Formal Representation and Verification the Continuous Systems in NΣ-labeled calculus

Aim of Study

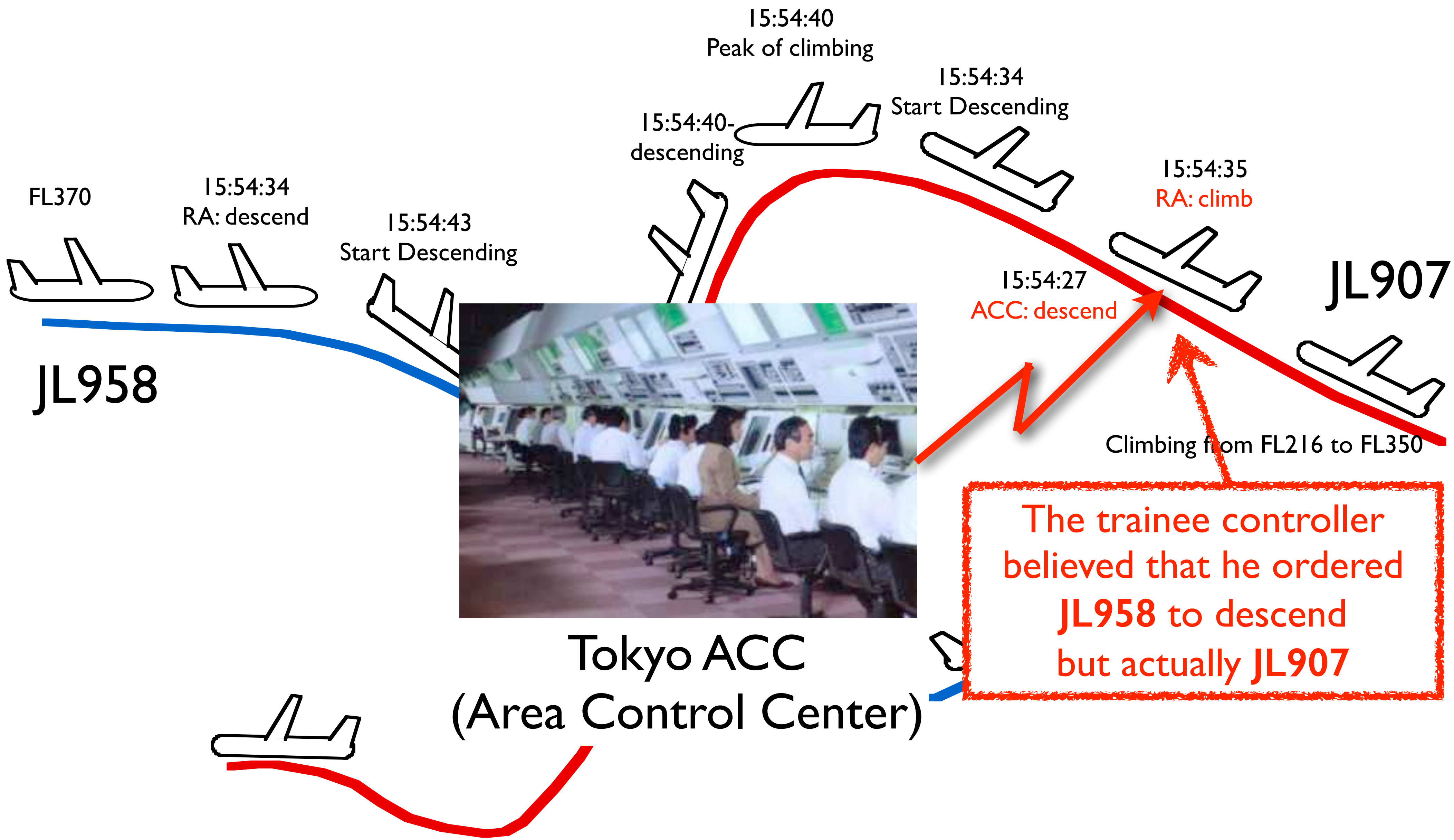
- It becomes more and more important to analyze and verify continuous time-concerned cooperative systems with human factors, like railway and airlines controlling systems.
- Serious accidents can be caused be human errors involved in recognition or decision.
- *NΣ-labeled calculus* will be introduced to describe
  time-concerned recognition, knowledge, belief and decision
  of humans or computer programs
  together with related external phenomena.

JAL Airplane Near Miss Accident [AICI2009, Shanghai]

On Jan. 31, 2001, JAL flight 907, a Boeing 747 had departed Tokyo-Haneda for a flight with destination Naha.
JAL Flight 958, a DC-10-40 was en route from Pusan to Tokyo-Narita.
A trainee controller at Tokyo ACC cleared flight 907 to climb to Flight Level 390 at 15:46.
Two minutes later JL958 reported at FL370.
Both flights were on an intersecting course near the Yaizu NDB.
At 15:54 the controller noticed this, but instead of ordering flight 958 to descend, he ordered the Boeing 747 to descend: "Japan air niner zero seven, descend and maintain flight level three five zero, begin descent due to traffic."
Immediately after this instruction, the crew of flight 907 were given an aural TCAS Resolution Advisory to climb in order to avoid a collision.
At the same time the crew of flight 958 were given an aural TCAS Resolution Advisory to descend.
The captain of flight 907 followed the instructions of the air traffic controller by descending.
The 747 now approaching close to Flight 958, because the DC-10 captain descended as well, following the advisory of his TCAS.
A collision was averted when the pilot of flight 907 then put his Boeing 747 into a nosedive.
The 747 missed the DC-10 by 105 to 165 meters in lateral distance and 20 to 60 meters in altitude difference.
About 100 crew and passengers on flight 907 sustained injuries due to emergency manoevre, while no one was injured on Flight 958. Flight 958 continued to Narita, while flight 907 returned to Haneda Airport.

Source: Aviation Safety Network. http://aviation-safety.net/database/record.php?id=20010131-2

JAL Airplane Near Miss Accident



NΣ-labeled Calculus

- Base: PA(∞): PA+∞+μ : *Pseudo-Arithmetic*
- ℓ , ℓ_1, ℓ_2, ... : labels
  - corresponding to *personalities*

- Tense: the time relative to reference observation time
- "@" : *coincidental operator*; to describe change of state
  - **A**@<**a**, ℓ > :

    ℓ believes (thinks) at tense **a** the fact that

    "a formula **A** holds *now*".

PA

N1.	$x + 1 \neq 0.$	N2.	$x + 1 = y + 1 \supset x = y.$
N3.	$x + 0 = x.$	N4.	$x + (y + 1) = (x + y) + 1.$
N5.	$x \times 0 = 0.$	N6.	$x \times (y + 1) = (x \times y) + x.$
N7.	$\neg(x < 0).$	N8.	$(x < y + 1 \equiv x \leq y).$

N9. $\mathbf{A}[0] \& \forall x(\quad \mathbf{A}[x] \supset \mathbf{A}[x+1]) \supset \forall x(\quad \mathbf{A}[x]),$

PA(∞)

N1.	$x + 1 \neq 0.$	N2.	$x < \infty \supset y < \infty \supset x + 1 = y + 1 \supset x = y.$
N3.	$x + 0 = x.$	N4.	$x < \infty \supset y < \infty \supset x + (y + 1) = (x + y) + 1.$
N5.	$x \times 0 = 0.$	N6.	$y < \infty \supset x \times (y + 1) = (x \times y) + x.$
N7.	$\neg(x < 0).$	N8.	$y < \infty \supset (x < y + 1 \equiv x \leq y).$
Axioms for ∞:			
N4$'$.	$x + \infty = \infty + x = \infty.$		
N5$'$.	$0 \times \infty = 0.$	N6$'$.	$0 < x \supset x \times \infty = \infty \times x = \infty.$
N7$'$.	$x \leq \infty.$		
The mathematical induction:			
N9.	$\mathbf{A}[0] \& \forall x (x < \infty \& \mathbf{A}[x] \supset \mathbf{A}[x + 1]) \supset \forall x (x < \infty \supset \mathbf{A}[x]),$		
The least number principle:			
N9$'$.	$\exists x \mathbf{A}[x] \supset \mathbf{A}[\mu x \mathbf{A}[x]] \& \forall y (\mathbf{A}[y] \supset \mu x \mathbf{A}[x] \leq y).$		

NΣ-labeled Calculus

- " ; " : *futurity operator*
  to move the observation time toward a future time-point.
  - Definition
    - **a** ; **b** $\Leftrightarrow$ **a**+μ*x*(*x*=**b**@**a**)

      the tense of **b** observed by **a**
    - **a** ; **A** $\Leftrightarrow$ μ*x*(**a**≤*x* & **A**@*x*)

      the earliest time when **A** comes to hold, or rises after the tense **a**

Proof System

Logical Axioms

(a) The equality substitution for @ : $x{=}y \supset \mathbf{A}@x \supset \mathbf{A}@y$.

(b) Elimination of tense 0 : $\mathbf{A}@0 \equiv \mathbf{A}$.

(c) Introspection

- consisitency: $\neg(\mathbf{false}@\ell)$
- necessitation: $\mathbf{A}@\ell$, if A is a logical axiom
- positive introspection: $\mathbf{A}@\ell \supset \mathbf{A}@\ell@\ell$
- negative introspection: $\neg(\mathbf{A}@\ell) \supset (\neg(\mathbf{A}@\ell))@\ell$

(d) Inductive Evaluation

- $\mathbf{false}@x \equiv x{=}\infty$,
- $(x \leq y)@\lambda \equiv \mu z(z{=}x@\lambda) \leq \mu z(z{=}y@\lambda)$,
- $\mathbf{A}@\ell@x \equiv \mathbf{A}@\langle x, \ell\rangle$,
- $x<\infty \supset ((\neg\mathbf{A})@x) \equiv \neg\mathbf{A}@x)$,
- $(\neg\mathbf{A}@\ell) \equiv (\neg\mathbf{A})@\ell$,
- $\forall y(\mathbf{A}@\lambda) \equiv (\forall y\mathbf{A}@\lambda)$, where λ is $\langle x, \ell\rangle$, x or ℓ

Proof System

Inference Rules

i. All the rules of NK are used with the only restriction as
∀-*elimination rule*:

$$\frac{\forall x(\mathbf{A}[x])}{\mathbf{A}[\mathbf{a}]}$$

where only a *tense-independent term* **a** can be substituted in place of *x*, if *x* occurs in **B**[*x*] in a subformula of **A** of the form

$\mathbf{B}[x]@\langle\mathbf{b}, \ell\rangle$ or $\mathbf{B}[x]@\mathbf{b}$,

of the premise (i.e. upper formulas).

Proof System

ii. Rules for @:

- @-introduction rule:

$$\frac{\mathbf{A}}{\mathbf{A}@x}$$

  where neither **A** nor its assumptions have a special constant.

- @-elimination rule:

$$\frac{\mathbf{A@a} \quad \mathbf{a<\infty}}{\mathbf{A}}$$

  where no special constant occurs in **A**.

Representation of Cooperative Systems

- Spur: α, β, γ, ... , κ, ...
  - Generalization of program schedulers, 'next' operators, etc.
  - Each process of a multi-CPU program, or external object, is assigned a distinct spur.

- Program labels : a, a1, a2, ...
  - expressed by mutually exclusive special boolean constants

Representation of Cooperative Programs

- Conservation Axioms
  - (CA1) the value of *J* does not change until the next step of any process rises:

    $J{=}z \supset x{<}\alpha \;\&\; x{<}\beta \;\&\; \ldots \;\&\; x{<}\kappa \supset J{=}z@x$

    for each *J* and all spurs $\alpha, \beta, \ldots, \kappa$

  - (CA2) *J* does not change within the block
    corresponding to a *program label a*:

    $J{=}z@a \supset \alpha{<}\beta \;\&\; \ldots \;\&\; \alpha{<}\kappa \supset a \leq x \leq \alpha \supset J{=}z@x$

    such that *J* does not occur in the 'act' part of corresponding program axiom

Representation of Cooperative Continuous Programs

- Approximation of Continuous System
  - For representation of continuity, the notion of *differentiation* is dealt with.
  - The first order time-derivatives, e.g. *speed*, are treated as program variables (special constants).
  - The primitives are defined by the *integral* of the higher-order one.
  - The integral is defined by the *Euler's approximation*.

Representation of Cooperative Continuous Programs

Definition

$$\sum_{0 \le x < 0} \mathbf{a}[x] = 0, \quad \sum_{0 \le x < y+1} \mathbf{a}[x] = \sum_{x<y} \mathbf{a}[x] + \mathbf{a}[y],$$

$$\sum_{0 \le x < \infty} \mathbf{a}[x] = \begin{cases} \sum_{0 \le x < \mu y (\forall z (y \le z \supset \mathbf{a}[z]=0))} \mathbf{a}[x], \\ \qquad\qquad \mathit{if}\ \exists y (\forall z (y \le z \supset \mathbf{a}[z] = 0)), \\ \infty, \qquad \mathit{otherwise.} \end{cases}$$

$$\int_{x=b}^{b+t} \mathbf{a}[x] \stackrel{\text{def}}{=} \sum_{0 \le y < n+1} h \cdot \mathbf{a}[b + yh], \quad \text{where } t{=}nh.$$

For a special constant *A*, $\dot{A}$ is defined as follows.

$$A[t] \stackrel{\text{def}}{=} \int_{x=0}^{t} \mu y (y = \dot{A} @ x)$$

Representation of Cooperative Continuous Programs

Definition.
Let $\dot{A}$ be a special constant. A is defined as follows.

$$A[t] \stackrel{\text{def}}{=} \int_{x=0}^{t} \mu y(y = \dot{A}@x)$$

Axiom Tableaux

$(\neg \mathit{Ecntl} \supset \gamma_{\boldsymbol{P}}=\mathit{ope}(\boldsymbol{P}, X)=D_6)@<\uparrow \mathit{RA}(\boldsymbol{P}, X)@\boldsymbol{P},\ \{\boldsymbol{P}, \mathit{ACC}\}>$
$\&(\neg \mathit{Ecntl} \supset \gamma_{\boldsymbol{P}}=\mathit{ope}(\boldsymbol{P}, X)=D_6)@\uparrow \mathit{RA}(\boldsymbol{P}, X)@\boldsymbol{P}$

index	condition/prefix	action	tense	label
10	$\neg \mathit{Ecntl}$	$\gamma_{\boldsymbol{P}}$	$\uparrow \mathit{RA}(\boldsymbol{P}, X)@\boldsymbol{P}$	$*, \boldsymbol{P}, \mathit{ACC}$

$\exists X\ Y(\beta=((\mathit{cntl}(A, X)\vee \mathit{cntl}(B, Y))\ \&\ (\mathit{cntl}(A, X)\equiv \mathit{Ecntl}@A)\ \&\ (\mathit{cntl}(B, Y)\equiv \mathit{Ecntl}@B))=D_2$
$@<\uparrow \mathit{acnticipateNM}(A, B)\ @\mathit{ACC},\ \ \mathit{ACC}>)$
$\&\ \ \exists X\ Y(\beta=((\mathit{cntl}(A, X)\vee \mathit{cntl}(B, Y))\ \&\ (\mathit{cntl}(A, X)\equiv \mathit{Ecntl}@A)\ \&\ (\mathit{cntl}(B, Y)\equiv \mathit{Ecntl}@B))=D_2$
$@\uparrow \mathit{acnticipateNM}(A, B)\ @\mathit{ACC})$

4	**forsome** *X*, *Y*	$\beta=$ $(\mathit{cntl}(A, X)\vee \mathit{cntl}(B, Y),$ $\mathit{cntl}(A, X)\equiv \mathit{Ecntl}@A,$ *cntl*	$\uparrow \mathit{acnticipateNM}(A, B)\ @\mathit{ACC}$	$*, \mathit{ACC}$

↑A : **¬A ; A** the tense when **A** rises

↑A@ℓ : (**¬A**)@ℓ ; **A@**ℓ the tense recognized by ℓ when **A**rises

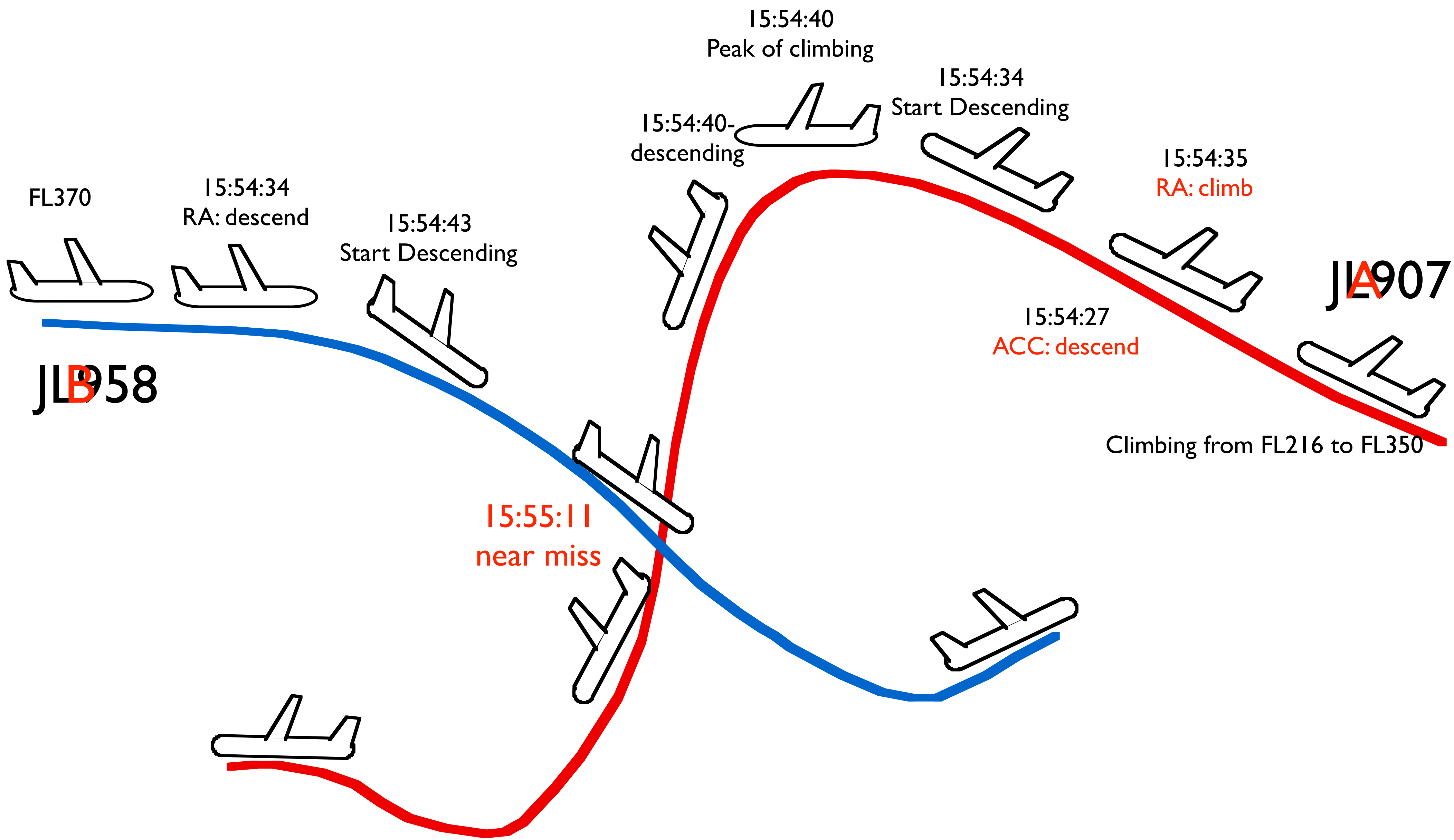
* : This fact (recognition) is reality.

JAL Airplane Near Miss Accident

On Jan. 31, 2001, JAL flight 907, a Boeing 747 had departed Tokyo-Haneda for a flight with destination Naha.
JAL Flight 958, a DC-10-40 was en route from Pusan to Tokyo-Narita.
A trainee controller cleared flight 907 to climb to Flight Level 390 at 15:46.
Two minutes later JL958 reported at FL370.
Both flights were on an intersecting course near the Yaizu NDB.
At 15:54 the controller noticed this, but instead of ordering flight 958 to descend, he ordered the Boeing 747 to descend: "Japan air niner zero seven, descend and maintain flight level three five zero, begin descent due to traffic."
Immediately after this instruction, the crew of flight 907 were given an aural TCAS Resolution Advisory to climb in order to avoid a collision.
At the same time the crew of flight 958 were given an aural TCAS Resolution Advisory to descend.
The captain of flight 907 followed the instructions of the air traffic controller by descending.
The 747 now approaching close to Flight 958, because the DC-10 captain descended as well, following the advisory of his TCAS.
A collision was averted when the pilot of flight 907 then put his Boeing 747 into a nosedive.
The 747 missed the DC-10 by 105 to 165 meters in lateral distance and 20 to 60 meters in altitude difference.
About 100 crew and passengers on flight 907 sustained injuries due to emergency manoevre, while no one was injured on Flight 958. Flight 958 continued to Narita, while flight 907 returned to Haneda Airport.

Source: Aviation Safety Network. http://aviation-safety.net/database/record.php?id=20010131-2

JAL Airplane Near Miss Accident



Formalization

Program Axioms

index	condition/prefix	action	tense	label
1		α=	↑*acnticipateNM*(*A*, *B*) @*Monitor*	*, *Monitor*
2		*acnticipateNM*(*A*, *B*)≡*CNF*		*, *ACC*
3		β=(	↑*CNF*	*, *ACC*
4	**forsome** *X*, *Y*	β=(*cntl*(*A*, *X*)∨*cntl*(*B*, *Y*), *cntl*(*A*, *X*)≡*Ecntl*@*A*, *cntl*(	↑*acnticipateNM*(*A*, *B*) @*ACC*	*, *ACC*
5	**forsome** *X*, *Y*	*cntl*(*A*		*, *ACC*
6		$\gamma_{\boldsymbol{P}}$=¬	↑*cntl*(***P***, *X*)@***P***	*, ***P***, *ACC*
7	**forsome** *X*	ρ_A=	↑*acnticipateNM*(*A*, *B*) @	*, *A*
8	**forsome** *X*	ρ_B=	↑*acnticipateNM*(*A*, *B*) @	*, *B*
9		$\gamma_{\boldsymbol{P}}$=	↑*cntl*(***P***, *X*)@***P***	*, ***P***, *ACC*
10	¬*Ecntl*	$\gamma_{\boldsymbol{P}}$=	↑*RA*(***P***, *X*)@***P***	*, ***P***, *ACC*
11		γ_A=(| 0	↑*ope*(*A*, <*v*, *h*>)	*, *A*, *B*, *ACC*

A: JL907, *B*: JL958   *a*: position of *A* ***P***: metasymbol over {*A*, *B*}

α, β, γ_A, γ_B. ρ_A, ρ_B: spurs of Monitor, ACC, *A*, *B*, $TCAS_A$, $TCAS_B$, respectively

D_i ($1 \leq i \leq 6$): delays

$\square_{180}Separation_{7,5}$: *A* and *B* keep the vertical distance 7[FL] and horizontal 5[nm] in 180[s]

↑**A**: tense when **A** rises   ↑**A**@ℓ : tense recognized by ℓ when **A** rises

* : This fact (recognition) is true.

X=<*v*, *h*>: value of climb, *v* : the vertical speed to climb, *h* : vertical position to go.

Formalization

Facts

index	condition/prefix	action	tense	label
12		↑*acnticipateNM*(*A*, *B*)=15:54’15”	*S*	*, *Monitor*
13		↑*cntl*(*A*, <⊥, 350[FL]>)=15:54’27”	*S*	*, *A*
14		↑(*cntl*(*A*, <⊥, 350[FL]>)≡*Ecntl*)=15:54’27”	*S*	*, *A*
15		↑*RA*(*A*, <1500ft/min, ⊥>)=15:54’35”	*S*	*, *A*
16		↑*RA*(*B*, <-1500ft/min, ⊥>)=15:54’34”	*S*	*, *B*
17		¬*Ecntl*, ¬*CNF*	*S*	*, *A*, *B*, *ACC*
18		↑*cntl*(*B*, <⊥, 350[FL]>)=15:54’27”	*S*	*ACC*
19	↑*ope* *hold*(*A*)	$\Box_{180}$	*S* ; 15:54’27”	*, *ACC*
20		*hold*(*A*)		*ACC*

S: start time of the system

Verification and Analysis

Theorem

$$\Diamond_{180} \neg \mathit{Separation}_{7,5} @ 15{:}54'34''$$

for the actual values
a_h=5[nm], b_h=-5[nm], $\dot{a}_h$=500[kt], $\dot{b}_h$=-500[kt], a_v=b_v=370[FL]
where
the horizontal origin is the position that the near miss occurred.

Other Cases

1. If the controller ordered correctly as

18		$\uparrow cntl(B, <\perp, 350[FL]>)=15{:}54'27''$	S	

instead of

13		$\uparrow cntl(A, <\perp, 350[FL]>)=15{:}54'27''$	S	

then the near miss did not occur, i.e,

$$\Box_{180} Separation_{7,5} @ 15{:}54'34''.$$

Other Cases

2. If the the crew of the airplane *A* followed the order from TCAS instead of that from ACC, then

$$\Box_{180} \mathit{Separation}_{7,5} @ 15{:}54'34''.$$

Other Cases

Axioms when ACC are given priority over TCAS (till September, 2002)

index	condition/prefix	action	tense	label
9		$\gamma_{\boldsymbol{P}}$	$\uparrow cntl(\boldsymbol{P}, X)@P$	$*, \boldsymbol{P}, ACC$
10	$\neg Ecntl$	$\gamma_{\boldsymbol{P}}$	$\uparrow RA(\boldsymbol{P}, X)@P$	$*, \boldsymbol{P}, ACC$

Axioms when TCAS are given priority over ACC (from October, 2002)

index	condition/prefix	action	tense	label
9'		$\gamma_{\boldsymbol{P}}$	$\uparrow RA(\boldsymbol{P}, X)@P$	$*, \boldsymbol{P}, ACC$
10'	$\neg RA(\boldsymbol{P}, Y)$	$\gamma_{\boldsymbol{P}}$	$\uparrow cntl(\boldsymbol{P}, X)@P$	$*, \boldsymbol{P}, ACC$

The rule that crews must follow whether TCAS or ACC if they contradict have changed.
Under the new rule,

$$\Box_{180} Separation_{7,5}@15{:}54'34''.$$