Evaluating Human-human Communication Protocols with Miscommunication Generation and Model Checking

Matthew L. Bolton
Department of Mechanical and Industrial Engineering
College of Engineering

Ellen J. Bass
The iSchool, College of Information Science and Technology
College of Nursing and Health Professions

Supported by NASA Ames Research Center award NextGenAA: Integrated model checking and simulation of NextGen authority and autonomy.

Voice Communications in Air Traffic Control

Primary means of communicating clearances to pilots

Voice Communications in Air Traffic Control

Primary means of communicating clearances to pilots

Readbacks are used to ensure information is properly communicated

Voice Communications in Air Traffic Control

Primary means of communicating clearances to pilots

DAL 123 Climb to FL 180

Readbacks are used to ensure information is properly communicated

Voice Communications in Air Traffic Control

Primary means of communicating clearances to pilots

DAL 123 Climb to FL 180

Readbacks are used to ensure information is properly communicated

Voice Communications in Air Traffic Control

Primary means of communicating clearances to pilots

Readbacks are used to ensure information is properly communicated

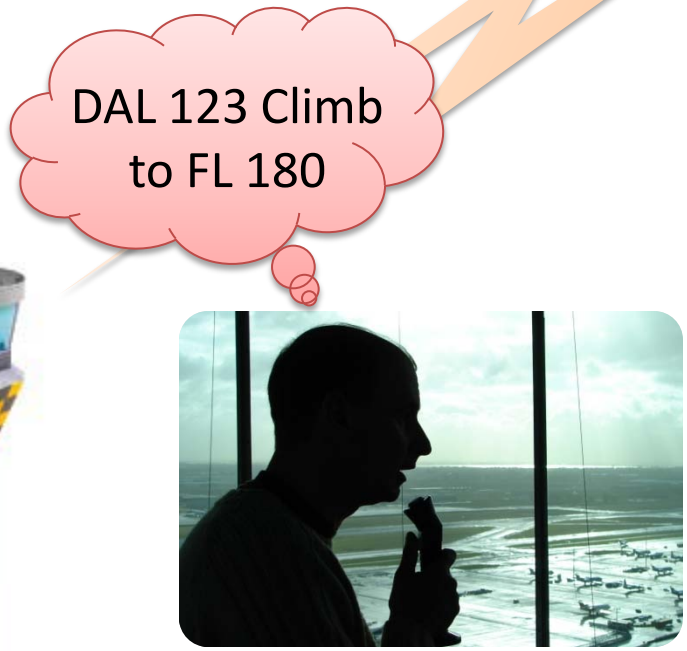
Voice Communications in Air Traffic Control

Primary means of communicating clearances to pilots

Readbacks are used to ensure information is properly communicated

Voice Communications in Air Traffic Control

Primary means of communicating clearances to pilots



Readbacks are used to ensure information is properly communicated

Voice Communications in Air Traffic Control

Primary means of communicating clearances to pilots

Miscommunications can still occur …

Voice Communications in Air Traffic Control

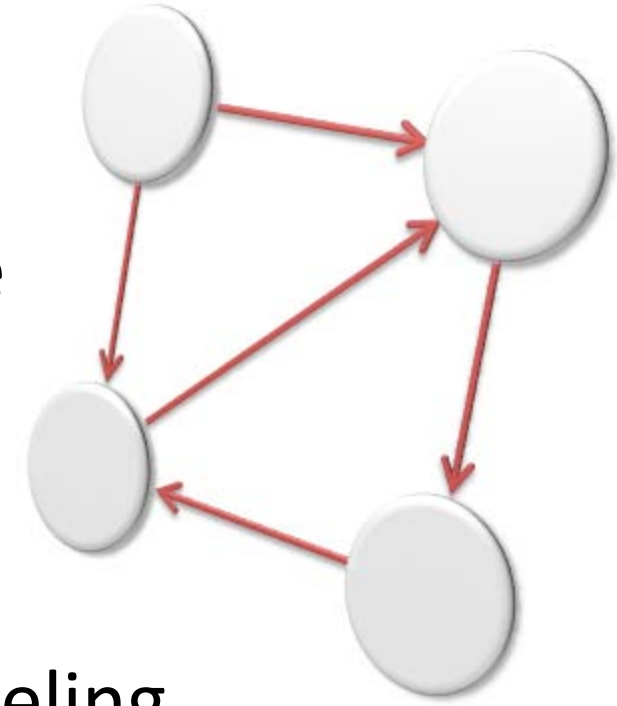
Primary means of communicating clearances to pilots

Miscommunications can still occur and result in accidents

Objective

Prove human-human communication protocols will always succeed with both **normative communications** and potentially unanticipated **miscommunications**

Formal Methods



- Tools and techniques capable of formally modeling and verifying communication protocols
- Available formalisms for modeling **machine** communication:
  - State Charts – Petri Nets – CSP ...

Human-human communication is different…

- It can manifest in many different ways:
  - Verbal statements
  - Gestures
  - Inarticulate noises
  - Body language

  …
- Communications can:
  - Occur in parallel
  - Have “crosstalk”
  - Be interrupted

  …

Human-human communication is different…

- Communication is an action
- Communications occur as part of a larger set of goal-directed behaviors
- Human factors engineers use **task analytic models** to represent such behavior

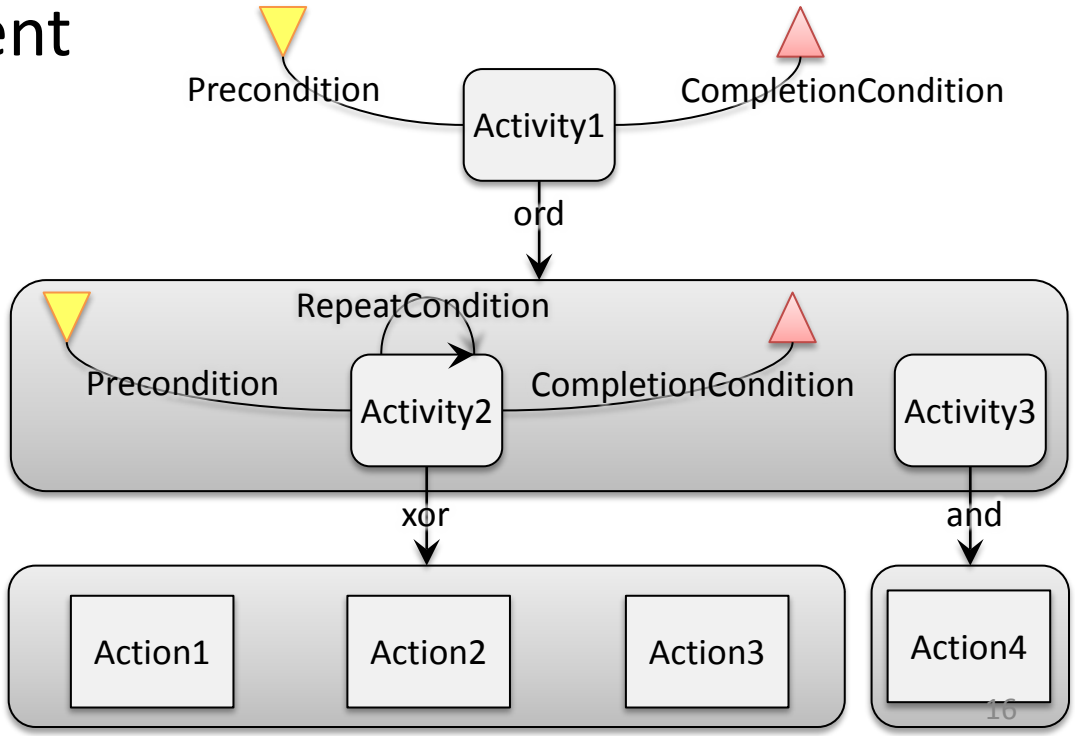
Human Task Analytic Behavior Models

- Product of a cognitive task analysis
- Hierarchy (network) of goal directed activities and actions
- Strategic knowledge controls when activities execute and complete
- Modifiers control relationships between activities and actions

Enhanced **O**perator **F**unction **M**odel (EOFM)

A generic task analytic modeling formalism

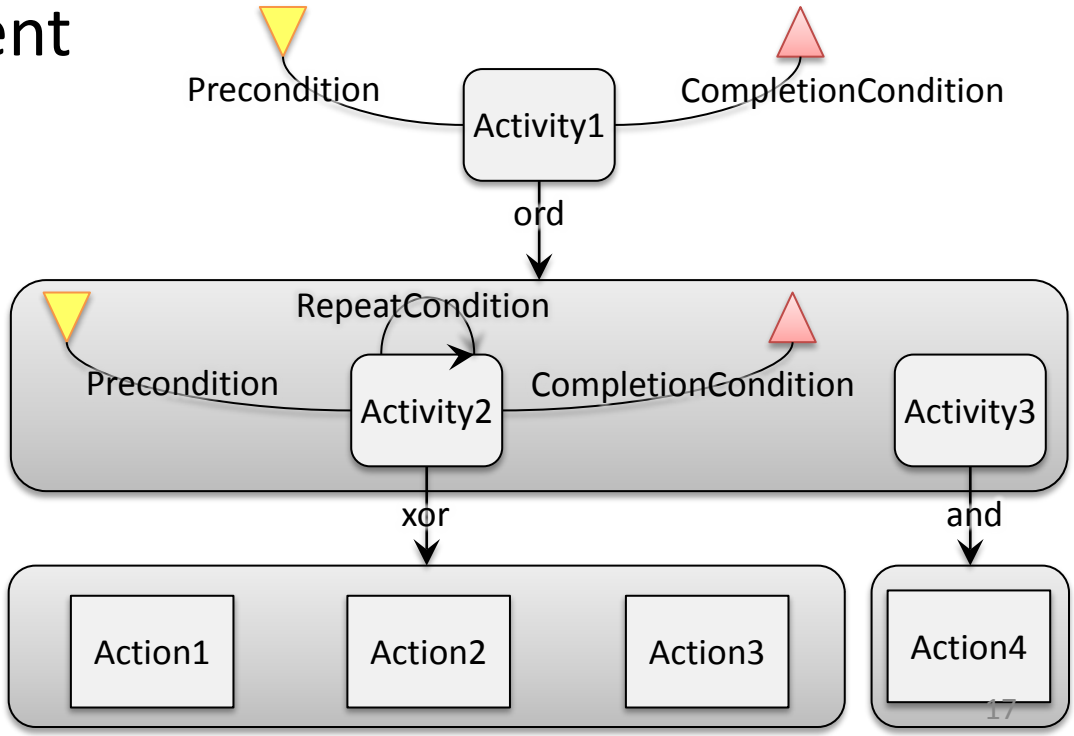
- Formal semantics (and EOFM to SAL translator)
- Input output model
- Platform-independent
- XML notation
- Visual notation



Enhanced **O**perator **F**unction **M**odel (EOFM)

A generic task analytic modeling formalism

- Formal semantics (and EOFM to SAL translator)
- Input output model
- Platform-independent
- XML notation
- Visual notation

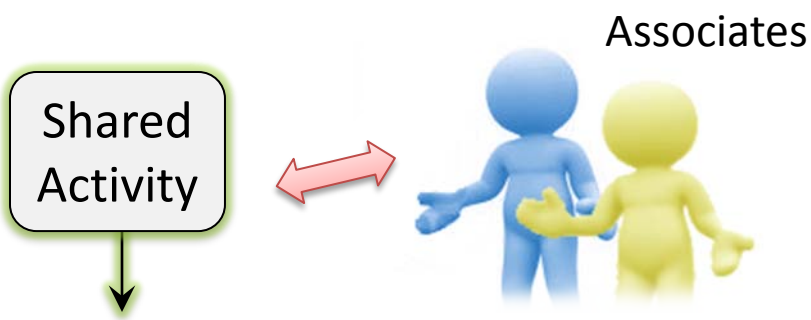


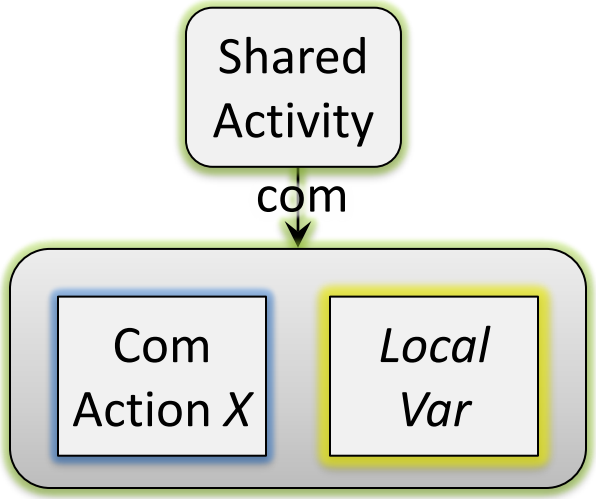
- **Poor support for coordination and communication**

EOFM$\mathcal{C}$ – EOFM with Communications

Extends EOFM to support coordination and communication protocols between humans

Shared tasks / activities allow for human operator coordination

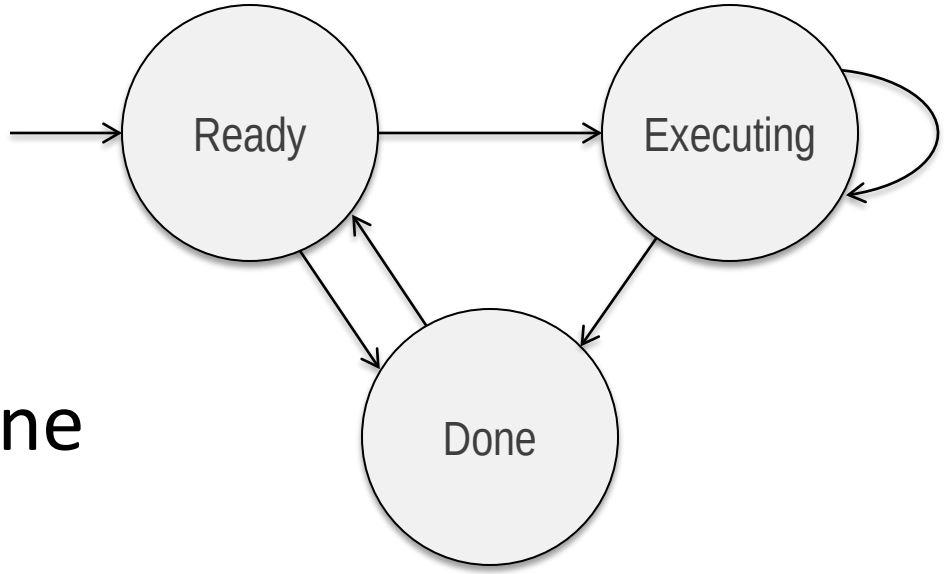




Communication actions allow for information transfer over a communication modality

EOFMC Formal Semantics

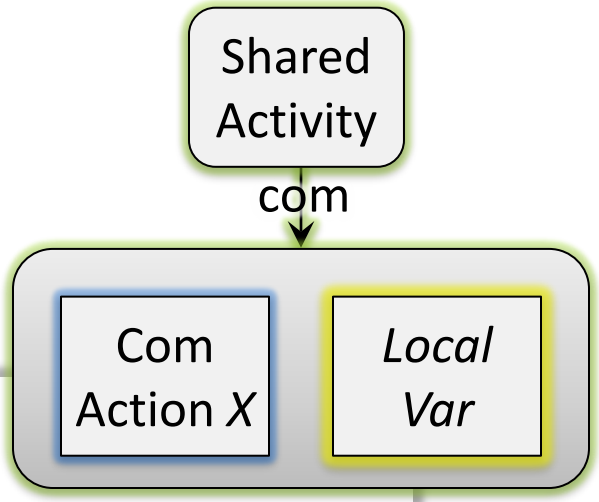
Each activity's and action's execution state is represented as a finite state machine



Parallel "composition" of individual and team (shared) behaviors

Formal Semantics

Communication actions transfer information from the communicator to a local variable of the recipient




```
[] Guard-->
   ComAction' = Done;
   ComActionValue' = X;
   LocalVar' = Done;
   LocalVarValue' = ComActionValue';
```

Miscommunications can manifest as …

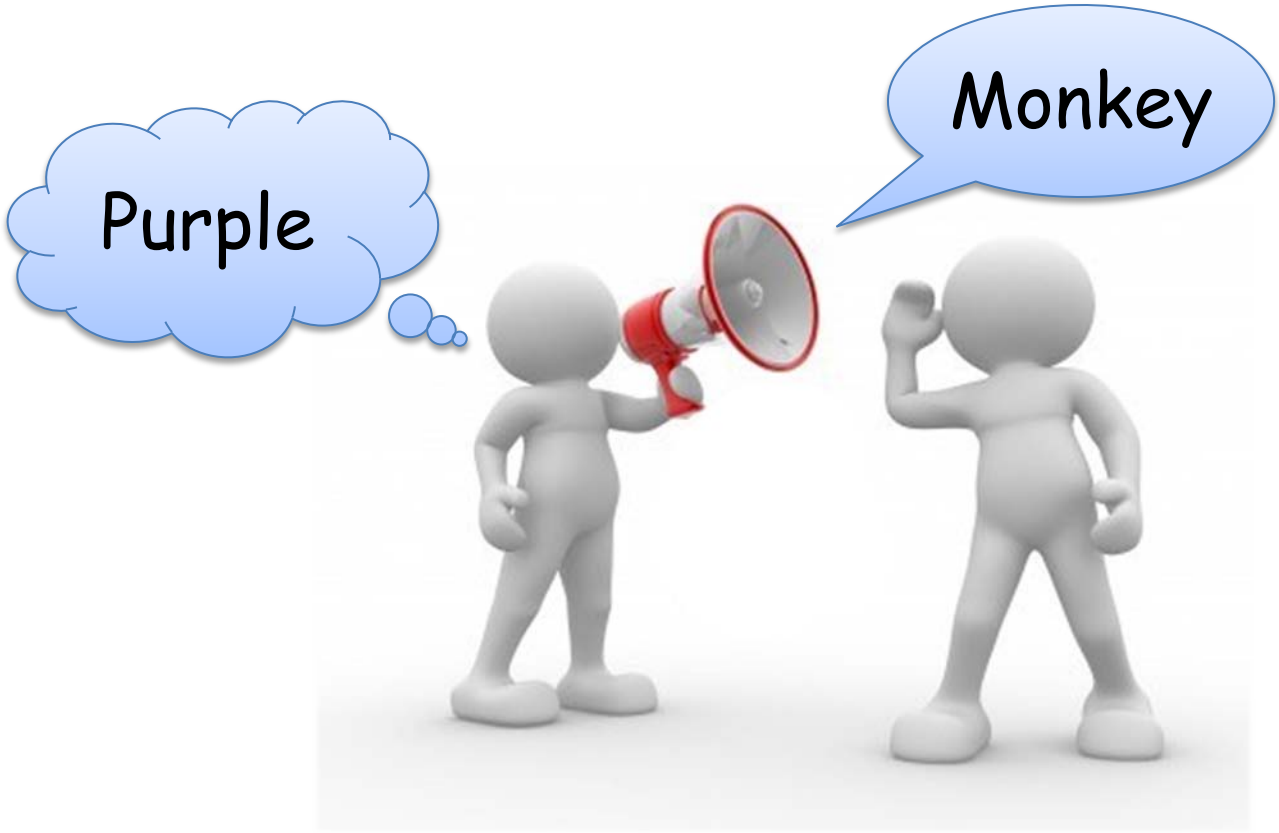
Action Failures:

The communicator conveys the wrong information

Miscommunications can manifest as …

Action Failures:

The communicator conveys the wrong information



Miscommunications can manifest as …

Action Failures:

The communicator conveys the wrong information

Miscommunications can manifest as …

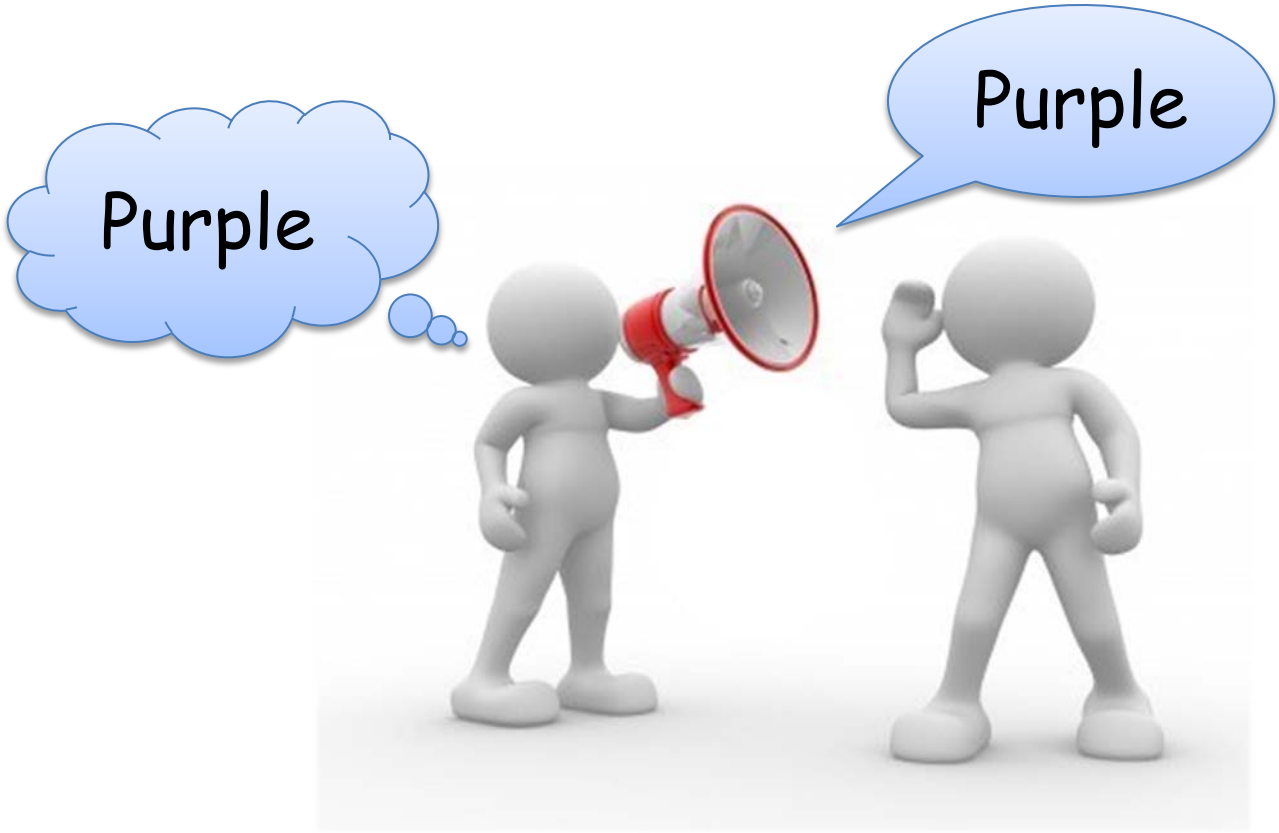
Misperceptions:

The recipient does not correctly receive the communicated information

Miscommunications can manifest as …

Misperceptions:

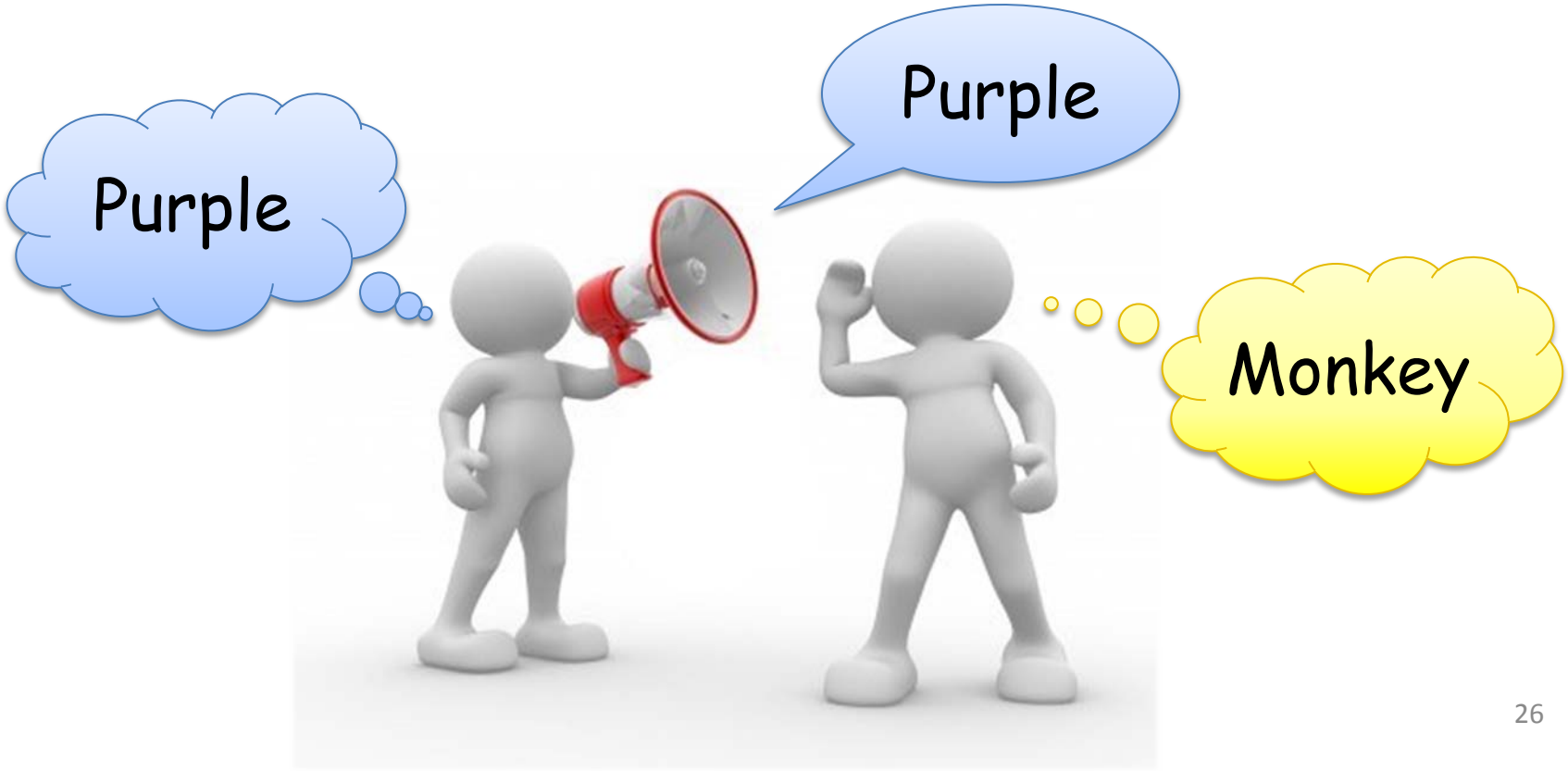
The recipient does not correctly receive the communicated information



Miscommunications can manifest as …

Misperceptions:

The recipient does not correctly receive the communicated information



Miscommunications can manifest as …

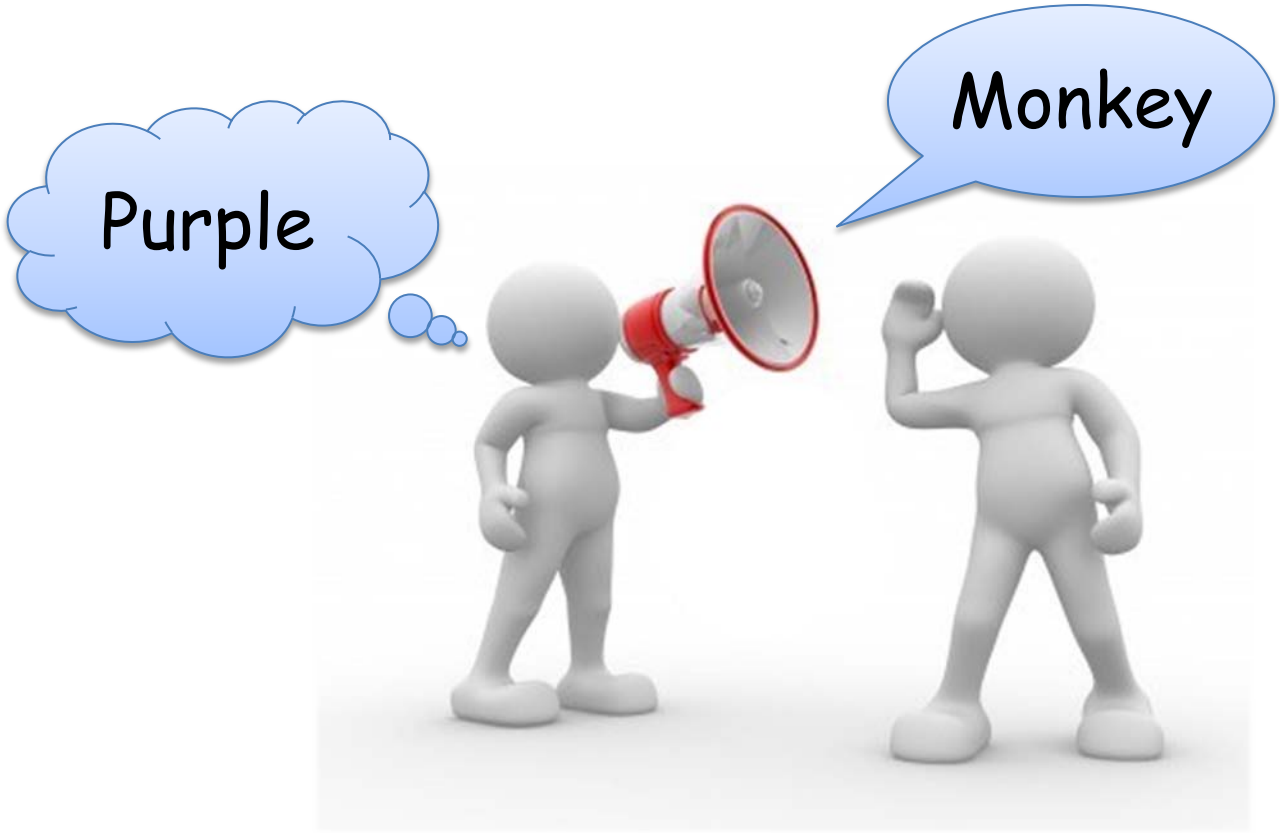
Action Failure and Misperception:

The communicator conveys the wrong information *and* the recipient does not correctly receive it

Miscommunications can manifest as …

Action Failure and Misperception:

The communicator conveys the wrong information *and* the recipient does not correctly receive it



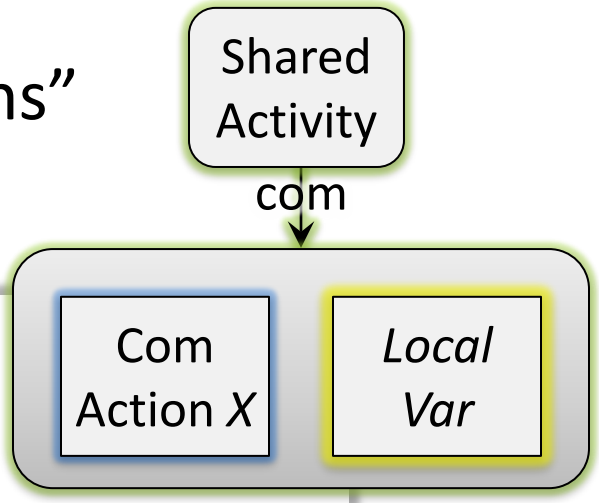
Miscommunications can manifest as …

Action Failure and Misperception:

The communicator conveys the wrong information *and* the recipient does not correctly receive it

Generating Miscommunications with EOFMC

Creating "miscommunication transitions" for every communication action

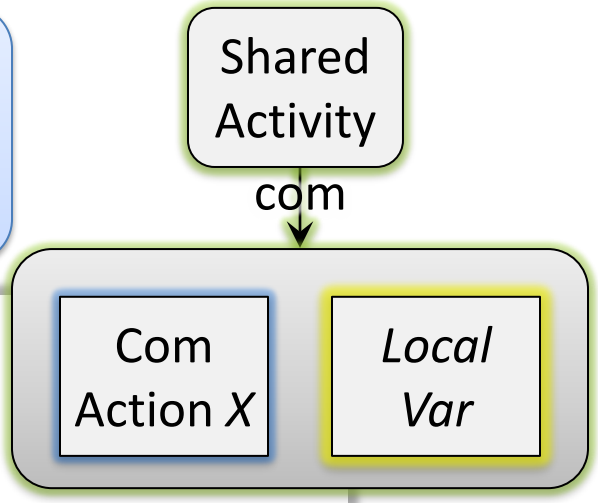



```
 ...
[] ... AND (Count < Max) -->
   ComAction' = Done;
   ComActionValue' IN {y: ComType | TRUE};
   LocalVar' = Done;
   LocalVarValue' IN {y: ComType | TRUE};
   Count' = IF ComActionValue' <> X
               OR LocalVarValue' <> X
            THEN Count + 1
            ELSE Count ENDIF;
```

SAL

Generating Miscommunications with EOFMC

Action Failure

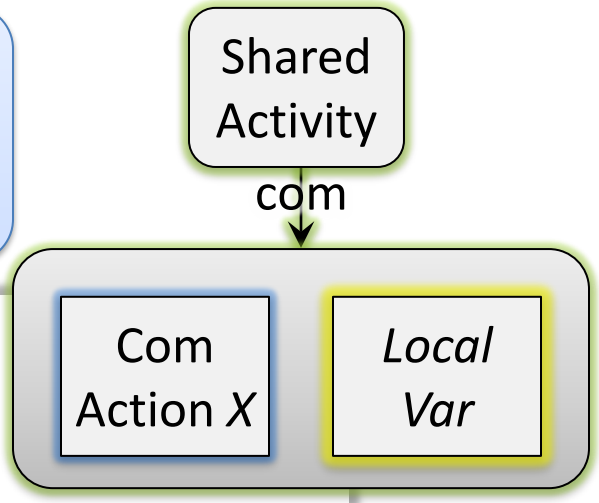



```
 ...
[] ... AND (Count < Max) -->
   ComAction' = Done;
   ComActionValue' IN {y: ComType | TRUE};
   LocalVar' = Done;
   LocalVarValue' IN {y: ComType | TRUE};
   Count' = IF ComActionValue' <> X
               OR LocalVarValue' <> X
            THEN Count + 1
            ELSE Count ENDIF;
```

SAL

Generating Miscommunications with EOFMC

Misperception

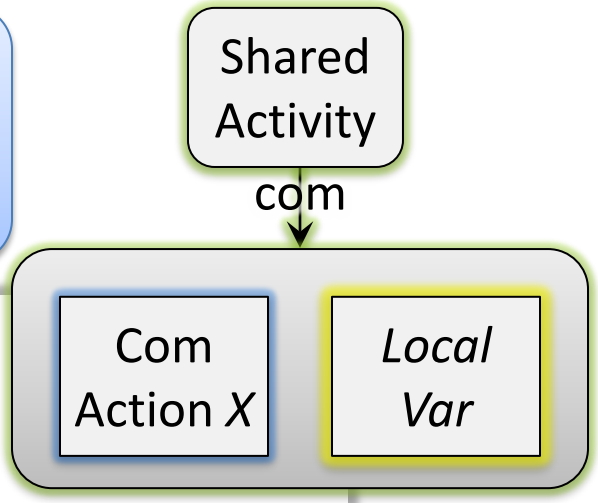



```
 ...
[] ... A   ount < Max) -->
   ComAct   = Done;
   ComActio Value' IN {y: ComType | TRUE};
   LocalVar' = Done;
   LocalVarValue' IN {y: ComType | TRUE};
   Count' = IF ComActionValue' <> X
               OR LocalVarValue' <> X
            THEN Count + 1
            ELSE Count ENDIF;
```

SAL

Generating Miscommunications with EOFMC

Count and **Max** limit the miscommunications




```
 ...
[] ... AND (Count < Max) -->
   ComAction' = Done;
   ComActionValue' IN {y: ComType | TRUE};
   LocalVar' = Done;
   LocalVarValue' IN {y: ComType | TRUE};
   Count' = IF ComActionValue' <> X
               OR LocalVarValue' <> X
            THEN Count + 1
            ELSE Count ENDIF;
```

SAL

Application: Heading Change from ATC

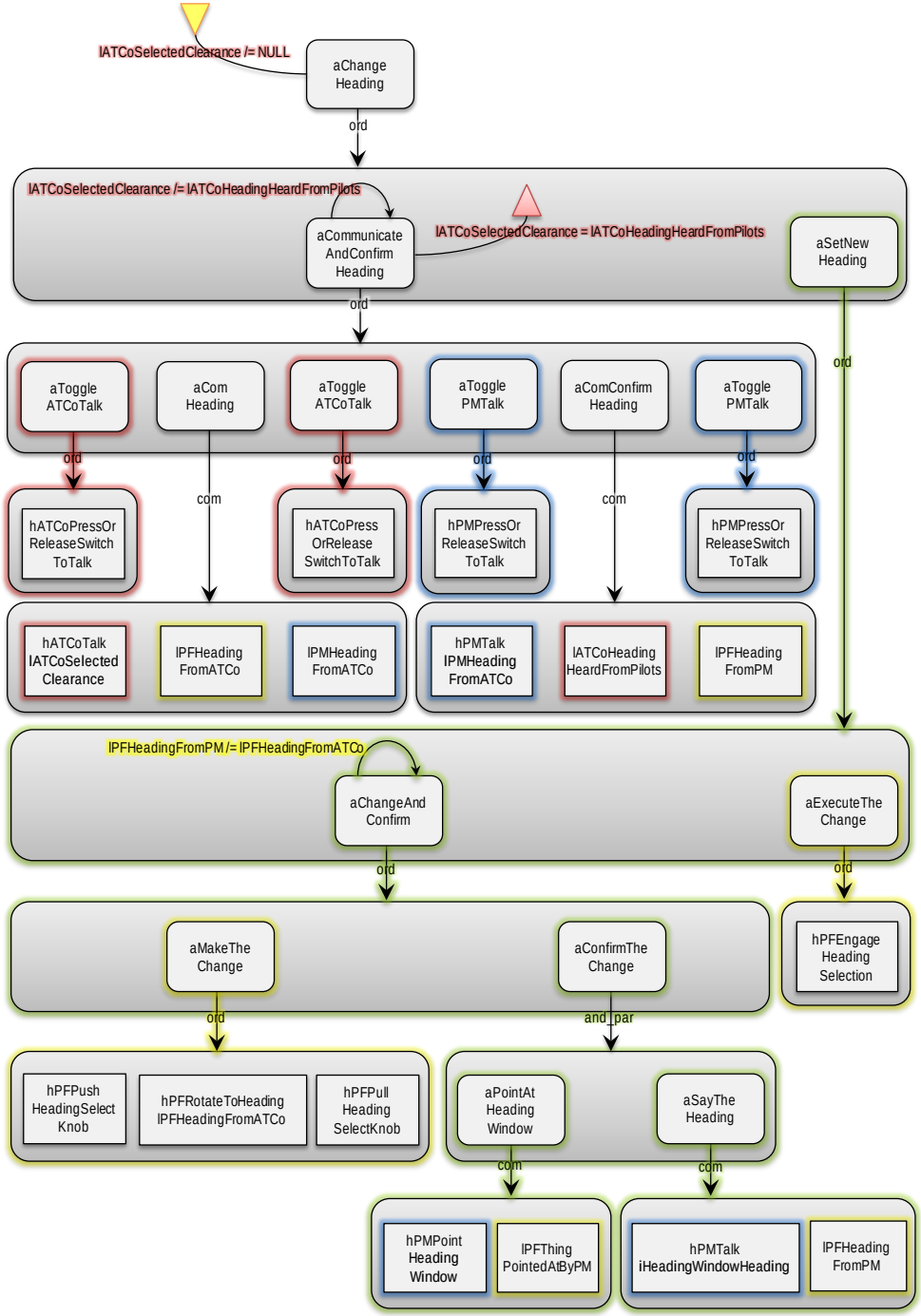
The air traffic controller initiates a heading change that the pilots must confirm and execute

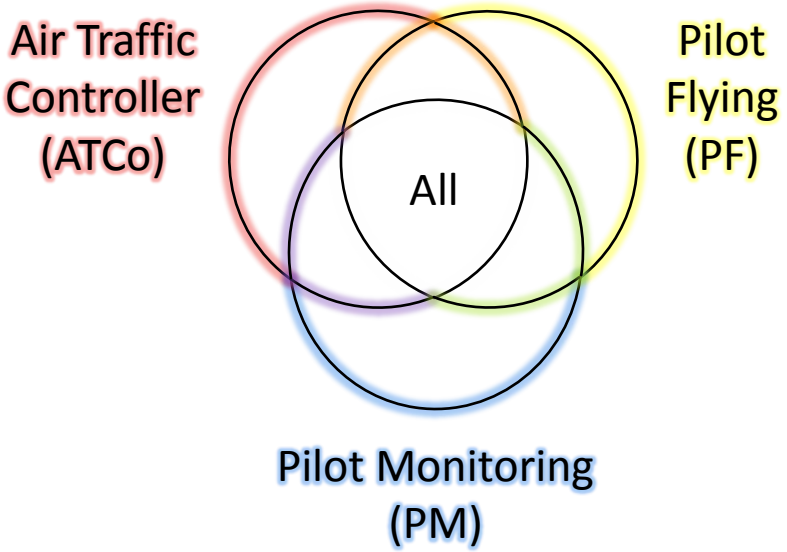
Pilot Flying

Pilot Monitoring

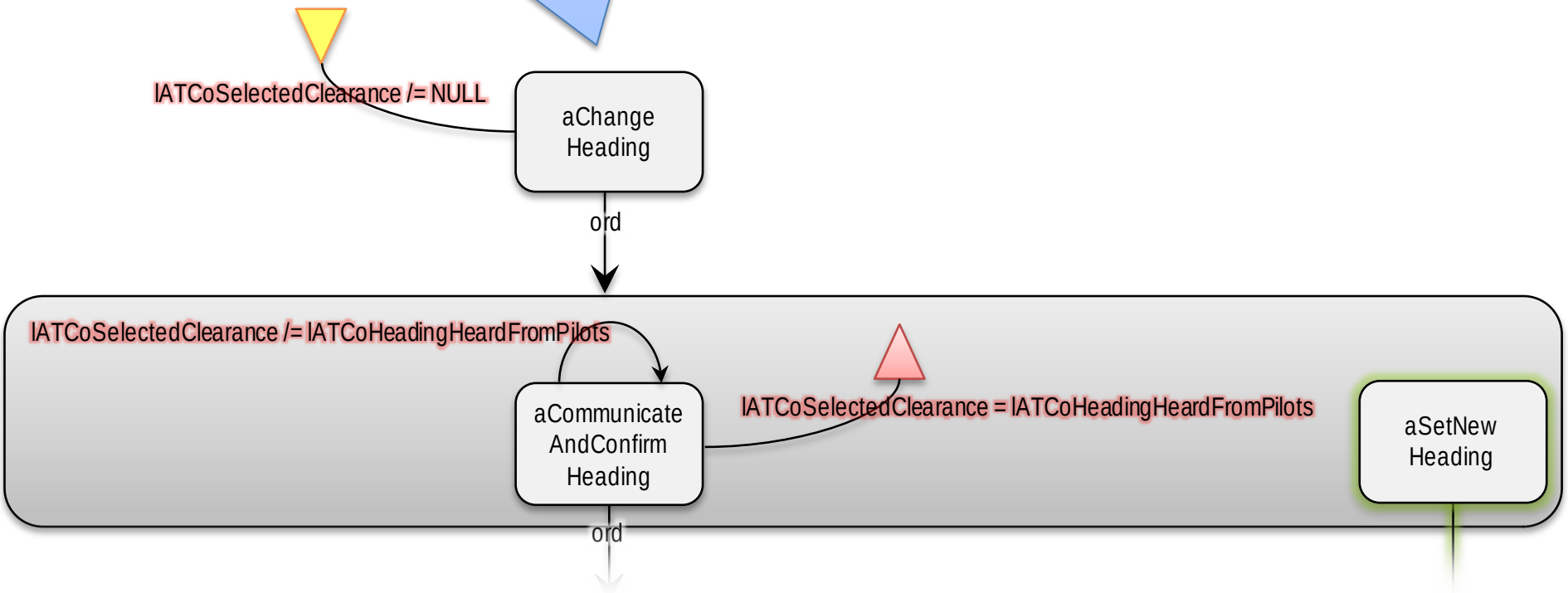
Air Traffic Controller

Communication Protocol

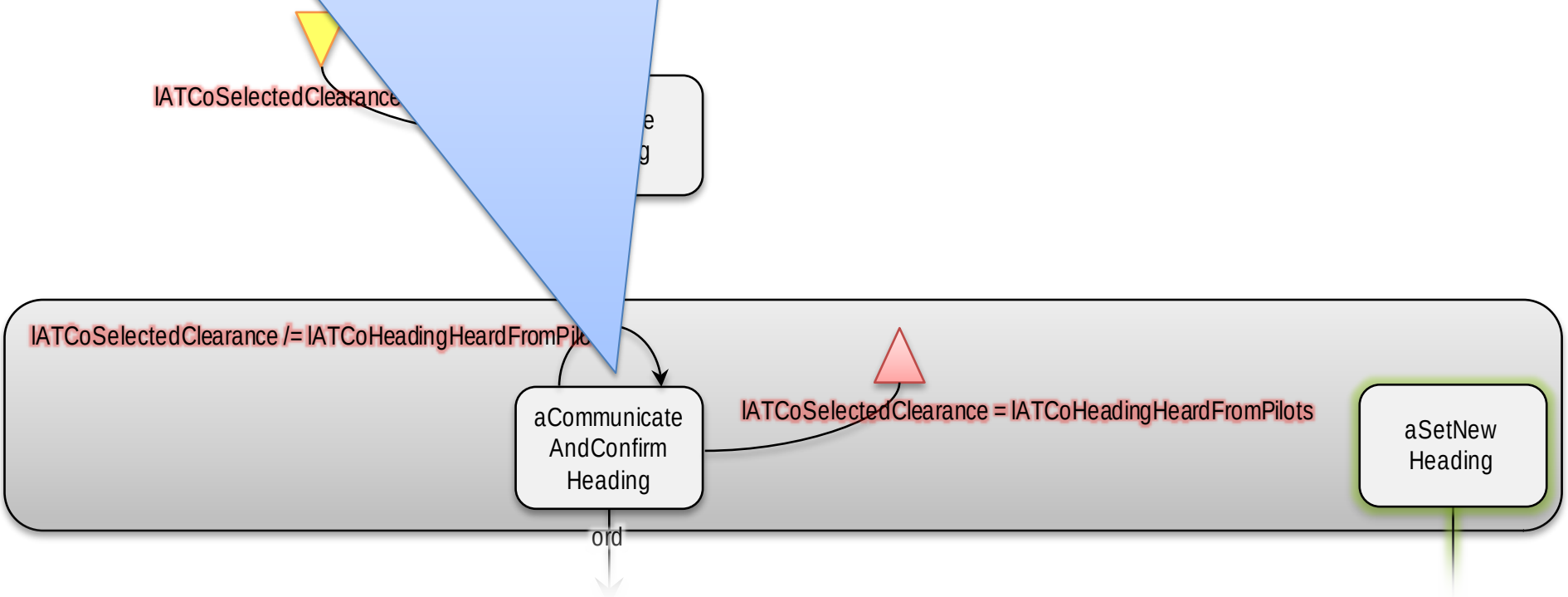




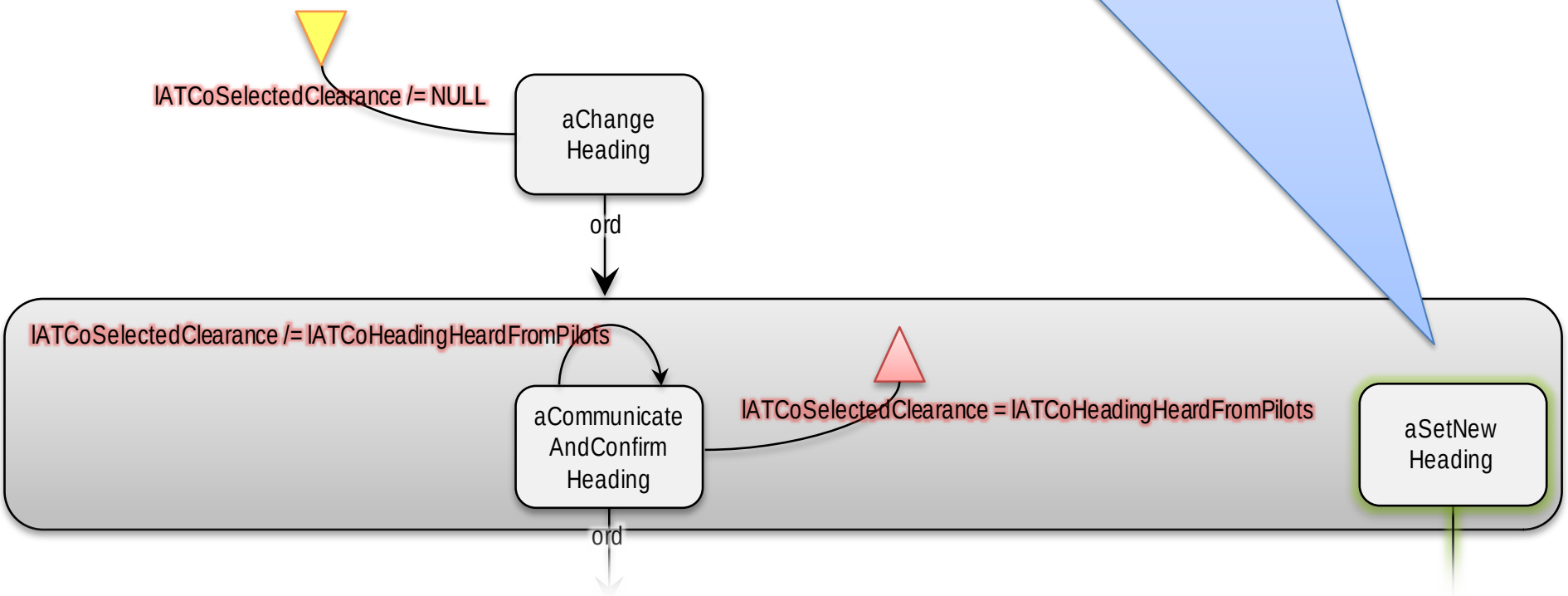
The ATCo initiates a heading change based on a new selected clearance

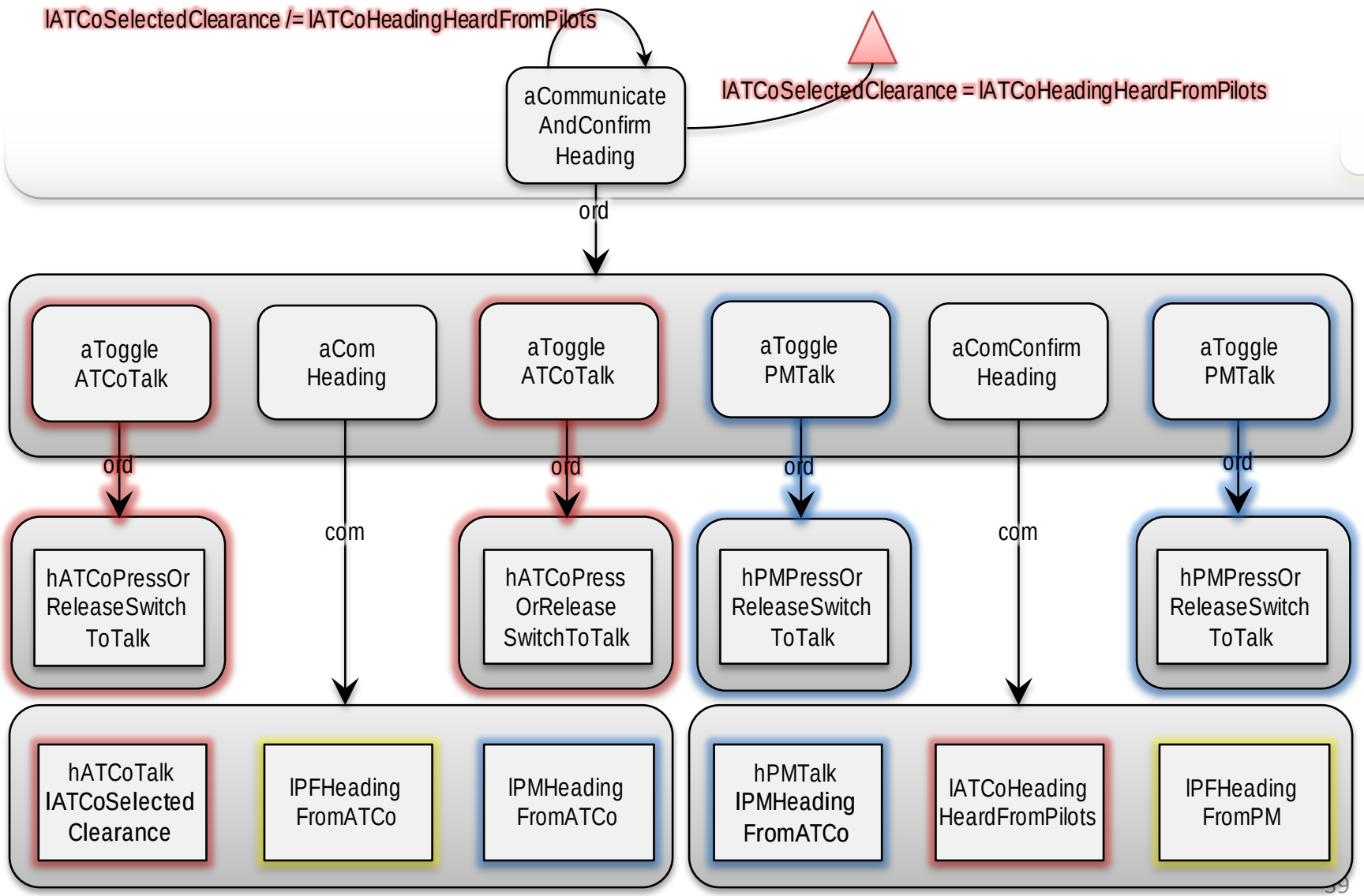


The new clearance is communicated to the pilots until the selected clearance matches what the ATCo hears read back by the pilots

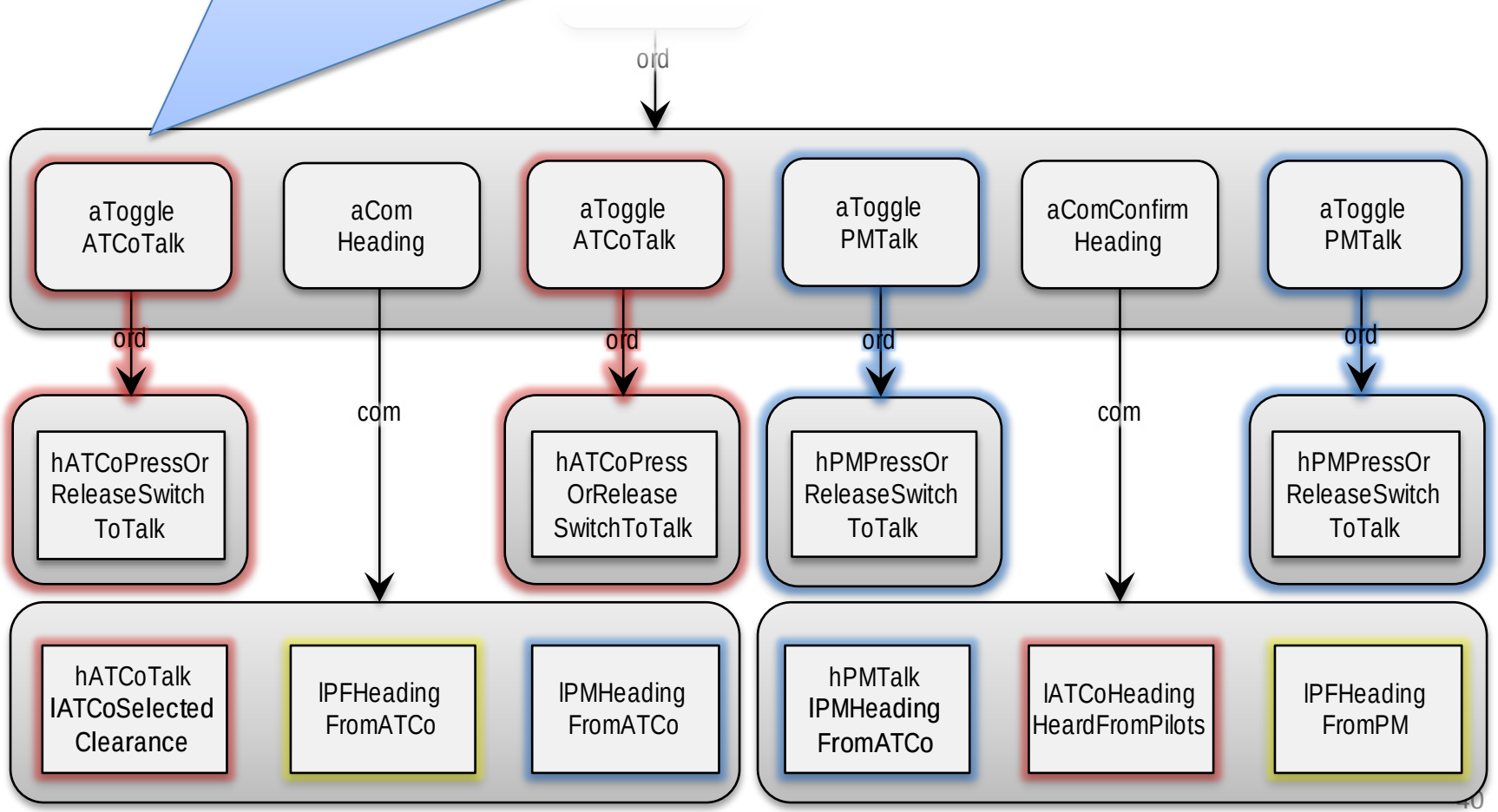


Then the new heading is set by the pilots

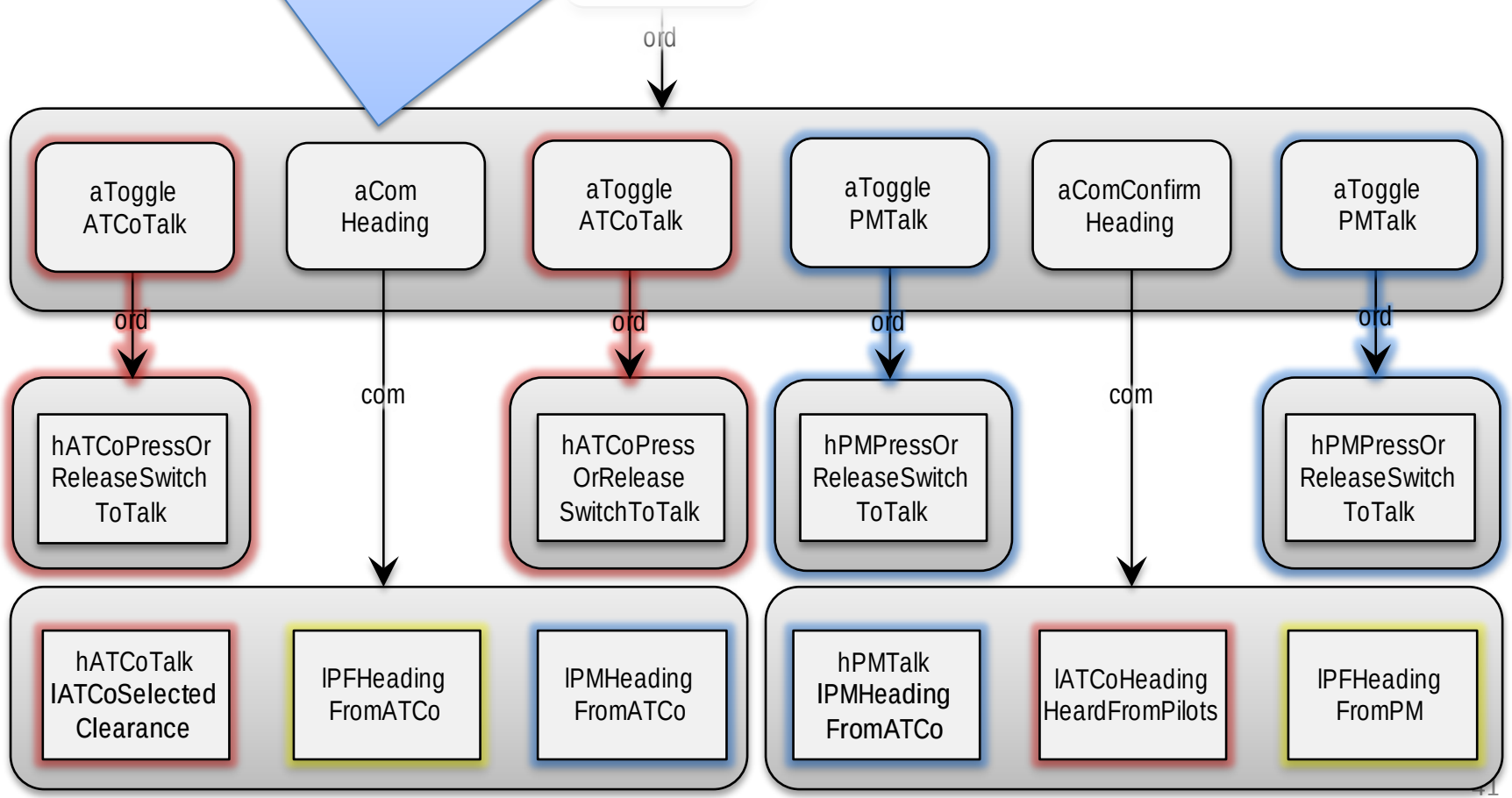



lATCoSelectedClearance /= lATCoHeadingHeardFromPilots
aCommunicate AndConfirm Heading
lATCoSelectedClearance = lATCoHeadingHeardFromPilots
ord
aToggle ATCoTalk
aCom Heading
aToggle ATCoTalk
aToggle PMTalk
aComConfirm Heading
aToggle PMTalk
ord
ord
ord
ord
hATCoPressOr ReleaseSwitch ToTalk
com
hATCoPress OrRelease SwitchToTalk
hPMPressOr ReleaseSwitch ToTalk
com
hPMPressOr ReleaseSwitch ToTalk
hATCoTalk lATCoSelected Clearance
lPFHeading FromATCo
lPMHeading FromATCo
hPMTalk lPMHeading FromATCo
lATCoHeading HeardFromPilots
lPFHeading FromPM

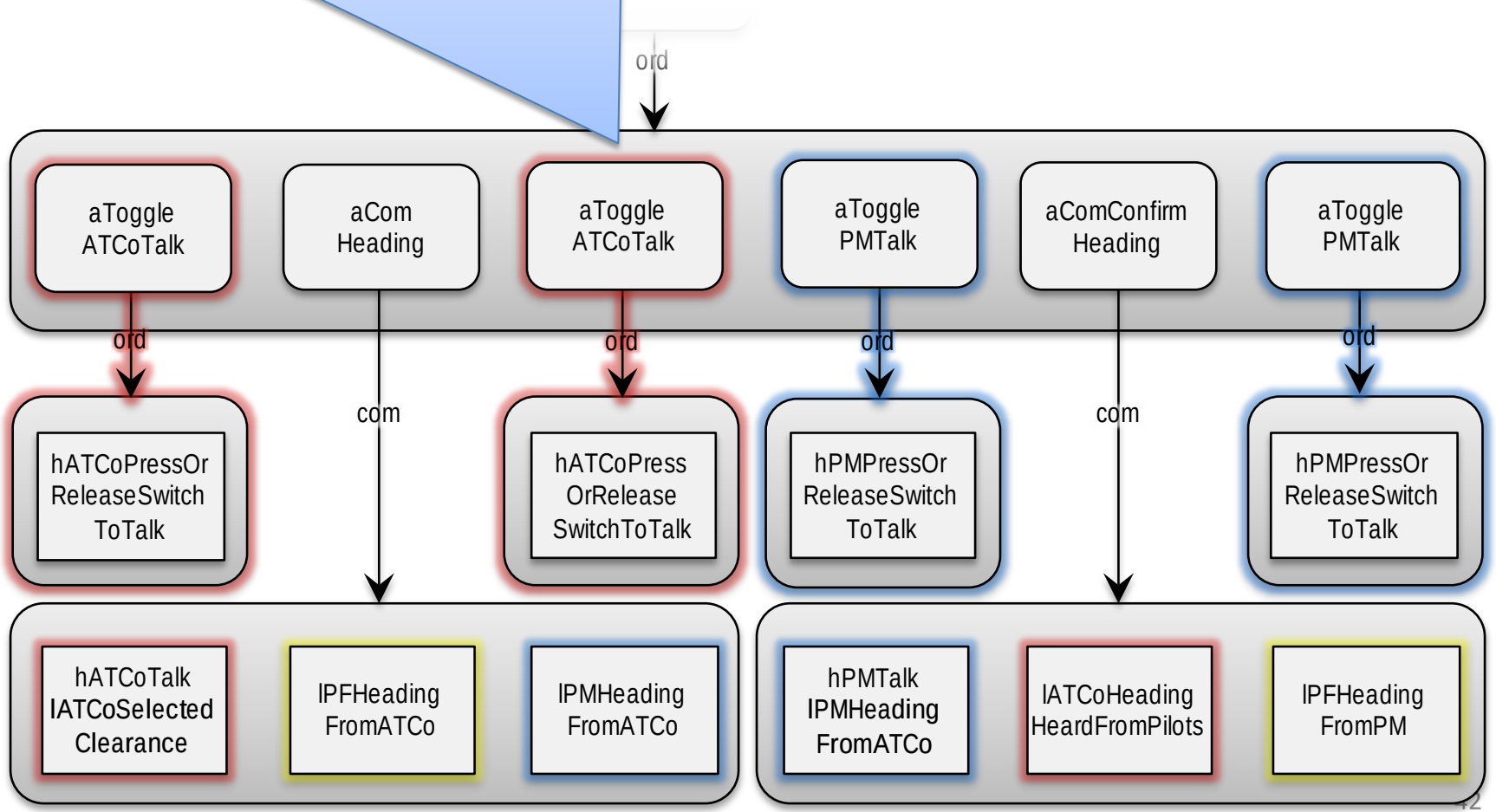
The ATCo presses the switch to talk



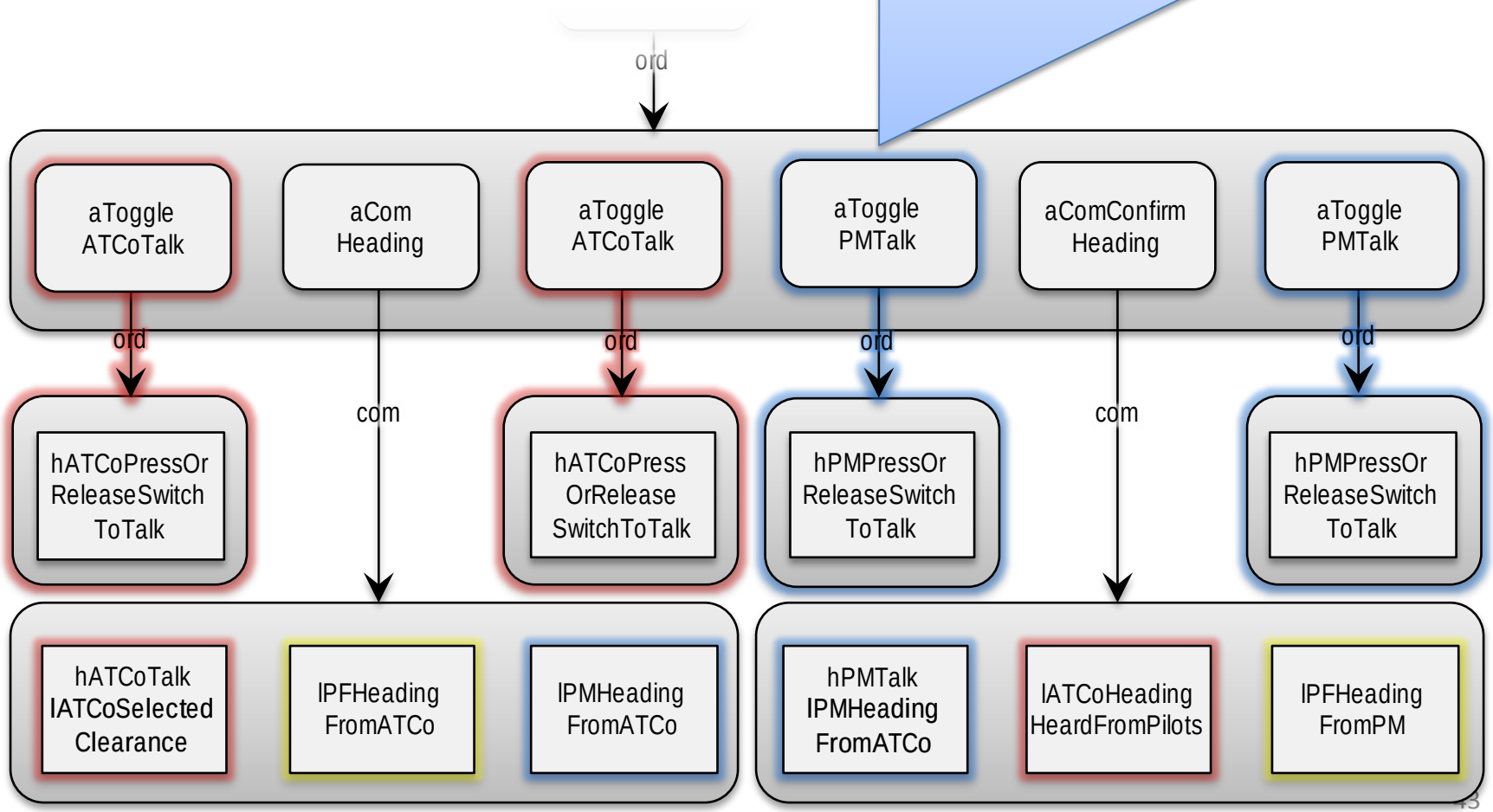
The ATCo verbally communicates the selected heading to the pilots



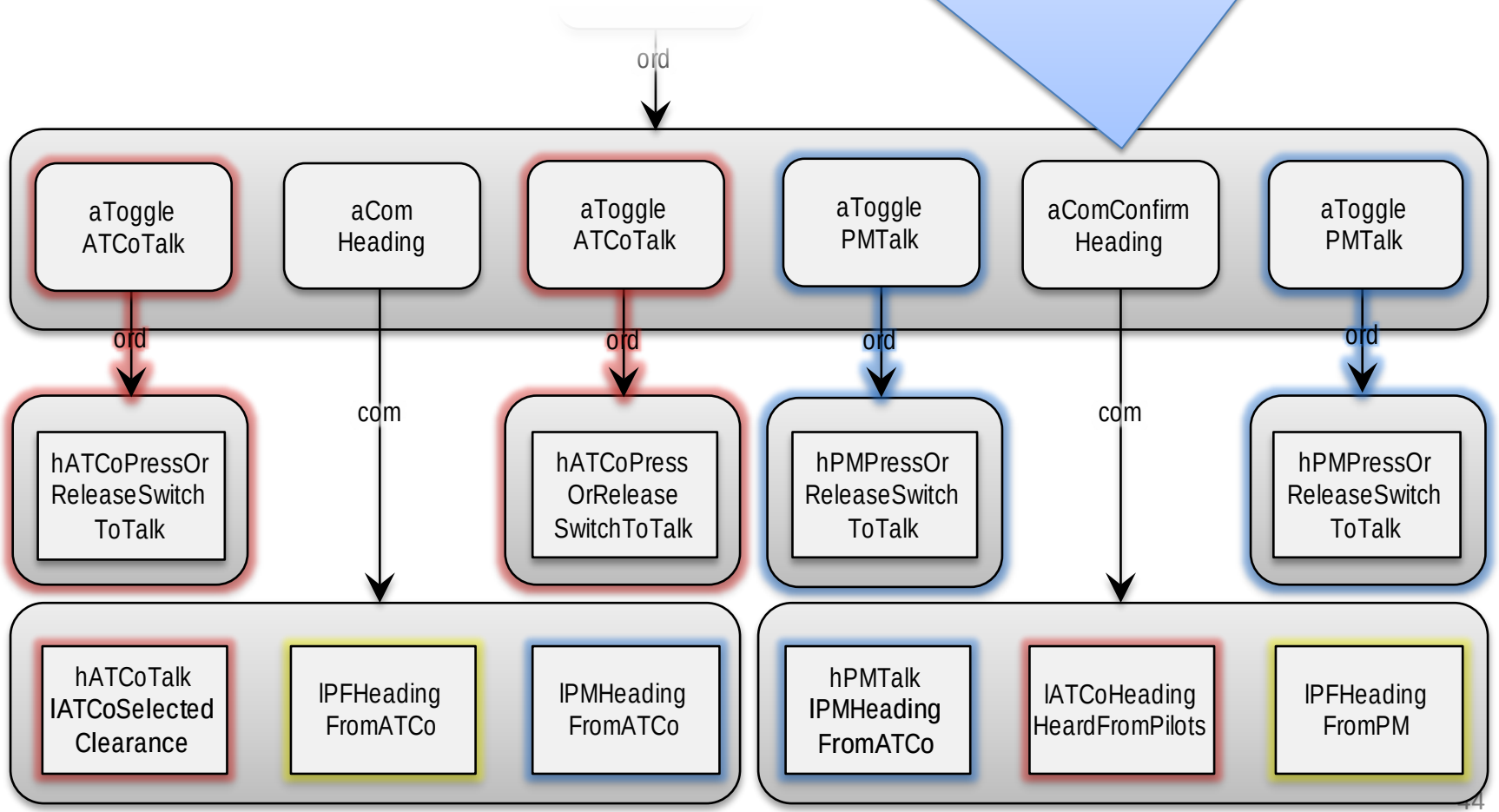
The ATCo releases the switch



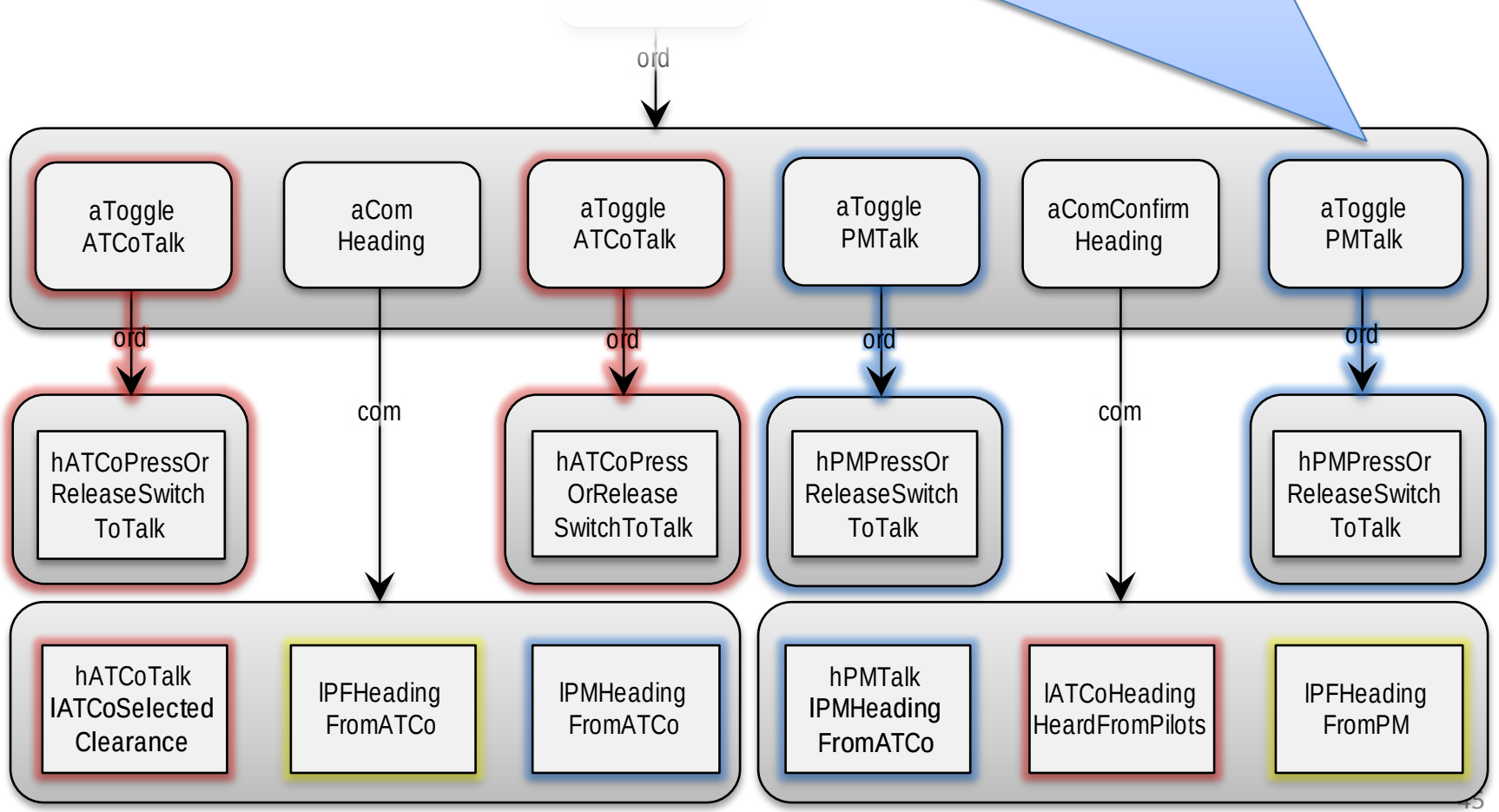
The PM presses the switch to talk

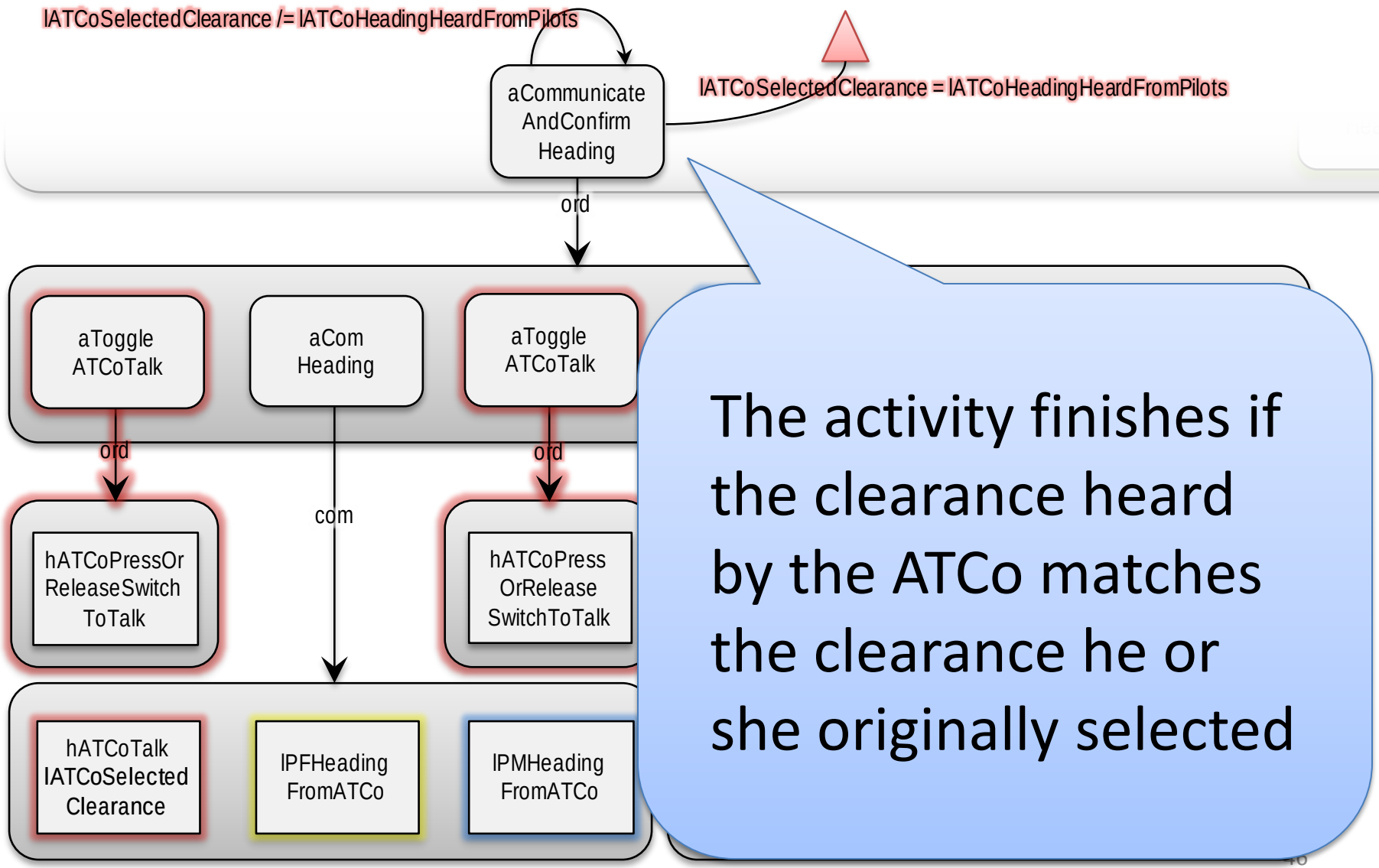


The PM communicates the heading he heard from ATC to the ATCo and the PF

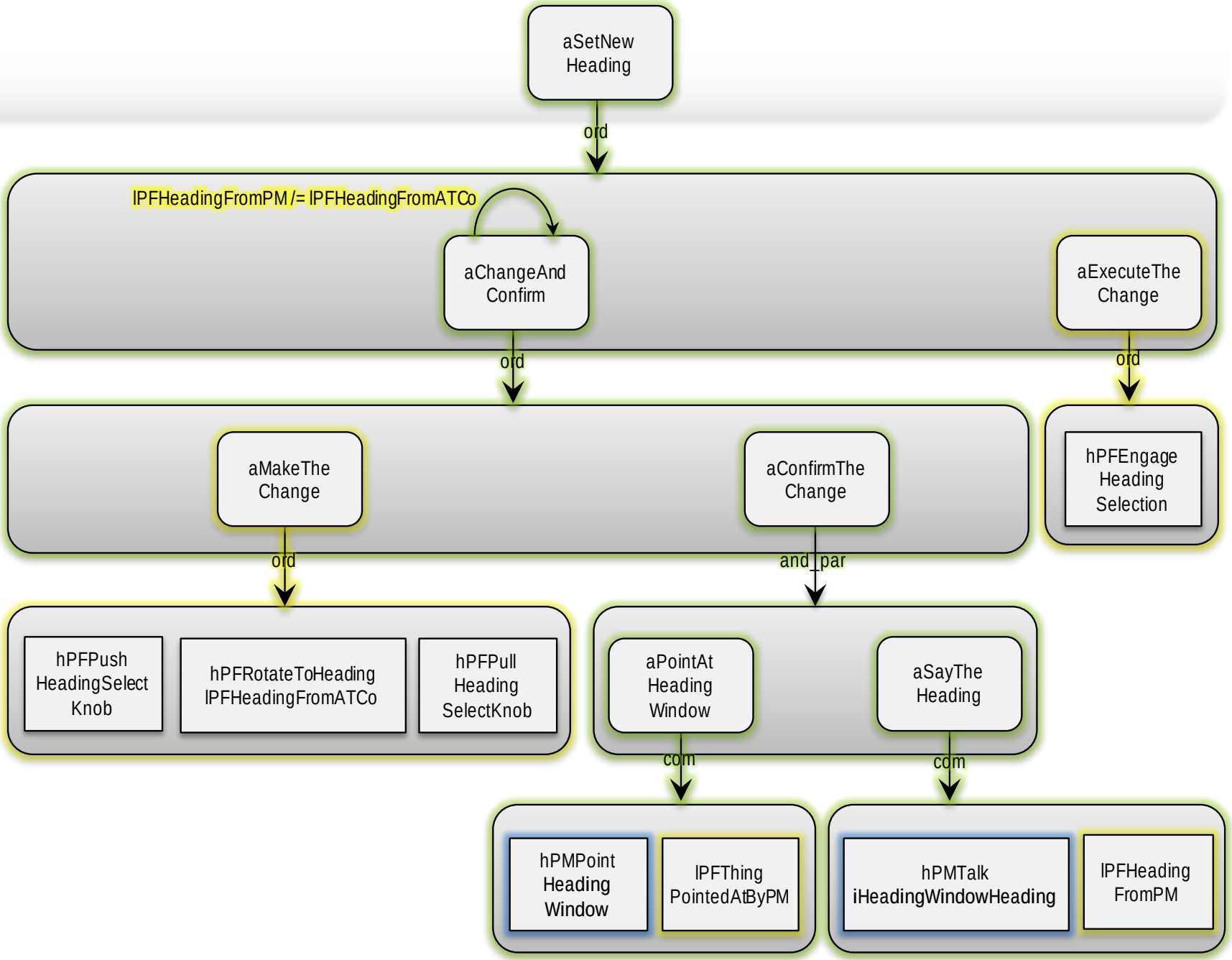


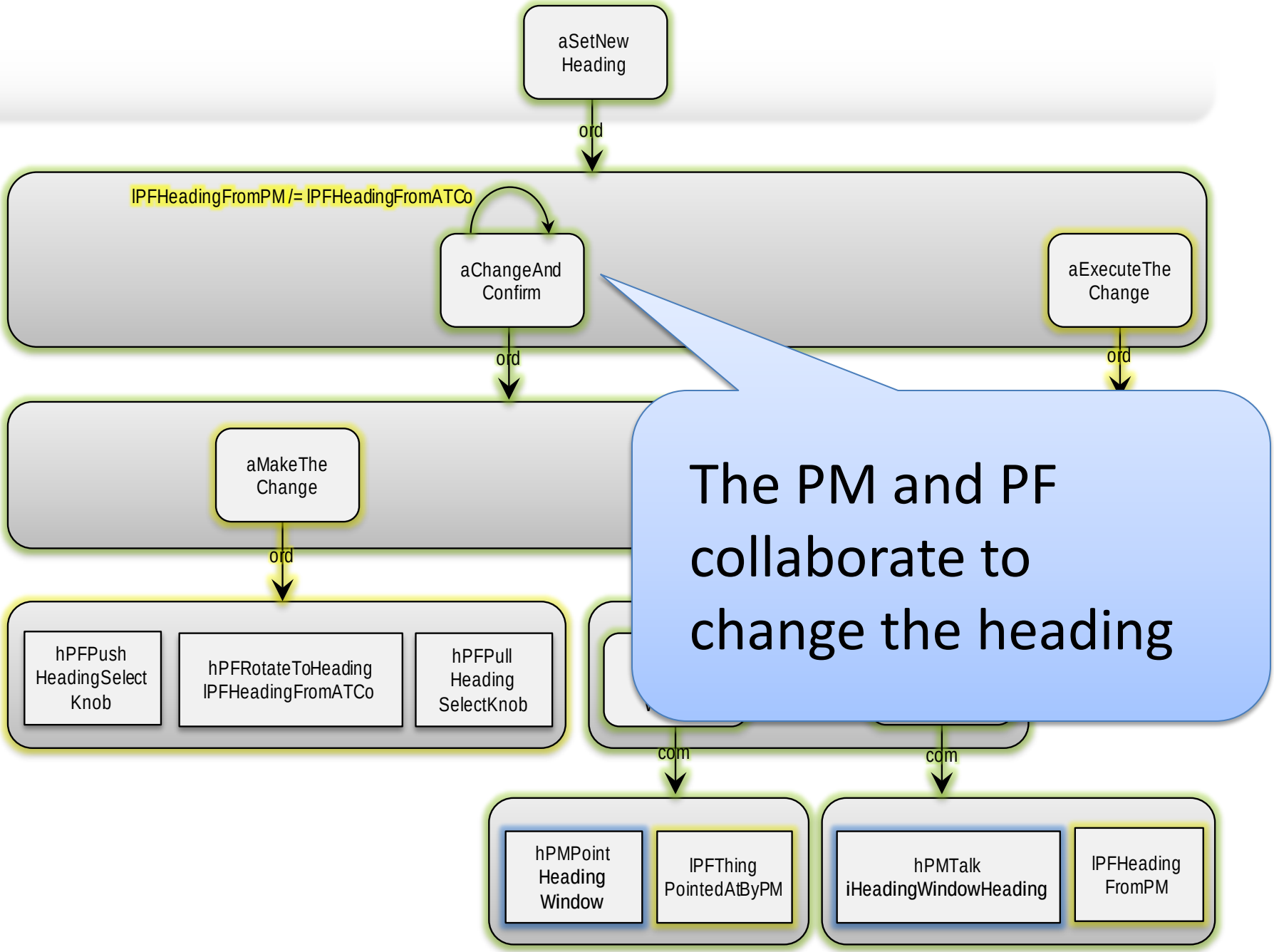
The PM releases the switch



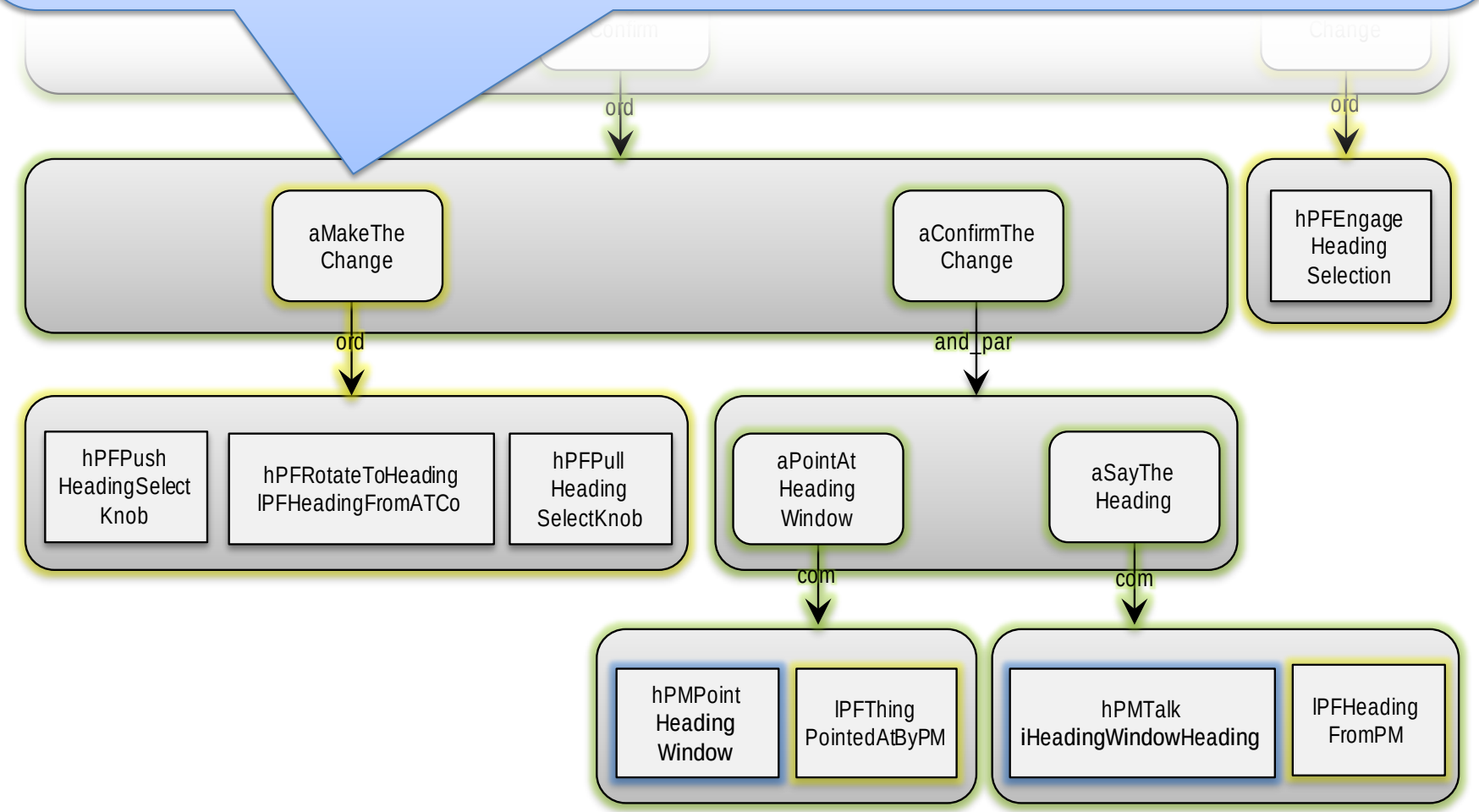


The activity finishes if the clearance heard by the ATCo matches the clearance he or she originally selected

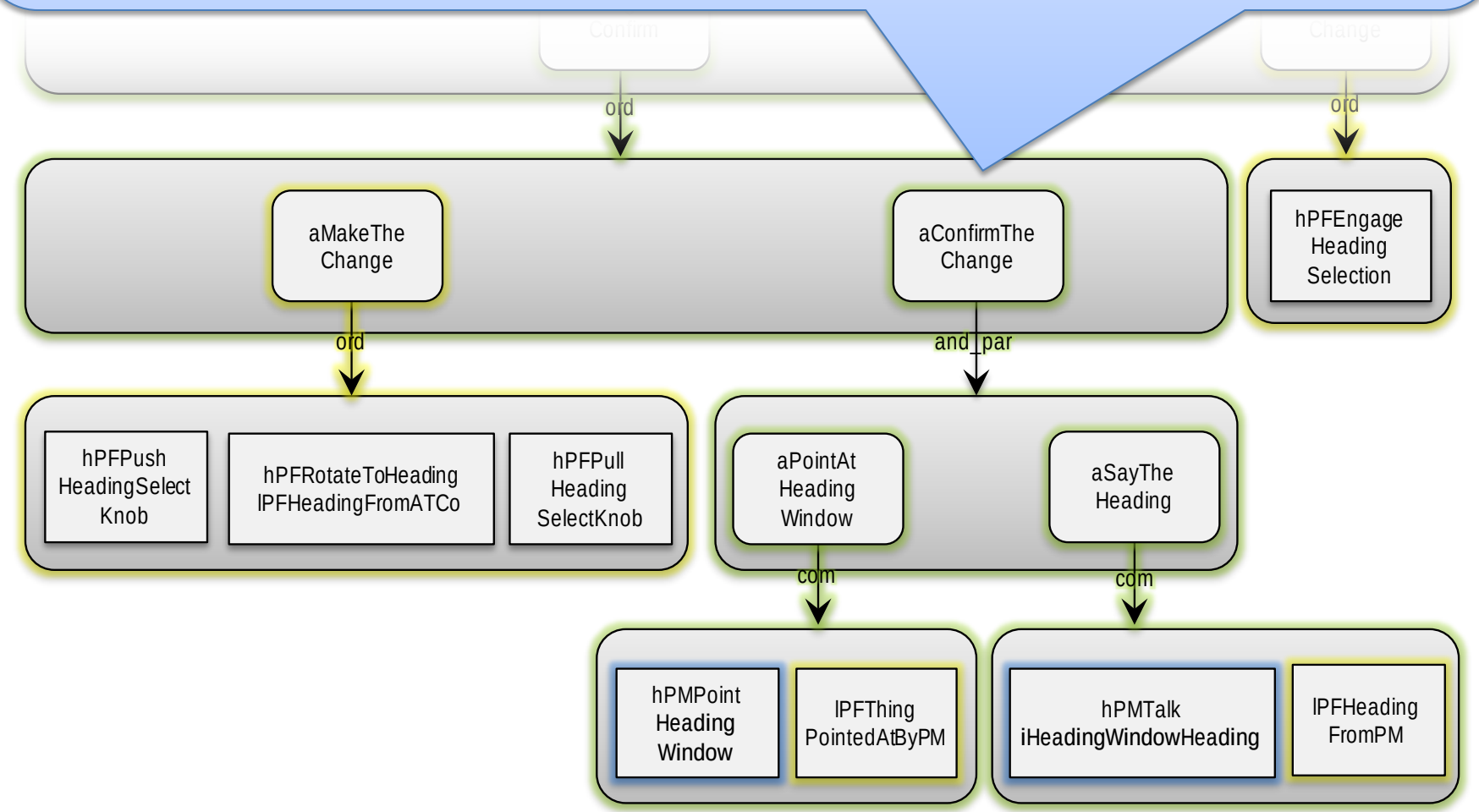

aSetNew Heading
ord
lPFHeadingFromPM /= lPFHeadingFromATCo
aChangeAnd Confirm
aExecuteThe Change
ord
ord
aMakeThe Change
aConfirmThe Change
hPFEngage Heading Selection
ord
and_par
hPFPush HeadingSelect Knob
hPFRotateToHeading lPFHeadingFromATCo
hPFPull Heading SelectKnob
aPointAt Heading Window
aSayThe Heading
com
com
hPMPoint Heading Window
lPFThing PointedAtByPM
hPMTalk iHeadingWindowHeading
lPFHeading FromPM

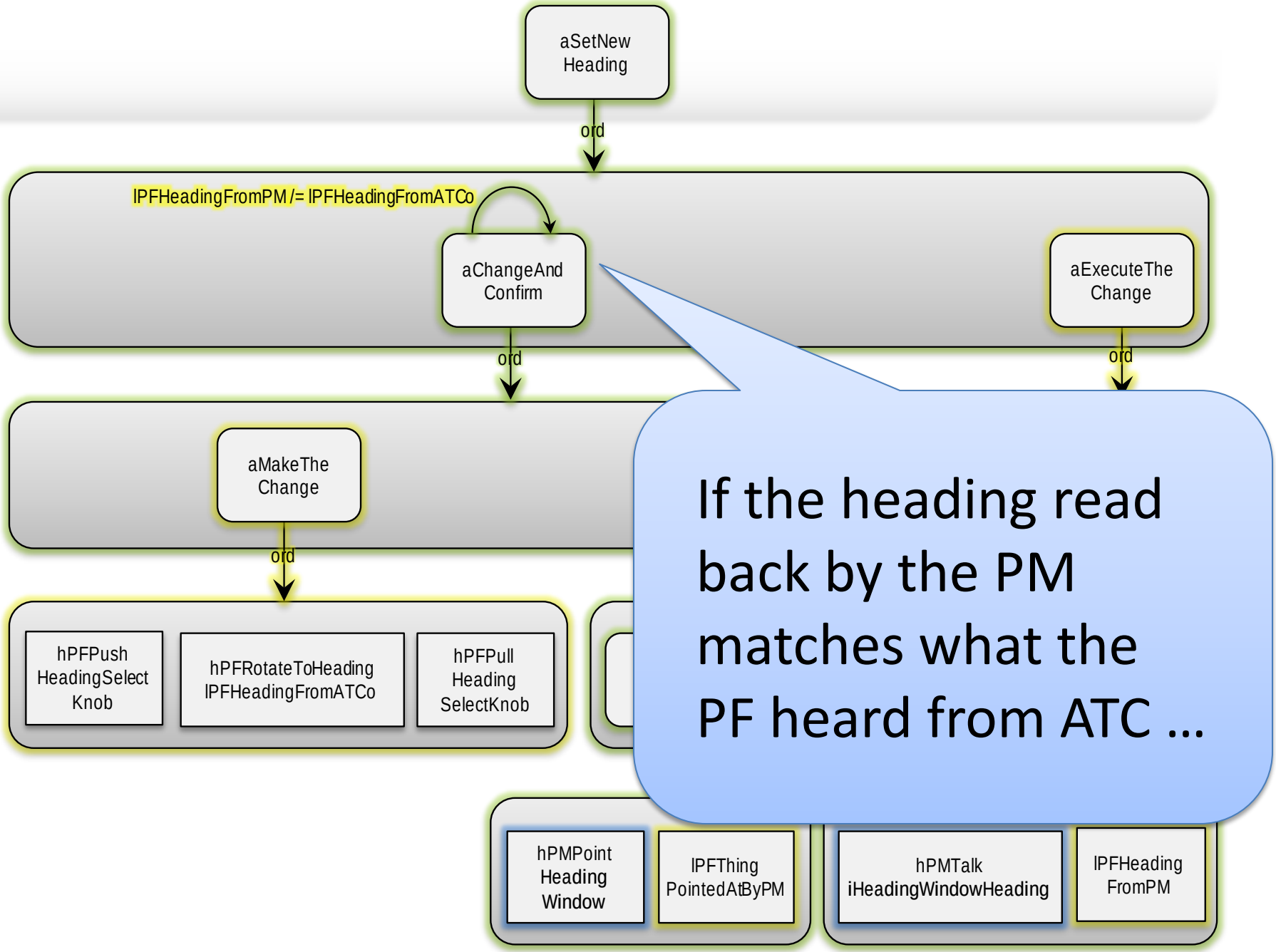

aSetNew Heading
ord
lPFHeadingFromPM /= lPFHeadingFromATCo
aChangeAnd Confirm
aExecuteThe Change
ord
ord
aMakeThe Change
ord
hPFPush HeadingSelect Knob
hPFRotateToHeading lPFHeadingFromATCo
hPFPull Heading SelectKnob
com
com
hPMPoint Heading Window
lPFThing PointedAtByPM
hPMTalk iHeadingWindowHeading
lPFHeading FromPM
The PM and PF collaborate to change the heading

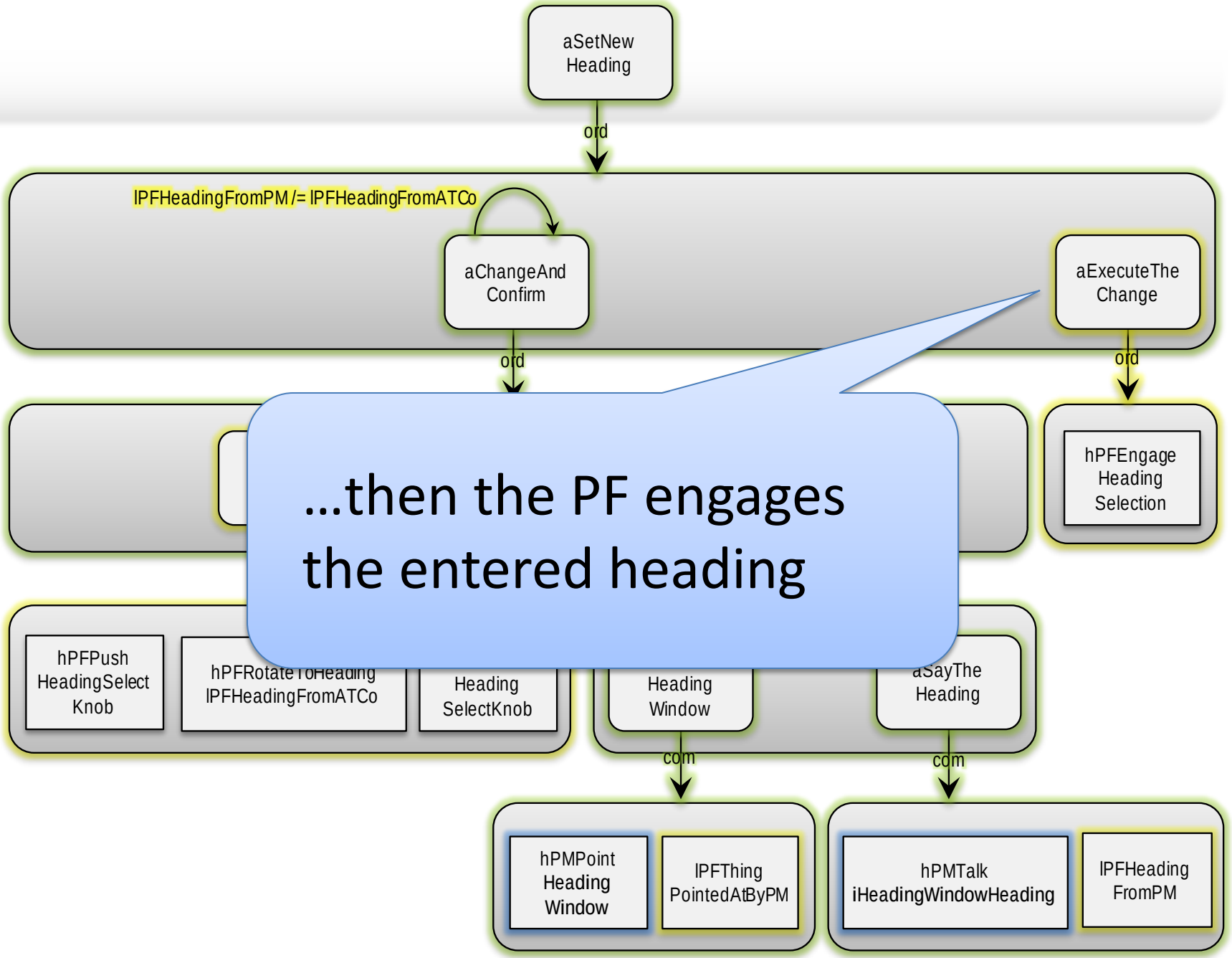
The PF pushes the heading-select knob, turns it to the heading heard from ATC and pulls the knob back out



The PM points to the heading window and repeats back the heading entered




aSetNew Heading
ord
lPFHeadingFromPM /= lPFHeadingFromATCo
aChangeAnd Confirm
aExecuteThe Change
ord
ord
aMakeThe Change
ord
hPFPush HeadingSelect Knob
hPFRotateToHeading lPFHeadingFromATCo
hPFPull Heading SelectKnob
hPMPoint Heading Window
lPFThing PointedAtByPM
hPMTalk iHeadingWindowHeading
lPFHeading FromPM
If the heading read back by the PM matches what the PF heard from ATC …



…then the PF engages the entered heading

Translation and Model Checking

The protocol was translated into SAL twice:

1. Normative behavior (*Max* = 0)
2. A maximum of one miscommunication (*Max* = 1)

Both were formally verified against the specification:

$$\mathbf{G}\left(\begin{array}{l}(aChangeHeading = Done)\\ \rightarrow (iHeadingWindowHeading = lATCSelectedClearance)\end{array}\right)$$

using SAL-SMC on a workstation with 3.0 Ghz dual-core Intel Xeon processor with 16 gigs of RAM

Verification Results

The *Max* = 0 Model

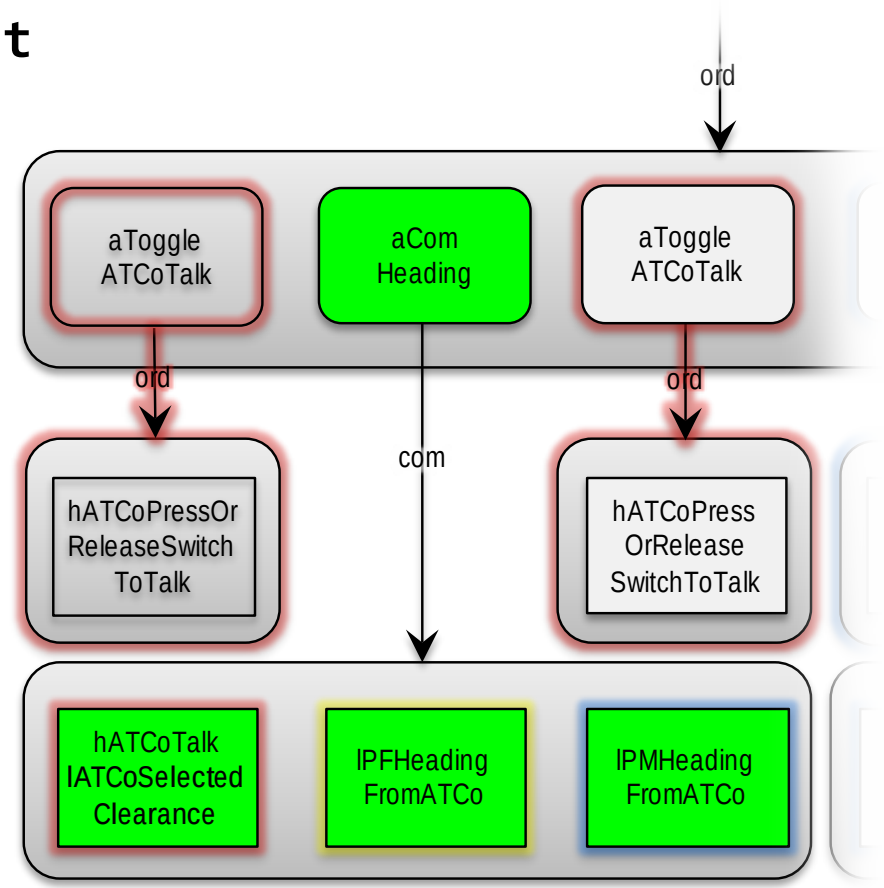
```
Result:                Confirmation
Verification Time:     2.52 seconds
Visited States:        559 states
```

The *Max* = 1 Model

```
Result:                Counterexample
Verification Time:     3.20 seconds
Visited States:        3726 states
```

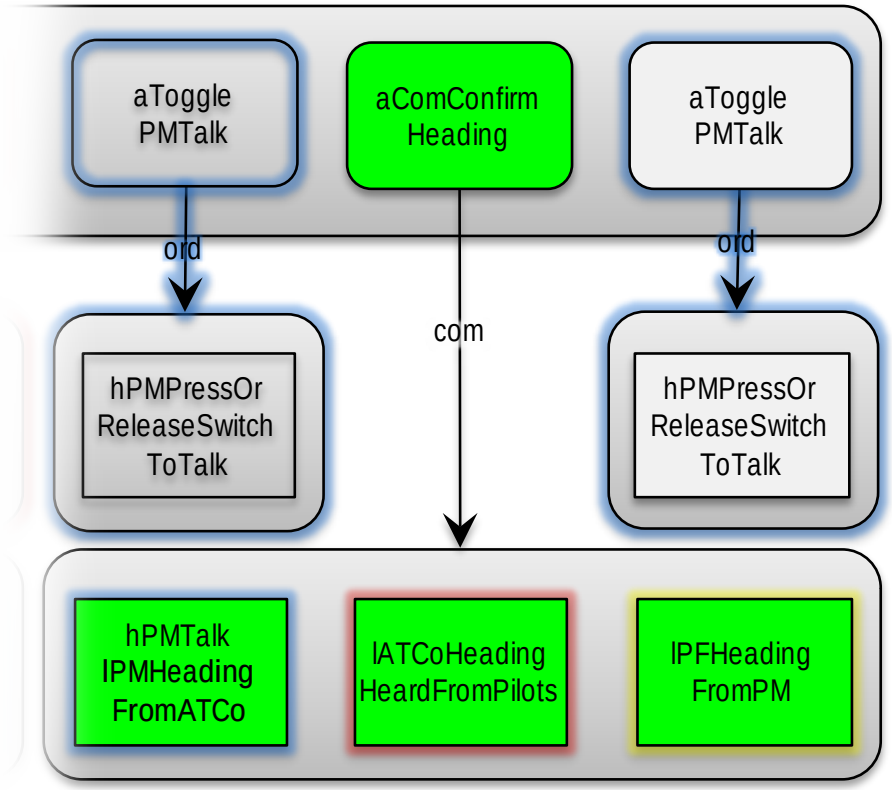
Counterexample Visualization

```
...
Count = 1
lATCoSelectedHeading = Correct
lPFHeadingFromATCo = Incorrect
lPMHeadingFromATCo = Correct
...
```



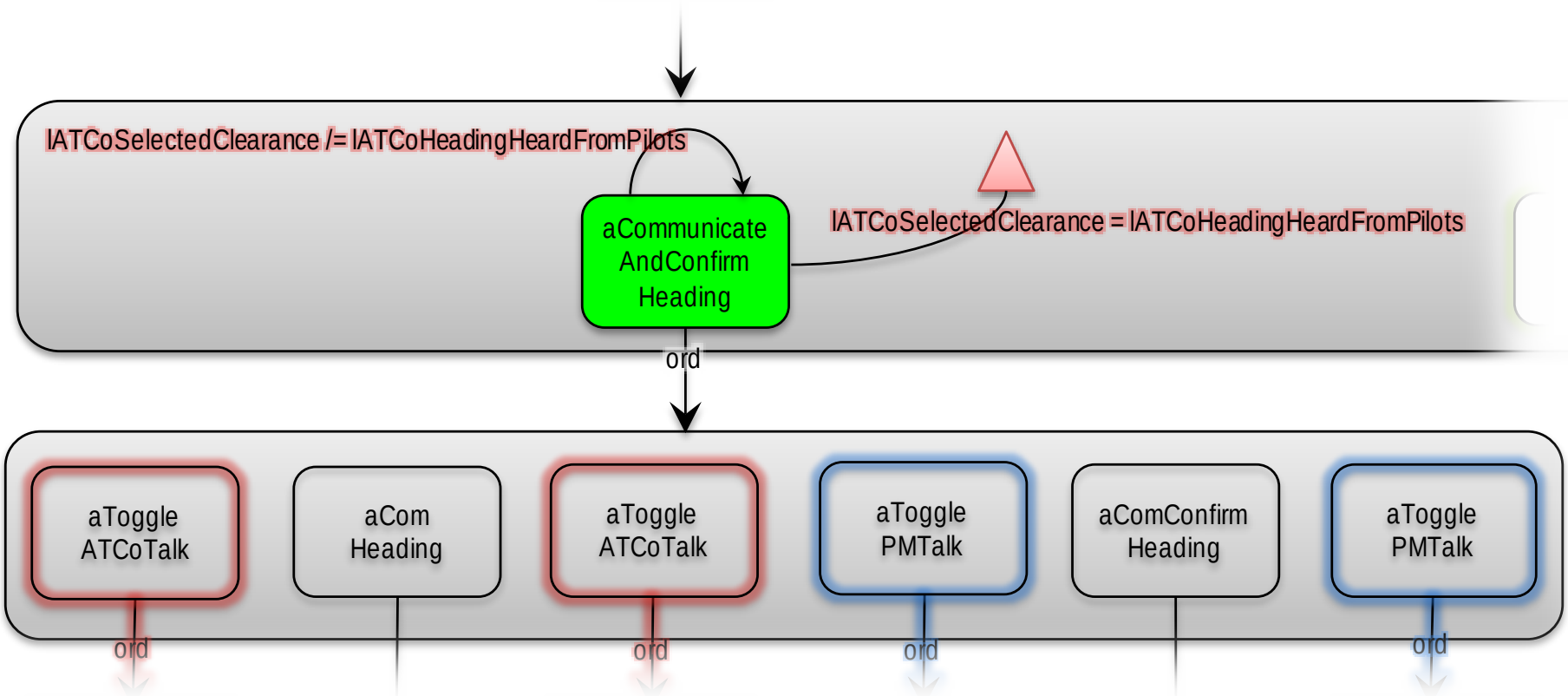
Counterexample Visualization

```
...
lPMHeadingFromATCo = Correct
lATCoHeadingHeardFromPilots = Correct
lPFHeadingFromPM = Correct
...
```



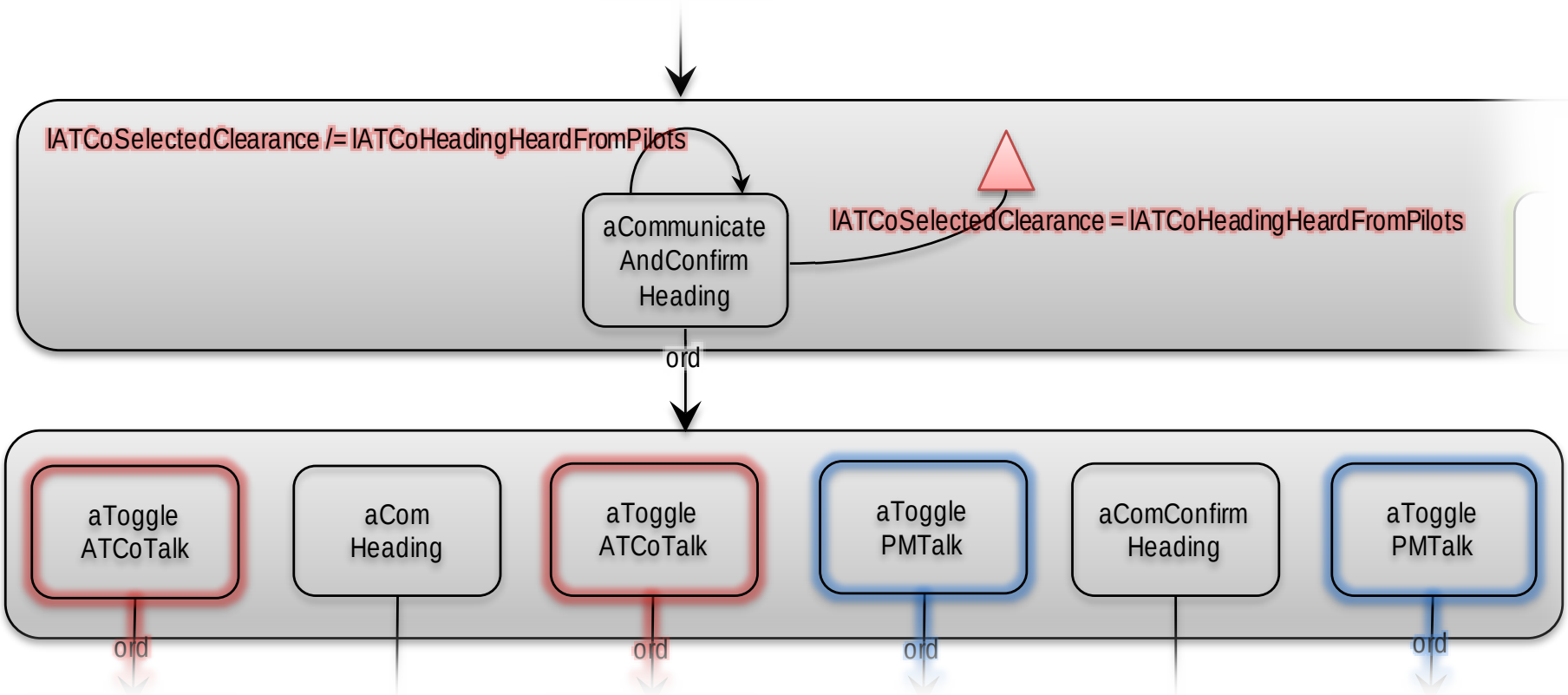
Counterexample Visualization

```
...
lATCoSelectedHeading = Correct
lATCoHeadingHeardFromPilots = Correct
...
```



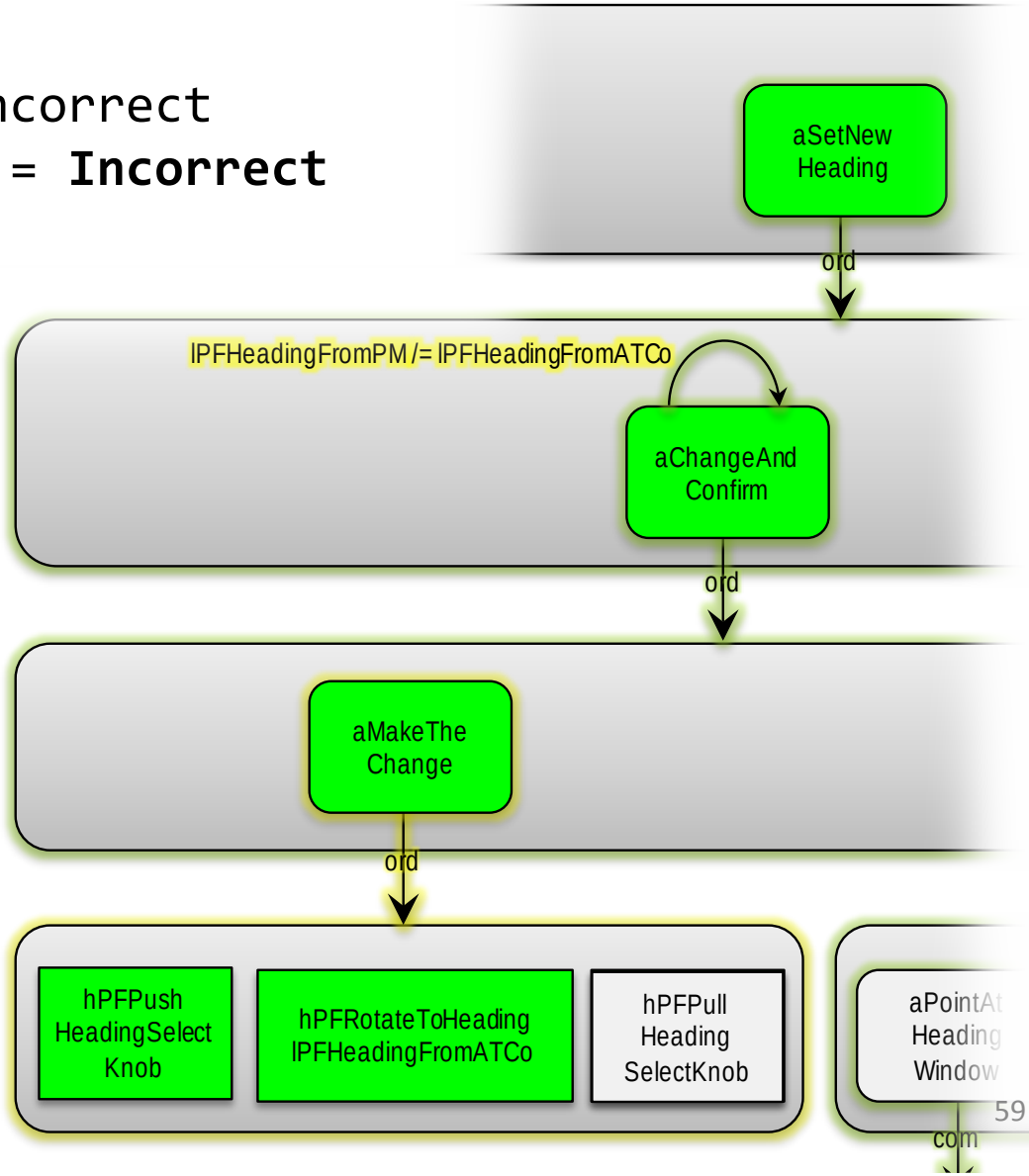
Counterexample Visualization

```
...
lATCoSelectedHeading = Correct
lATCoHeadingHeardFromPilots = Correct
...
```



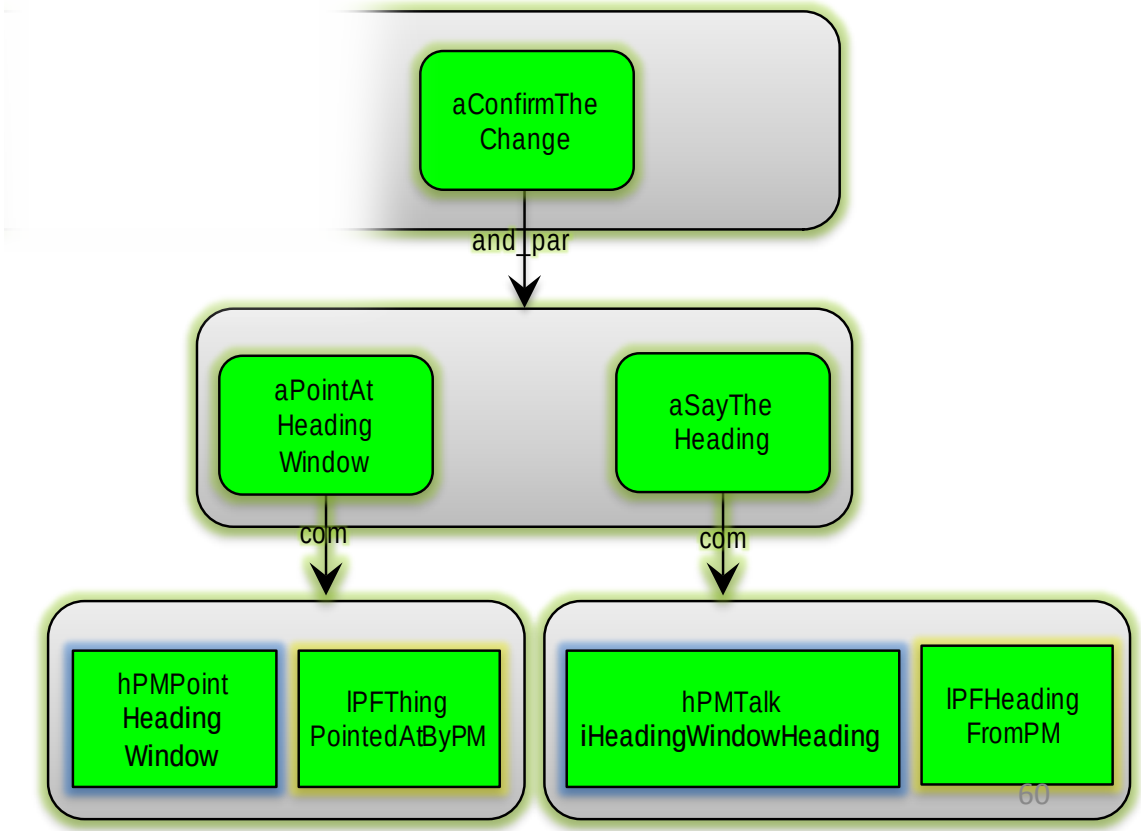
Counterexample Visualization

```
...
lPFHeadingFromATC = Incorrect
iHeadingWindowHeading = Incorrect
...
```



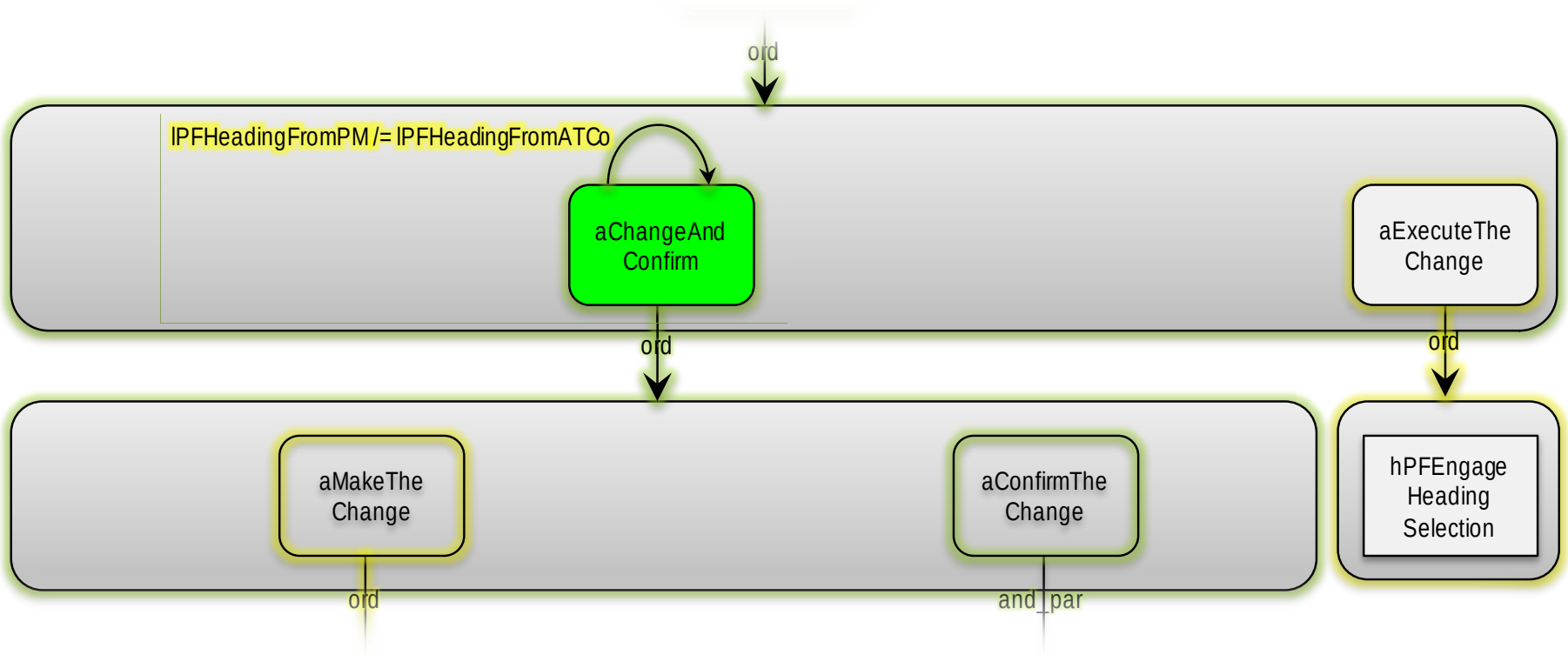
Counterexample Visualization

```
...
iHeadingWindowHeading = Incorrect
lPFHeadingFromATC = Incorrect
lPFHeadingFromPM = Incorrect
lPHThingPointedAtByPM = HeadingWindow
...
```



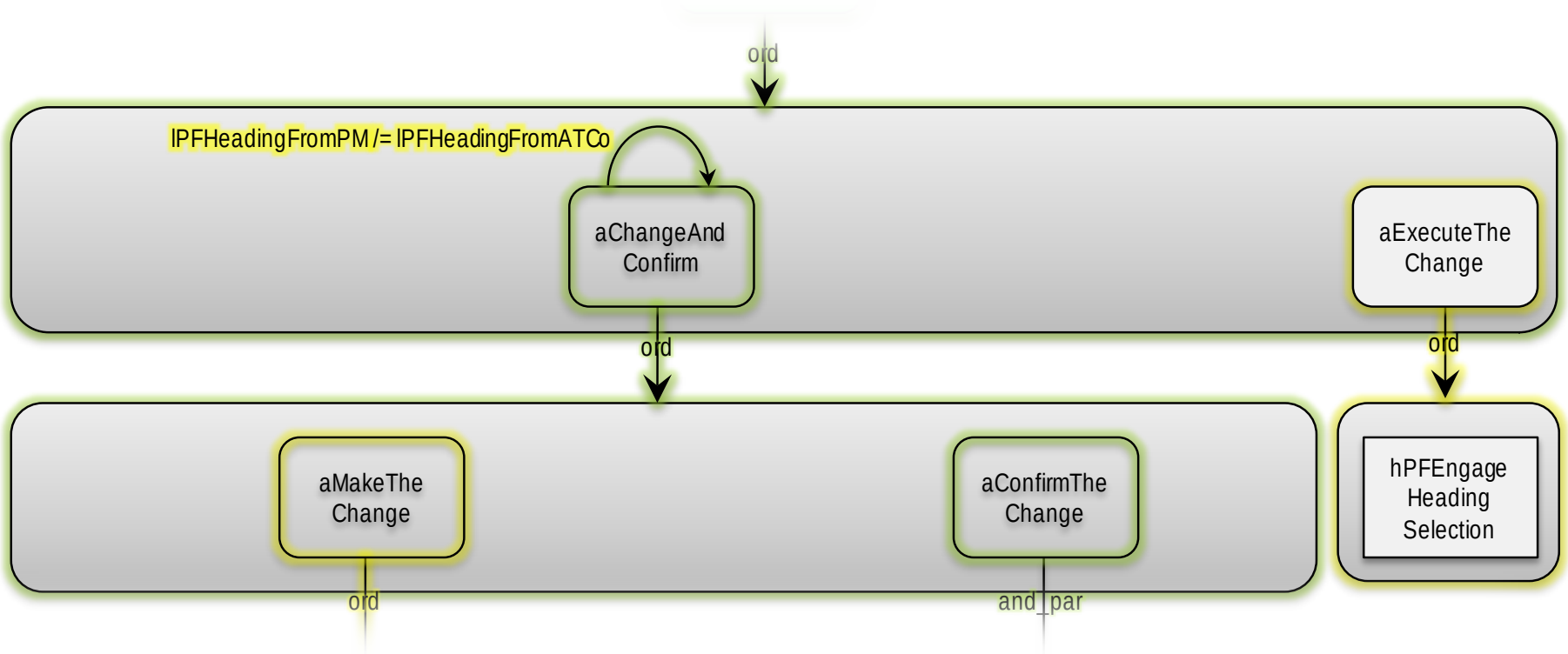
Counterexample Visualization

```
...
iHeadingWindowHeading = Incorrect
lPFHeadingFromPM = Incorrect
lPFHeadingFromATC = Incorrect
...
```



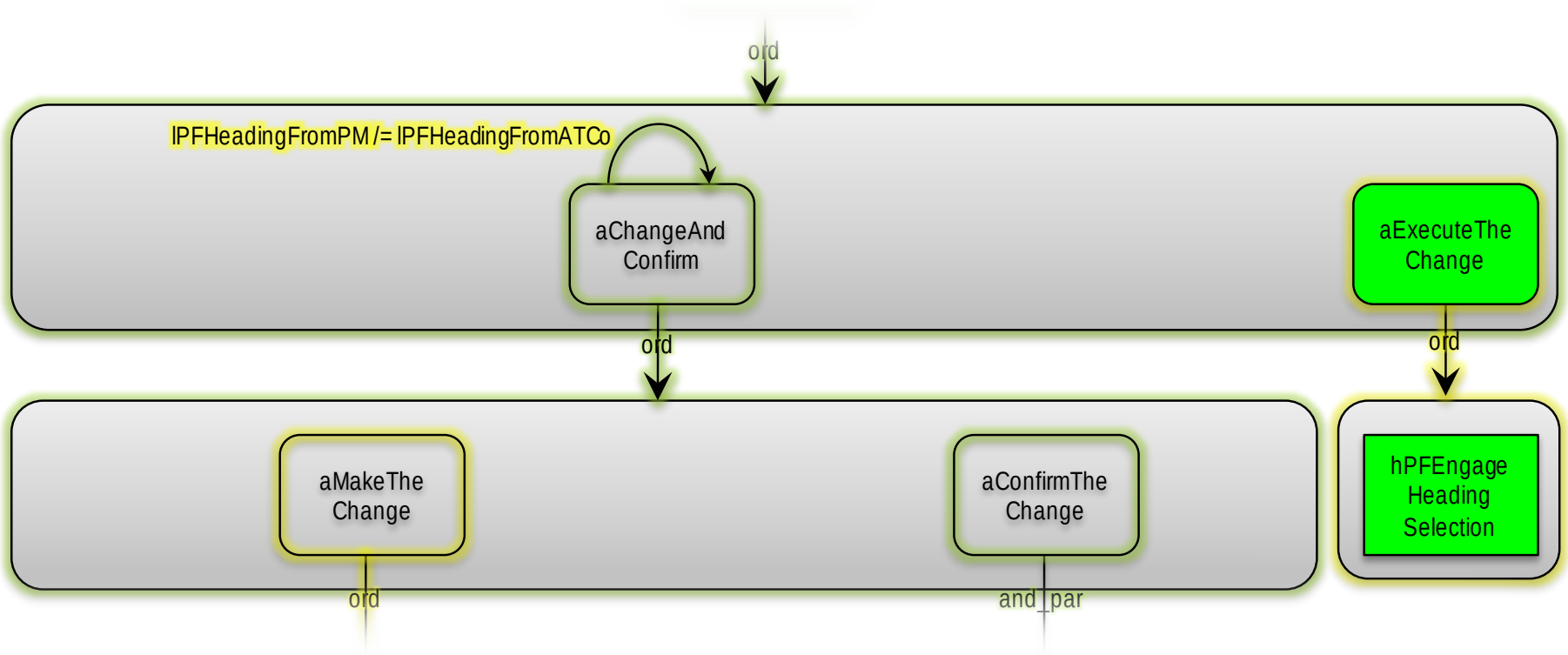
Counterexample Visualization

```
...
iHeadingWindowHeading = Incorrect
lPFHeadingFromPM = Incorrect
lPFHeadingFromATC = Incorrect
...
```



Counterexample Visualization

```
...
iHeadingWindowHeading = Incorrect
lPFHeadingFromPM = Incorrect
lPFHeadingFromATC = Incorrect
...
```



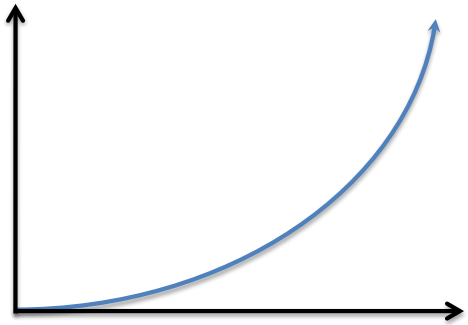
Contributions

- A method for formally modeling and verifying human-human communication protocols with task analytic models
- A novel means of generating miscommunications
- A means of proving the robustness of communication protocols with generated miscommunications
- An example that demonstrates the method's power

Limitations and Future Work

Investigating design interventions and running additional analyses

Improving the scalability of the method through re-architecting and the use of other formalisms



Incorporating other elements of human-human interaction and communication problems

Questions?

References

1. Airbus: Effective pilot / controller communications. In: Human Performance. Flight Operations Briefing Notes, Airbus, Blagnac Cedex (2006)
2. Arg´on, P., Delzanno, G., Mukhopadhyay, S., Podelski, A.: Model checking communication protocols. In: Proceedings of the 28th Conference on Current Trends in Theory and Practice of Informatics. pp. 160–170. Springer, Berlin (2001)
3. Austin, J.: How to do things with words, vol. 88. Harvard University Press (1975)
4. Bass, E.J., Bolton, M.L., Feigh, K., Griffith, D., Gunter, E., Mansky, W., Rushby, J.: Toward a multi-method approach to formalizing human-automation interaction and human-human communications. In: Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics. pp. 1817–1824. IEEE, Piscataway (2011)
5. Bass, E.J., Baxter, G.D., Ritter, F.E.: Creating models to control simulations: A generic approach. AI and Simulation of Behaviour Quarterly 93, 18–25 (1995)
6. Bastide, R., Basnyat, S.: Error patterns: Systematic investigation of deviations in task models. In: Task Models and Diagrams for Users Interface Design. pp. 109–121. Springer, Berlin (2007)
7. Baxter, G.D., Bass, E.J.: Human error revisited: Some lessons for situation awareness. In: Human Interaction with Complex Systems, 1998. Proceedings., Fourth Annual Symposium on. pp. 81–87. IEEE (1998)
8. Bochmann, G., Sunshine, C.: Formal methods in communication protocol design. IEEE Transactions on Communications 28(4), 624–631 (1980)
9. Bolton, M.L.: Automatic validation and failure diagnosis of human-device interfaces using task analytic models and model checking. Computational and Mathematical Organization Theory pp. 1–25 (2012), http://dx.doi.org/10.1007/s10588-012-9138-6
10. Bolton, M.L., Bass, E.J.: Enhanced operator function model: A generic human task behavior modeling language. In: Proceedings of the IEEE International Conference on Systems Man and Cybernetics. pp. 2983–2990. IEEE, Piscataway (2009)
11. Bolton, M.L., Bass, E.J.: A method for the formal verification of human interactive systems. In: Proceedings of the 53rd Annual Meeting of the Human Factors and Ergonomics Society. pp. 764–768. HFES, Santa Monica (2009)
12. Bolton, M.L., Bass, E.J.: Formally verifying human-automation interaction as part of a system model: Limitations and tradeoffs. Innovations in Systems and Software Engineering: A NASA Journal 6(3), 219–231 (2010)
13. Bolton, M.L., Bass, E.J.: Using task analytic models to visualize model checker counterexamples. In: Proceedings of the 2010 IEEE International Conference on Systems, Man, and Cybernetics. pp. 2069–2074. IEEE, Piscataway (2010)
14. Bolton, M.L., Bass, E.J.: Evaluating human-automation interaction using task analytic behavior models, strategic knowledge-based erroneous human behavior generation, and model checking. In: Proceedings of the IEEE International Conference on Systems Man and Cybernetics. pp. 1788–1794. IEEE, Piscataway (2011)
15. Bolton, M.L., Bass, E.J.: Using model checking to explore checklist-guided pilot behavior. International Journal of Aviation Psychology 22, 343–366 (2012)
16. Bolton, M.L., Bass, E.J., Siminiceanu, R.I.: Using phenotypical erroneous human behavior generation to evaluate human-automation interaction using model checking. International Journal of Human-Computer Studies 70, 888–906 (2012)
17. Bolton, M.L., Bass, E.J., Siminiceanu, R.I.: Using formal verification to evaluate human-automation interaction in safety critical systems, a review. IEEE Transactions on Systems, Man and Cybernetics: Systems (in press, expected 2013)
18. Bolton, M.L., Siminiceanu, R.I., Bass, E.J.: A systematic approach to model checking human-automation interaction using task-analytic models. IEEE Transactions on Systems, Man, and Cybernetics, Part A 41(5), 961–976 (2011)
19. Clarke, E.M., Grumberg, O., Peled, D.A.: Model checking. MIT Press, Cambridge (1999)
20. De Moura, L., Owre, S., Shankar, N.: The SAL language manual. Tech. Rep. CSL-01-01, Computer Science Laboratory, SRI International, Menlo Park (2003)
21. Dietrich, F., Hubaux, J.: Formal methods for communication services. Tech. Rep. SSC/1999/023, Institute for Computer Communications and Applications, Swiss Federal Institute of Technology (1999)
22. Edelkamp, S., Leue, S., Lluch-Lafuente, A.: Directed explicit-state model checking in the validation of communication protocols. International Journal on Software Tools for Technology Transfer 5(2), 247–267 (2004)
23. Fields, R.E.: Analysis of Erroneous Actions in the Design of Critical Systems. Ph.D. thesis, University of York, York (2001)
24. Gibson, W., Megaw, E., Young, M., Lowe, E.: A taxonomy of human communication errors and application to railway track maintenance. Cognition, Technology & Work 8(1), 57–66 (2006)