

# Contents

<b>1</b>	<b>example1 Theory</b>	<b>3</b>
1.1	Datatypes . . . . .	3
1.2	Theorems . . . . .	3
<b>2</b>	<b>solutions1 Theory</b>	<b>4</b>
2.1	Theorems . . . . .	4
<b>3</b>	<b>conops0Solution Theory</b>	<b>5</b>
3.1	Datatypes . . . . .	5
3.2	Theorems . . . . .	6



# 1 example1 Theory

**Built:** 19 March 2019

**Parent Theories:** acIDrules

## 1.1 Datatypes

*commands* = go | nogo | launch | abort

*staff* = Alice | Bob | Carol | Dan

## 1.2 Theorems

[example1Theorem]

$\vdash (M, Oi, Os) \text{ sat Name Alice says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Alice controls prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop go}$

[example1TheoremA]

$\vdash (M, Oi, Os) \text{ sat Name Alice says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Alice controls prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop go}$

[example1TheoremB]

$\vdash (M, Oi, Os) \text{ sat Name Alice says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Alice controls prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop go}$

[example2Theorem]

$\vdash (M, Oi, Os) \text{ sat Name Alice says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Alice speaks_for Name Bob} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Bob controls prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop go}$

[example2TheoremA]

$\vdash (M, Oi, Os) \text{ sat Name Alice says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Alice speaks_for Name Bob} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Bob controls prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop go}$

[example2TheoremB]

$\vdash (M, Oi, Os) \text{ sat Name Alice says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Alice speaks\_for Name Bob} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Bob controls prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop go}$

[example3Theorem]

$\vdash (M, Oi, Os) \text{ sat prop go impf prop launch} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Carol says prop launch}$

[example3TheoremA]

$\vdash (M, Oi, Os) \text{ sat prop go impf prop launch} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Carol says prop launch}$

[Mono\_Reps\_Theorem]

$\vdash (M, Oi, Os) \text{ sat } Q \text{ controls } f \Rightarrow$   
 $(M, Oi, Os) \text{ sat reps } P \ Q \ f \Rightarrow$   
 $(M, Oi, Os) \text{ sat } P' \text{ quoting } Q' \text{ says } f \Rightarrow$   
 $(M, Oi, Os) \text{ sat } P' \text{ speaks\_for } P \Rightarrow$   
 $(M, Oi, Os) \text{ sat } Q' \text{ speaks\_for } Q \Rightarrow$   
 $(M, Oi, Os) \text{ sat } f$

## 2 solutions1 Theory

**Built:** 19 March 2019

**Parent Theories:** example1

### 2.1 Theorems

[aclExercise1]

$\vdash (M, Oi, Os) \text{ sat Name Alice says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Bob says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Alice meet Name Bob says prop go}$

[aclExercise1A]

$\vdash (M, Oi, Os) \text{ sat Name Alice says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Bob says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Alice meet Name Bob says prop go}$

[aclExercise1B]

$\vdash (M, Oi, Os) \text{ sat Name Alice says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Bob says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Alice meet Name Bob says prop go}$

[aclExercise2]

$\vdash (M, Oi, Os) \text{ sat Name Alice says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Alice controls prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop go impf prop launch} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Bob says prop launch}$

[aclExercise2A]

$\vdash (M, Oi, Os) \text{ sat Name Alice says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Alice controls prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop go impf prop launch} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Bob says prop launch}$

[aclExercise2B]

$\vdash (M, Oi, Os) \text{ sat Name Alice says prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Alice controls prop go} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop go impf prop launch} \Rightarrow$   
 $(M, Oi, Os) \text{ sat Name Bob says prop launch}$

### 3 conops0Solution Theory

**Built:** 19 March 2019

**Parent Theories:** aclDrules

#### 3.1 Datatypes

*commands* = go | nogo | launch | abort | activate | stand\_down

*keyPrinc* = Staff people | Role roles | Ap num

*people* = Alice | Bob

*principals* = PR keyPrinc | Key keyPrinc

*roles* = Commander | Operator | CA

### 3.2 Theorems

#### [ApRuleActivate\_thm]

$\vdash (M, Oi, Os) \text{ sat}$   
 $\text{Name (PR (Role Operator)) controls prop launch} \Rightarrow$   
 $(M, Oi, Os) \text{ sat}$   
 $\text{reps (Name (PR (Staff Bob))) (Name (PR (Role Operator)))}$   
 $\quad (\text{prop launch}) \Rightarrow$   
 $(M, Oi, Os) \text{ sat}$   
 $\text{Name (Key (Staff Bob)) quoting Name (PR (Role Operator)) says}$   
 $\text{prop launch} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop launch impf prop activate} \Rightarrow$   
 $(M, Oi, Os) \text{ sat}$   
 $\text{Name (Key (Role CA)) speaks_for Name (PR (Role CA))} \Rightarrow$   
 $(M, Oi, Os) \text{ sat}$   
 $\text{Name (Key (Role CA)) says}$   
 $\text{Name (Key (Staff Bob)) speaks_for Name (PR (Staff Bob))} \Rightarrow$   
 $(M, Oi, Os) \text{ sat}$   
 $\text{Name (PR (Role CA)) controls}$   
 $\text{Name (Key (Staff Bob)) speaks_for Name (PR (Staff Bob))} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop activate}$

#### [ApRuleStandDown\_thm]

$\vdash (M, Oi, Os) \text{ sat Name (PR (Role Operator)) controls prop abort} \Rightarrow$   
 $(M, Oi, Os) \text{ sat}$   
 $\text{reps (Name (PR (Staff Bob))) (Name (PR (Role Operator)))}$   
 $\quad (\text{prop abort}) \Rightarrow$   
 $(M, Oi, Os) \text{ sat}$   
 $\text{Name (Key (Staff Bob)) quoting Name (PR (Role Operator)) says}$   
 $\text{prop abort} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop abort impf prop stand_down} \Rightarrow$   
 $(M, Oi, Os) \text{ sat}$   
 $\text{Name (Key (Role CA)) speaks_for Name (PR (Role CA))} \Rightarrow$   
 $(M, Oi, Os) \text{ sat}$   
 $\text{Name (Key (Role CA)) says}$   
 $\text{Name (Key (Staff Bob)) speaks_for Name (PR (Staff Bob))} \Rightarrow$   
 $(M, Oi, Os) \text{ sat}$   
 $\text{Name (PR (Role CA)) controls}$   
 $\text{Name (Key (Staff Bob)) speaks_for Name (PR (Staff Bob))} \Rightarrow$   
 $(M, Oi, Os) \text{ sat prop stand_down}$

#### [OpRuleAbort\_thm]

$\vdash (M, Oi, Os) \text{ sat Name (PR (Role Commander)) controls prop nogo} \Rightarrow$   
 $(M, Oi, Os) \text{ sat}$

```

reps (Name (PR (Staff Alice))) (Name (PR (Role Commander)))
  (prop nogo) ⇒
(M, Oi, Os) sat
Name (Key (Staff Alice)) quoting
Name (PR (Role Commander)) says prop nogo ⇒
(M, Oi, Os) sat prop nogo impf prop abort ⇒
(M, Oi, Os) sat
Name (Key (Role CA)) speaks_for Name (PR (Role CA)) ⇒
(M, Oi, Os) sat
Name (Key (Role CA)) says
Name (Key (Staff Alice)) speaks_for Name (PR (Staff Alice)) ⇒
(M, Oi, Os) sat
Name (PR (Role CA)) controls
Name (Key (Staff Alice)) speaks_for Name (PR (Staff Alice)) ⇒
(M, Oi, Os) sat
Name (Key (Staff Bob)) quoting Name (PR (Role Operator)) says
prop abort

```

[OpRuleLaunch\_thm]

```

⊢ (M, Oi, Os) sat Name (PR (Role Commander)) controls prop go ⇒
(M, Oi, Os) sat
reps (Name (PR (Staff Alice))) (Name (PR (Role Commander)))
  (prop go) ⇒
(M, Oi, Os) sat
Name (Key (Staff Alice)) quoting
Name (PR (Role Commander)) says prop go ⇒
(M, Oi, Os) sat prop go impf prop launch ⇒
(M, Oi, Os) sat
Name (Key (Role CA)) speaks_for Name (PR (Role CA)) ⇒
(M, Oi, Os) sat
Name (Key (Role CA)) says
Name (Key (Staff Alice)) speaks_for Name (PR (Staff Alice)) ⇒
(M, Oi, Os) sat
Name (PR (Role CA)) controls
Name (Key (Staff Alice)) speaks_for Name (PR (Staff Alice)) ⇒
(M, Oi, Os) sat
Name (Key (Staff Bob)) quoting Name (PR (Role Operator)) says
prop launch

```





## Index

### **conops0Solution Theory**, 5

- Datatypes, 5
- Theorems, 6
  - ApRuleActivate.thm, 6
  - ApRuleStandDown.thm, 6
  - OpRuleAbort.thm, 6
  - OpRuleLaunch.thm, 7

### **example1 Theory**, 3

- Datatypes, 3
- Theorems, 3
  - example1Theorem, 3
  - example1TheoremA, 3
  - example1TheoremB, 3
  - example2Theorem, 3
  - example2TheoremA, 3
  - example2TheoremB, 4
  - example3Theorem, 4
  - example3TheoremA, 4
  - Mono\_Reps\_Theorem, 4

### **solutions1 Theory**, 4

- Theorems, 4
  - aclExercise1, 4
  - aclExercise1A, 4
  - aclExercise1B, 5
  - aclExercise2, 5
  - aclExercise2A, 5
  - aclExercise2B, 5