

Figure 1: This is a caption for this figure.

Abstract

Copyright

Disclaimer

The views discussed in this master thesis are that of the author's. They do not in anyway represent the views of the United States Air Force Research Laboratory (AFRL) in Rome, NY or Professor Shiu-Kai Chin from the College of Engineering and Computer Science at Syracuse University. They are also the sole written work of the author and thus do not represent the views of the other participants in this research.

Acknowledgements

This research began in the summer of 2017 as part of the Assured by Design (ABD) program funded by the United States Air Force Research Laboratory (AFRL) in Rome, NY and managed by the principal investigator Professor Shiu-Kai Chin from the College of Engineering and Computer Science at Syracuse University. This project was envisioned by Professor Shiu-Kai Chin to satisfy the needs of the ABD program. This master thesis evolved directly from this work.

Thanks and recognition go to the following people for their contribution to this project. Professor Shiu-kai Chin for providing me with the opportunity and for his faith in me and my capabilities on this project. Eric Devendhorf at AFRL for making the ABD program happen. Mizra Tihic for making this happen, especially with respect to funding.

To properly acknowledge the contribution of others requires some description of the workflow. The actual work began as a collaboration between the subject matter expert from the United States Army and me, the author of this master thesis. The subject matter expert was Jesse Nathaniel Hall, a Captain [rank?] in the United States Army and also a graduate student in the iSchool (School of Information Science) at Syracuse University. Given the objective of demonstrating CSBD on the patrol base operation (or demonstrating its failure), we collaborated on the Systems Security Engineering (SSE) goals of the project. This work comprised a significant part of this research and is describe in the chapter on Systems Security Engineering. From thereon, the work was divided among the two of us with weekly updates and collaboration to resolve any potential conflicts. Jesse modeled the patrol base operations in Visio based on his interpretations of the patrol base operations in the Ranger Handbook [1]. A diagram of his work was included as a Visio file with this project. In addition, a squished version of this diagram was included in the chapter on the Patrol Base Operations. The result of this work was discussed in this context. On the other hand, I focused on the actual application of CSBD to the model as it was being developed. I continued to work on this aspect of the project after collaboration ceased.

In addition to the work done by Jesse and myself, another student worked with us on the project. This was YiHong Guo, an undergraduate student in the College of Engineering and Computer Science at Syracuse University. He helped us organize the original documentation of this work in LaTeX, a rather large project. (That documentation is separate from this master thesis.)

Table Of Contents

Abstract	i
List of Figures	ix
List of Tables	x
List of Acronyms	xi
1 Introduction	1
1.1 Motivation	1
1.1.1 Systems Are Everywhere	1
1.2 This Master Thesis	1
2 Background	2
2.1 Complete Mediation	2
2.2 Formal Methods	2
2.3 Functional Programming	3
2.4 Higher Order Logic (HOL) Interactive Theorem Prover	4
2.5 Other Interactive Theorem Provers	5
2.6 How to Compile The Included Files	5
3 Systems Security Engineering & Patrol Base Operations	6
3.1 The Systems Perspective	6
3.2 Systems Engineering	7
3.3 NIST Special Publication 800-160	10
3.4 Systems Security Engineering	10
3.5 Systems Security Engineering Framework	12
3.5.1 Problem	13
3.5.2 Solution	15
3.5.3 Trustworthiness	17
3.6 Trustworthiness	17
3.6.1 Verification & Documentation	18
3.6.1.1 Verification	18
3.6.1.2 Formal Verification	18
3.6.1.3 Documentation	18
3.6.2 Reproducibility	18
3.6.3 Accountability	18
3.6.4 Assurance Claims	18

4	Certified Security by Design (CSBD) & Access-Control Logic (ACL)	19
4.1	Certified Security by Design (CSBD)	19
4.1.1	Formal Verification & Documentation	20
4.1.2	Computer-aided Reasoning	20
4.1.2.1	Higher Order Logic (HOL) Interactive Theorem Prover	20
4.1.3	The Principle of Complete Mediation	20
4.2	Access-Control Logic (ACL)	20
4.2.1	ACL: A Command and Control (C2) Calculus	20
4.2.2	Principals	21
4.2.3	Propositional Variables, Requests, Authority, and Jurisdiction	21
4.2.4	Well-formed Formulas	23
4.2.5	Kripke Structure	23
4.2.5.1	satisfies	24
4.2.5.2	soundness	24
4.2.6	Inference Rules	24
4.2.7	Complete mediation	24
4.3	ACL in HOL	27
4.3.1	Complete Mediation	28
4.3.2	satList	28
5	Patrol Base Operations	29
5.1	Motivation	29
5.2	Ranger Handbook Description	29
5.3	Modeling the Patrol Base Operations from the Ranger Handbook	29
5.4	Overview of The Hierarchy of Secure State Machines	30
5.5	Hierarchy of Secure State Machines	33
5.5.1	Diagrammatic Description in Visio	33
5.5.2	OMNI-Level	35
5.5.3	Escape	35
5.5.4	Top Level	35
5.5.5	Horizontal Slice	35
5.5.5.1	ssmPlanPB	35
5.5.5.2	ssmMoveToORP	35
5.5.5.3	ssmConductORP	35
5.5.5.4	ssmMoveToPB	35
5.5.5.5	ssmConductPB	35
5.5.6	Vertical Slice	35
5.5.6.1	ssmSecureHalt	35
5.5.6.2	ssmORPRecon	35
5.5.6.3	ssmMoveToORP4L	35
5.5.6.4	ssmFormRT	35
6	Secure State Machine Model	36
6.1	State Machines	37
6.1.1	Configuration	37
6.1.2	Next-state Function	37
6.1.3	Next-output Function	37
6.1.4	Transition Commands	37

6.2	Secure State Machines	37
6.2.1	State Machine Versus Secure State Machine	37
6.2.2	Monitors	37
6.2.3	Configuration	37
6.2.4	Transition Types	37
	6.2.4.1 <i>exec</i>	37
	6.2.4.2 <i>trap</i>	37
	6.2.4.3 <i>discard</i>	37
6.2.5	Authentication	37
6.2.6	Authorization	37
6.3	Secure State Machines in HOL	37
6.3.1	Parameterizable Secure State Machine	37
6.3.2	Parameterization	37
6.3.3	Configurations: five parts	37
	6.3.3.1 State Interpretation	37
	6.3.3.2 Security context	37
	6.3.3.3 Input stream	37
	6.3.3.4 State	37
	6.3.3.5 Output stream	37
6.3.4	Configuration Interpretation	37
6.3.5	Authentication	37
6.3.6	Authorization	37
6.3.7	Transition Definitions	37
7	Patrol Base Operations as Secure State Machines	38
7.1	ssmPB: An Example from the Hierarchy	39
	7.1.1 Principals	39
	7.1.2 States	39
	7.1.3 Commands	39
	7.1.4 Next-State Function	39
	7.1.5 Next-Output Function	39
	7.1.6 Authentication	39
	7.1.7 Authorization	39
	7.1.8 Proved Theorems	39
	7.1.8.1 Platoon Leader Is Trusted on plCommands	39
7.2	Other Variations	39
	7.2.1 ssmPlanPB: Non-sequential Transitions	39
	7.2.2 ssmConductORP: Principals Authorized for Subsets of Commands	39
8	Discussion	40
8.1	Recap	40
8.2	Mission Accomplished	40
8.3	Stop-Gaps, Lessons Learned, & Advice	40
8.4	Other Verifiable Theories	40
	8.4.1 Authentication: Roles and Crypto	41
	8.4.2 Soldier Theory	41
	8.4.3 Platoon Theory	41
	8.4.4 Squad And Fire Team Theories	41

9	Future Work & Implications	42
9.1	...on The Patrol Base Operations	42
9.2	...on Other Non-automated Human-Centered Systems	42
9.3	Accountability Systems	43
9.4	Further Applicability	43
9.5	The Bigger Framework of Systems Security Engineering	44
	Appendices	45
A	Access Control Logic Theories: Pretty-Printed Theories	46
B	Secure State Machine & Patrol Base Operations: Pretty-Printed Theories	69
C	Secure State Machine Theories: HOL Script Files	144
C.1	ssm	144
C.2	satList	149
D	Secure State Machine Theories Applied to Patrol Base Operations: HOL Script Files	151
D.1	OMNILEvel	151
D.2	escapeLevel	152
D.3	TopLevel	152
D.3.1	PBTypeIntegrated Theory: Type Definitions	152
D.3.2	PBIntegratedDef Theory: Authentication & Authorization Definitions	154
D.3.3	ssmPlanPBIntegrated Theory: Theorems	155
D.4	Horizontal Slice	159
D.4.1	ssmPlanPB	159
D.4.1.1	PlanPBType Theory: Type Definitions	159
D.4.1.2	PlanPBDef Theory: Authentication & Authorization Definitions	159
D.4.1.3	ssmPlanPB Theory: Theorems	159
D.4.2	ssmMoveToORP	159
D.4.2.1	MoveToORPType Theory: Type Definitions	159
D.4.2.2	MoveToORPDef Theory: Authentication & Authorization Definitions	159
D.4.2.3	ssmMoveToORP Theory: Theorems	159
D.4.3	ssmConductORP	159
D.4.3.1	ConductORPType Theory: Type Definitions	159
D.4.3.2	ConductORPDef Theory: Authentication & Authorization Definitions	159
D.4.3.3	ssmConductORP Theory: Theorems	159
D.4.4	ssmMoveToPB	159
D.4.4.1	MoveToPBType Theory: Type Definitions	159
D.4.4.2	MoveToPBDef Theory: Authentication & Authorization Definitions	159
D.4.4.3	ssmMoveToPB Theory: Theorems	159
D.4.5	ssmConductPB	159

D.4.5.1	ConductPBType Theory: Type Definitions	159
D.4.5.2	ConductPBDef Theory: Authentication & Authorization Definitions	159
D.4.5.3	ssmConductPB Theory: Theorems	159
D.5	Vertical Slice	159
D.5.1	ssmSecureHalt	159
D.5.1.1	SecureHaltType Theory: Type Definitions	159
D.5.1.2	SecureHaltDef Theory: Authentication & Authorization Definitions	159
D.5.1.3	ssmSecureHalt Theory: Theorems	159
D.5.2	ssmORPRecon	159
D.5.2.1	ORPReconType Theory: Type Definitions	159
D.5.2.2	ORPReconDef Theory: Authentication & Authorization Definitions	159
D.5.2.3	ssmORPRecon Theory: Theorems	159
D.5.3	ssmMoveToORP4L	159
D.5.3.1	MoveToORP4LType Theory: Type Definitions	159
D.5.3.2	MoveToORP4LDef Theory: Authentication & Authoriza- tion Definitions	159
D.5.3.3	ssmMoveToORP4L Theory: Theorems	159
D.5.4	ssmFormRT	159
D.5.4.1	FormRTType Theory: Type Definitions	159
D.5.4.2	FormRTDef Theory: Authentication & Authorization Def- initions	159
D.5.4.3	ssmFormRT Theory: Theorems	159
E	Map of The File Folder Structure	160
	References	161

List of Figures

1	This is a caption for this figure.	i
3.1	Systems security engineering in relation to systems engineering. (Image from NIST Special Publication 800-160: Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.)	11
3.2	Systems security engineering Framework. (Image from NIST Special Publication 800-160: Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.)	13
4.1	Kripke semantics. Image taken from <i>Access Control, Security, and Trust: A Logical Approach</i> [2]	24
4.2	The access-control logic (ACL) inference rules. Image taken from <i>Access Control, Security, and Trust: A Logical Approach</i> [2]	25
4.3	The <i>Controls</i> inference rule. Image taken from <i>Access Control, Security, and Trust: A Logical Approach</i> [2]	25
4.4	The <i>Reps</i> inference rule. Image taken from <i>Access Control, Security, and Trust: A Logical Approach</i> [2]	26
4.5	The <i>Derived Speaks For</i> inference rule. Image taken from <i>Access Control, Security, and Trust: A Logical Approach</i> [2]	26
4.6	The ACL formulas in HOL. Image taken from <i>Access Control, Security, and Trust: A Logical Approach</i> [2]	27
5.1	A diagram of the most abstract level in the hierarchy of secure state machines. Image generated by Jesse Nathaniel as part of the research involved in this master thesis. Shall I get his permission?	30
5.2	Diagrammatic description of patrol base operations as a hierarchy of secure state machines. (Generated by Jesse Nathaniel Hall.)	33

List of Tables

List of Acronyms

ACL access-control logic.

CSBD Certified Security by Design.

WFF well-formed formula.

Chapter 1

Introduction

1.1 Motivation

1.1.1 Systems Are Everywhere

1.2 This Master Thesis

This master thesis describes a method for designing secure systems. The method is called Certified Security by Design (CSBD). CSBD has been successfully demonstrated on automated systems such as ... and But, until this research, it has not been demonstrated on non-automated, human-centered systems.

Systems span the range of fully automated to fully non-automated. This master thesis focuses on one end of this range: non-automated, human-centered systems.

- The first question addressed in this master thesis is whether CSBD could be successfully applied to non-automated, human-centered systems. This is the

primary objective. An example of a non-automated, human-centered system is the patrol base operations defined in the United States Army Ranger Handbook[1].

Patrol base operations exemplify a non-automated, human-centered system wherein security is critical to mission success. In this master thesis, the results of applying CSBD to patrol base operations is discussed.

- The patrol base operations are also an example of a predefined system. This means that this thesis also addresses the question of whether CSBD could be successfully applied to a pre-designed, non-automated, human-centered system. This is important because many such systems in use today are already designed and implemented. CSBD demonstrates that it can verify and document the security properties of current, in-use systems.
- These thesis describes a hierarchy of secure state machines (SSMs) used to model the patrol base operations. This approach demonstrates that formal methods can be applied to large scale and complicated systems. The hierarchy manages patrol base operations by successful levels of decreasing abstraction. Each level in the hierarchy consists of one or more SSMs. Each SSM is modularized and models one aspect of the patrol base operations at one level of abstraction. The levels and modules are connected together by an OMNI level, all-seeing, principal. Each module only needs to be aware of this OMNI level principal. They do not need to be aware of the details of any other module. With this divide-and-conquer approach, CSBD can be readily applied to large and complicated systems.
- The successful application of CSBD to patrol base operations also suggests its use in combining automation with human-centered systems. The approach employed by this master thesis involves describing the patrol base operations as a hierarchy of secure state machines. This hierarchy has the property that it is easy to demonstrate security properties of the system, which is the goal of CSBD. But, it also has the property that it describes the patrol base operations as a system that is amiable to automation. Such automations of pre-defined non-automated,

human-centered systems could include, for example, accountability systems for tracking supplies and personnel.

In the not-so-distant future, the military, in particular, will most likely seek tracking and accountability systems for pre-existing, non-automated military operations. These systems, like all security-sensitive military systems, should be designed according to NIST 800-160 standards. These standards require the formal verification and documentation provided by CSBD and demonstrated in this thesis.

Chapter 2

Background

This section aims to provide some background on subjects discussed in this master thesis. These subjects are not directly addressed in other areas of this master thesis. Nevertheless, knowledge of them is either necessary or useful to understanding what follows.

2.1 Complete Mediation

Complete mediation is discussed throughout this master thesis. It is described in this section so as to eliminate the need to repeatedly describe it in the ensuing chapters.

2.2 Formal Methods

(Primary source for this section is [3])

Formal methods are aimed at improving the reliability and correctness of systems[4].

They are applied to all phases of systems engineering. Formal methods employ mathematics to verify desired aspects of a system. Mathematics adds a degree of rigor to the verification process that is amiable to automation.

The primary tools of formal methods are model checking and theorem proving. Model checking typically involves testing all possible states of a system for correctness. For large systems, model checking can be resource intensive. Theorem proving, on the other hand, employs a formal logic to verify that a system satisfies desired properties. Theorem proving is usually applied to a system after it is modeled (referred to as specification). Theorem proving is typically partially or fully automated. Although, proofs by hand can also be employed.

This master thesis applies formal verification methods to prove the security properties of a system. It uses a formal logic based on modal propositional logic. The logic, called access-control logic (ACL), is implemented in the Higher Order Logic (HOL) Interactive theorem prover. Theorem proving is partially automated.

2.3 Functional Programming

(Primary source for this section is [5])

Functional programming is a style of programming that uses functions to define program behavior. Functional programming is inherently different than procedural or object-oriented programming. These styles of program use procedures or objects and classes to define program behavior. c and Pascal are examples of procedural programming languages. c++ and Java are examples of object-oriented programming languages. Haskell and ML (meta language) are examples of functional programming languages. Functional programming languages are thought to be more pure. They have fewer side effects than procedural or object-oriented programming. They produce fewer

bugs. Functional programming languages are thus considered more reliable. This master thesis relies on the Higher Order Logic (HOL) Interactive theorem prover. HOL is implemented in the functional programming language polyML.

2.4 Higher Order Logic (HOL) Interactive Theorem Prover

The Higher Order Logic (HOL) Interactive theorem prover is a proof assistant. HOL has proved to be a very reliable theorem proving system. It is widely trusted in the interactive theorem proving community.

At its core, HOL implements a small set of axioms and a formal logic. All inferences and theorems must be derived from this small set of axioms using the formal logic. Reasoning logically with a small set of axioms contributes to the trustworthiness of the system. The user only has to trust the small set of axioms and the logic (in addition to HOL). Beyond the competence of the programmer, if it can't be proved in HOL then it can be proved.

HOL is a strongly-typed system. This means that data has a predefined type. As in all purely functional programming languages, the type of these data can not change. This adds to the reliability of HOL by preventing side-effect. HOL has several built-in data types. But, the user can also define her own data type. In addition to datatypes, the user can define her own set of axioms and definitions.

With user-defined types, axioms, and definitions, the user can describe a system in HOL and then use HOL's formal logic to prove properties of this system. This is the basis for theorem proving in formal methods.

This master thesis describes an access-control logic (ACL) that is implemented in HOL. Using this ACL, secure state machines (SSMs) are also described in HOL. With the ACL implemented in HOL, this thesis proves security properties of the SMMs. These proofs are considered formal verification of the security properties of the SSMs. As the patrol base operations are modeled as a hierarchy of SSMs, these proofs also provide formal verification of the security properties of the patrol base operations.

2.5 Other Interactive Theorem Provers

2.6 How to Compile The Included Files

Chapter 3

Systems Security Engineering & Patrol Base Operations

3.1 The Systems Perspective

A system is a set of interacting and interdependent components that act as a whole to perform some behavior or function. Examples of systems include the human body, socio-political systems, and computer systems.

The patrol base operations satisfy this definition of a system. As a whole, the patrol base operations perform some function(s). This function is described in the Ranger Handbook [1] and discussed in chapter 5. The patrol base operations are comprised of interdependent and interacting components. In general these components are the individual soldiers. But, the way this master thesis defines the patrol base operations, the definition of a component varies.

This master thesis defines the patrol base operations as a system of systems. More specifically, this thesis models the patrol base operations as a hierarchy of secure state

machines. Chapter 6 describes SSMS in general. Section 5.3 describes this model of the patrol base operations.

This model presents the patrol base operations as a hierarchy wherein each level of the hierarchy represents a decreasing level of abstraction. At the top and most abstract level, the components are phases of the patrol base operations. These phases commence in a sequential order to achieve the goal of the patrol base operations. Each lower level of the hierarchy is composed of less abstract phases. At each level, the components function sequentially (typically) to achieve the ultimate goal.

This system of systems also contains non-hierarchically defined components. For example, an escape-level component models situations wherein the patrol base operations are aborted. The escape level component is reachable from any component at any level of the hierarchy. Soldiers (as in a soldier model) also function within this system of systems in a non-hierarchical manner. However, the soldier module is not verified using the ACL because of time constraints. Nevertheless, a soldier module is discussed in the Discussions chapter 8 of this thesis.

In this way, the patrol base operations represent a system and are amiable to the systems engineering perspective.

3.2 Systems Engineering

The recognized authoritative standard on systems engineering is ISO/IEC/IEEE 15288 [6]. This document is titled "Systems And Software Engineering–System Life Cycle Processing." A precursor to this standard is ISO/IEC TR 24748 1 [7] titled "Systems And Software Engineering–Life Cycle Management–Part 1: Guide for Life Cycle Management." These are the primary sources for this section.

Systems engineering is an interdisciplinary approach aimed at solving problems involved in the various phases of the life cycle of a system. ISO/IEC/IEEE 15288 and ISO/IEC TR 24748 1 define five major phases of the this life cycle: concept, development, production, utilization, support, and retirement.

This master thesis focuses on the Certified Security by Design (CSBD). The key premise of CSBD is that security should be built into the systems from the start, i.e., the design phase. This is the leading notion in systems engineering and its sub-discipline Systems Security Engineering. It is instructive to see how CSBD and its application to the patrol base operations fits into this framework described by the ISO standards.

Concept The concept phase describes stakeholders and the Concept of Operations (ConOps). Stakeholders are those who have a stake in the system. ConOps are defined in a variety of ways. Wikipedia defines ConOps as "...a document describing the characteristics of a proposed system from the viewpoint of an individual who will use that system [?]. U.S. Air Force Policy Directive 10-28 defines ConOps as "a high level concept whose purpose is to describe operational mission areas, enablers and effects necessary to achieve desired results/outcomes" [8]. ConOps are context specific.

The patrol base operations are already modeled and implemented. The mission areas, enablers, and effects to achieve the desired goal are already in place. The aim for this thesis is to maintain the structure of the patrol base operations and model it in a way that is amiable to verification and documentation of complete mediation.

It is also possible to look at this thesis as the modification of an already in-use systems. For example, an accountability system involving the patrol base operations may require a remodeling of the operations with few, if any, changes in the actual operations themselves. This is discussed in more detail in the Future Works & Implications Chapter in section 9.3.

CSBD is intended to be applied to this phase of the systems engineering process.

Development The development stage involves refinement of the ConOps and production of the productions. The development of the patrol base operations took place a long time ago. Regardless, the products for this master thesis are the verification and subsequent documentation of complete mediation.

In an accountability system, for example, the principle of complete mediation verified and documented would be embedded in the implementation of any procedures worked out at this phase of the system life-cycle.

The aim is to model the patrol base operations in a manner that is amiable to verifying specific security properties of the system. Specifically, the patrol base operations must satisfy the property of complete mediation.

But, this thesis does not aim to build a new system. Rather this thesis remodels an existing system. This is necessary because the goal of this thesis is to determine whether or not it is possible to verify the specific security properties on the subclass of systems that we are exploring. Most people would agree that testing a new method on a new system would be unwise. This is why this thesis did not do that.

This approach has the side-effect of also demonstrating CSBDs utility in the life-cycle phase of systems engineering. It follows readily from the news today that many systems are not designed with security in mind. Eliminating already-in-use systems and legacy systems may not always be practical or desirable. Nevertheless, security remains an important aspect of system performance. This, in part, justifies a re-look at (or remodeling of) of an already existing system.

There are additional benefits to systematically modeling the patrol base operations in a way that is amiable to formal verification. This type of thinking provides new insights

and suggests areas for improvement¹. This is a known benefit. For example, Wikipedia [3] notes that "Sometimes, the motivation for proving the correctness of a system is not the obvious need for reassurance of the correctness of the system, but a desire to understand the system better." A greater understanding of a system applies to all phases of systems engineering.

3.3 NIST Special Publication 800-160

One work in the field of Systems Security Engineering is such a critical component to the field of SSE that it warrants pointing out. The National Institute of Standards and Technology (NIST) defines its mission as such: "To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." [9]. As their name suggests, NIST develops standards for various industries of relevance to the nation.

The relevant standard for SSE is NIST Special Publication 800-160 Volumes 1 and 2. The title of volume 1 is "Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems." The title of volume 2 is "Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems." These, in particular volume 1, are the primary sources for the following two sections.

¹The subject matter expert who focused on the details of the patrol base operations also noted areas for improvement. He was not available to provide details at the writing of this master thesis.

3.4 Systems Security Engineering

Systems security engineering (SSE) is a sub-discipline of systems engineering. Figure 3.1 shows SSE in relation to systems engineering and other sub-disciplines of SSE. This master thesis falls into one of the Security Specialties in this diagram.

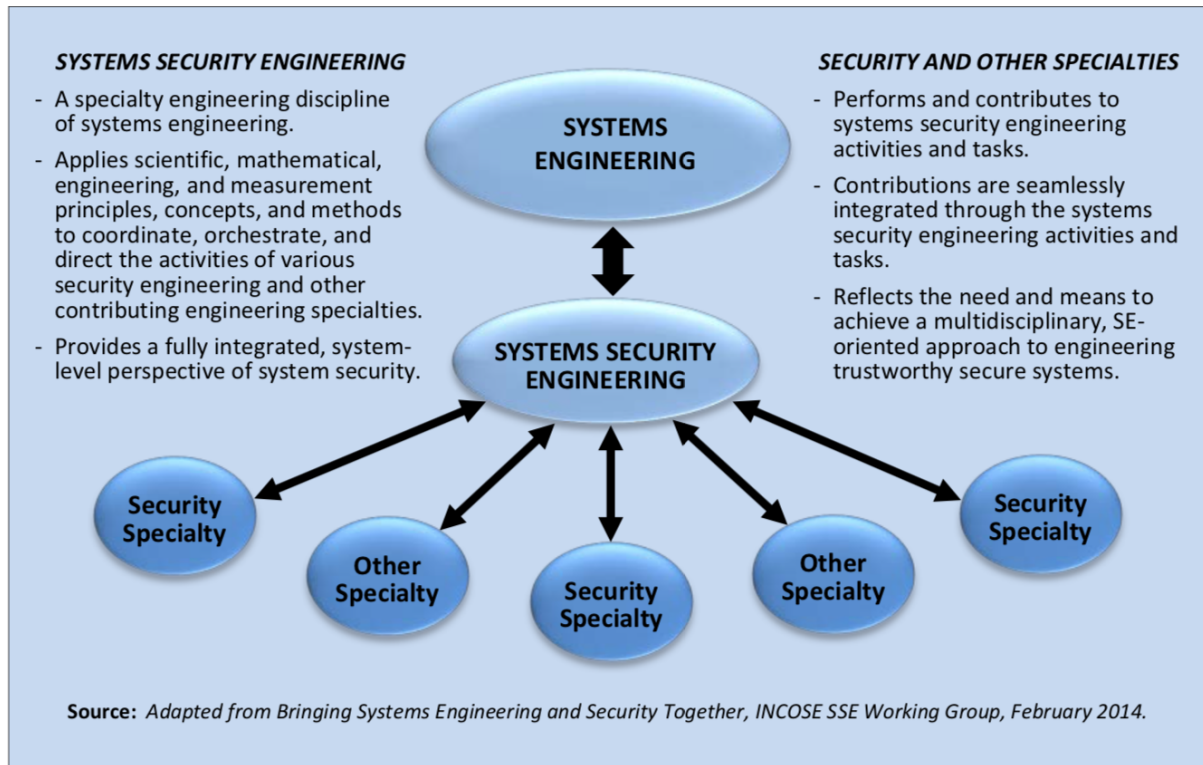


Figure 3.1: Systems security engineering in relation to systems engineering. (Image from NIST Special Publication 800-160: Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.)

According to NIST Special Publication 800-160, "Systems security engineering focuses on the protection of stakeholder and system assets so as to exercise control over asset loss and the associated consequences." Three key concepts in SSE are stakeholder, asset, and unacceptable losses. In modeling the patrol base operations, this thesis first defines these key concepts.

Stakeholder The stakeholder controls the design of the system. The stakeholder defines what the system should do. The stakeholder also defines what the system should not do and what are unacceptable losses. The stakeholder for the patrol

base operations are ultimately the U.S. military. This was critical to the original design of the patrol base operations. But, this thesis has a different purpose, that of demonstrating specific security properties of the patrol base operations using CSBD. These security properties are that of complete mediation. For this master thesis, the stakeholders are everyone involved in this research.

Asset An asset is anything that is of value to the stakeholder. In the patrol base operations, this includes soldiers, equipment, and the mission.

Unacceptable losses Unacceptable losses are self-defining. Unacceptable losses for the patrol base operations are defined broadly as any event that would cause the patrol base operation as a whole to abort. These are: contact with the enemy, casualties, a change in mission from higher-up.

It is also a critical objective of SSE to identify and define the security goals of the stakeholder in a way that minimizes asset loss and avoids unacceptable losses. The security properties of the patrol base operations are already built-in to the design of the operations from the Ranger Handbook. These are undoubtedly the result of years of military expertise. Our goal is not to define the security features of the patrol base operations, but to describe them in manner amiable to verification of complete mediation. Identification of assets and unacceptable losses from the Ranger Handbook is sufficient to do this.

To cover the unacceptable losses, this master thesis models an escape-level secure state machine (SSM). If at any phase in the patrol base operations any authenticated principal (i.e., the platoon leader) reports an abortable event, the escape-level SSM will abort the patrol base operations. This includes casualties or unacceptable equipment failure. By creating one escape-level SSM, this thesis creates an modularized yet expandable treatment of unacceptable losses.

To further describe the model of the patrol base operations in the context of SSE, a few

more concepts are necessary.

3.5 Systems Security Engineering Framework

NIST 800-160 describes the systems security engineering framework shown in figure 3.2 as "contexts within which systems security engineering activities are conducted." CSBD focuses primarily on demonstrating trustworthiness. Nevertheless, this master thesis also addressed other aspects of the framework.

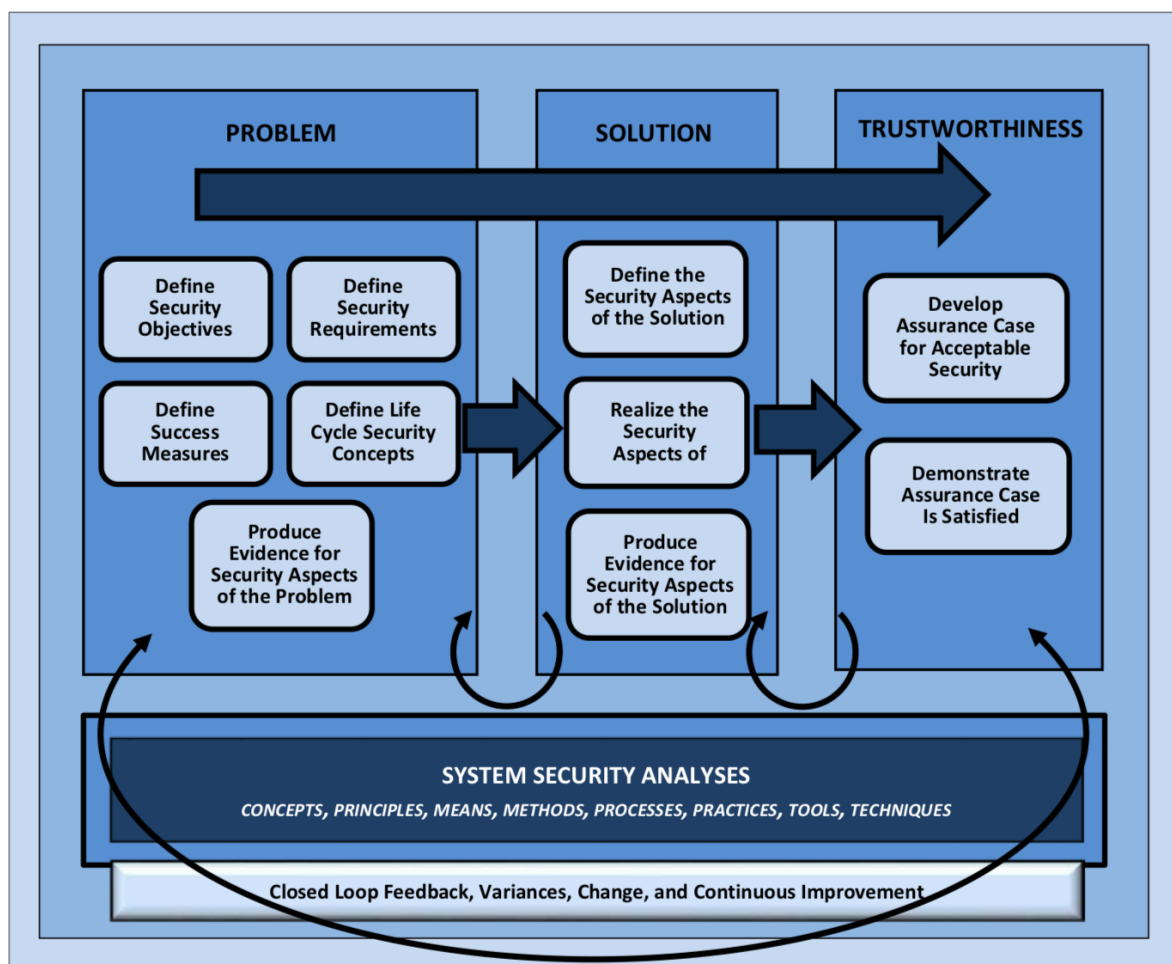


Figure 3.2: Systems security engineering Framework. (Image from NIST Special Publication 800-160: Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.)

The problem and solution phases for the patrol base operations take a different

approach in the context of this master thesis. It is not our goal to outline the potential security threats and then to find solutions for them. This was, hopefully, already done when the patrol base operations were originally defined. Nonetheless, it is necessary to identify the problem and solution within the patrol base operations in order to verify their security properties.

3.5.1 Problem

The security objective from the perspective of this master thesis is to ensure complete mediation of all actions. Complete mediation requires that we identify objects to be accessed, the accessors, the means of authenticating the accessors, and the a policy for authentication.

The objects to be accessed varies at each level of abstraction. At the top and most abstract level, the objects are the transitions. That is, control over the transitions between phases (or states) of the patrol base operations are to be protected. Objects are defined similarly for each module and at each level for the entire hierarchy of the model. These are deducible from the descriptions of each module (or SSM) in their appropriate section (see section 5.5.2 to start). For the sake of brevity, this section only discusses the top level to illustrate the key concepts.

The accessors are the leaders designated at each level of abstraction. The best way to negotiate access to objects is by the principle of least privilege. This principle assigns privilege to only those who are deemed necessary and to no others. At the top level, the platoon leader (and only the platoon leader) is designated as the accessor. This means that only the platoon leader can issue commands to move-on to the next phase (or state) in the patrol base operations. Some of the other modules have more than one accessor. These accessors are typically assigned privileges to specific objects within the module. The rights of each accessor are determined by the policy.

In the real patrol base operations, soldiers recognize each other by face. Thus, it is sufficient to just authenticate the platoon leader at each level without requiring any passwords or other means of authentication².

Policy is determined for each module and at each level of the patrol base operations model. The model includes not only "who" is authorized to do what, but also what preconditions are necessary prior to authorization. This is more complicated than authentication.

At the top level, there are only two requirements for the patrol base operations to move to the next phase of the operations: (1) the previous phase is complete, and (2) the platoon leader issues the command to move to the next phase. This creates a potential conflict between the goal of modularizing each component and creating a hierarchy wherein each level of the hierarchy expands upon the one above it. In general, If the top level requires some signal from the lower level that it is complete, then these two levels are not independent.

To solve this problem, an OMNI level module is created. The OMNI level module is thought of as all-knowing. This module relays information from all modules as needed. With this construct, the top level does not need to "know" if the lower level module is complete. It only needs to know that the OMNI level says that it is complete. The OMNI level is given the authority to determine when any module is complete.

With this solution in mind, the top level policy looks like this.

if OMNI-Level says the previous phase is complete³, and
Platoon Leader says move to the next phase
then Platoon Leader has the authority to move to the next phase

²The author and subject matter expert discussed authentication in the context of an accountability system wherein passwords or chips were required for authentication. But, we did not implement such authentication techniques in this project.

3.5.2 Solution

The simplest solution to this problem is to model the patrol base operations as a hierarchy of secure state machines (SSM). The hierarchy simplifies the design of the solution by creating decreasing levels of abstraction with multiple modules at each level. This allows for focus on one level and one module at time. This essentially amounts to a system of systems approach. Furthermore, this allows for greater separation of work. After one level of the hierarchy is complete, CSBD is applied to that level while the next level of the hierarchy is being designed.

SSMs are readily defined with complete mediation embedded into their design. SSMs are discussed in detail in Chapter 6. In fact, a parameterizable model of an SSM⁴ was already designed and implemented in HOL prior to the start of this project. The constraints of this project suggested Improvements⁵ to this parameterizable SSM⁶.

The most useful property of the SSM is that complete mediation is made a condition for transitions among states. That is, to transition from one state to another the accessor (requestor) must be properly authenticated and authorized. Authentication and authorization are described above in the description of the problem. For example, at the top level, transition commands in an SSM look like this.

*if Platoon Leader's identity is authenticated, and
Platoon Leader says move to the next phase, and
Platoon Leader has the authority to move to the next phase
then move to the next phase.*

⁴This SSM was modeled and implemented in HOL by Professor Shiu-kai Chin and used with his permission.

⁵Because these improvements were significant, the original author (Professor Shiu-kai Chin) made them.

⁶Much to the chagrin of the author, a significant portion of the SSMs had to be redone with the new parameterizable SSM.

The first line ensures authentication of the Platoon Leader. The second line is a request from the Platoon Leader to access the object (i.e., move to the next phase). The third line is the output of a policy as described in the section above and shown in the box above.

Note that this is an "if and only if" conditional. This means that if the Platoon Leader is authenticated, authorized on, and issues the command then the command is executed. It also means the converse. If the command is executed, then the Platoon Leader is authenticated, authorized on, and issues the command to do so.

3.5.3 Trustworthiness

There are two requirement for trustworthiness relevant to this master thesis: (1) Defining trustworthiness for the purposes of this master thesis, and (2) demonstrating that trustworthiness is achieved. The former is easy for this model. This master thesis focuses on the trustworthiness aspect of SSE. Therefore, this master thesis elaborates on trustworthiness in the following sections.

3.6 Trustworthiness

This master thesis defines trustworthiness in the context of complete mediation⁷.

Therefore, a measure of trustworthiness is weather or not the patrol base operations satisfy the properties of complete mediation. There are two aspects to this: (1) building complete mediation into the model of the patrol base operations, and (2) demonstrating that this is indeed the fact.

⁷Note that there are certainly other measures of trustworthiness in any system. Nonetheless, the focus of this thesis is to demonstrate CSBD as a viable method for one aspect of the systems security engineering process. The author does not aim to claim that the patrol base operations are deemed trustworthy solely because they satisfy the property of complete mediation. CSBD is one piece of the larger puzzle.

3.6.1 Verification & Documentation

3.6.1.1 Verification

3.6.1.2 Formal Verification

3.6.1.3 Documentation

A common idiom of science and engineering is "if you didn't document it then it didn't happen." There is some leeway in engineering because the presence of a system is indicative that "you did it." However, this hides the important details regarding the security of the system. Maybe "you did it" but "did you do it right?" This is where documentation is important.

"systems security engineering provides a sufficient base of evidence that supports claims that the desired level of trustworthiness has been achieved..."

3.6.2 Reproducibility

3.6.3 Accountability

Internet Hall of Fame Inductee Vint Cerf commented on the importance of accountability in SSE at a recorded conference in 2016. The conference titled "Exploring the Dimensions of Trustworthiness: Challenges and Opportunities" was presented by NIST.

3.6.4 Assurance Claims

Chapter 4

Certified Security by Design (CSBD) & Access-Control Logic (ACL)

4.1 Certified Security by Design (CSBD)

In 1970 The Rand Corporation published a report[10] for the Office of The Director of Defense Research And Engineering. This report titled, Security Controls For Computer Systems, noted that "Providing satisfactory security controls in a computer system is in itself a system design problem." NIST 800-160 also highlights the importance of incorporating security into the design phase of the system engineering process. CSBD focuses on the design phase of systems engineering, applying formal methods to verify that a system satisfies the principle of complete mediation.

More specifically, CSBD is a method for formally verifying and documenting the security properties of a systems. It focuses on designing systems that satisfy the principle of complete mediation. It uses an access-control logic (ACL) to reason about

access to security sensitive objects of a system. It uses computer-aided reasoning such as the Higher Order Logic (HOL) Interactive theorem prover to formally verify and document these security properties. The outcomes of CSBD applied to a system conform to the guidelines set fourth in NIST 800-160 [verify and discuss this.]

In addition to providing formal proofs that demonstrate satisfiability of complete mediation, CDBD is reproducible. This means that third parties can also verify the formal proofs. This touches on the heart of formal verification of satisfiability: "don't just take my word for it, prove it for yourself."

4.1.1 Formal Verification & Documentation

4.1.2 Computer-aided Reasoning

4.1.2.1 Higher Order Logic (HOL) Interactive Theorem Prover

4.1.3 The Principle of Complete Mediation

4.2 Access-Control Logic (ACL)

4.2.1 ACL: A Command and Control (C2) Calculus

This section discusses the access-control logic in sufficient detail to understand the research reported in this master thesis. The material is adapted from *Access Control, Security, and Trust: A Logical Approach*[2]. For more indepth coverage of the ACL, read the text. Any references to "the text" in this section refer to the aforementioned text book.

ACL is a logic for reasoning about access to object. In the jargon of the day it is a command and control (C2) calculus¹.

4.2.2 Principals

Principals should be thought of as actors in the access-control logic. Principals can make statements or requests. They can be assigned privileges or authority over objects or actions. The text defines allowable principals using the identifier **Princ**:

$$\mathbf{Princ} ::= \mathbf{PName} / \mathbf{Princ} \ \& \ \mathbf{Princ} / \mathbf{Princ} \ |\mathbf{Princ}$$

This is a recursive definition. *PName* refers to the name of a principal (i.e., Jane, PlatoonLeader, sensor1). *Princ & Princ* is read "Princ with Princ" or "Princ and Princ" (i.e., Principal1 with Principal2). *Princ |Princ* is read as "Princ quoting Princ" (i.e., Principal1 quoting Principal2).

4.2.3 Propositional Variables, Requests, Authority, and Jurisdiction

To reason about access-control and trust, the ACL uses propositional variables, requests, authority, and jurisdiction to make statements.

Propositions in logic are assertions that are either true or false. For example, "I am reading this master thesis" is a proposition because either you are or you are not reading this. Propositional variables are just place holders for propositions. For example, "I am reading something", where the propositional variable "something" is what you are reading.

¹command and control being self-evident and calculus being a method for reasoning

Principals can make requests. In the ACL, principals make requests using the *says* operator. Requests have the form $P \text{ says } \varphi$, where P represents some principal and φ represents some assertion. For example, *PlatoonLeader says platoonHalt*. In this example, the Platoon Leader is issuing a command (or request) for the platoon to halt.

Principals can have authority over assertions. In the ACL, authority is conveyed using the *controls* operator. Statements of authority have the form $P \text{ controls } \varphi$, where P represents some principal and φ represents some assertion. For example, *PlatoonLeader controls platoonHalt*. This example states that the Platoon Leader has the authority to issue the command (or request) for the platoon to halt.

Principals can also have jurisdiction over assertions. Both authority and jurisdiction use the *controls* operator. Statements of jurisdiction have the same form as statements of authority. Statements of authority are typically defined in an organization's policy. Statements of jurisdiction are statements that are readily believed given the context. For example, *PresidentOfUS controls (PlatoonLeader controls platoonHalt)*. In this example, the President of the United States, per the U.S. Constitution, has jurisdiction over the authority invested in the Platoon Leader. In particular, the President of the United States has the jurisdiction to give the Platoon Leader the authority to command her platoon to halt.

In addition, principals can speak for other principals. Principals do this using the *speaks for* operator. The ACL represents the *speaks for* operator with the symbol \Rightarrow . These types of statements have the form $P \Rightarrow Q$, where both P and Q are principals. For example, *PlatoonLeader \Rightarrow PresidentOfUS*. This example states that the Platoon Leader speaks for the President of the United States.

4.2.4 Well-formed Formulas

Well-formed formulas (WFFs) are valid statements in the ACL. All statements must be a WFF. The text book defines the set of WFFs using the identifier **Form**:

$$\begin{aligned} \mathbf{Form} ::= & \mathbf{PropVar} / \neg \mathbf{Form} / (\mathbf{Form} \vee \mathbf{Form}) / \\ & (\mathbf{Form} \wedge \mathbf{Form}) / (\mathbf{Form} \supset \mathbf{Form}) / (\mathbf{Form} \equiv \mathbf{Form}) / \\ & (\mathbf{Princ} \Rightarrow \mathbf{Princ}) / (\mathbf{Princ} \text{ says } \mathbf{Princ}) / (\mathbf{Princ} \text{ controls } \mathbf{Form}) \end{aligned}$$

This is a recursive definition. ***PropVar*** is a propositional variable. The symbols \neg , \vee , \wedge , \subset , and \equiv are the standard set and logical symbols. They represent "not", "or", "and", "subset", and "equivalence", respectively. This master thesis primarily reasons with statements (WFFs) of the form ***Princ** says **Princ*** and ***Princ** controls **Form***.

4.2.5 Kripke Structure

A Kripke structure deals with three things: worlds, propositions, and principals. The worlds can be thought of as possible states or configurations of some system.

Propositions are just statements that are either true or false. And, principals are just actors. A Kripke structure $\mathcal{M} = \langle W, I, J \rangle$ is defined as a three-tuple consisting of a set of worlds W , a function I that maps propositions to worlds, and a functions J that maps principals to relations on worlds. A more formal definition is definition 2.1 in the text:

- *W is a nonempty set, whose elements are called worlds.*
- *$I : \mathbf{PropVar} \rightarrow \mathcal{P}(W)$ is an interpretation function that maps each propositional variable to a set of worlds.*
- *$J : \mathbf{PName} \rightarrow \mathcal{P}((W \times W))$ is a function that maps each principal name to a relation on worlds.*

$$\begin{aligned}
\mathcal{E}_{\mathcal{M}}[p] &= I(p) \\
\mathcal{E}_{\mathcal{M}}[\neg\varphi] &= W - \mathcal{E}_{\mathcal{M}}[\varphi] \\
\mathcal{E}_{\mathcal{M}}[\varphi_1 \wedge \varphi_2] &= \mathcal{E}_{\mathcal{M}}[\varphi_1] \cap \mathcal{E}_{\mathcal{M}}[\varphi_2] \\
\mathcal{E}_{\mathcal{M}}[\varphi_1 \vee \varphi_2] &= \mathcal{E}_{\mathcal{M}}[\varphi_1] \cup \mathcal{E}_{\mathcal{M}}[\varphi_2] \\
\mathcal{E}_{\mathcal{M}}[\varphi_1 \supset \varphi_2] &= (W - \mathcal{E}_{\mathcal{M}}[\varphi_1]) \cup \mathcal{E}_{\mathcal{M}}[\varphi_2] \\
\mathcal{E}_{\mathcal{M}}[\varphi_1 \equiv \varphi_2] &= \mathcal{E}_{\mathcal{M}}[\varphi_1 \supset \varphi_2] \cap \mathcal{E}_{\mathcal{M}}[\varphi_2 \supset \varphi_1] \\
\mathcal{E}_{\mathcal{M}}[P \Rightarrow Q] &= \begin{cases} W, & \text{if } \hat{J}(Q) \subseteq \hat{J}(P) \\ \emptyset, & \text{otherwise} \end{cases} \\
\mathcal{E}_{\mathcal{M}}[P \text{ says } \varphi] &= \{w \mid \hat{J}(P)(w) \subseteq \mathcal{E}_{\mathcal{M}}[\varphi]\} \\
\mathcal{E}_{\mathcal{M}}[P \text{ controls } \varphi] &= \mathcal{E}_{\mathcal{M}}[(P \text{ says } \varphi) \supset \varphi] \\
\mathcal{E}_{\mathcal{M}}[P \text{ reps } Q \text{ on } \varphi] &= \mathcal{E}_{\mathcal{M}}[(P \mid Q \text{ says } \varphi) \supset Q \text{ says } \varphi]
\end{aligned}$$

Figure 4.1: Kripke semantics. Image taken from *Access Control, Security, and Trust: A Logical Approach*[2]

4.2.5.1 satisfies

4.2.5.2 soundness

4.2.6 Inference Rules

The inference rules for the access-control logic (ACL) are shown in figure 4.2. All the inference rules are sound. Details of proofs of soundness can be found in *Access Control, Security, and Trust: A Logical Approach*[2].

4.2.7 Complete mediation

Fundamental to this work is the concept of complete mediation (discussed in section 4.1.3). In the ACL, this means that each principal must be authenticated and authorized on each request. ACL does this primarily by the *Controls* inference rule in

$$\begin{array}{l}
P \text{ controls } \varphi \stackrel{\text{def}}{=} (P \text{ says } \varphi) \supset \varphi \quad P \text{ reps } Q \text{ on } \varphi \stackrel{\text{def}}{=} P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi \\
\\
\text{Modus Ponens} \quad \frac{\varphi \quad \varphi \supset \varphi'}{\varphi'} \quad \text{Says} \quad \frac{\varphi}{P \text{ says } \varphi} \quad \text{Controls} \quad \frac{P \text{ controls } \varphi \quad P \text{ says } \varphi}{\varphi} \\
\\
\text{Derived Speaks For} \quad \frac{P \Rightarrow Q \quad P \text{ says } \varphi}{Q \text{ says } \varphi} \quad \text{Reps} \quad \frac{Q \text{ controls } \varphi \quad P \text{ reps } Q \text{ on } \varphi \quad P \mid Q \text{ says } \varphi}{\varphi} \\
\\
\& \text{ Says (1)} \quad \frac{P \& Q \text{ says } \varphi}{P \text{ says } \varphi \wedge Q \text{ says } \varphi} \quad \& \text{ Says (2)} \quad \frac{P \text{ says } \varphi \wedge Q \text{ says } \varphi}{P \& Q \text{ says } \varphi} \\
\\
\text{Quoting (1)} \quad \frac{P \mid Q \text{ says } \varphi}{P \text{ says } Q \text{ says } \varphi} \quad \text{Quoting (2)} \quad \frac{P \text{ says } Q \text{ says } \varphi}{P \mid Q \text{ says } \varphi} \\
\\
\text{Idempotency of } \Rightarrow \quad \frac{}{P \Rightarrow P} \quad \text{Monotonicity of } \Rightarrow \quad \frac{P' \Rightarrow P \quad Q' \Rightarrow Q}{P' \mid Q' \Rightarrow P \mid Q}
\end{array}$$

Figure 4.2: The ACL inference rules. Image taken from *Access Control, Security, and Trust: A Logical Approach*[2]

figure 4.2 and shown again here in figure 4.3.

$$\text{Controls} \quad \frac{P \text{ controls } \varphi \quad P \text{ says } \varphi}{\varphi}$$

Figure 4.3: The *Controls* inference rule. Image taken from *Access Control, Security, and Trust: A Logical Approach*[2]

ACL refers to the left statement as an authorization². The principal P controls (is authorized on) some action φ . ACL refers to the right statement in this inference rule as a request³. The principal P requests some action φ . The conjunction of the authorization and the request of P on φ results in the action φ . That is, if $P \text{ controls } \varphi$ and $P \text{ says } \varphi$ then φ is true.

The *Controls* rule is sufficient for basic authorization involving one principal and some action. It is the only rule applied in this master thesis. But, there are more complicated rules that allow for additional authentication and authorization schemes.

The *Reps* (shown in figure 4.4) rule also demonstrates complete mediation. It follows a

²or a *control* in the C2 calculus

³or a *command* in the C2 calculus

$$\text{Reps} \quad \frac{Q \text{ controls } \varphi \quad P \text{ reps } Q \text{ on } \varphi \quad P \mid Q \text{ says } \varphi}{\varphi}$$

Figure 4.4: The *Reps* inference rule. Image taken from *Access Control, Security, and Trust: A Logical Approach*[2]

similar logic. But, this rule has two principals, in this case P and Q. The idea is that Q controls (is authorized on) some action φ . And also, P represents Q on that action. In the ACL, this means that $P \text{ Reps } Q \text{ on } \varphi$. Thus, $P \text{ says } \varphi$ is irrelevant because P does not have authority on φ . But, $P \mid Q \text{ says } \varphi$ (short for, $P \text{ says } Q \text{ says } \varphi$) is relevant because P represents Q and Q has authority. Spelled out, the rule follows as such: if $Q \text{ controls } \varphi$ and $P \text{ reps } Q \text{ on } \varphi$ and $P \mid Q \text{ on } \varphi$ then φ is true.

The *Reps* rule represents a principal acting in a role. For example, soldier G.I. Jane may be acting as the Platoon Leader. In this situation, it is the Platoon Leader (Q) who is granted authority over the action φ . But, it is G.I.Jane (P) acting in the role of Platoon Leader who (Q) is actually issuing the command φ .

$$\text{Derived Speaks For} \quad \frac{P \Rightarrow Q \quad P \text{ says } \varphi}{Q \text{ says } \varphi}$$

Figure 4.5: The *Derived Speaks For* inference rule. Image taken from *Access Control, Security, and Trust: A Logical Approach*[2]

The *Derived Speaks For* rule also allows for variation in authentication and authorization. This rule is shown in figure 4.5. This also uses two principals and deals mainly with the concept of jurisdiction and authentication. In this case, the principal P is "speaking for" the principal Q. Again, the symbol \Rightarrow means "speaks for." Thus, if $P \Rightarrow Q$ and $P \text{ says } \varphi$ then we believe that $Q \text{ says } \varphi$.

The most common use of the *Derived Speaks For* rule is in jurisdictional case. For example, the United States Army has jurisdiction over who serves in the role of Platoon Leader. The U.S. Army may, in turn, issue i.d. cards with a soldier's photo (or in the

future chips) that say, for example, soldier G.I.Jane is who she says she is. If we believe the i.d. card is genuine and it belongs to G.I.Jane, then the i.d. card speaks for G.I.Jane. So, if the i.d. card says issue G.I.Jane her equipment, then it follows that G.I.Jane says to issue her the equipment. It is somewhat more complicated, because the U.S. Army has jurisdiction over who gets what equipment. The i.d. card is not saying that G.I.Jane has control over her equipment. It only says that she is asking for the equipment.

The *Derived Speaks For* rule is critical to authentication, whereas the *Controls* and *Reps* rules are critical for authentication.

4.3 ACL in HOL

The equivalence of the ACL formulas implemented in HOL are shown in figure 4.6.

Access-Control Logic Formula	HOL Syntax
$\langle \text{jump} \rangle$	prop jump
$\neg \langle \text{jump} \rangle$	notf (prop jump)
$\langle \text{run} \rangle \wedge \langle \text{jump} \rangle$	prop run andf prop jump
$\langle \text{run} \rangle \vee \langle \text{stop} \rangle$	prop run orf prop stop
$\langle \text{run} \rangle \supset \langle \text{jump} \rangle$	prop run impf prop jump
$\langle \text{walk} \rangle \equiv \langle \text{stop} \rangle$	prop walk eqf prop stop
<i>Alice</i> says $\langle \text{jump} \rangle$	Name Alice says prop jump
<i>Alice</i> & <i>Bob</i> says $\langle \text{stop} \rangle$	Name Alice meet Name Bob says prop stop
<i>Bob</i> <i>Carol</i> says $\langle \text{run} \rangle$	Name Bob quoting Name Carol says prop run
<i>Bob</i> controls $\langle \text{walk} \rangle$	Name Bob controls prop walk
<i>Bob</i> reps <i>Alice</i> on $\langle \text{jump} \rangle$	reps (Name Bob) (Name Alice) (prop jump)
<i>Carol</i> \Rightarrow <i>Bob</i>	Name Carol speaks_for Name Bob

Figure 4.6: The ACL formulas in HOL. Image taken from *Access Control, Security, and Trust: A Logical Approach*[2]

Using this syntax, an ACL request of the form P says φ would have the form

$$\text{Name } P \text{ says prop } \varphi$$

4.3.1 Complete Mediation

4.3.2 satList

Chapter 5

Patrol Base Operations

5.1 Motivation

5.2 Ranger Handbook Description

5.3 Modeling the Patrol Base Operations from the Ranger Handbook

Modeling a system requires the knowledge of an expert on the system. This is necessary because only someone who is familiar with the system, especially with regards to security, can detail its nuances. For this reason, a subject matter expert from the United States Army (Jesse Nathaniel Hall) is employed to develop a model of the patrol base operations.

The model of the patrol base operations needs to be amiable to complete mediation and verification using an access-control logic (section 4.2). This is necessary to prove

security properties of the patrol base operations. To do this, the patrol base operations are abstracted from the Ranger Manual and modeled in Visio¹. The result of doing this is a hierarchy of secure state machines (SSMs). (SSMs are described in section 6.2.)

5.4 Overview of The Hierarchy of Secure State Machines

Each level of the hierarchy of SSMs represents a level of abstraction of the patrol base operations. The most abstract level of the hierarchy is the top level SSM. A diagram of this most abstract level is shown in figure 5.1.

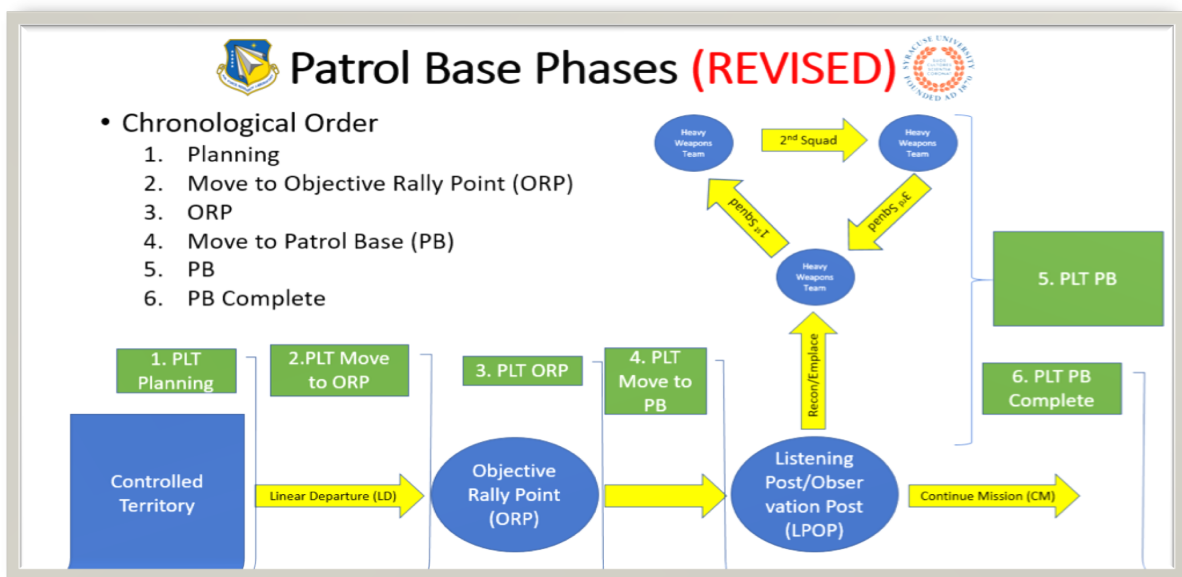


Figure 5.1: A diagram of the most abstract level in the hierarchy of secure state machines. Image generated by Jesse Nathaniel as part of the research involved in this master thesis. Shall I get his permission?

The diagram describes a chronological order of abstract phases (modeled as states) of

¹This work began as a collaboration between Jesse Nathaniel Hall and the author. Once the hierarchy of secure state machines was decided upon, the abstraction of the Ranger Handbook was done by Jesse Nathaniel Hall with only structural consultation with the author. Concurrently, the author focused on proving the properties of complete mediation in the ACL using HOL. Thus, there was a great deal of separation of work. Jesse's work is described here because it is necessary to put the entire system into context for this master thesis. This means that Jesse's work provided the model of the system for which the principle of complete mediation was proved, verified and documented.

the patrol base operations. The operations begin with the planning phase (1). Next, they move to the objective rally point (ORP) (2). At the ORP, operations commence (3). When these are complete, the patrol base operations move to the actual patrol base (4). At the patrol base, operations proceed (5). Finally, the patrol base operations are complete (6). These are the six states in the top level SSM.

The next level of abstraction in the hierarchy of SSMs represents a horizontal slice through the patrol base operations. This is the second level of the hierarchical description of the patrol base operations. It is referred to as the sub level. In this documentation, SSMs at this level are referred to as the sub-level, sublevel, or subLevel SSMs. This slice describes the patrol base operations at a lower level of abstraction. It expands each of the states in the top level (except for the last state PB Complete). For example, the planning phase (1) in figure 5.1 is expanded into an SSM of its own. This is called `ssmPlanPB`. It consists of several states (see section 5.5.5.1) which detail activities conducted during the planning phase of the patrol base operations. Each state in the top level (except for PB Complete) has it's own SSM (see the next section).

At yet another lower level of abstraction is the sub-sub (3rd) level. In this documentation, SSMs at this level are referred to as the sub-sub-level, subsublevel, or subsubLevel SSMs. This level expands upon the states in the sub level (one level above) in the same manner that the sub level expands upon the states in the top level SSM. In this manner, each level is a lower level of abstraction than the level above it.

A vertical slice through the diagram is also modeled. This slice models the patrol base operations from the top level down to the most detailed level (level 8). This vertical slice consists of a series of SSMs. Each SSM expands upon only one state in the level above it. This differs from the horizontal slice which expands upon all states in the level above it. Expanding upon only one state focuses on a vertical slice through all 8 states of the hierarchy of SSMs.

The vertical slice begins at the top level SSM. Next, it expands upon one state at this level, the *move to ORP* state (2). This results in a sub level SSM named *ssmMoveToORP*. The vertical slice progresses in this manner, by expanding one state at each level into a new SSM. From *ssmMoveToORP*, the state *secure halt* is expanded to *ssmSecureHalt*. From within this SSM, the state *ORP Recon* is expanded into *ssmORPRecon*. From within this SSM, the state *Move to ORP 4L* (fourth level move to ORP state) is expanded into *ssmMoveToORP4L*. Finally, from within this SSM, the state *Form RT* is expanded into *ssmFormRT*.

The vertical slice spans the all eight levels. However, not all levels are represented with an SSM. The last SSM in the vertical slice, *ssmFormRT*, is actually at the 5th level of the hierarchy. This SSM, consists of three states. These three states reside at the 7th level because *ssmFormRT* does not have states at the 6th level (it skips the 6th level). Furthermore, the 7th level states are not expanded into an SSM because each of these 7th level states expand into only one state at the 8th level.

In addition to the horizontal and vertical slices, an escape level is also modeled. Actions in the escape level are reachable from any phase of the patrol base operations. These actions are the unacceptable circumstances that require the patrol base operations to abort. For example, if the patrol base contacts the enemy in any phase of the operations, then the command *react to combat* is issued. The patrol base operations are subsequently aborted.

Excluding the escape level, there are eight levels of the hierarchy of SSMs.

Note that, the purpose of this master thesis is to demonstrate that the properties of complete mediation could be applied and verified on a non-automated, human-centered systems. Thus, it is sufficient to demonstrate this on a horizontal and vertical slice of the patrol base operations.

5.5 Hierarchy of Secure State Machines

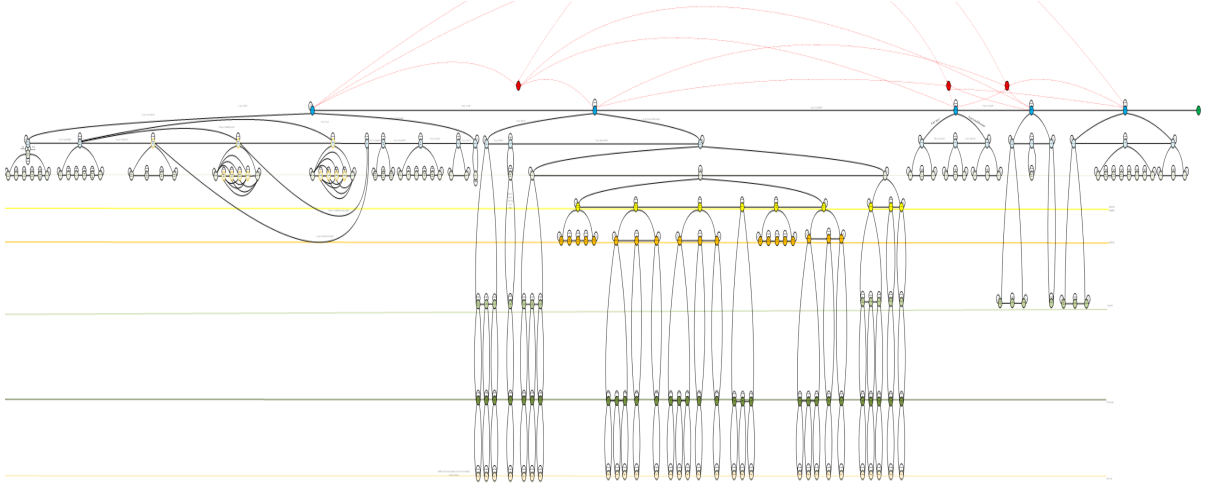


Figure 5.2: Diagrammatic description of patrol base operations as a hierarchy of secure state machines. (Generated by Jesse Nathaniel Hall.)

5.5.1 Diagrammatic Description in Visio

The enormity of the hierarchy of SSMs is evident in figure 5.2. This is a squashed version of the Visio diagram for the hierarchy of SSMs. The diagram is included as a Visio file with the files for this project (LaTeX/figures/diagram.vis).

The straight, colored lines that span the diagram in figure 5.2 delineate levels of the hierarchy of SSMs. The top lines are obscured by the size of this squashed version of the diagram. The most visible bright yellow line delineates the sub-sub-sub (4th) level of the hierarchy, for example.

The small, colored dots in figure 5.2 represent states (phases) of the patrol base operations. The red dots are an exception. The labels for these states are not readable in this diagram. The dots are color coded. The colors correspond to the level of those states. For example, the dots at the top level (level below the red dots) are all dark blue.

In figure 5.2, the red dots at the top of the diagram represent the escape level SSM.

But, they do not represent states in the SSM. This is because the escape level SSM is accessible by all phases of the patrol base operations. This means that it can not be ascribed to any one level of the hierarchy.

The dots representing states are connected to each other by lines. These lines represent allowable transitions from one state to another. The escape level is again an exception. If no line connects one state to another then no transition is allowed.

The red dots representing the escape level SSM are best thought of as multiple copies of a floating SSM. The escape level SSM acts as a sub-SSM for all SSMs in the hierarchy. During patrol base operations, abortion of the patrol base operations can occur at any action from any state at any level. This means that any state at any level can be terminated by the escape level SSM. Drawing lines from all states to the escape level SSM and drawing really long lines clutters the diagram. Therefore, only lines at the top level are drawn and the red dots are duplicated.

The lines in the diagram are annotated by SSM requests. (Annotations are visible in the original Visio diagram, but not in this squashed version.) For example, a line connecting the top level state PLAN_PB is annotated with the request *PlatoonLeader says crossLD*. crossLD is an abbreviation for "cross the line of discrimination" and it is the command to transition to the MOVE_TO_ORP state. Lines are not annotated beyond the sub level.

Details of each level follow in the next section.

5.5.2 OMNI-Level

5.5.3 Escape

5.5.4 Top Level

5.5.5 Horizontal Slice

5.5.5.1 ssmPlanPB

5.5.5.2 ssmMoveToORP

5.5.5.3 ssmConductORP

5.5.5.4 ssmMoveToPB

5.5.5.5 ssmConductPB

5.5.6 Vertical Slice

5.5.6.1 ssmSecureHalt

5.5.6.2 ssmORPRecon

5.5.6.3 ssmMoveToORP4L

5.5.6.4 ssmFormRT

Chapter 6

Secure State Machine Model

6.1 State Machines

6.1.1 Configuration

6.1.2 Next-state Function

6.1.3 Next-output Function

6.1.4 Transition Commands

6.2 Secure State Machines

6.2.1 State Machine Versus Secure State Machine

6.2.2 Monitors

6.2.3 Configuration

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

There were other modules and complexities in the patrol base operations that were discussed during the course of the work. However, because of time constraints they were not verified in the ACL and HOL.

8.4.1 Authentication: Roles and Cypto

This master thesis discussed authentication as a visual confirmation among the soldiers. For example, most often, most soldiers in a platoon know who their platoon leader is and do not require a password. But, this is not always the case. One example where it may not be readily obvious is when the platoon leader has been incapacitated and can no longer function in that role. The military has a clearly defined succession hierarchy and soldier are (or should be) aware of this. But, computers aren't as smart as soldiers...unless they are designed to be so. In this case, the concept of soldiers acting in roles is useful.

The idea behind defining the platoon leader as the authorized principal in, for example, the top level SSM allows for the system to work regardless of who the platoon leader is. Nevertheless, it is the soldier acting in the role of the platoon leader who is actually authorized. This can also be represented in the SSM model. In fact, a parametrizable SSM is already designed and implemented in HOL to do this.

In this model, the *reps* rule from figure 4.2 does this.

8.4.2 Soldier Theory

8.4.3 Platoon Theory

8.4.4 Squad And Fire Team Theories

Chapter 9

Future Work & Implications

9.1 ...on The Patrol Base Operations

9.2 ...on Other Non-automated Human-Centered Systems

Emergency Management systems require human communications. As with most systems of communication, the communicators need to work with the confidence that they are receiving instructions from the right source with the right authority. A remodeling of the system with complete mediation in mind. From the work in this thesis, the system could simply be modeled in a way that highlights communication avenues and applies CSBD to verify complete mediation.

On perhaps a smaller scale, but no less significant, are non-automated, human-centered school drills such as fire drills and active shooter drills. Clearly, a systems engineering approach could be used to model these drills. The systems security engineering aspect

would cover things such as verifying that safety zones are assigned and reasonably accessible, "what to do if" scenarios problems are discussed and solved, and who to trust under what circumstances are solved. Complete mediation would be intertwined within this system design. For example, when should students leave their classrooms after lock-down? Who says so? How do you know if that person is trust worthy? If its the teacher or a police officer, then authentication is typically a matter of visual recognition as it is with authentication in the patrol base operations. Regardless of how these are decided, these things should be decided during the design phase of the drill and the concepts of complete mediation should be built-in to the design.

9.3 Accountability Systems

9.4 Further Applicability

Thinking about complete mediation should accompany any system design, big or small. For example, parents often sends their child(ren) to school with instructions to come home safely. But, what does that mean. By thinking about complete mediation, the parents should ask some important questions. Many of these questions and answers involve concepts of complete mediation. Does the bus driver have the authority to drive you home on the bus? How do you recognize this bus from the wrong bus? Does a stranger have the authority to pick your child(ren) up from school? If so, under what circumstances? An emergency? How do you know that this stranger really is a friend of your parents? A key word? A note from your mom?

9.5 The Bigger Framework of Systems Security Engineering

The span of manmade systems.

Appendices

Appendix A

Access Control Logic Theories: Pretty-Printed Theories

Contents

1	acfoundation Theory	3
1.1	Datatypes	3
1.2	Definitions	3
1.3	Theorems	4
2	acsemanatics Theory	6
2.1	Definitions	6
2.2	Theorems	8
3	aclrules Theory	10
3.1	Definitions	11
3.2	Theorems	11
4	aclDrules Theory	17
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]

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

[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]

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

[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]

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

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]

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

[doms_def]

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

[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: aclrules

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
 - Lsfndef, 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

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

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

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

[escCommand_distinct_clauses]

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

[escOutput_distinct_clauses]

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

[escState_distinct_clauses]

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

[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]

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


```

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) ⇔

```

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

[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]

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

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

[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]

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

[TR_ind]

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

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

[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]

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

[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]

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

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]

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

```

(CFG elementTest stateInterp context ins
  (NS s (exec (inputList x)))
  (Out s (exec (inputList x))::outs))) ∧
(∀ elementTest NS M Oi Os Out s context stateInterp x ins
  outs.
  authenticationTest elementTest x ∧
  CFGInterpret (M, Oi, Os)
    (CFG elementTest stateInterp context (x::ins) s outs) ⇒
  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))) ∧
  ∀ elementTest NS M Oi Os Out s context stateInterp x ins outs.
    ¬authenticationTest elementTest x ⇒
    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)))

```

[TR_strongind]

```

⊢ ∀ TR'.
  (∀ elementTest NS M Oi Os Out s context stateInterp x ins
    outs.
    authenticationTest elementTest x ∧
    CFGInterpret (M, Oi, Os)
      (CFG elementTest stateInterp context (x::ins) s
        outs) ⇒
    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))) ∧
    (∀ elementTest NS M Oi Os Out s context stateInterp x ins
      outs.
      authenticationTest elementTest x ∧
      CFGInterpret (M, Oi, Os)
        (CFG elementTest stateInterp context (x::ins) s
          outs) ⇒
      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))) ∧
      (∀ elementTest NS M Oi Os Out s context stateInterp x ins
        outs.
        ¬authenticationTest elementTest x ⇒
        TR' (M, Oi, Os) (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]

$\vdash \forall P.$

$P \text{ PLAN_PB (exec (SLc crossLD))} \wedge$
 $P \text{ PLAN_PB (exec (SLc incomplete))} \wedge$
 $P \text{ MOVE_TO_ORP (exec (SLc conductORP))} \wedge$
 $P \text{ MOVE_TO_ORP (exec (SLc incomplete))} \wedge$
 $P \text{ CONDUCT_ORP (exec (SLc moveToPB))} \wedge$
 $P \text{ CONDUCT_ORP (exec (SLc incomplete))} \wedge$
 $P \text{ MOVE_TO_PB (exec (SLc conductPB))} \wedge$
 $P \text{ MOVE_TO_PB (exec (SLc incomplete))} \wedge$
 $P \text{ CONDUCT_PB (exec (SLc completePB))} \wedge$
 $P \text{ CONDUCT_PB (exec (SLc incomplete))} \wedge$
 $(\forall s \text{ cmd. } P s \text{ (trap (SLc cmd))}) \wedge$
 $(\forall s \text{ cmd. } P s \text{ (discard (SLc cmd))}) \wedge$
 $(\forall s v_6. P s \text{ (discard (ESCc } v_6))) \wedge$
 $(\forall s v_9. P s \text{ (trap (ESCc } v_9))) \wedge$
 $(\forall v_{12}. P \text{ PLAN_PB (exec (ESCc } v_{12}))) \wedge$
 $P \text{ PLAN_PB (exec (SLc conductORP))} \wedge$
 $P \text{ PLAN_PB (exec (SLc moveToPB))} \wedge$
 $P \text{ PLAN_PB (exec (SLc conductPB))} \wedge$
 $P \text{ PLAN_PB (exec (SLc completePB))} \wedge$
 $(\forall v_{15}. P \text{ MOVE_TO_ORP (exec (ESCc } v_{15}))) \wedge$
 $P \text{ MOVE_TO_ORP (exec (SLc crossLD))} \wedge$
 $P \text{ MOVE_TO_ORP (exec (SLc moveToPB))} \wedge$
 $P \text{ MOVE_TO_ORP (exec (SLc conductPB))} \wedge$
 $P \text{ MOVE_TO_ORP (exec (SLc completePB))} \wedge$
 $(\forall v_{18}. P \text{ CONDUCT_ORP (exec (ESCc } v_{18}))) \wedge$
 $P \text{ CONDUCT_ORP (exec (SLc crossLD))} \wedge$
 $P \text{ CONDUCT_ORP (exec (SLc conductORP))} \wedge$
 $P \text{ CONDUCT_ORP (exec (SLc conductPB))} \wedge$
 $P \text{ CONDUCT_ORP (exec (SLc completePB))} \wedge$
 $(\forall v_{21}. P \text{ MOVE_TO_PB (exec (ESCc } v_{21}))) \wedge$
 $P \text{ MOVE_TO_PB (exec (SLc crossLD))} \wedge$
 $P \text{ MOVE_TO_PB (exec (SLc conductORP))} \wedge$
 $P \text{ MOVE_TO_PB (exec (SLc moveToPB))} \wedge$
 $P \text{ MOVE_TO_PB (exec (SLc completePB))} \wedge$
 $(\forall v_{24}. P \text{ CONDUCT_PB (exec (ESCc } v_{24}))) \wedge$
 $P \text{ CONDUCT_PB (exec (SLc crossLD))} \wedge$
 $P \text{ CONDUCT_PB (exec (SLc conductORP))} \wedge$
 $P \text{ CONDUCT_PB (exec (SLc moveToPB))} \wedge$
 $P \text{ CONDUCT_PB (exec (SLc conductPB))} \wedge$
 $(\forall v_{26}. P \text{ COMPLETE_PB (exec } v_{26})) \Rightarrow$
 $\forall v v_1. P v v_1$

[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]

```

⊢ (secContext PLAN_PB (x::xs) =
  [prop (SOME (SLc (OMNI ssmPlanPBComplete))) impf
   Name PlatoonLeader controls
   prop (SOME (SLc (PL crossLD)))]) ∧
(secContext MOVE_TO_ORP (x::xs) =
  [prop (SOME (SLc (OMNI ssmMoveToORPComplete))) impf
   Name PlatoonLeader controls
   prop (SOME (SLc (PL conductORP)))]) ∧
(secContext CONDUCT_ORP (x::xs) =
  [prop (SOME (SLc (OMNI ssmConductORPComplete))) impf
   Name PlatoonLeader controls

```

```

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

```

[secContext_ind]

```

 $\vdash \forall P.$ 
  ( $\forall x\ xs. P\ \text{PLAN\_PB}\ (x::xs)$ )  $\wedge$ 
  ( $\forall x\ xs. P\ \text{MOVE\_TO\_ORP}\ (x::xs)$ )  $\wedge$ 
  ( $\forall x\ xs. P\ \text{CONDUCT\_ORP}\ (x::xs)$ )  $\wedge$ 
  ( $\forall x\ xs. P\ \text{MOVE\_TO\_PB}\ (x::xs)$ )  $\wedge$ 
  ( $\forall x\ xs. P\ \text{CONDUCT\_PB}\ (x::xs)$ )  $\wedge$  ( $\forall v_4. P\ v_4\ []$ )  $\wedge$ 
  ( $\forall v_5\ v_6. P\ \text{COMPLETE\_PB}\ (v_5::v_6)$ )  $\Rightarrow$ 
   $\forall v\ v_1. P\ v\ v_1$ 

```

8 ssmConductORP Theory

Built: 13 May 2018

Parent Theories: ConductORPType, ssm11, OMNITYPE

8.1 Definitions

[secContextConductORP_def]

```

 $\vdash \forall plcmd\ psgcmd\ incomplete.$ 
  secContextConductORP 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]

```

[ssmConductORPStateInterp_def]

```

 $\vdash \forall slState. \text{ssmConductORPStateInterp}\ slState = \text{TT}$ 

```

8.2 Theorems

[authTestConductORP_cmd_reject_lemma]

```

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

```

[authTestConductORP_def]

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

[conductORPOut_def]

\vdash (conductORPOut CONDUCT_ORP (exec (PL secure)) = Secure) \wedge
 (conductORPOut CONDUCT_ORP (exec (PL plIncomplete)) =
 ConductORP) \wedge
 (conductORPOut SECURE (exec (PSG actionsIn)) = ActionsIn) \wedge
 (conductORPOut SECURE (exec (PSG psgIncomplete)) = Secure) \wedge
 (conductORPOut ACTIONS_IN (exec (PL withdraw)) = Withdraw) \wedge
 (conductORPOut ACTIONS_IN (exec (PL plIncomplete)) =
 ActionsIn) \wedge
 (conductORPOut WITHDRAW (exec (PL complete)) = Complete) \wedge
 (conductORPOut WITHDRAW (exec (PL plIncomplete)) =
 Withdraw) \wedge
 (conductORPOut s (trap (PL cmd')) = unauthorized) \wedge
 (conductORPOut s (trap (PSG cmd)) = unauthorized) \wedge
 (conductORPOut s (discard (PL cmd')) = unAuthenticated) \wedge
 (conductORPOut s (discard (PSG cmd)) = unAuthenticated)

[conductORPOut_ind]

$\vdash \forall P.$
 P CONDUCT_ORP (exec (PL secure)) \wedge
 P CONDUCT_ORP (exec (PL plIncomplete)) \wedge
 P SECURE (exec (PSG actionsIn)) \wedge
 P SECURE (exec (PSG psgIncomplete)) \wedge
 P ACTIONS_IN (exec (PL withdraw)) \wedge
 P 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]

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

[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]

$$\begin{aligned}
& \vdash \forall P. \\
& \quad P \text{ MOVE_TO_ORP (exec (SLc pltForm))} \wedge \\
& \quad P \text{ MOVE_TO_ORP (exec (SLc incomplete))} \wedge \\
& \quad P \text{ PLT_FORM (exec (SLc pltMove))} \wedge \\
& \quad P \text{ PLT_FORM (exec (SLc incomplete))} \wedge \\
& \quad P \text{ PLT_MOVE (exec (SLc pltSecureHalt))} \wedge \\
& \quad P \text{ PLT_MOVE (exec (SLc incomplete))} \wedge
\end{aligned}$$

$$\begin{aligned}
& P \text{ PLT_SECURE_HALT } (\text{exec } (\text{SLc complete})) \wedge \\
& P \text{ PLT_SECURE_HALT } (\text{exec } (\text{SLc incomplete})) \wedge \\
& (\forall s \text{ cmd. } P \ s \ (\text{trap } (\text{SLc cmd}))) \wedge \\
& (\forall s \text{ cmd. } P \ s \ (\text{discard } (\text{SLc cmd}))) \wedge \\
& (\forall s \ v_6. \ P \ s \ (\text{discard } (\text{ESCc } v_6))) \wedge \\
& (\forall s \ v_9. \ P \ s \ (\text{trap } (\text{ESCc } v_9))) \wedge \\
& (\forall v_{12}. \ P \ \text{MOVE_TO_ORP } (\text{exec } (\text{ESCc } v_{12}))) \wedge \\
& P \ \text{MOVE_TO_ORP } (\text{exec } (\text{SLc pltMove})) \wedge \\
& P \ \text{MOVE_TO_ORP } (\text{exec } (\text{SLc pltSecureHalt})) \wedge \\
& P \ \text{MOVE_TO_ORP } (\text{exec } (\text{SLc complete})) \wedge \\
& (\forall v_{15}. \ P \ \text{PLT_FORM } (\text{exec } (\text{ESCc } v_{15}))) \wedge \\
& P \ \text{PLT_FORM } (\text{exec } (\text{SLc pltForm})) \wedge \\
& P \ \text{PLT_FORM } (\text{exec } (\text{SLc pltSecureHalt})) \wedge \\
& P \ \text{PLT_FORM } (\text{exec } (\text{SLc complete})) \wedge \\
& (\forall v_{18}. \ P \ \text{PLT_MOVE } (\text{exec } (\text{ESCc } v_{18}))) \wedge \\
& P \ \text{PLT_MOVE } (\text{exec } (\text{SLc pltForm})) \wedge \\
& P \ \text{PLT_MOVE } (\text{exec } (\text{SLc pltMove})) \wedge \\
& P \ \text{PLT_MOVE } (\text{exec } (\text{SLc complete})) \wedge \\
& (\forall v_{21}. \ P \ \text{PLT_SECURE_HALT } (\text{exec } (\text{ESCc } v_{21}))) \wedge \\
& P \ \text{PLT_SECURE_HALT } (\text{exec } (\text{SLc pltForm})) \wedge \\
& P \ \text{PLT_SECURE_HALT } (\text{exec } (\text{SLc pltMove})) \wedge \\
& P \ \text{PLT_SECURE_HALT } (\text{exec } (\text{SLc pltSecureHalt})) \wedge \\
& (\forall v_{23}. \ P \ \text{COMPLETE } (\text{exec } v_{23})) \Rightarrow \\
& \forall v \ v_1. \ P \ v \ v_1
\end{aligned}$$

[moveToORPOut_def]

$$\begin{aligned}
& \vdash (\text{moveToORPOut } \text{MOVE_TO_ORP } (\text{exec } (\text{SLc pltForm})) = \text{PLTForm}) \wedge \\
& (\text{moveToORPOut } \text{MOVE_TO_ORP } (\text{exec } (\text{SLc incomplete})) = \\
& \quad \text{MoveToORP}) \wedge \\
& (\text{moveToORPOut } \text{PLT_FORM } (\text{exec } (\text{SLc pltMove})) = \text{PLTMove}) \wedge \\
& (\text{moveToORPOut } \text{PLT_FORM } (\text{exec } (\text{SLc incomplete})) = \text{PLTForm}) \wedge \\
& (\text{moveToORPOut } \text{PLT_MOVE } (\text{exec } (\text{SLc pltSecureHalt})) = \\
& \quad \text{PLTSecureHalt}) \wedge \\
& (\text{moveToORPOut } \text{PLT_MOVE } (\text{exec } (\text{SLc incomplete})) = \text{PLTMove}) \wedge \\
& (\text{moveToORPOut } \text{PLT_SECURE_HALT } (\text{exec } (\text{SLc complete})) = \\
& \quad \text{Complete}) \wedge \\
& (\text{moveToORPOut } \text{PLT_SECURE_HALT } (\text{exec } (\text{SLc incomplete})) = \\
& \quad \text{PLTSecureHalt}) \wedge \\
& (\text{moveToORPOut } s \ (\text{trap } (\text{SLc cmd})) = \text{unAuthorized}) \wedge \\
& (\text{moveToORPOut } s \ (\text{discard } (\text{SLc cmd})) = \text{unAuthenticated})
\end{aligned}$$

[moveToORPOut_ind]

$$\begin{aligned}
& \vdash \forall P. \\
& \quad P \ \text{MOVE_TO_ORP } (\text{exec } (\text{SLc pltForm})) \wedge \\
& \quad P \ \text{MOVE_TO_ORP } (\text{exec } (\text{SLc incomplete})) \wedge \\
& \quad P \ \text{PLT_FORM } (\text{exec } (\text{SLc pltMove})) \wedge \\
& \quad P \ \text{PLT_FORM } (\text{exec } (\text{SLc incomplete})) \wedge \\
& \quad P \ \text{PLT_MOVE } (\text{exec } (\text{SLc pltSecureHalt})) \wedge \\
& \quad P \ \text{PLT_MOVE } (\text{exec } (\text{SLc incomplete})) \wedge
\end{aligned}$$

P PLT_SECURE_HALT (exec (SLc complete)) \wedge
 P PLT_SECURE_HALT (exec (SLc incomplete)) \wedge
 $(\forall s \text{ cmd}. P \ s \ (\text{trap} \ (\text{SLc} \ \text{cmd}))) \wedge$
 $(\forall s \text{ cmd}. P \ s \ (\text{discard} \ (\text{SLc} \ \text{cmd}))) \wedge$
 $(\forall s \ v_6. P \ s \ (\text{discard} \ (\text{ESCc} \ v_6))) \wedge$
 $(\forall s \ v_9. P \ s \ (\text{trap} \ (\text{ESCc} \ v_9))) \wedge$
 $(\forall v_{12}. P \ \text{MOVE_TO_ORP} \ (\text{exec} \ (\text{ESCc} \ v_{12}))) \wedge$
 $P \ \text{MOVE_TO_ORP} \ (\text{exec} \ (\text{SLc} \ \text{pltMove})) \wedge$
 $P \ \text{MOVE_TO_ORP} \ (\text{exec} \ (\text{SLc} \ \text{pltSecureHalt})) \wedge$
 $P \ \text{MOVE_TO_ORP} \ (\text{exec} \ (\text{SLc} \ \text{complete})) \wedge$
 $(\forall v_{15}. P \ \text{PLT_FORM} \ (\text{exec} \ (\text{ESCc} \ v_{15}))) \wedge$
 $P \ \text{PLT_FORM} \ (\text{exec} \ (\text{SLc} \ \text{pltForm})) \wedge$
 $P \ \text{PLT_FORM} \ (\text{exec} \ (\text{SLc} \ \text{pltSecureHalt})) \wedge$
 $P \ \text{PLT_FORM} \ (\text{exec} \ (\text{SLc} \ \text{complete})) \wedge$
 $(\forall v_{18}. P \ \text{PLT_MOVE} \ (\text{exec} \ (\text{ESCc} \ v_{18}))) \wedge$
 $P \ \text{PLT_MOVE} \ (\text{exec} \ (\text{SLc} \ \text{pltForm})) \wedge$
 $P \ \text{PLT_MOVE} \ (\text{exec} \ (\text{SLc} \ \text{pltMove})) \wedge$
 $P \ \text{PLT_MOVE} \ (\text{exec} \ (\text{SLc} \ \text{complete})) \wedge$
 $(\forall v_{21}. P \ \text{PLT_SECURE_HALT} \ (\text{exec} \ (\text{ESCc} \ v_{21}))) \wedge$
 $P \ \text{PLT_SECURE_HALT} \ (\text{exec} \ (\text{SLc} \ \text{pltForm})) \wedge$
 $P \ \text{PLT_SECURE_HALT} \ (\text{exec} \ (\text{SLc} \ \text{pltMove})) \wedge$
 $P \ \text{PLT_SECURE_HALT} \ (\text{exec} \ (\text{SLc} \ \text{pltSecureHalt})) \wedge$
 $(\forall v_{23}. P \ \text{COMPLETE} \ (\text{exec} \ v_{23})) \Rightarrow$
 $\forall v \ v_1. P \ v \ v_1$

[PlatoonLeader_exec_slCommand_justified_thm]

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

[PlatoonLeader_slCommand_lemma]

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

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

13 MoveToORPType Theory

Built: 13 May 2018

Parent Theories: indexedLists, patternMatches

13.1 Datatypes

$\text{slCommand} = \text{pltForm} \mid \text{pltMove} \mid \text{pltSecureHalt} \mid \text{complete}$
 $\quad \mid \text{incomplete}$
 $\text{slOutput} = \text{MoveToORP} \mid \text{PLTForm} \mid \text{PLTMove} \mid \text{PLTSecureHalt}$
 $\quad \mid \text{Complete} \mid \text{unAuthorized} \mid \text{unAuthenticated}$
 $\text{slState} = \text{MOVE_TO_ORP} \mid \text{PLT_FORM} \mid \text{PLT_MOVE} \mid \text{PLT_SECURE_HALT}$
 $\quad \mid \text{COMPLETE}$
 $\text{stateRole} = \text{PlatoonLeader}$

13.2 Theorems

[slCommand_distinct_clauses]

$\vdash \text{pltForm} \neq \text{pltMove} \wedge \text{pltForm} \neq \text{pltSecureHalt} \wedge$
 $\text{pltForm} \neq \text{complete} \wedge \text{pltForm} \neq \text{incomplete} \wedge$
 $\text{pltMove} \neq \text{pltSecureHalt} \wedge \text{pltMove} \neq \text{complete} \wedge$
 $\text{pltMove} \neq \text{incomplete} \wedge \text{pltSecureHalt} \neq \text{complete} \wedge$
 $\text{pltSecureHalt} \neq \text{incomplete} \wedge \text{complete} \neq \text{incomplete}$

[slOutput_distinct_clauses]

$\vdash \text{MoveToORP} \neq \text{PLTForm} \wedge \text{MoveToORP} \neq \text{PLTMove} \wedge$
 $\text{MoveToORP} \neq \text{PLTSecureHalt} \wedge \text{MoveToORP} \neq \text{Complete} \wedge$
 $\text{MoveToORP} \neq \text{unAuthorized} \wedge \text{MoveToORP} \neq \text{unAuthenticated} \wedge$
 $\text{PLTForm} \neq \text{PLTMove} \wedge \text{PLTForm} \neq \text{PLTSecureHalt} \wedge$
 $\text{PLTForm} \neq \text{Complete} \wedge \text{PLTForm} \neq \text{unAuthorized} \wedge$
 $\text{PLTForm} \neq \text{unAuthenticated} \wedge \text{PLTMove} \neq \text{PLTSecureHalt} \wedge$
 $\text{PLTMove} \neq \text{Complete} \wedge \text{PLTMove} \neq \text{unAuthorized} \wedge$
 $\text{PLTMove} \neq \text{unAuthenticated} \wedge \text{PLTSecureHalt} \neq \text{Complete} \wedge$
 $\text{PLTSecureHalt} \neq \text{unAuthorized} \wedge$
 $\text{PLTSecureHalt} \neq \text{unAuthenticated} \wedge \text{Complete} \neq \text{unAuthorized} \wedge$
 $\text{Complete} \neq \text{unAuthenticated} \wedge \text{unAuthorized} \neq \text{unAuthenticated}$

[slState_distinct_clauses]

$\vdash \text{MOVE_TO_ORP} \neq \text{PLT_FORM} \wedge \text{MOVE_TO_ORP} \neq \text{PLT_MOVE} \wedge$
 $\text{MOVE_TO_ORP} \neq \text{PLT_SECURE_HALT} \wedge \text{MOVE_TO_ORP} \neq \text{COMPLETE} \wedge$
 $\text{PLT_FORM} \neq \text{PLT_MOVE} \wedge \text{PLT_FORM} \neq \text{PLT_SECURE_HALT} \wedge$
 $\text{PLT_FORM} \neq \text{COMPLETE} \wedge \text{PLT_MOVE} \neq \text{PLT_SECURE_HALT} \wedge$
 $\text{PLT_MOVE} \neq \text{COMPLETE} \wedge \text{PLT_SECURE_HALT} \neq \text{COMPLETE}$

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]

$$\begin{aligned}
&\vdash (\text{moveToPBNS MOVE_TO_PB (exec (SLc pltForm))} = \text{PLT_FORM}) \wedge \\
&\quad (\text{moveToPBNS MOVE_TO_PB (exec (SLc incomplete))} = \\
&\quad \quad \text{MOVE_TO_PB}) \wedge \\
&\quad (\text{moveToPBNS PLT_FORM (exec (SLc pltMove))} = \text{PLT_MOVE}) \wedge \\
&\quad (\text{moveToPBNS PLT_FORM (exec (SLc incomplete))} = \text{PLT_FORM}) \wedge \\
&\quad (\text{moveToPBNS PLT_MOVE (exec (SLc pltHalt))} = \text{PLT_HALT}) \wedge \\
&\quad (\text{moveToPBNS PLT_MOVE (exec (SLc incomplete))} = \text{PLT_MOVE}) \wedge \\
&\quad (\text{moveToPBNS PLT_HALT (exec (SLc complete))} = \text{COMPLETE}) \wedge \\
&\quad (\text{moveToPBNS PLT_HALT (exec (SLc incomplete))} = \text{PLT_HALT}) \wedge \\
&\quad (\text{moveToPBNS } s \text{ (trap (SLc cmd))} = s) \wedge \\
&\quad (\text{moveToPBNS } s \text{ (discard (SLc cmd))} = s)
\end{aligned}$$

[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 WARN0 (exec x) =
  if
    (getRecon x = [SOME (SLc (PL recon))]) ∧
    (getTentativePlan x = [SOME (SLc (PL tentativePlan))]) ∧
    (getReport x = [SOME (SLc (PL report1))]) ∧
    (getInitMove x = [SOME (SLc (PSG initiateMovement))])
  then
    REPORT1
  else WARN0) ∧
(planPBNS PLAN_PB (exec x) =
  if getPlCom x = receiveMission then RECEIVE_MISSION
  else PLAN_PB) ∧
(planPBNS RECEIVE_MISSION (exec x) =
  if getPlCom x = warn0 then WARN0 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 WARN0 (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 WARN0 (exec x) =
  if
    (getRecon x = [SOME (SLc (PL recon))]) ∧
    (getTentativePlan x = [SOME (SLc (PL tentativePlan))]) ∧
    (getReport x = [SOME (SLc (PL report1))]) ∧
    (getInitMove x = [SOME (SLc (PSG initiateMovement))])
  then
    REPORT1
  else WARN0)

```

```

then
  Report1
  else unauthorized) ∧
(planPBOut PLAN_PB (exec x) =
  if getPlCom x = receiveMission then ReceiveMission
  else unauthorized) ∧
(planPBOut RECEIVE_MISSION (exec x) =
  if getPlCom x = warno then Warno else unauthorized) ∧
(planPBOut REPORT1 (exec x) =
  if getPlCom x = completePlan then CompletePlan
  else unauthorized) ∧
(planPBOut COMPLETE_PLAN (exec x) =
  if getPlCom x = opoid then Opoid else unauthorized) ∧
(planPBOut OPOID (exec x) =
  if getPlCom x = supervise then Supervise
  else unauthorized) ∧
(planPBOut SUPERVISE (exec x) =
  if getPlCom x = report2 then Report2 else unauthorized) ∧
(planPBOut REPORT2 (exec x) =
  if getPlCom x = complete then Complete else unauthorized) ∧
(planPBOut s (trap v0) = unauthorized) ∧
(planPBOut s (discard v1) = unAuthenticated)

```

[planPBOut_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

```

[PlatoonLeader_notWARNO_notreport1_exec_plCommand_justified_lemma]

```

⊢ s ≠ WARNO ⇒
  plCommand ≠ invalidPlCommand ⇒
  plCommand ≠ report1 ⇒
  ∀ NS Out M Oi Os.
    TR (M, Oi, Os)
      (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  $\Rightarrow$ 

```

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

[PlatoonLeader_psgCommand_notDiscard_thm]

$\vdash \forall NS \ Out \ M \ O_i \ O_s.$
 $\neg TR \ (M, O_i, O_s)$
 (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]

$\vdash \forall NS \ Out \ M \ O_i \ O_s.$
 TR (M, O_i, O_s)
 (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) WARNNO outs)
(NS WARNNO
  (exec
    [SOME (SLc (PL recon));
     SOME (SLc (PL tentativePlan));
     SOME (SLc (PSG initiateMovement));
     SOME (SLc (PL report1))])
  (Out WARNNO
    (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) WARNNO 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]

$\vdash \forall M \text{ } Oi \text{ } Os.$
 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) \Rightarrow
 (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)))]

[PlatoonSergeant_trap_plCommand_justified_lemma]

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

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

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 escapeLevel

D.3 TopLevel

D.3.1 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.3.2 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.3.3 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 topLeve. 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.4 Horizontal Slice

D.4.1 ssmPlanPB

D.4.1.1 PlanPBType Theory: Type Definitions

D.4.1.2 PlanPBDef Theory: Authentication & Authorization Definitions

D.4.1.3 ssmPlanPB Theory: Theorems

D.4.2 ssmMoveToORP

D.4.2.1 MoveToORPType Theory: Type Definitions

D.4.2.2 MoveToORPDef Theory: Authentication & Authorization Definitions

D.4.2.3 ssmMoveToORP Theory: Theorems

D.4.3 ssmConductORP

D.4.3.1 ConductORPType Theory: Type Definitions

D.4.3.2 ConductORPDef Theory: Authentication & Authorization Definitions

D.4.3.3 ssmConductORP Theory: Theorems

D.4.4 ssmMoveToPB

D.4.4.1 MoveToPBType Theory: Type Definitions

D.4.4.2 MoveToPBDef Theory: Authentication & Authorization Definitions

D.4.4.3 ssmMoveToPB Theory: Theorems

D.4.5 ssmConductPB

Appendix E

Map of The File Folder Structure

References

- [1] United States Army Ranger School, ATTN: ATSH-RB, 10850 Schneider Rd, Bldg 5024, Ft Benning, GA 31905. *Ranger handbook*, April 2017.
- [2] 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.
- [3] Formal methods. *Wikipedia*, February 2018.
- [4] Edmund M. Clarke and et al Jeannette M. Wing. Formal methods: State of the art and future directions, December 1996.
- [5] Jagatheesan Kunasaikaran, Azlan Iqbal, Jalan Dua, and Chan Sow Lin. A brief overview of functional programming languages, 2016.
- [6] ISO/IEC/IEEE 15288 international standard - systems and software engineering – system life cycle processes. Technical Report ISO/IEC/IEEE 15288:2015(E), International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC) & Institute of Electrical and Electronics Engineers (IEEE), 3 Park Avenue, New York, NY 10016-5997, USA, May 2015.
- [7] ISO. Systems and software engineering–life cycle management–part 1: guide for life cycle management. Technical Report ISO/IEC TR 24748-1:2010(E), International Organization for Standardization (ISO), September 2010.
- [8] Lt Gen Charles F. Wald or Lt Col Sanders. Air force policy directive 10-28: Conops development. Operations 10-28, Secrtary of The Air Force, January 2002.
- [9] NIST. Nist mission, vision, core competencies, and core values.
- [10] The Rand Corporation. Security controls for computer systems: Report of defence science board task force on computer security. Technical report, Office of the Director of Defence Research And Engineering, Washington D.C. 20301, February 1970.