\Rightarrow$   
 $(M, O_i, O_s)$  satList  
 propCommandList  
 [Name PlatoonLeader says prop (SOME (SLc (PL recon)));  
 Name PlatoonLeader says  
 prop (SOME (SLc (PL tentativePlan)));  
 Name PlatoonSergeant says  
 prop (SOME (SLc (PSG initiateMovement)));  
 Name PlatoonLeader says prop (SOME (SLc (PL report1)))]

**[PlatoonSergeant\_trap\_plCommand\_justified\_lemma]**

$\vdash \forall NS \ Out \ M \ O_i \ O_s.$   
 TR  $(M, O_i, O_s)$   
 (trap  
 (inputList  
 [Name PlatoonSergeant says  
 prop (SOME (SLc (PL plCommand)))]))  
 (CFG inputOK secContext secContextNull  
 ([Name PlatoonSergeant says  
 prop (SOME (SLc (PL plCommand)))]::ins) s outs)  
 (CFG inputOK secContext secContextNull ins  
 (NS s  
 (trap  
 (inputList  
 [Name PlatoonSergeant says  
 prop (SOME (SLc (PL plCommand)))])))  
 (Out s  
 (trap  
 (inputList  
 [Name PlatoonSergeant says  
 prop (SOME (SLc (PL plCommand)))])))::  
 outs))  $\iff$   
 authenticationTest inputOK  
 [Name PlatoonSergeant says  
 prop (SOME (SLc (PL plCommand)))]  $\wedge$   
 CFGInterpret  $(M, O_i, O_s)$   
 (CFG inputOK secContext secContextNull  
 ([Name PlatoonSergeant says



prop (SOME (SLc (PL *plCommand*))))]::ins) *s outs*) ∧  
(*M, Oi, Os*) sat prop NONE

[PlatoonSergeant\_trap\_plCommand\_justified\_thm]

⊢ ∀ *NS Out M Oi Os*.  
TR (*M, Oi, Os*) (trap [SOME (SLc (PL *plCommand*))])  
(CFG inputOK secContext secContextNull  
([Name PlatoonSergeant says  
prop (SOME (SLc (PL *plCommand*))))]::ins) *s outs*)  
(CFG inputOK secContext secContextNull *ins*  
(*NS s* (trap [SOME (SLc (PL *plCommand*))]))  
(*Out s* (trap [SOME (SLc (PL *plCommand*))])::outs)) ⇔  
authenticationTest inputOK  
[Name PlatoonSergeant says  
prop (SOME (SLc (PL *plCommand*)))] ∧  
CFGInterpret (*M, Oi, Os*)  
(CFG inputOK secContext secContextNull  
([Name PlatoonSergeant says  
prop (SOME (SLc (PL *plCommand*))))]::ins) *s outs*) ∧  
(*M, Oi, Os*) sat prop NONE

[PlatoonSergeant\_trap\_plCommand\_lemma]

⊢ ∀ *M Oi Os*.  
CFGInterpret (*M, Oi, Os*)  
(CFG inputOK secContext secContextNull  
([Name PlatoonSergeant says  
prop (SOME (SLc (PL *plCommand*))))]::ins) *s outs*) ⇒  
(*M, Oi, Os*) sat prop NONE

## 17 PlanPBType Theory

**Built:** 13 May 2018

**Parent Theories:** indexedLists, patternMatches

### 17.1 Datatypes

*plCommand* = receiveMission | warno | tentativePlan | recon  
| report1 | completePlan | opoid | supervise | report2  
| complete | plIncomplete | invalidPlCommand

*psgCommand* = initiateMovement | psgIncomplete  
| invalidPsgCommand

*slCommand* = PL *plCommand* | PSG *psgCommand*

*slOutput* = PlanPB | ReceiveMission | Warno | TentativePlan  
| InitiateMovement | Recon | Report1 | CompletePlan  
| Opoid | Supervise | Report2 | Complete  
| unAuthenticated | unauthorized

$$slState = \text{PLAN\_PB} \mid \text{RECEIVE\_MISSION} \mid \text{WARNO} \mid \text{TENTATIVE\_PLAN} \\ \mid \text{INITIATE\_MOVEMENT} \mid \text{RECON} \mid \text{REPORT1} \mid \text{COMPLETE\_PLAN} \\ \mid \text{OPOID} \mid \text{SUPERVISE} \mid \text{REPORT2} \mid \text{COMPLETE}$$

$$stateRole = \text{PlatoonLeader} \mid \text{PlatoonSergeant}$$

## 17.2 Theorems

### [plCommand\_distinct\_clauses]

$$\begin{aligned} \vdash & \text{receiveMission} \neq \text{warno} \wedge \text{receiveMission} \neq \text{tentativePlan} \wedge \\ & \text{receiveMission} \neq \text{recon} \wedge \text{receiveMission} \neq \text{report1} \wedge \\ & \text{receiveMission} \neq \text{completePlan} \wedge \text{receiveMission} \neq \text{opoid} \wedge \\ & \text{receiveMission} \neq \text{supervise} \wedge \text{receiveMission} \neq \text{report2} \wedge \\ & \text{receiveMission} \neq \text{complete} \wedge \text{receiveMission} \neq \text{plIncomplete} \wedge \\ & \text{receiveMission} \neq \text{invalidPlCommand} \wedge \text{warno} \neq \text{tentativePlan} \wedge \\ & \text{warno} \neq \text{recon} \wedge \text{warno} \neq \text{report1} \wedge \text{warno} \neq \text{completePlan} \wedge \\ & \text{warno} \neq \text{opoid} \wedge \text{warno} \neq \text{supervise} \wedge \text{warno} \neq \text{report2} \wedge \\ & \text{warno} \neq \text{complete} \wedge \text{warno} \neq \text{plIncomplete} \wedge \\ & \text{warno} \neq \text{invalidPlCommand} \wedge \text{tentativePlan} \neq \text{recon} \wedge \\ & \text{tentativePlan} \neq \text{report1} \wedge \text{tentativePlan} \neq \text{completePlan} \wedge \\ & \text{tentativePlan} \neq \text{opoid} \wedge \text{tentativePlan} \neq \text{supervise} \wedge \\ & \text{tentativePlan} \neq \text{report2} \wedge \text{tentativePlan} \neq \text{complete} \wedge \\ & \text{tentativePlan} \neq \text{plIncomplete} \wedge \\ & \text{tentativePlan} \neq \text{invalidPlCommand} \wedge \text{recon} \neq \text{report1} \wedge \\ & \text{recon} \neq \text{completePlan} \wedge \text{recon} \neq \text{opoid} \wedge \text{recon} \neq \text{supervise} \wedge \\ & \text{recon} \neq \text{report2} \wedge \text{recon} \neq \text{complete} \wedge \text{recon} \neq \text{plIncomplete} \wedge \\ & \text{recon} \neq \text{invalidPlCommand} \wedge \text{report1} \neq \text{completePlan} \wedge \\ & \text{report1} \neq \text{opoid} \wedge \text{report1} \neq \text{supervise} \wedge \text{report1} \neq \text{report2} \wedge \\ & \text{report1} \neq \text{complete} \wedge \text{report1} \neq \text{plIncomplete} \wedge \\ & \text{report1} \neq \text{invalidPlCommand} \wedge \text{completePlan} \neq \text{opoid} \wedge \\ & \text{completePlan} \neq \text{supervise} \wedge \text{completePlan} \neq \text{report2} \wedge \\ & \text{completePlan} \neq \text{complete} \wedge \text{completePlan} \neq \text{plIncomplete} \wedge \\ & \text{completePlan} \neq \text{invalidPlCommand} \wedge \text{opoid} \neq \text{supervise} \wedge \\ & \text{opoid} \neq \text{report2} \wedge \text{opoid} \neq \text{complete} \wedge \text{opoid} \neq \text{plIncomplete} \wedge \\ & \text{opoid} \neq \text{invalidPlCommand} \wedge \text{supervise} \neq \text{report2} \wedge \\ & \text{supervise} \neq \text{complete} \wedge \text{supervise} \neq \text{plIncomplete} \wedge \\ & \text{supervise} \neq \text{invalidPlCommand} \wedge \text{report2} \neq \text{complete} \wedge \\ & \text{report2} \neq \text{plIncomplete} \wedge \text{report2} \neq \text{invalidPlCommand} \wedge \\ & \text{complete} \neq \text{plIncomplete} \wedge \text{complete} \neq \text{invalidPlCommand} \wedge \\ & \text{plIncomplete} \neq \text{invalidPlCommand} \end{aligned}$$

### [psgCommand\_distinct\_clauses]

$$\begin{aligned} \vdash & \text{initiateMovement} \neq \text{psgIncomplete} \wedge \\ & \text{initiateMovement} \neq \text{invalidPsgCommand} \wedge \\ & \text{psgIncomplete} \neq \text{invalidPsgCommand} \end{aligned}$$

### [slCommand\_distinct\_clauses]

$$\vdash \forall a' a. \text{PL } a \neq \text{PSG } a'$$

[slCommand\_one\_one]

$$\vdash (\forall a \ a'. (PL \ a = PL \ a') \iff (a = a')) \wedge \\ \forall a \ a'. (PSG \ a = PSG \ a') \iff (a = a')$$

[slOutput\_distinct\_clauses]

$$\begin{aligned} &\vdash PlanPB \neq ReceiveMission \wedge PlanPB \neq Warno \wedge \\ &PlanPB \neq TentativePlan \wedge PlanPB \neq InitiateMovement \wedge \\ &PlanPB \neq Recon \wedge PlanPB \neq Report1 \wedge PlanPB \neq CompletePlan \wedge \\ &PlanPB \neq Opoid \wedge PlanPB \neq Supervise \wedge PlanPB \neq Report2 \wedge \\ &PlanPB \neq Complete \wedge PlanPB \neq unAuthenticated \wedge \\ &PlanPB \neq unAuthorized \wedge ReceiveMission \neq Warno \wedge \\ &ReceiveMission \neq TentativePlan \wedge \\ &ReceiveMission \neq InitiateMovement \wedge ReceiveMission \neq Recon \wedge \\ &ReceiveMission \neq Report1 \wedge ReceiveMission \neq CompletePlan \wedge \\ &ReceiveMission \neq Opoid \wedge ReceiveMission \neq Supervise \wedge \\ &ReceiveMission \neq Report2 \wedge ReceiveMission \neq Complete \wedge \\ &ReceiveMission \neq unAuthenticated \wedge \\ &ReceiveMission \neq unAuthorized \wedge Warno \neq TentativePlan \wedge \\ &Warno \neq InitiateMovement \wedge Warno \neq Recon \wedge Warno \neq Report1 \wedge \\ &Warno \neq CompletePlan \wedge Warno \neq Opoid \wedge Warno \neq Supervise \wedge \\ &Warno \neq Report2 \wedge Warno \neq Complete \wedge \\ &Warno \neq unAuthenticated \wedge Warno \neq unAuthorized \wedge \\ &TentativePlan \neq InitiateMovement \wedge TentativePlan \neq Recon \wedge \\ &TentativePlan \neq Report1 \wedge TentativePlan \neq CompletePlan \wedge \\ &TentativePlan \neq Opoid \wedge TentativePlan \neq Supervise \wedge \\ &TentativePlan \neq Report2 \wedge TentativePlan \neq Complete \wedge \\ &TentativePlan \neq unAuthenticated \wedge \\ &TentativePlan \neq unAuthorized \wedge InitiateMovement \neq Recon \wedge \\ &InitiateMovement \neq Report1 \wedge \\ &InitiateMovement \neq CompletePlan \wedge InitiateMovement \neq Opoid \wedge \\ &InitiateMovement \neq Supervise \wedge InitiateMovement \neq Report2 \wedge \\ &InitiateMovement \neq Complete \wedge \\ &InitiateMovement \neq unAuthenticated \wedge \\ &InitiateMovement \neq unAuthorized \wedge Recon \neq Report1 \wedge \\ &Recon \neq CompletePlan \wedge Recon \neq Opoid \wedge Recon \neq Supervise \wedge \\ &Recon \neq Report2 \wedge Recon \neq Complete \wedge \\ &Recon \neq unAuthenticated \wedge Recon \neq unAuthorized \wedge \\ &Report1 \neq CompletePlan \wedge Report1 \neq Opoid \wedge \\ &Report1 \neq Supervise \wedge Report1 \neq Report2 \wedge \\ &Report1 \neq Complete \wedge Report1 \neq unAuthenticated \wedge \\ &Report1 \neq unAuthorized \wedge CompletePlan \neq Opoid \wedge \\ &CompletePlan \neq Supervise \wedge CompletePlan \neq Report2 \wedge \\ &CompletePlan \neq Complete \wedge CompletePlan \neq unAuthenticated \wedge \\ &CompletePlan \neq unAuthorized \wedge Opoid \neq Supervise \wedge \\ &Opoid \neq Report2 \wedge Opoid \neq Complete \wedge \\ &Opoid \neq unAuthenticated \wedge Opoid \neq unAuthorized \wedge \\ &Supervise \neq Report2 \wedge Supervise \neq Complete \wedge \\ &Supervise \neq unAuthenticated \wedge Supervise \neq unAuthorized \wedge \\ &Report2 \neq Complete \wedge Report2 \neq unAuthenticated \wedge \end{aligned}$$

Report2  $\neq$  unauthorized  $\wedge$  Complete  $\neq$  unAuthenticated  $\wedge$   
 Complete  $\neq$  unauthorized  $\wedge$  unAuthenticated  $\neq$  unauthorized

[slRole\_distinct\_clauses]

$\vdash$  PlatoonLeader  $\neq$  PlatoonSergeant

[slState\_distinct\_clauses]

$\vdash$  PLAN\_PB  $\neq$  RECEIVE\_MISSION  $\wedge$  PLAN\_PB  $\neq$  WARNO  $\wedge$   
 PLAN\_PB  $\neq$  TENTATIVE\_PLAN  $\wedge$  PLAN\_PB  $\neq$  INITIATE\_MOVEMENT  $\wedge$   
 PLAN\_PB  $\neq$  RECON  $\wedge$  PLAN\_PB  $\neq$  REPORT1  $\wedge$   
 PLAN\_PB  $\neq$  COMPLETE\_PLAN  $\wedge$  PLAN\_PB  $\neq$  OPOID  $\wedge$   
 PLAN\_PB  $\neq$  SUPERVISE  $\wedge$  PLAN\_PB  $\neq$  REPORT2  $\wedge$   
 PLAN\_PB  $\neq$  COMPLETE  $\wedge$  RECEIVE\_MISSION  $\neq$  WARNO  $\wedge$   
 RECEIVE\_MISSION  $\neq$  TENTATIVE\_PLAN  $\wedge$   
 RECEIVE\_MISSION  $\neq$  INITIATE\_MOVEMENT  $\wedge$   
 RECEIVE\_MISSION  $\neq$  RECON  $\wedge$  RECEIVE\_MISSION  $\neq$  REPORT1  $\wedge$   
 RECEIVE\_MISSION  $\neq$  COMPLETE\_PLAN  $\wedge$  RECEIVE\_MISSION  $\neq$  OPOID  $\wedge$   
 RECEIVE\_MISSION  $\neq$  SUPERVISE  $\wedge$  RECEIVE\_MISSION  $\neq$  REPORT2  $\wedge$   
 RECEIVE\_MISSION  $\neq$  COMPLETE  $\wedge$  WARNO  $\neq$  TENTATIVE\_PLAN  $\wedge$   
 WARNO  $\neq$  INITIATE\_MOVEMENT  $\wedge$  WARNO  $\neq$  RECON  $\wedge$  WARNO  $\neq$  REPORT1  $\wedge$   
 WARNO  $\neq$  COMPLETE\_PLAN  $\wedge$  WARNO  $\neq$  OPOID  $\wedge$  WARNO  $\neq$  SUPERVISE  $\wedge$   
 WARNO  $\neq$  REPORT2  $\wedge$  WARNO  $\neq$  COMPLETE  $\wedge$   
 TENTATIVE\_PLAN  $\neq$  INITIATE\_MOVEMENT  $\wedge$  TENTATIVE\_PLAN  $\neq$  RECON  $\wedge$   
 TENTATIVE\_PLAN  $\neq$  REPORT1  $\wedge$  TENTATIVE\_PLAN  $\neq$  COMPLETE\_PLAN  $\wedge$   
 TENTATIVE\_PLAN  $\neq$  OPOID  $\wedge$  TENTATIVE\_PLAN  $\neq$  SUPERVISE  $\wedge$   
 TENTATIVE\_PLAN  $\neq$  REPORT2  $\wedge$  TENTATIVE\_PLAN  $\neq$  COMPLETE  $\wedge$   
 INITIATE\_MOVEMENT  $\neq$  RECON  $\wedge$  INITIATE\_MOVEMENT  $\neq$  REPORT1  $\wedge$   
 INITIATE\_MOVEMENT  $\neq$  COMPLETE\_PLAN  $\wedge$   
 INITIATE\_MOVEMENT  $\neq$  OPOID  $\wedge$  INITIATE\_MOVEMENT  $\neq$  SUPERVISE  $\wedge$   
 INITIATE\_MOVEMENT  $\neq$  REPORT2  $\wedge$  INITIATE\_MOVEMENT  $\neq$  COMPLETE  $\wedge$   
 RECON  $\neq$  REPORT1  $\wedge$  RECON  $\neq$  COMPLETE\_PLAN  $\wedge$  RECON  $\neq$  OPOID  $\wedge$   
 RECON  $\neq$  SUPERVISE  $\wedge$  RECON  $\neq$  REPORT2  $\wedge$  RECON  $\neq$  COMPLETE  $\wedge$   
 REPORT1  $\neq$  COMPLETE\_PLAN  $\wedge$  REPORT1  $\neq$  OPOID  $\wedge$   
 REPORT1  $\neq$  SUPERVISE  $\wedge$  REPORT1  $\neq$  REPORT2  $\wedge$   
 REPORT1  $\neq$  COMPLETE  $\wedge$  COMPLETE\_PLAN  $\neq$  OPOID  $\wedge$   
 COMPLETE\_PLAN  $\neq$  SUPERVISE  $\wedge$  COMPLETE\_PLAN  $\neq$  REPORT2  $\wedge$   
 COMPLETE\_PLAN  $\neq$  COMPLETE  $\wedge$  OPOID  $\neq$  SUPERVISE  $\wedge$   
 OPOID  $\neq$  REPORT2  $\wedge$  OPOID  $\neq$  COMPLETE  $\wedge$  SUPERVISE  $\neq$  REPORT2  $\wedge$   
 SUPERVISE  $\neq$  COMPLETE  $\wedge$  REPORT2  $\neq$  COMPLETE

## Index

### **ConductORPType Theory**, 38

Datatypes, 38

Theorems, 39

plCommand\_distinct\_clauses, 39

psgCommand\_distinct\_clauses, 39

slCommand\_distinct\_clauses, 39

slCommand\_one\_one, 39

slOutput\_distinct\_clauses, 39

slRole\_distinct\_clauses, 39

slState\_distinct\_clauses, 39

### **ConductPBType Theory**, 45

Datatypes, 45

Theorems, 45

plCommandPB\_distinct\_clauses, 45

psgCommandPB\_distinct\_clauses, 45

slCommand\_distinct\_clauses, 45

slCommand\_one\_one, 45

slOutput\_distinct\_clauses, 46

slRole\_distinct\_clauses, 46

slState\_distinct\_clauses, 46

### **MoveToORPType Theory**, 51

Datatypes, 51

Theorems, 51

slCommand\_distinct\_clauses, 51

slOutput\_distinct\_clauses, 51

slState\_distinct\_clauses, 51

### **MoveToPBType Theory**, 56

Datatypes, 56

Theorems, 56

slCommand\_distinct\_clauses, 56

slOutput\_distinct\_clauses, 57

slState\_distinct\_clauses, 57

### **OMNIType Theory**, 3

Datatypes, 3

Theorems, 3

command\_distinct\_clauses, 3

command\_one\_one, 3

escCommand\_distinct\_clauses, 3

escOutput\_distinct\_clauses, 3

escState\_distinct\_clauses, 3

output\_distinct\_clauses, 4

output\_one\_one, 4

principal\_one\_one, 4

state\_distinct\_clauses, 4

state\_one\_one, 4

### **PBIntegratedDef Theory**, 28

Definitions, 28

secAuthorization\_def, 28

secHelper\_def, 28

Theorems, 28

getOmniCommand\_def, 28

getOmniCommand\_ind, 31

secContext\_def, 32

secContext\_ind, 33

### **PBTypeIntegrated Theory**, 26

Datatypes, 26

Theorems, 27

omniCommand\_distinct\_clauses, 27

plCommand\_distinct\_clauses, 27

slCommand\_distinct\_clauses, 27

slCommand\_one\_one, 27

slOutput\_distinct\_clauses, 27

slState\_distinct\_clauses, 28

stateRole\_distinct\_clauses, 28

### **PlanPBType Theory**, 67

Datatypes, 67

Theorems, 68

plCommand\_distinct\_clauses, 68

psgCommand\_distinct\_clauses, 68

slCommand\_distinct\_clauses, 68

slCommand\_one\_one, 69

slOutput\_distinct\_clauses, 69

slRole\_distinct\_clauses, 70

slState\_distinct\_clauses, 70

### **satList Theory**, 21

Definitions, 21

satList\_def, 21

Theorems, 21

- satList\_conj, 21
- satList\_CONS, 21
- satList\_nil, 21
- ssm Theory**, 11
  - Datatypes, 11
  - Definitions, 12
    - authenticationTest\_def, 12
    - commandList\_def, 12
    - inputList\_def, 12
    - propCommandList\_def, 12
    - TR\_def, 12
  - Theorems, 13
    - CFGInterpret\_def, 13
    - CFGInterpret\_ind, 13
    - configuration\_one\_one, 13
    - extractCommand\_def, 13
    - extractCommand\_ind, 13
    - extractInput\_def, 14
    - extractInput\_ind, 14
    - extractPropCommand\_def, 15
    - extractPropCommand\_ind, 15
    - TR\_cases, 16
    - TR\_discard\_cmd\_rule, 17
    - TR\_EQ\_rules\_thm, 17
    - TR\_exec\_cmd\_rule, 17
    - TR\_ind, 18
    - TR\_rules, 18
    - TR\_strongind, 19
    - TR\_trap\_cmd\_rule, 20
    - TRrule0, 20
    - TRrule1, 20
    - trType\_distinct\_clauses, 20
    - trType\_one\_one, 21
- ssm11 Theory**, 4
  - Datatypes, 4
  - Definitions, 4
    - TR\_def, 4
  - Theorems, 5
    - CFGInterpret\_def, 5
    - CFGInterpret\_ind, 6
    - configuration\_one\_one, 6
    - order\_distinct\_clauses, 6
    - order\_one\_one, 6
- TR\_cases, 6
- TR\_discard\_cmd\_rule, 7
- TR\_EQ\_rules\_thm, 7
- TR\_exec\_cmd\_rule, 8
- TR\_ind, 8
- TR\_rules, 9
- TR\_strongind, 9
- TR\_trap\_cmd\_rule, 10
- TRrule0, 10
- TRrule1, 11
- trType\_distinct\_clauses, 11
- trType\_one\_one, 11
- ssmConductORP Theory**, 33
  - Definitions, 33
    - secContextConductORP\_def, 33
    - ssmConductORPStateInterp\_def, 33
  - Theorems, 33
    - authTestConductORP\_cmd\_reject\_lemma, 33
    - authTestConductORP\_def, 34
    - authTestConductORP\_ind, 34
    - conductORPNS\_def, 35
    - conductORPNS\_ind, 35
    - conductORPOut\_def, 36
    - conductORPOut\_ind, 36
    - PlatoonLeader\_exec\_plCommand\_justified\_thm, 37
    - PlatoonLeader\_plCommand\_lemma, 37
    - PlatoonSergeant\_exec\_psgCommand\_justified\_thm, 38
    - PlatoonSergeant\_psgCommand\_lemma, 38
- ssmConductPB Theory**, 39
  - Definitions, 40
    - secContextConductPB\_def, 40
    - ssmConductPBStateInterp\_def, 40
  - Theorems, 40
    - authTestConductPB\_cmd\_reject\_lemma, 40
    - authTestConductPB\_def, 40
    - authTestConductPB\_ind, 41
    - conductPBNS\_def, 42
    - conductPBNS\_ind, 42

conductPBOut\_def, 43  
 conductPBOut\_ind, 43  
 PlatoonLeader\_exec\_plCommandPB\_-justified\_thm, 44  
 PlatoonLeader\_plCommandPB\_lemma, 44  
 PlatoonSergeant\_exec\_psgCommandPB\_-justified\_thm, 44  
 PlatoonSergeant\_psgCommandPB\_lemma, 45  
**ssmMoveToORP Theory**, 46  
 Definitions, 46  
 secContextMoveToORP\_def, 46  
 ssmMoveToORPStateInterp\_def, 46  
 Theorems, 46  
 authTestMoveToORP\_cmd\_reject\_lemma, 46  
 authTestMoveToORP\_def, 47  
 authTestMoveToORP\_ind, 47  
 moveToORPNS\_def, 48  
 moveToORPNS\_ind, 48  
 moveToORPOut\_def, 49  
 moveToORPOut\_ind, 49  
 PlatoonLeader\_exec\_slCommand\_justified\_thm, 50  
 PlatoonLeader\_slCommand\_lemma, 50  
**ssmMoveToPB Theory**, 52  
 Definitions, 52  
 secContextMoveToPB\_def, 52  
 ssmMoveToPBStateInterp\_def, 52  
 Theorems, 52  
 authTestMoveToPB\_cmd\_reject\_lemma, 52  
 authTestMoveToPB\_def, 52  
 authTestMoveToPB\_ind, 53  
 moveToPBNS\_def, 53  
 moveToPBNS\_ind, 54  
 moveToPBOut\_def, 54  
 moveToPBOut\_ind, 55  
 PlatoonLeader\_exec\_slCommand\_justified\_thm, 55  
 PlatoonLeader\_slCommand\_lemma, 56  
**ssmPB Theory**, 21  
 Definitions, 21  
 secContext\_def, 21  
 ssmPBStateInterp\_def, 21  
 Theorems, 22  
 authenticationTest\_cmd\_reject\_lemma, 22  
 authenticationTest\_def, 22  
 authenticationTest\_ind, 22  
 PBNS\_def, 23  
 PBNS\_ind, 23  
 PBOut\_def, 24  
 PBOut\_ind, 25  
 PlatoonLeader\_exec\_slCommand\_justified\_thm, 26  
 PlatoonLeader\_slCommand\_lemma, 26  
**ssmPlanPB Theory**, 57  
 Theorems, 57  
 inputOK\_def, 57  
 inputOK\_ind, 58  
 planPBNS\_def, 59  
 planPBNS\_ind, 59  
 planPBOut\_def, 59  
 planPBOut\_ind, 60  
 PlatoonLeader\_notWARNO\_notreport1\_exec\_plCommand\_justified\_lemma, 60  
 PlatoonLeader\_notWARNO\_notreport1\_exec\_plCommand\_justified\_thm, 61  
 PlatoonLeader\_notWARNO\_notreport1\_exec\_plCommand\_lemma, 61  
 PlatoonLeader\_psgCommand\_notDiscard\_thm, 62  
 PlatoonLeader\_trap\_psgCommand\_justified\_lemma, 62  
 PlatoonLeader\_trap\_psgCommand\_lemma, 63  
 PlatoonLeader\_WARNO\_exec\_report1\_justified\_lemma, 63  
 PlatoonLeader\_WARNO\_exec\_report1\_justified\_thm, 64  
 PlatoonLeader\_WARNO\_exec\_report1\_lemma, 66  
 PlatoonSergeant\_trap\_plCommand\_justified\_lemma, 66

PlatoonSergeant\_trap\_plCommand\_justified.thm, 67  
PlatoonSergeant\_trap\_plCommand\_lemma, 67



# Appendix C

## Secure State Machine Theories: HOL Script Files

### C.1 ssm

```
(*****)
(* Secure State Machine Theory: authentication, authorization, and state *)
(* interpretation. *)
(* Author: Shiu-Kai Chin *)
(* Date: 27 November 2015 *)
(*****)

structure ssmScript = struct

  (* ===== Interactive mode ===== *)
  app load ["TypeBase", "ssminfRules", "listTheory", "optionTheory", "acl_infRules",
            "satListTheory", "ssmTheory"];
  open TypeBase listTheory ssminfRules optionTheory acl_infRules satListTheory ssmTheory

  app load ["TypeBase", "ssminfRules", "listTheory", "optionTheory", "acl_infRules",
            "satListTheory"];
  open TypeBase listTheory ssminfRules optionTheory acl_infRules satListTheory
        ssmTheory
  ===== end interactive mode ===== *)

open HolKernel boolLib Parse bossLib
open TypeBase listTheory optionTheory ssminfRules acl_infRules satListTheory
  (*****)
  (* create a new theory *)
  (*****)
val _ = new_theory "ssm";

  (* ----- *)
  (* Define the type of transition: discard, execute, or trap. We discard from *)
  (* the input stream those inputs that are not of the form P says command. We *)
  (* execute commands that users and supervisors are authorized for. We trap *)
  (* commands that users are not authorized to execute. *)
  (* ----- *)

  (* ----- *)
  (* In keeping with virtual machine design principles as described by Popek *)
  (* and Goldberg, we add a TRAP instruction to the commands by users. *)
  (* In effect, we are LIFTING the commands available to users to include the *)
  (* TRAP instruction used by the state machine to handle authorization errors. *)
  (* ----- *)
```

```

val _ =
Datatype


```

```

val extractCommand_def =
Define
'extractCommand (P says (prop (SOME cmd)):( 'command option , 'principal , 'd , 'e)Form) =
  cmd';

val commandList_def =
Define
'commandList (x:( 'command option , 'principal , 'd , 'e)Form list) =
  MAP extractCommand x';

val extractPropCommand_def =
Define
'(extractPropCommand (P says (prop (SOME cmd)):( 'command option , 'principal , 'd , 'e)Form) =
  ((prop (SOME cmd)):( 'command option , 'principal , 'd , 'e)Form))';

val propCommandList_def =
Define
'propCommandList (x:( 'command option , 'principal , 'd , 'e)Form list) =
  MAP extractPropCommand x';

val extractInput_def =
Define
'extractInput (P says (prop x):( 'command option , 'principal , 'd , 'e)Form) = x';

val inputList_def =
Define
'inputList (xs:( 'command option , 'principal , 'd , 'e)Form list) =
  MAP extractInput xs';

(* ----- *)
(* Define transition relation among configurations. This definition is *)
(* parameterized in terms of next-state transition function and output *)
(* function. *)
(* ----- *)
val (TR_rules , TR_ind , TR_cases) =
Hol_reln
'(! (elementTest:( 'command option , 'principal , 'd , 'e)Form -> bool)
  (NS: 'state -> ( 'command option list) trType -> 'state) M Oi Os Out (s: 'state)
  (context:( ( 'command option , 'principal , 'd , 'e)Form list) ->
    (( 'command option , 'principal , 'd , 'e)Form list))
  (stateInterp: 'state -> ( 'command option , 'principal , 'd , 'e)Form list ->
    ( 'command option , 'principal , 'd , 'e)Form list)
  (x:( 'command option , 'principal , 'd , 'e)Form list)
  (ins:( 'command option , 'principal , 'd , 'e)Form list list)
  (outs: 'output list)).
(authenticationTest elementTest x) /\
(CFGInterpret (M,Oi,Os)
  (CFG elementTest stateInterp context (x::ins) s outs)) ==>
(TR
  ((M:( 'command option , 'b , 'principal , 'd , 'e)Kripke),Oi: 'd po,Os: 'e po)
  (exec (inputList x))
  (CFG elementTest stateInterp context (x::ins) s outs)
  (CFG elementTest stateInterp context ins
    (NS s (exec (inputList x))))
  ((Out s (exec (inputList x)))::outs)))) /\
'(! (elementTest:( 'command option , 'principal , 'd , 'e)Form -> bool)
  (NS: 'state -> ( 'command option list) trType -> 'state) M Oi Os Out (s: 'state)
  (context:( ( 'command option , 'principal , 'd , 'e)Form list) ->
    (( 'command option , 'principal , 'd , 'e)Form list))
  (stateInterp: 'state -> ( 'command option , 'principal , 'd , 'e)Form list ->
    ( 'command option , 'principal , 'd , 'e)Form list)
  (x:( 'command option , 'principal , 'd , 'e)Form list)
  (ins:( 'command option , 'principal , 'd , 'e)Form list list)
  (outs: 'output list)).
(authenticationTest elementTest x) /\
(CFGInterpret (M,Oi,Os)
  (CFG elementTest stateInterp context (x::ins) s outs)) ==>
(TR
  ((M:( 'command option , 'b , 'principal , 'd , 'e)Kripke),Oi: 'd po,Os: 'e po)
  (trap (inputList x))
  (CFG elementTest stateInterp context (x::ins) s outs)
  (CFG elementTest stateInterp context ins

```

```

      (NS s (trap (inputList x)))
      ((Out s (trap (inputList x)))::outs)))) /\
(! (elementTest:( 'command option , 'principal , 'd , 'e)Form -> bool)
  (NS: 'state -> ( 'command option list ) trType -> 'state) M Oi Os Out (s: 'state)
  (context:(( 'command option , 'principal , 'd , 'e)Form list) ->
    (( 'command option , 'principal , 'd , 'e)Form list))
  (stateInterp: 'state -> ( 'command option , 'principal , 'd , 'e)Form list ->
    ( 'command option , 'principal , 'd , 'e)Form list)
  (x:( 'command option , 'principal , 'd , 'e)Form list)
  (ins:( 'command option , 'principal , 'd , 'e)Form list list)
  (outs: 'output list).
~(authenticationTest elementTest x) ==>
(TR
  ((M:( 'command option , 'b , 'principal , 'd , 'e)Kripke), Oi: 'd po, Os: 'e po)
  (discard (inputList x))
  (CFG elementTest stateInterp context (x::ins) s outs)
  (CFG elementTest stateInterp context ins
    (NS s (discard (inputList x)))
    ((Out s (discard (inputList x)))::outs)))) ‘

(* ----- *)
(* Split up TR_rules into individual clauses *)
(* ----- *)
val [rule0, rule1, rule2] = CONJUNCTS TR_rules

(* ----- *)
(* Prove the converse of rule0, rule1, and rule2 *)
(* ----- *)
val TR_lemma0 =
TAC.PROOF([[] , flip_TR_rules rule0),
DISCH_TAC THEN
IMP.RES_TAC TR_cases THEN
PAT.ASSUM
  ‘‘exec cmd = y‘‘
  (fn th => ASSUME_TAC(REWRITE_RULE[trType_one_one, trType_distinct_clauses]th)) THEN
PROVE_TAC[configuration_one_one, list_11, trType_distinct_clauses])

val TR_lemma1 =
TAC.PROOF([[] , flip_TR_rules rule1),
DISCH_TAC THEN
IMP.RES_TAC TR_cases THEN
PAT.ASSUM
  ‘‘trap cmd = y‘‘
  (fn th => ASSUME_TAC(REWRITE_RULE[trType_one_one, trType_distinct_clauses]th)) THEN
PROVE_TAC[configuration_one_one, list_11, trType_distinct_clauses])

val TR_lemma2 =
TAC.PROOF([[] , flip_TR_rules rule2),
DISCH_TAC THEN
IMP.RES_TAC TR_cases THEN
PAT.ASSUM
  ‘‘discard (inputList x) = y‘‘
  (fn th => ASSUME_TAC(REWRITE_RULE[trType_one_one, trType_distinct_clauses]th)) THEN
PROVE_TAC[configuration_one_one, list_11, trType_distinct_clauses])

val TR_rules_converse =
TAC.PROOF([[] , flip_TR_rules TR_rules),
REWRITE_TAC[TR_lemma0, TR_lemma1, TR_lemma2])

val TR_EQ_rules_thm = TR_EQ_rules TR_rules TR_rules_converse

val _ = save_thm("TR_EQ_rules_thm", TR_EQ_rules_thm)

val [TRrule0, TRrule1, TR_discard_cmd_rule] = CONJUNCTS TR_EQ_rules_thm

val _ = save_thm("TRrule0", TRrule0)
val _ = save_thm("TRrule1", TRrule1)
val _ = save_thm("TR_discard_cmd_rule", TR_discard_cmd_rule)

(* ----- *)
(* If (CFGInterpret *)

```

```

(*      (M,Oi,Os) *)
(*      (CFG elementTest stateInterpret certList *)
(*      ((P says (prop (CMD cmd))::ins) s outs) ==> *)
(*      ((M,Oi,Os) sat (prop (CMD cmd)))) *)
(* is a valid inference rule, then executing cmd the exec(CMD cmd) transition *)
(* occurs if and only if prop (CMD cmd), elementTest, and *)
(* CFGInterpret (M,Oi,Os) *)
(* (CFG elementTest stateInterpret certList (P says prop (CMD cmd)::ins) s outs) *)
(* are true. *)
(* ----- *)
val TR_exec_cmd_rule =
TAC.PROOF([[] ,
  “!elementTest context stateInterp (x:(’command option,’principal,’d,’e)Form list)
    ins s outs.
  (!M Oi Os.
  (CFGInterpret
    (M :(’command option,’b,’principal,’d,’e) Kripke),(Oi :’d po), (Os :’e po))
    (CFG elementTest
      (stateInterp:’state -> (’command option,’principal,’d,’e)Form list ->
        (’command option,’principal,’d,’e)Form list) context
      (x::ins)
      (s:’state) (outs:’output list))) ==>
    (M,Oi,Os) satList (propCommandList (x:(’command option,’principal,’d,’e)Form list))) ==>
  (!NS Out M Oi Os.
  TR
    ((M :(’command option,’b,’principal,’d,’e) Kripke),(Oi :’d po),
    (Os :’e po)) (exec (inputList x))
    (CFG (elementTest :(’command option,’principal,’d,’e) Form -> bool)
      (stateInterp:’state -> (’command option,’principal,’d,’e)Form list ->
        (’command option,’principal,’d,’e)Form list)
      (context :(’command option,’principal,’d,’e) Form list ->
        (’command option,’principal,’d,’e) Form list)
      (x::ins)
      (s :’state) (outs :’output list))
    (CFG elementTest stateInterp context ins
      ((NS :’state -> ’command option list trType -> ’state) s (exec (inputList x)))
      (Out s (exec (inputList x))::outs)) <=>
    (authenticationTest elementTest x) /\
    (CFGInterpret (M,Oi,Os)
      (CFG elementTest stateInterp context (x::ins) s outs)) /\
    (M,Oi,Os) satList (propCommandList x))’),
REWRITE_TAC[TRrule0] THEN
REPEAT STRIP_TAC THEN
EQ_TAC THEN
REPEAT STRIP_TAC THEN
PROVE_TAC[]])

```

```

val - = save_thm("TR_exec_cmd_rule",TR_exec_cmd_rule)

```

```

(* ----- *)
(* If (CFGInterpret *)
(*      (M,Oi,Os) *)
(*      (CFG elementTest stateInterpret certList *)
(*      ((P says (prop (CMD cmd))::ins) s outs) ==> *)
(*      ((M,Oi,Os) sat (prop TRAP))) *)
(* is a valid inference rule, then executing cmd the trap(CMD cmd) transition *)
(* occurs if and only if prop TRAP, elementTest, and *)
(* CFGInterpret (M,Oi,Os) *)
(* (CFG elementTest stateInterpret certList (P says prop (CMD cmd)::ins) *)
(*      s outs) are true. *)
(* ----- *)
val TR_trap_cmd_rule =
TAC.PROOF(
  ([[] , “!elementTest context stateInterp (x:(’command option,’principal,’d,’e)Form list)
    ins s outs.
  (!M Oi Os.
  (CFGInterpret
    (M :(’command option,’b,’principal,’d,’e) Kripke),(Oi :’d po), (Os :’e po))
    (CFG elementTest
      (stateInterp:’state -> (’command option,’principal,’d,’e)Form list ->
        (’command option,’principal,’d,’e)Form list) context
      (x::ins)
      (s:’state) (outs:’output list))) ==>

```

```

(M,Oi,Os) sat (prop NONE)) ==>
(!NS Out M Oi Os.
TR
((M :('command option, 'b, 'principal, 'd, 'e) Kripke),(Oi : 'd po),
(Os : 'e po)) (trap (inputList x))
(CFG (elementTest :('command option, 'principal, 'd, 'e) Form -> bool)
(stateInterp : 'state -> ('command option, 'principal, 'd, 'e) Form list ->
('command option, 'principal, 'd, 'e) Form list)
(context :('command option, 'principal, 'd, 'e) Form list ->
('command option, 'principal, 'd, 'e) Form list)
(x::ins)
(s : 'state) (outs : 'output list))
(CFG elementTest stateInterp context ins
((NS : 'state -> 'command option list trType -> 'state) s (trap (inputList x)))
(Out s (trap (inputList x))::outs)) <=>
(authenticationTest elementTest x) /\
(CFGInterpret (M,Oi,Os)
(CFG elementTest stateInterp context (x::ins) s outs)) /\
(M,Oi,Os) sat (prop NONE)) ' ',
REWRITE_TAC[TRrule1] THEN
REPEAT STRIP_TAC THEN
EQ_TAC THEN
REPEAT STRIP_TAC THEN
PROVE_TAC[]

val _ = save_thm("TR_trap_cmd_rule", TR_trap_cmd_rule)

(* ===== start here =====
===== end here ===== *)

val _ = export_theory ();
val _ = print_theory " ";

end (* structure *)

```

## C.2 satList

```

(* ----- *)
(* Definition of satList for conjunctions of ACL formulas *)
(* Author: Shiu-Kai Chin *)
(* Date: 24 July 2014 *)
(* ----- *)
structure satListScript = struct

(* interactive mode
app load
["TypeBase","listTheory","acl_infRules"];
*)
open HolKernel boolLib Parse bossLib
open TypeBase acl_infRules listTheory

(* *****
* create a new theory
* ***** *)
val _ = new_theory "satList";

(* *****
(* Configurations and policies are represented by lists *)
(* of formulas in the access-control logic. *)
(* Previously, for a formula f in the access-control logic, *)
(* we ultimately interpreted it within the context of a *)
(* Kripke structure M and partial orders Oi:'Int po and *)
(* Os:'Sec po. This is represented as (M,Oi,Os) sat f. *)
(* The natural extension is to interpret a list of formulas *)
(* [f0;...;fn] as a conjunction: *)
(* (M,Oi,Os) sat f0 /\ ... /\ (M,Oi,Os) sat fn *)
(* ***** *)

val _ = set_fixity "satList" (Infixr 540);

```

```

val satList_def =
Define
‘((M:( ’prop, ’world, ’pName, ’Int, ’Sec)Kripke),(Oi: ’Int po),(Os: ’Sec po))
satList
formList =
FOLDR
(\x y. x /\ y) T
(MAP
(\ (f:( ’prop, ’pName, ’Int, ’Sec)Form).
((M:( ’prop, ’world, ’pName, ’Int, ’Sec)Kripke),
Oi: ’Int po,Os: ’Sec po) sat f)formList) ‘;

(*****
(* Properties of satList *)
*****)
val satList_nil =
TAC.PROOF(
([],
‘((M:( ’prop, ’world, ’pName, ’Int, ’Sec)Kripke),(Oi: ’Int po),(Os: ’Sec po)) satList [] ‘),
REWRITE_TAC[satList_def,FOLDR,MAP])

val _ = save_thm("satList_nil",satList_nil)

val satList_conj =
TAC.PROOF(
([],
‘!l1 l2 M Oi Os.(((M:( ’prop, ’world, ’pName, ’Int, ’Sec)Kripke),(Oi: ’Int po),(Os: ’Sec po))
satList l1) /\
((M:( ’prop, ’world, ’pName, ’Int, ’Sec)Kripke),(Oi: ’Int po),(Os: ’Sec po))
satList l2) =
((M:( ’prop, ’world, ’pName, ’Int, ’Sec)Kripke),(Oi: ’Int po),(Os: ’Sec po))
satList (l1 ++ l2)) ‘),
Induct THEN
REWRITE_TAC[APPEND,satList_nil] THEN
REWRITE_TAC[satList_def,MAP] THEN
CONV_TAC(DEPTHCONV BETA.CONV) THEN
REWRITE_TAC[FOLDR] THEN
CONV_TAC(DEPTHCONV BETA.CONV) THEN
REWRITE_TAC[GSYM satList_def] THEN
PROVE_TAC[])

val _ = save_thm("satList_conj",satList_conj)

val satList_CONS =
TAC.PROOF(([],
‘!h t M Oi Os.(((M:( ’prop, ’world, ’pName, ’Int, ’Sec)Kripke),(Oi: ’Int po),(Os: ’Sec po))
satList (h::t)) =
((M,Oi,Os) sat h) /\
((M:( ’prop, ’world, ’pName, ’Int, ’Sec)Kripke),(Oi: ’Int po),(Os: ’Sec po))
satList t)) ‘),
REPEAT STRIP_TAC THEN
REWRITE_TAC[satList_def,MAP] THEN
CONV_TAC(DEPTHCONV BETA.CONV) THEN
REWRITE_TAC[FOLDR] THEN
CONV_TAC(DEPTHCONV BETA.CONV) THEN
REWRITE_TAC[])

val _ = save_thm("satList_CONS",satList_CONS)

val _ = export_theory ();
val _ = print_theory "–";

end (* structure *)

```

# Appendix D

## Secure State Machine Theories Applied to Patrol Base Operations: HOL Script Files

### D.1 OMNILEvel

```
(*****  
(* OMNIScript *)  
(* Author: Lori Pickering *)  
(* Date: 10 May 2018 *)  
(* This file is intended to allow for integration among the ssms. The idea *)  
(* is to provide an OMNI-level integrating theory, in the sense of a super- *)  
(* conscious that knows when each ssm is complete and provides that info to *)  
(* higher-level state machines. *)  
(*****)  
  
structure OMNIScript = struct  
  
  (* ===== Interactive Mode =====  
  app load ["TypeBase","listTheory", "optionTheory",  
           "OMNITypeTheory",  
           "acl_infRules","aclDrulesTheory","aclrulesTheory"];  
  open TypeBase listTheory optionTheory  
        OMNITypeTheory  
        acl_infRules aclDrulesTheory aclrulesTheory  
        ===== End Interactive Mode ===== *)  
  
  open HolKernel Parse boolLib bossLib;  
  open TypeBase listTheory optionTheory  
  open OMNITypeTheory  
  open acl_infRules aclDrulesTheory aclrulesTheory  
  
  val _ = new_theory "OMNI";  
  (*****  
  (* Define slCommands for OMNI. *)  
  (*****  
  (* ===== Area 52 =====  
  
  val _ =  
  Datatype 'stateRole = Omni'
```



```

val _ =
  Datatype 'omniCommand = ssmPlanPBComplete
                        | ssmMoveToORPComplete
                        | ssmConductORPComplete
                        | ssmMoveToPBComplete
                        | ssmConductPBComplete '

val omniCommand_distinct_clauses = distinct_of ' ':omniCommand'
val _ = save_thm("omniCommand_distinct_clauses",
                 omniCommand_distinct_clauses)

val _ =
  Datatype 'slCommand = OMNI omniCommand'

val omniAuthentication_def =
  Define
  '(omniAuthentication
    (Name Omni says prop (cmd:((slCommand command) option))
      :((slCommand command) option, stateRole, 'd, 'e)Form) = T) /\
    (omniAuthentication _ = F)'

val omniAuthorization_def =
  Define
  '(omniAuthorization
    (Name Omni controls prop (cmd:((slCommand command) option))
      :((slCommand command) option, stateRole, 'd, 'e)Form) = T) /\
    (omniAuthorization _ = F)'

This may not be necessary...But, it is interesting. Save for a later time.
(*****
(* Prove that *)
(* Omni says omniCommand ==> omniCommand *)
(*****)

set_goal([],
  '(Name Omni says prop (cmd:((slCommand command) option))
    :((slCommand command) option, stateRole, 'd, 'e)Form) ==>
    prop (cmd:((slCommand command) option))'

val th1 = ASSUME' '(Name Omni says prop (cmd:((slCommand command) option))
  :((slCommand command) option, stateRole, 'd, 'e)Form) = TT'
val th2 = REWRITE_RULE[omniAuthentication_def]th1

===== End Area 52 ===== *)

val _ = export_theory()
end

```

## D.2 TopLevel

### D.2.1 PBTypeIntegrated Theory: Type Definitions

```

(*****
(* PBTypeIntegrated *)
(* Author: Lori Pickering *)
(* Date 12 May 2018 *)
(* This theory contains the type definitions for ssmPBIntegrated *)
(*****)
structure PBTypeIntegratedScript = struct

```

```

(* ===== Interactive Mode =====
app load ["TypeBase"]
open TypeBase
===== end Interactive Mode ===== *)

open HolKernel Parse boolLib bossLib;
open TypeBase OMNITypeTheory

val _ = new_theory "PBTypeIntegrated";

(* *****
(* Define types
(* ***** *)
val _ =
Datatype 'plCommand = crossLD (* Move to MOVE_TO_ORP state *)
| conductORP
| moveToPB
| conductPB
| completePB
| incomplete '

val plCommand_distinct_clauses = distinct_of '':plCommand'
val _ = save_thm("plCommand_distinct_clauses",
plCommand_distinct_clauses)

val _ =
Datatype 'omniCommand = ssmPlanPBComplete
| ssmMoveToORPComplete
| ssmConductORPComplete
| ssmMoveToPBComplete
| ssmConductPBComplete
| invalidOmniCommand '

val omniCommand_distinct_clauses = distinct_of '':omniCommand'
val _ = save_thm("omniCommand_distinct_clauses",
omniCommand_distinct_clauses)

val _ =
Datatype 'slCommand = PL plCommand
| OMNI omniCommand '

val slCommand_distinct_clauses = distinct_of '':slCommand'
val _ = save_thm("slCommand_distinct_clauses",
slCommand_distinct_clauses)

val slCommand_one_one = one_one_of '':slCommand'
val _ = save_thm("slCommand_one_one", slCommand_one_one)

val _ =
Datatype 'stateRole = PlatoonLeader | Omni '

val stateRole_distinct_clauses = distinct_of '':stateRole'
val _ = save_thm("stateRole_distinct_clauses",
stateRole_distinct_clauses)

val _ =
Datatype 'slState = PLAN_PB
| MOVE_TO_ORP
| CONDUCT_ORP
| MOVE_TO_PB
| CONDUCT_PB
| COMPLETE_PB '

val slState_distinct_clauses = distinct_of '':slState'
val _ = save_thm("slState_distinct_clauses", slState_distinct_clauses)

```

```

val _ =
  Datatype 'slOutput = PlanPB
    | MoveToORP
    | ConductORP
    | MoveToPB
    | ConductPB
    | CompletePB
    | unAuthenticated
    | unAuthorized '

val slOutput_distinct_clauses = distinct_of ' ':slOutput '
val _ = save_thm("slOutput_distinct_clauses",slOutput_distinct_clauses)

val _ = export_theory();
end

```

## D.2.2 PBIntegratedDef Theory: Authentication & Authorization Definitions

```

(*****
(* PBIntegratedDefTheory *)
(* Author: Lori Pickering *)
(* Date: 7 May 2018 *)
(* Definitions for ssmPBIntegratedTheory. *)
(*****)
structure PBIntegratedDefScript = struct

  (* ===== Interactive Mode =====
  app load ["TypeBase", "listTheory","optionTheory",
            "uavUtilities",
            "OMNITypeTheory",
            "PBIntegratedDefTheory","PBTypeIntegratedTheory"];

  open TypeBase listTheory optionTheory
        aclsemanticsTheory aclfoundationTheory
        uavUtilities
        OMNITypeTheory
        PBIntegratedDefTheory PBTypeIntegratedTheory
        ===== end Interactive Mode ===== *)

  open HolKernel Parse boolLib bossLib;
  open TypeBase listTheory optionTheory
  open uavUtilities
  open OMNITypeTheory PBTypeIntegratedTheory

  val _ = new_theory "PBIntegratedDef";
  (* ----- *)
  (* state Interpretation function *)
  (* ----- *)
  (* This function doesn't do anything but is necessary to specialize other *)
  (* theorems. *)
  (* ----- *)
  val secContext_def = Define '
    secContext (x:((slCommand command)option, stateRole, 'd,'e)Form list) =
      [(TT:((slCommand command)option, stateRole, 'd,'e)Form)] '

  val secHelper =
    Define '
      (secHelper (cmd:omniCommand) =
        [(Name Omni) controls prop (SOME (SLc (OMNI (cmd:omniCommand))))]) '

  val getOmniCommand_def =
    Define '
      (getOmniCommand ([]:((slCommand command)option, stateRole, 'd,'e)Form list)
        = invalidOmniCommand:omniCommand) /\
      (getOmniCommand (((Name Omni) controls prop (SOME (SLc (OMNI cmd))))::xs)
        = (cmd:omniCommand)) /\
      (getOmniCommand ((x:((slCommand command)option, stateRole, 'd,'e)Form)::xs)
        = (getOmniCommand xs)) '

```

```

val secAuthorization_def =
Define '
  (secAuthorization (xs:((slCommand command)option, stateRole, 'd,'e)Form list)
    = secHelper (getOmniCommand xs)) '

val secContext_def =
Define '
  (secContext (PLAN_PB) ((x:((slCommand command)option, stateRole, 'd,'e)Form)::xs) =
    [(prop (SOME (SLc (OMNI (ssmPlanPBComplete))))
      :((slCommand command)option, stateRole, 'd,'e)Form) impf
      (Name PlatoonLeader) controls prop (SOME (SLc (PL crossLD)))
      :((slCommand command)option, stateRole, 'd,'e)Form]] /\
  (secContext (MOVE_TO_ORP) ((x:((slCommand command)option, stateRole, 'd,'e)Form)::xs) =
    [prop (SOME (SLc (OMNI (ssmMoveToORPComplete)))) impf
      (Name PlatoonLeader) controls prop (SOME (SLc (PL conductORP))))] /\
  (secContext (CONDUCT_ORP) ((x:((slCommand command)option, stateRole, 'd,'e)Form)::xs) =
    [prop (SOME (SLc (OMNI (ssmConductORPComplete)))) impf
      (Name PlatoonLeader) controls prop (SOME (SLc (PL moveToPB))))] /\
  (secContext (MOVE_TO_PB) ((x:((slCommand command)option, stateRole, 'd,'e)Form)::xs) =
    [prop (SOME (SLc (OMNI (ssmMoveToPBComplete)))) impf
      (Name PlatoonLeader) controls prop (SOME (SLc (PL conductPB))))] /\
  (secContext (CONDUCT_PB) ((x:((slCommand command)option, stateRole, 'd,'e)Form)::xs) =
    [prop (SOME (SLc (OMNI (ssmConductPBComplete)))) impf
      (Name PlatoonLeader) controls prop (SOME (SLc (PL completePB))))] '

(* ===== Area 52 =====

===== End Area 52 ===== *)

val _ = export_theory();
end

```

### D.2.3 ssmPlanPBIntegrated Theory: Theorems

```

(*****
(* ssmPBIntegratedTheory *)
(* Author: Lori Pickering *)
(* Date: 7 May 2018 *)
(* This theory aims to integrate the topLevel ssm with the sublevel ssms. It *)
(* does this by adding a condition to the security context. In particular, *)
(* it requires that the "COMPLETE" state in the subLevel ssm must precede *)
(* transition to the next state at the topLevel. I.e., *)
(* planPBComplete ==> *)
(* PlatoonLeader controls crossLD. *)
(* In the ssmPlanPB ssm, the last state is COMPLETE. This is reached when the *)
(* the appropriate authority says complete and the transition is made. *)
(* Note that following the ACL, if P says x and P controls x, then x. *)
(* Therefore, it is not necessary for anyone to say x at the topLevel, because *)
(* it is already proved at the lower level. *)
(* However, indicating that at the topLevel remains something to workout. *)
(*****)

```

```

structure ssmPBIntegratedScript = struct

```

```

(* ===== Interactive Mode =====
app load ["TypeBase", "listTheory", "optionTheory", "listSyntax",
  "acl_infRules", "aclDrulesTheory", "aclrulesTheory",
  "aclsemanticsTheory", "aclfoundationTheory",
  "satListTheory", "ssmTheory", "ssminfRules", "uavUtilities",
  "OMNITypeTheory", "PBTypeIntegratedTheory", "PBIntegratedDefTheory",
  "ssmPBIntegratedTheory"];

```

```

open TypeBase listTheory optionTheory listSyntax
  acl_infRules aclDrulesTheory aclrulesTheory
  aclsemanticsTheory aclfoundationTheory
  satListTheory ssmTheory ssminfRules uavUtilities
  OMNITypeTheory PBTypeIntegratedTheory PBIntegratedDefTheory
  ssmPBIntegratedTheory

```

```

===== end Interactive Mode ===== *)

open HolKernel Parse boolLib bossLib;
open TypeBase listTheory optionTheory
open acl_infRules aclDrulesTheory aclrulesTheory
open satListTheory ssmTheory ssmInfRules uavUtilities
open OMNITypeTheory PBTypeIntegratedTheory PBIntegratedDefTheory

val _ = new_theory "ssmPBIntegrated";

(* ***** *)
(* Define next-state and next-output functions *)
(* ***** *)
val PBNS_def =
Define '
(PBNS PLAN_PB      (exec [SOME (SLc (PL crossLD))]) = MOVE_TO_ORP) /\
(PBNS MOVE_TO_ORP  (exec [SOME (SLc (PL conductORP))]) = CONDUCT_ORP) /\
(PBNS CONDUCT_ORP  (exec [SOME (SLc (PL moveToPB))]) = MOVE_TO_PB) /\
(PBNS MOVE_TO_PB   (exec [SOME (SLc (PL conductPB))]) = CONDUCT_PB) /\
(PBNS CONDUCT_PB   (exec [SOME (SLc (PL completePB))]) = COMPLETE_PB) /\
(PBNS (s:slState) (trap _) = s) /\
(PBNS (s:slState) (discard _) = s) '

val PBOut_def =
Define '
(PBOut PLAN_PB      (exec [SOME (SLc (PL crossLD))]) = MoveToORP) /\
(PBOut MOVE_TO_ORP  (exec [SOME (SLc (PL conductORP))]) = ConductORP) /\
(PBOut CONDUCT_ORP  (exec [SOME (SLc (PL moveToPB))]) = MoveToPB) /\
(PBOut MOVE_TO_PB   (exec [SOME (SLc (PL conductPB))]) = ConductPB) /\
(PBOut CONDUCT_PB   (exec [SOME (SLc (PL completePB))]) = CompletePB) /\
(PBOut (s:slState) (trap _) = unauthorized) /\
(PBOut (s:slState) (discard _) = unauthenticated) '

(* ***** *)
(* Define authentication function *)
(* ***** *)
val inputOK_def =
Define '
(inputOK (((Name PlatoonLeader) says prop (cmd:((slCommand command)option)))
          :((slCommand command)option, stateRole, 'd, 'e)Form) = T) /\
(inputOK (((Name Omni) says prop (cmd:((slCommand command)option)))
          :((slCommand command)option, stateRole, 'd, 'e)Form) = T) /\
(inputOK _ = F) '

(* ***** *)
(* Prove that commands are rejected unless that are requested by a properly *)
(* authenticated principal. *)
(* ***** *)

val inputOK_cmd_reject_lemma =
Q.prove ('!cmd. ~(inputOK
                  ((prop (SOME cmd)))) ' ,
         (PROVE_TAC[inputOK_def]))

(* ===== Just playing around with this ===== *)
val inputOK_not_reject_lemma =
Q.prove ('!cmd.
~(
  (inputOK (((Name PlatoonLeader) says prop (cmd:((slCommand command)option)))
            :((slCommand command)option, stateRole, 'd, 'e)Form)) \/\
  (inputOK (((Name Omni) says prop (cmd:((slCommand command)option)))
            :((slCommand command)option, stateRole, 'd, 'e)Form)))

===== OK, done fooling around ===== *)

val _ = export_theory ();

```

end



## D.3 Horizontal Slice

### D.3.1 ssmPlanPB

#### D.3.1.1 PlanPBType Theory: Type Definitions

#### D.3.1.2 PlanPBDef Theory: Authentication & Authorization Definitions

#### D.3.1.3 ssmPlanPB Theory: Theorems

### D.3.2 ssmMoveToORP

#### D.3.2.1 MoveToORPType Theory: Type Definitions

#### D.3.2.2 MoveToORPDef Theory: Authentication & Authorization Definitions

#### D.3.2.3 ssmMoveToORP Theory: Theorems

### D.3.3 ssmConductORP

#### D.3.3.1 ConductORPType Theory: Type Definitions

#### D.3.3.2 ConductORPDef Theory: Authentication & Authorization Definitions

#### D.3.3.3 ssmConductORP Theory: Theorems

### D.3.4 ssmMoveToPB

#### D.3.4.1 MoveToPBType Theory: Type Definitions

#### D.3.4.2 MoveToPBDef Theory: Authentication & Authorization Definitions

#### D.3.4.3 ssmMoveToPB Theory: Theorems

### D.3.5 ssmConductPB



## Appendix E

### Map of The File Folder Structure

# References

- [1] Shiu-Kai Chin and Susan Beth Older. *Access Control, Security, and Trust: A Logical Approach*. Chapman & Hall: CRC Cryptography and Network Security Series. Chapman and Hall/CRC, July 2010.