Comparing Different Functional Allocations in Automated Air Traffic Control Design

FMCAD 2015, September 27-30

Cristian Mattarei[1], Alessandro Cimatti[1], Marco Gario[1], Stefano Tonetta[1], and Kristin Y. Rozier[2]

[1]Fondazione Bruno Kessler, Trento, Italy

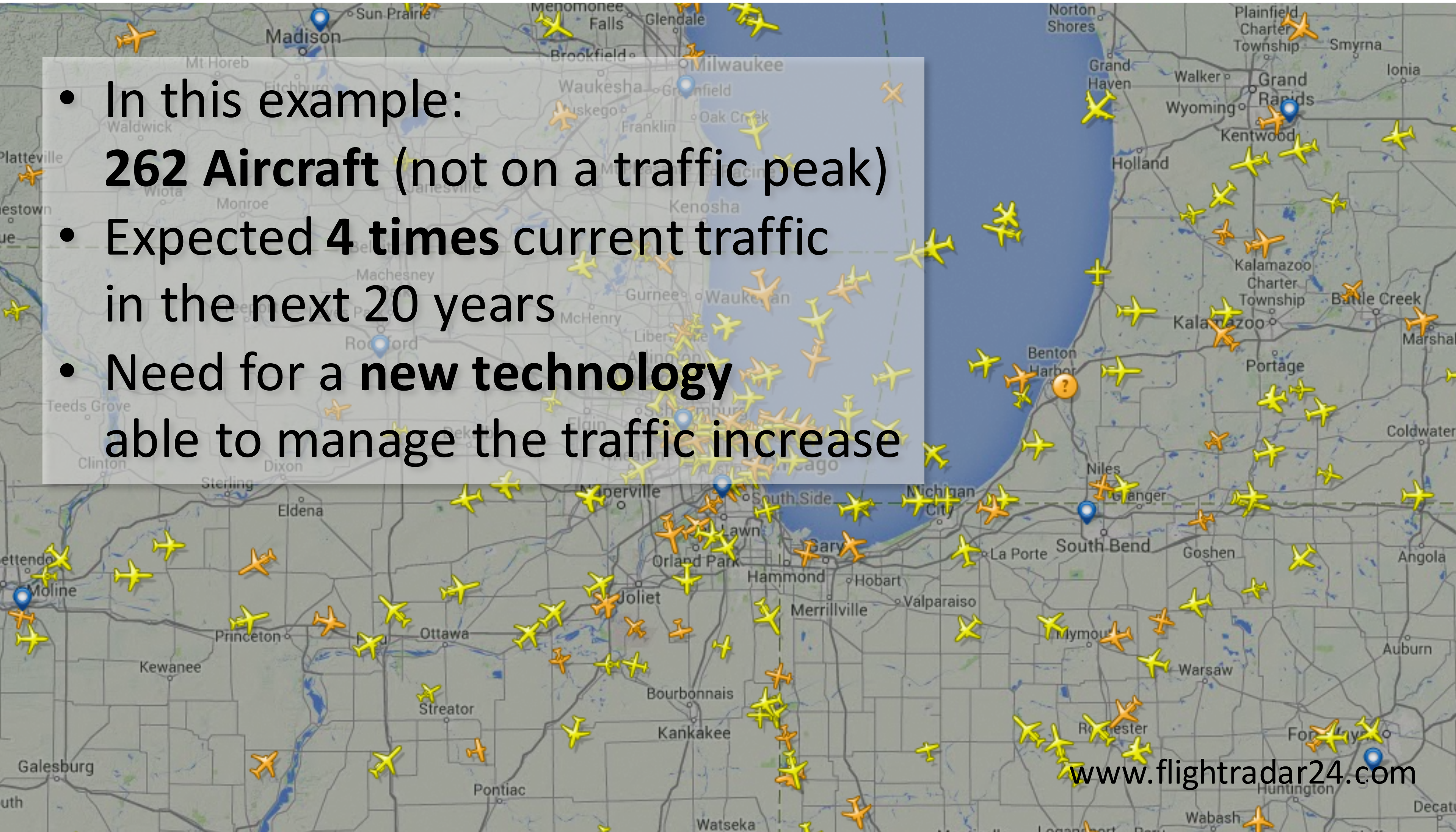
[2]University of Cincinnati, Ohio, USA

Air Traffic Control: Chicago-region Air Sector

www.flightradar24.com

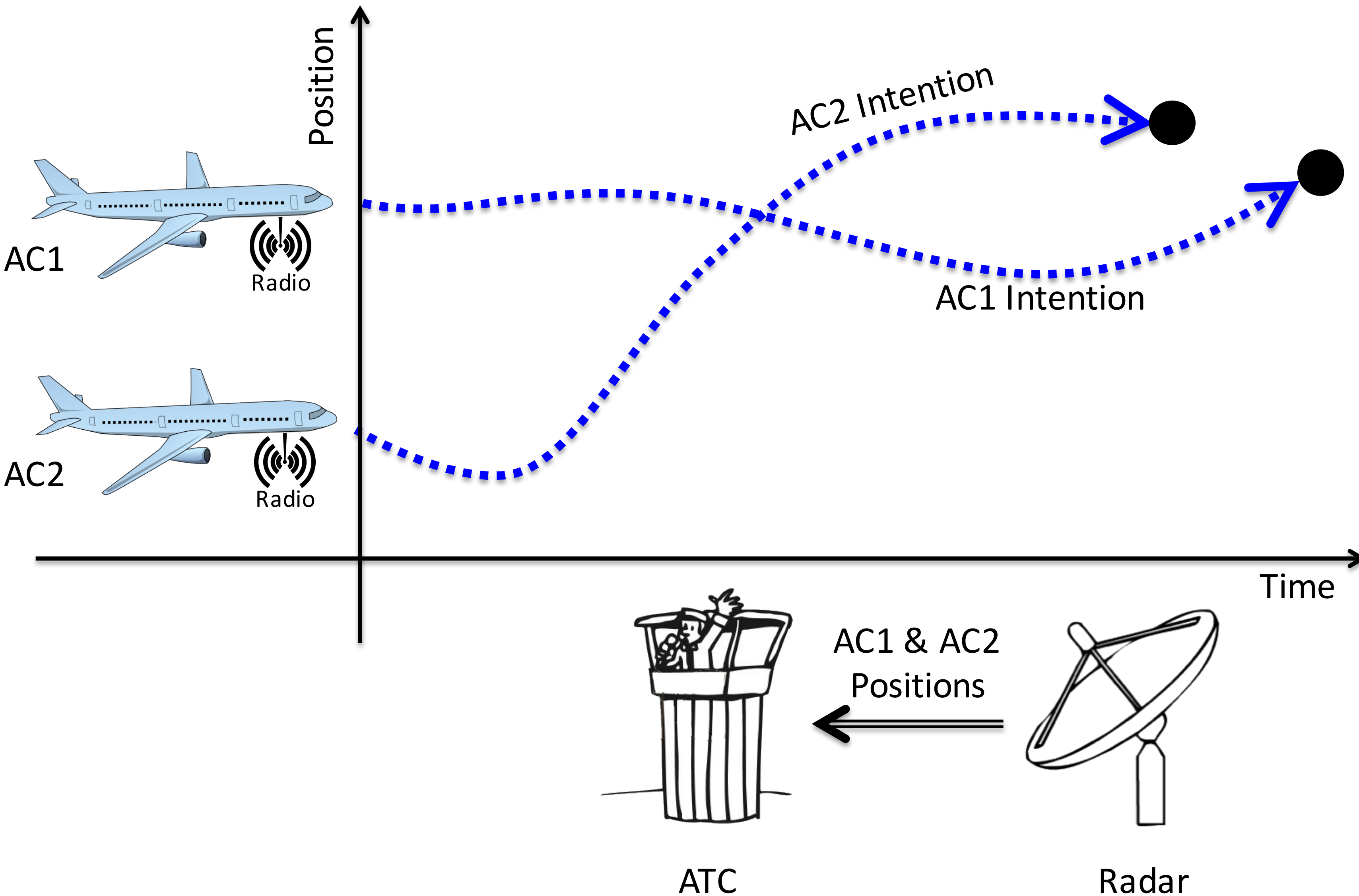
Air Traffic Control:
Chicago-region Air Sector

- In this example:
  262 Aircraft (not on a traffic peak)
- Expected **4 times** current traffic
  in the next 20 years
- Need for a **new technology**
  able to manage the traffic increase

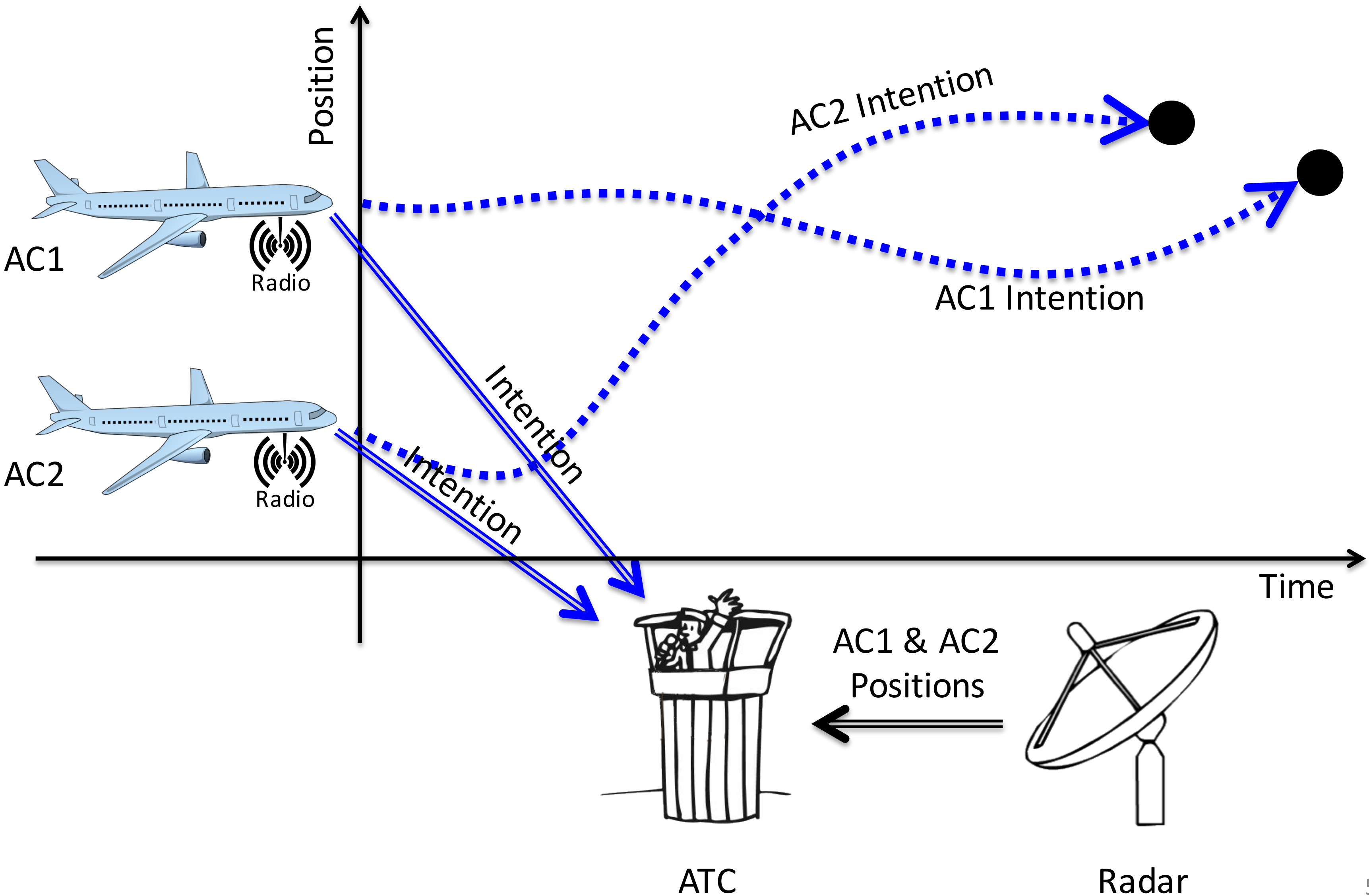


www.flightradar24.com

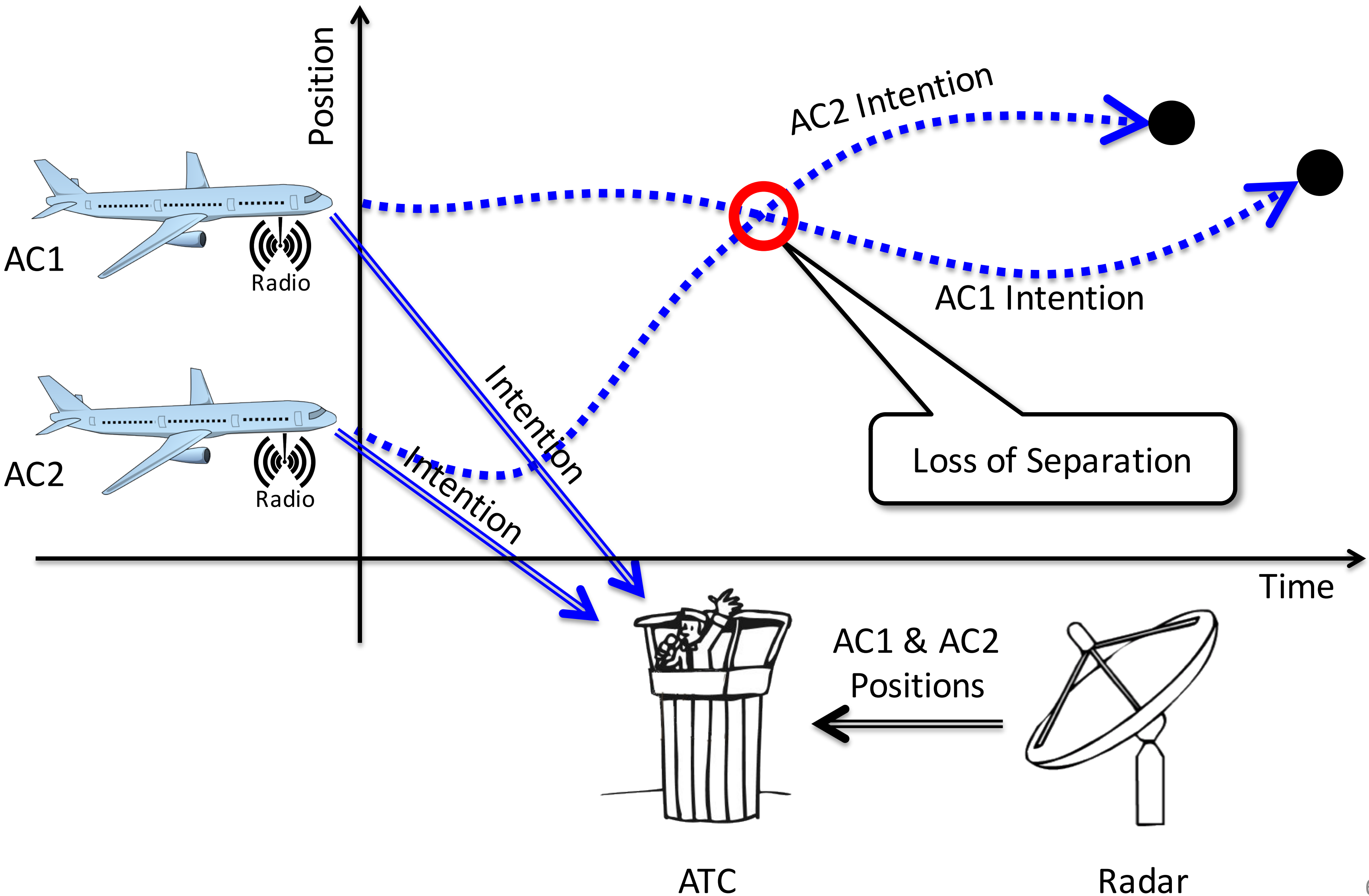
Air Traffic Control: Current Approach



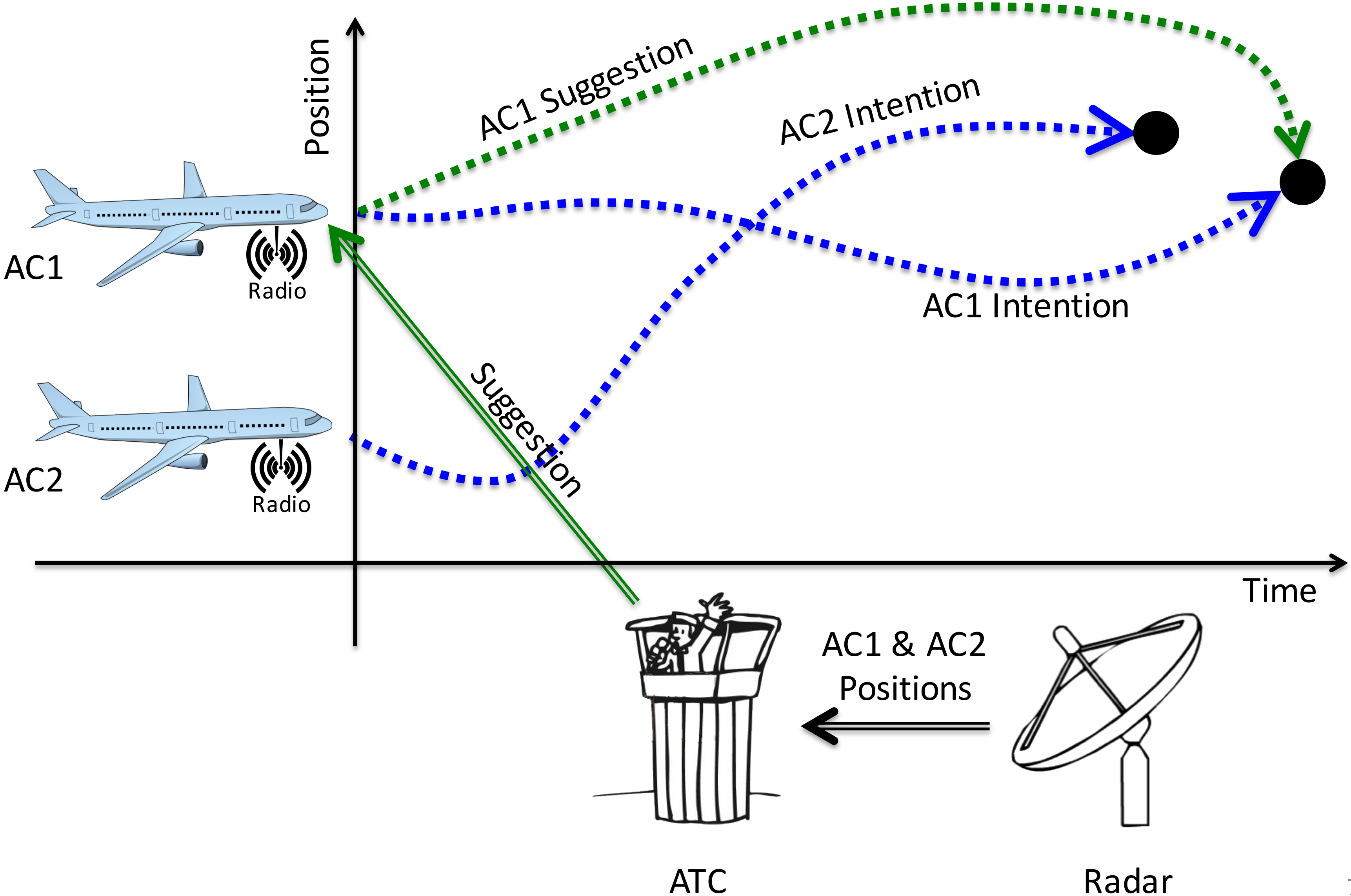
Air Traffic Control: Current Approach



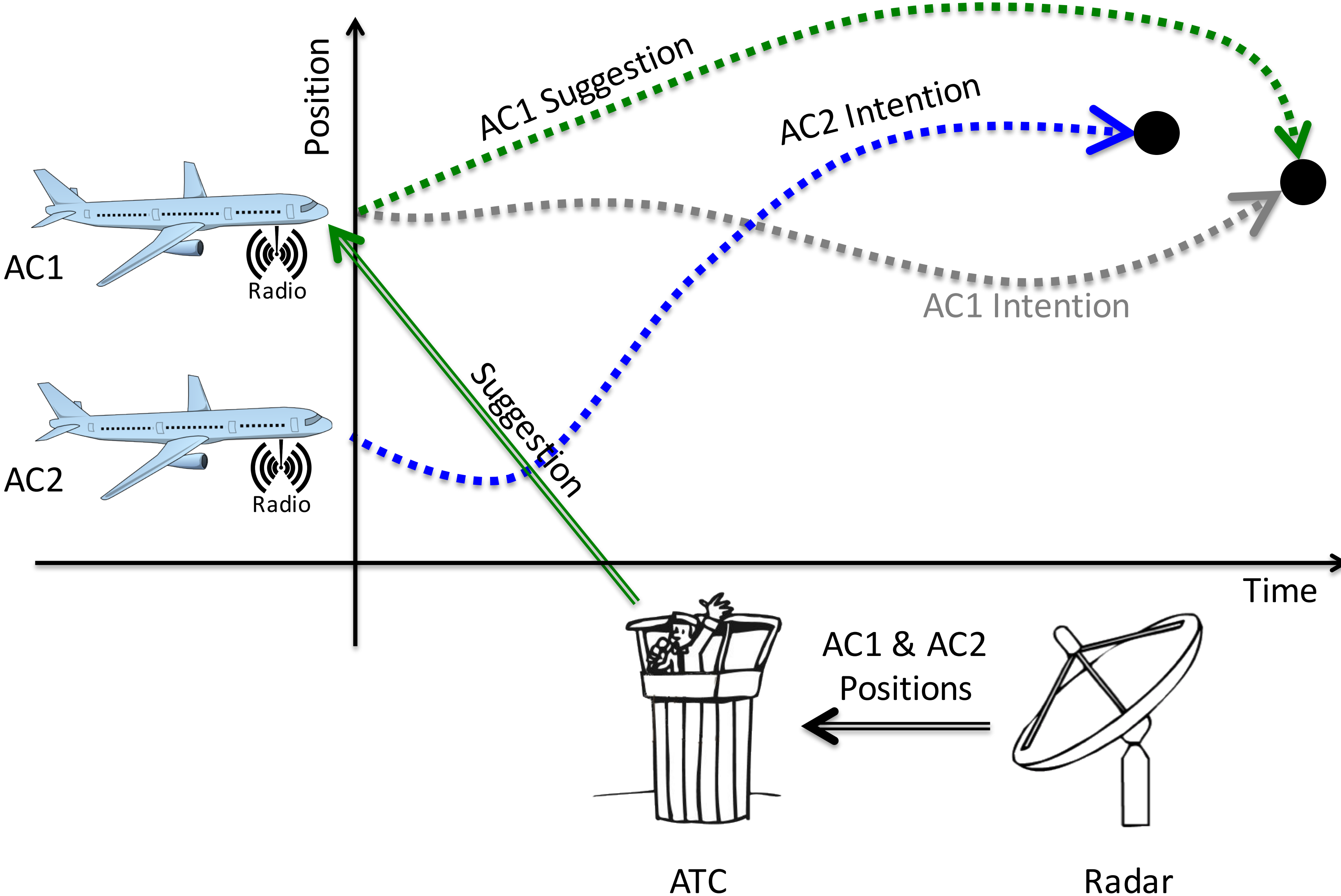
Air Traffic Control: Current Approach



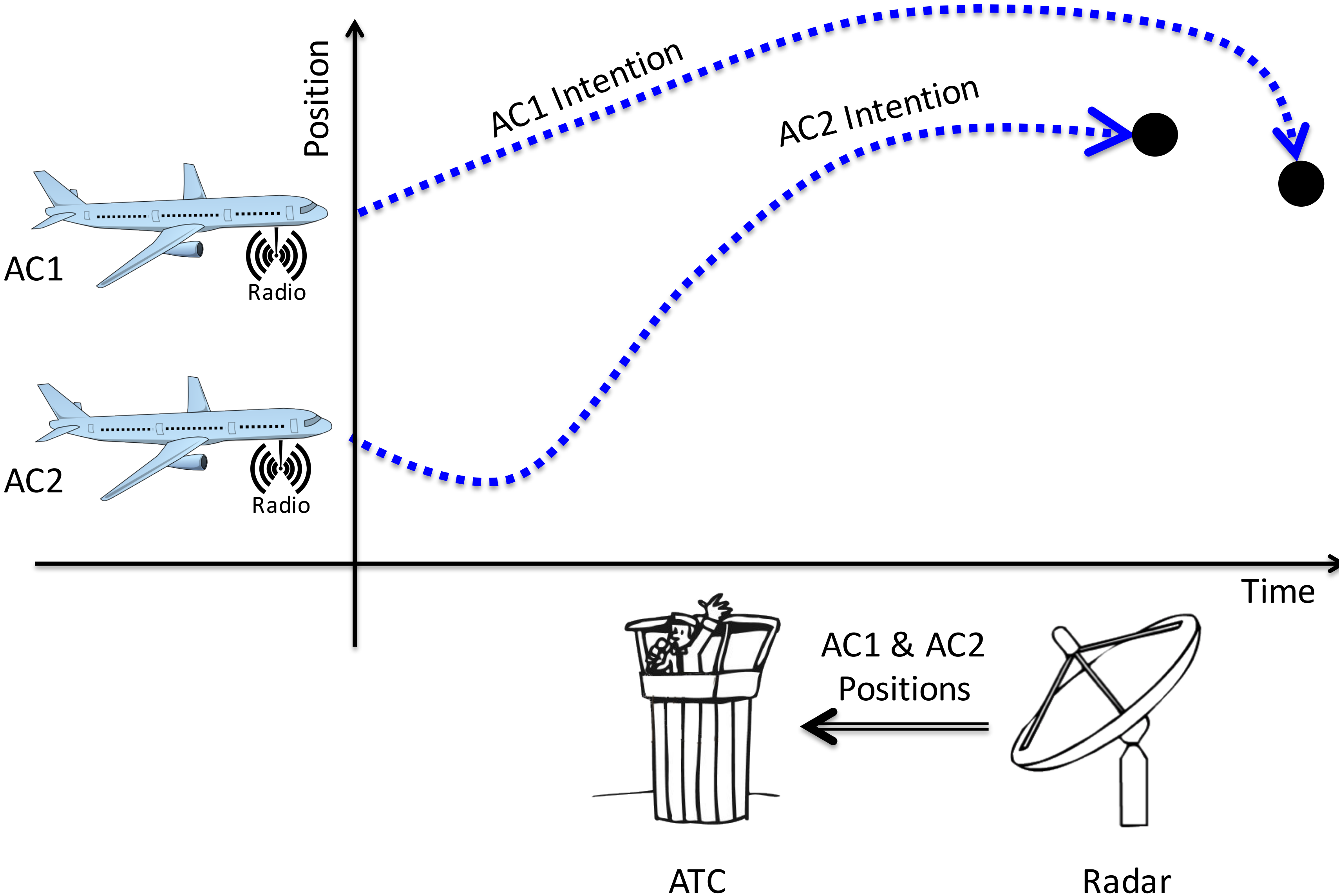
Air Traffic Control: Current Approach



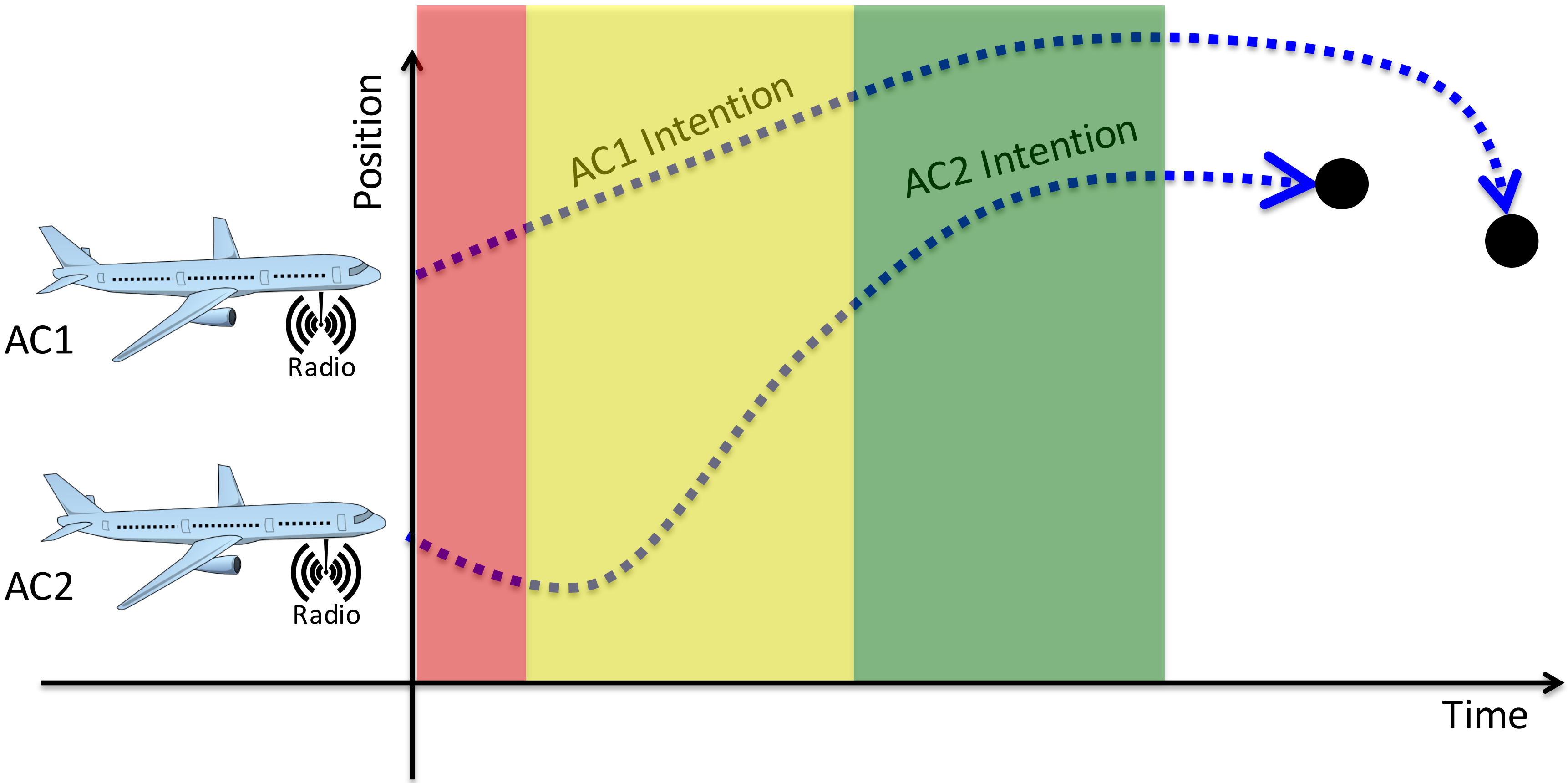
Air Traffic Control: Current Approach



Air Traffic Control: Current Approach

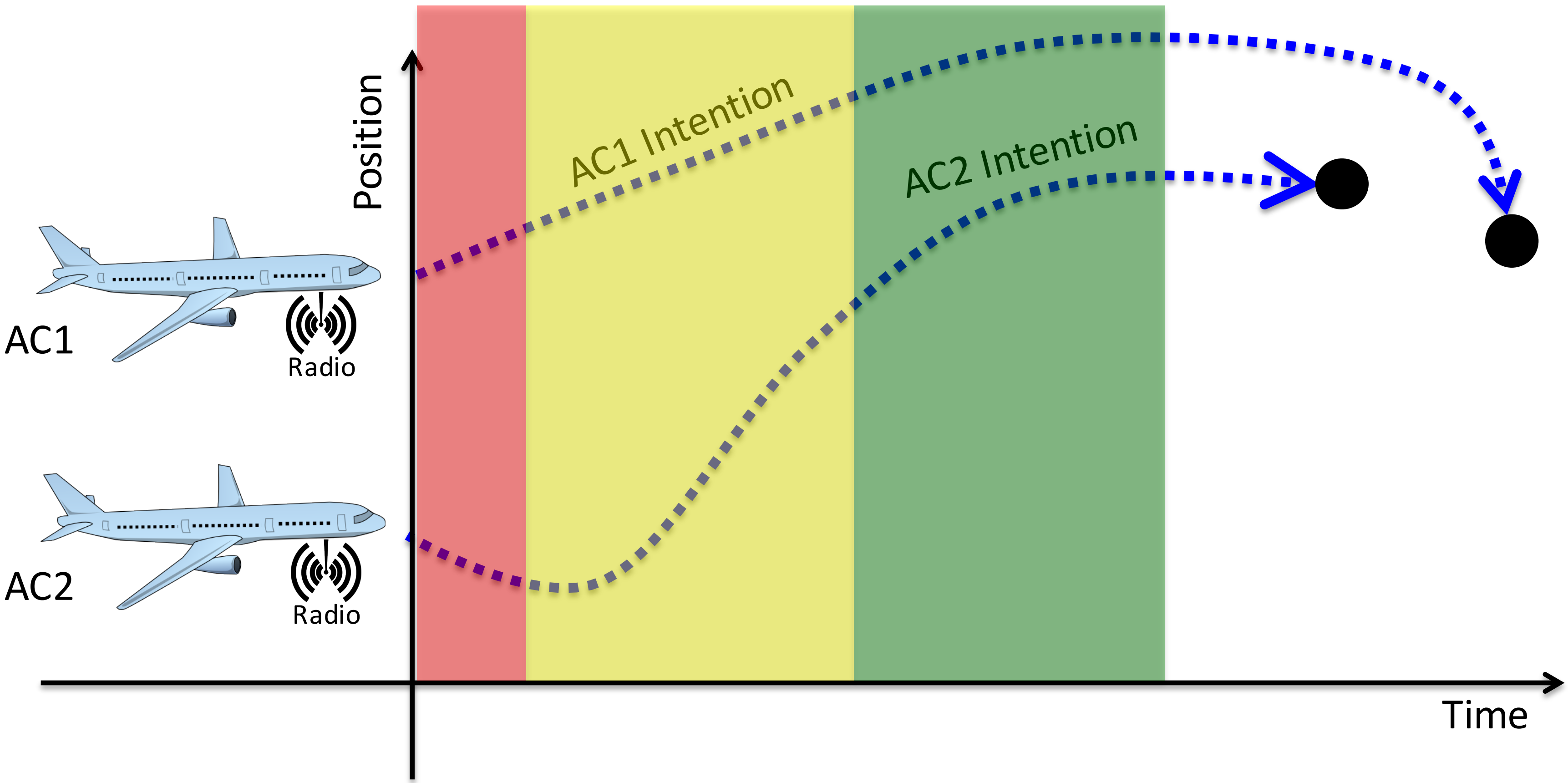


Air Traffic Control: Current Approach



	System Function	Technology	Allocation
(red)	Collision Avoidance	TCAS	On-Board
(yellow)	Tactical Separation	Controller/ATC	On-Ground
(green)	Strategic Separation	Controller/ATC	On-Ground

Air Traffic Control: Functional Allocation Questions



	System Function	Technology	Allocation
(red)	*Collision Avoidance*	*TCAS/ACAS-X*	*On-Board*
(yellow)	Tactical Separation	Controller/ATC	On-Ground **-> Distributed? On-Board?**
(green)	Strategic Separation	Controller/ATC	On-Ground **-> Distributed? On-Board?**

NASA project:
NextGen of the Air Traffic Control

- Need for a more **robust**, **reliable**, and **safe** approach
- A lot of different perspectives to be taken into account e.g., political and environmental impact, cost analysis, usability, safety, …
- Different **function allocations**, and implementations need to be analyzed

NASA NextGen of ATC:
The Functional Allocation Project

- Provide a **partial order** over the set of ways to allocate system functions, from a **safety** point of view
- Rely on a **Formal Validation, Verification, and Safety Assessment** approach, based on symbolic model checking
- Define formal model and system requirements from a **preliminary design** of the system architecture

NASA NextGen of ATC: The Functional Allocation Project

In this work

- **Formal modeling** of a set of different possible functional allocations
- Adaptation of **Formal Validation, Verification, and Safety Assessment** to compare early system designs
- **Real-world case study** from a tight collaboration with "Flight Dynamics, Trajectory and Controls Branch” of NASA Ames https://es-static.fbk.eu/projects/nasa-aac/

Formal Modeling for Comparative Analysis

Functional Allocation: GSEP and SSEP

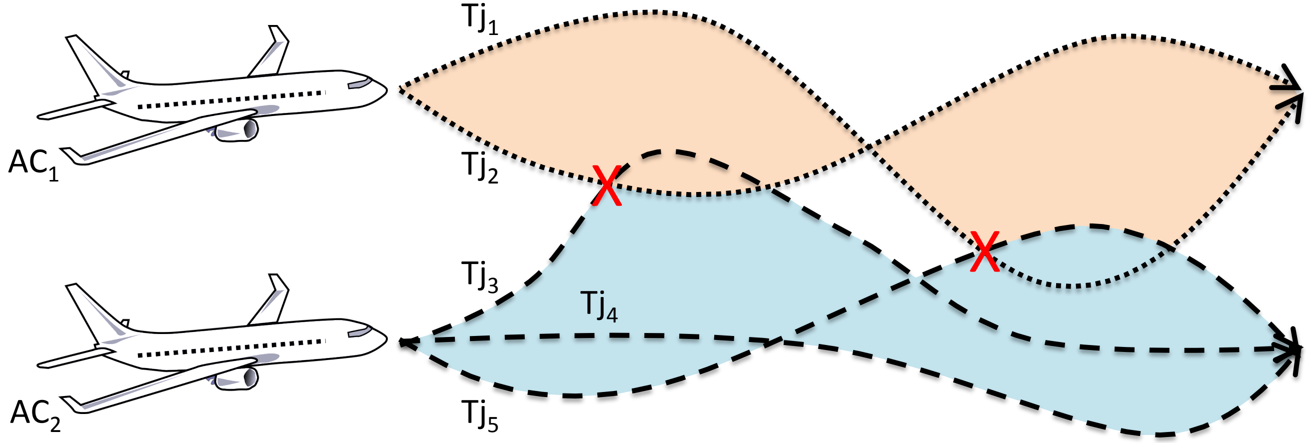
Current Approach:
Only Ground Separated Aircraft (GSEP)

	Collision Avoidance	**Tactical Separation**	**Strategic Separation**
TCAS/ACAS-X			
ATC			

With additional distributed Conflict Detection and Resolution (CD&R) on-board:
Ground and Self Separated Aircraft (SSEP)

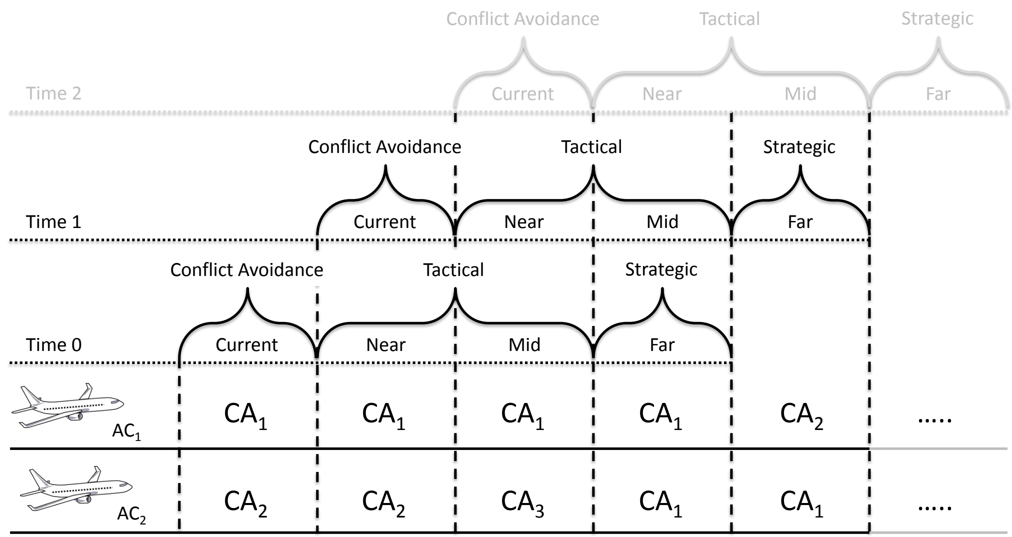
	Collision Avoidance	**Tactical Separation**	**Strategic Separation**
TCAS/ACAS-X			
ATC			Backup
CD&R OnBoard			Primary

Formal Modeling: Conflict Areas



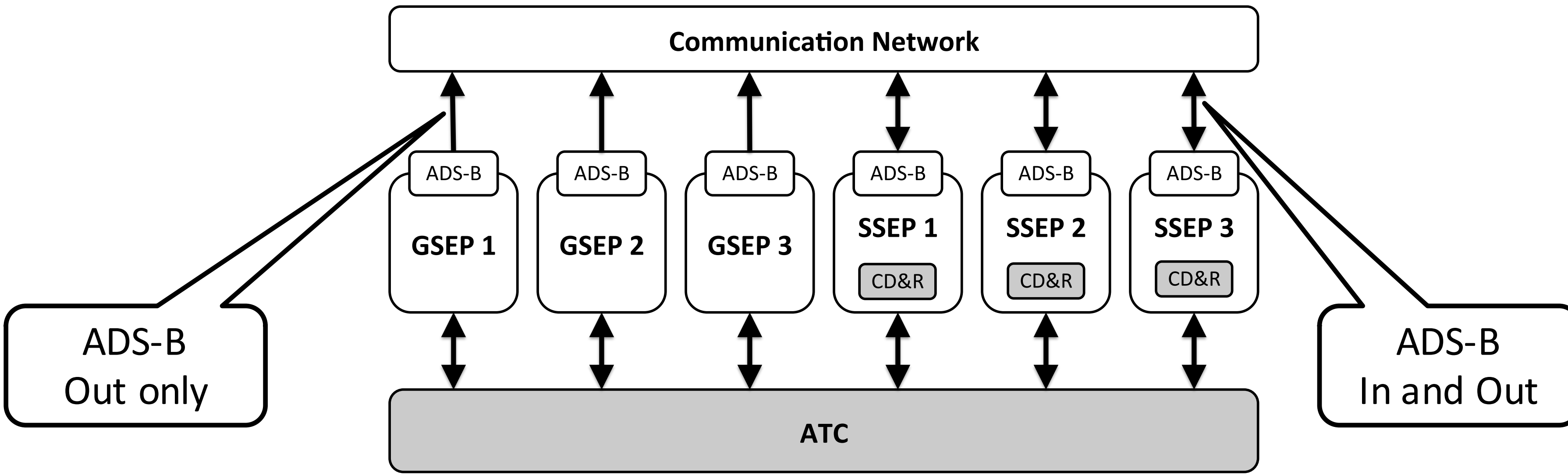
- Abstract concrete trajectories with Conflict Areas (CA)
- Two aircraft are in the same conflict area if their trajectories intersect in a given interval of time
- Example: if AC_1 and AC_2 follow T_{J2} and T_{j3} they are in the same Conflict Area

Formal Modeling: Time Windows



- Four different time windows:
  - Conflict Avoidance: Current
  - Tactical Separation: Near and Mid
  - Strategic Separation: Far
- The passage of a unit of time causes a window shifting
- A **Loss of Separation (LOS)** occurs when two aircraft are in the same CA in the current time window

Formal Modeling: System Components



- GSEP: Ground Separated Aircraft
- SSEP: Self Separated Aircraft with CD&R (Conflict Detection and Resolution) on-board
- ADS-B: Automatic Dependent Surveillance Broadcast

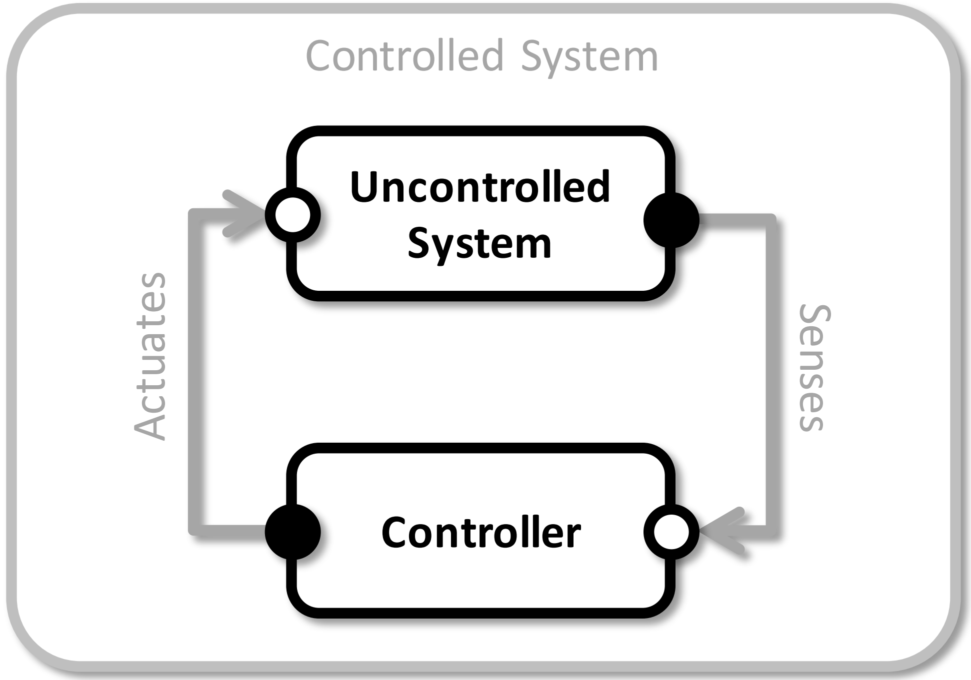
Formal Modeling: Scenarios Instantiation

Scenario Code	GSEPs	SSEPs	#Bool Vars
G	3	0	122
M1	3	1	185
M2	2	2	193
M3	1	3	201
S	0	3	146
ALL	3	3	353

- Non-Mixed (only G/SSEP) and Mixed (both G/SSEP) operations considered
- Multiple implementation options (Enabled or Disabled)
  - GSEP-Far: GSEPs send Far intentions over ADS-B Out
  - SSEP-Far: SSEPs send Far intentions to ATC.

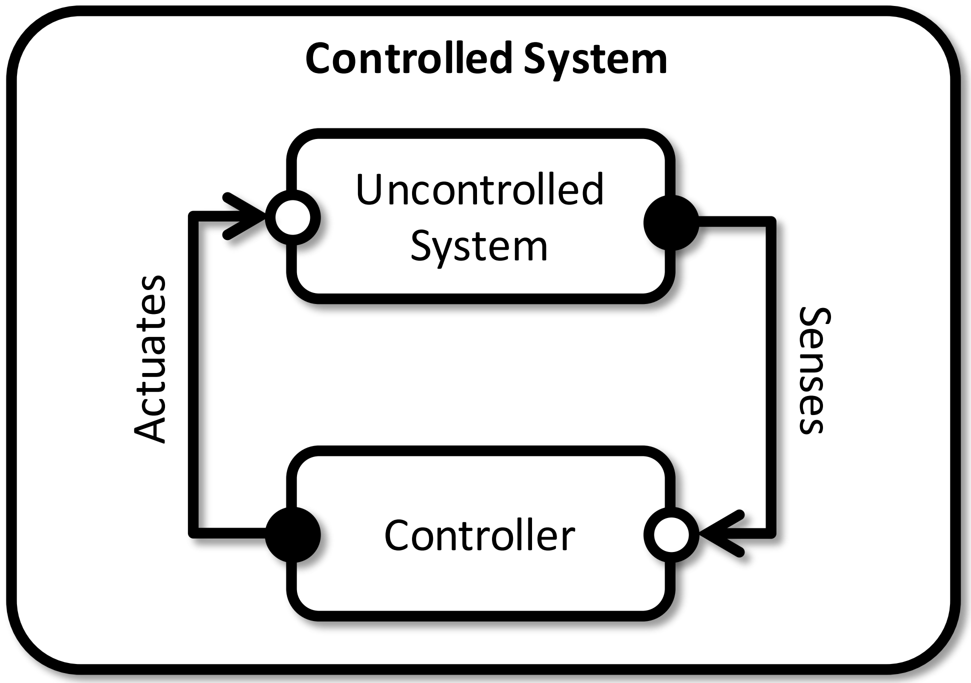
Formal Validation and Verification

Formal Validation



- Pure Airspace as **Uncontrolled System** and CD&R agents (ATC, and CD&R on-board) as **Controllers**
- Separated Validation for Uncontrolled System and Controllers
- All 37 properties CTL and LTL properties validated using nuXmv model checker

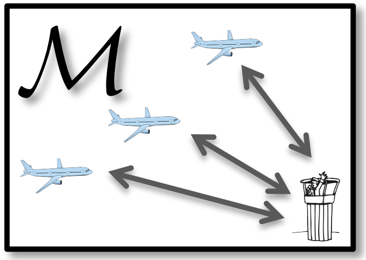
Formal Verification



- 93 LTL properties verified, using nuXmv, on all 20 possible configurations (of the controlled system) by varying:
  - Number of involved GSEPs and SSEPs aircraft
  - Information sharing implementation
- Outcome: table representing pass/fail results

Formal Safety Analysis

Formal Validation and Verification



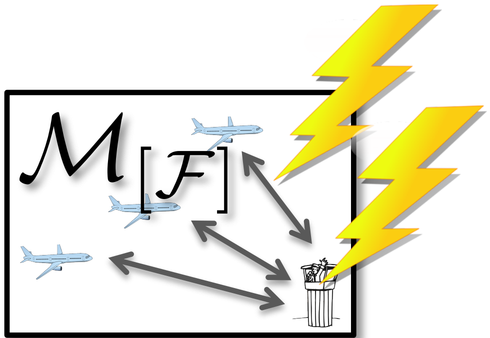
It is not possible to reach a Loss of Separation. φ

$$\mathcal{M} \models \varphi$$

Yes

No + Counterexample

Formal Safety Assessment



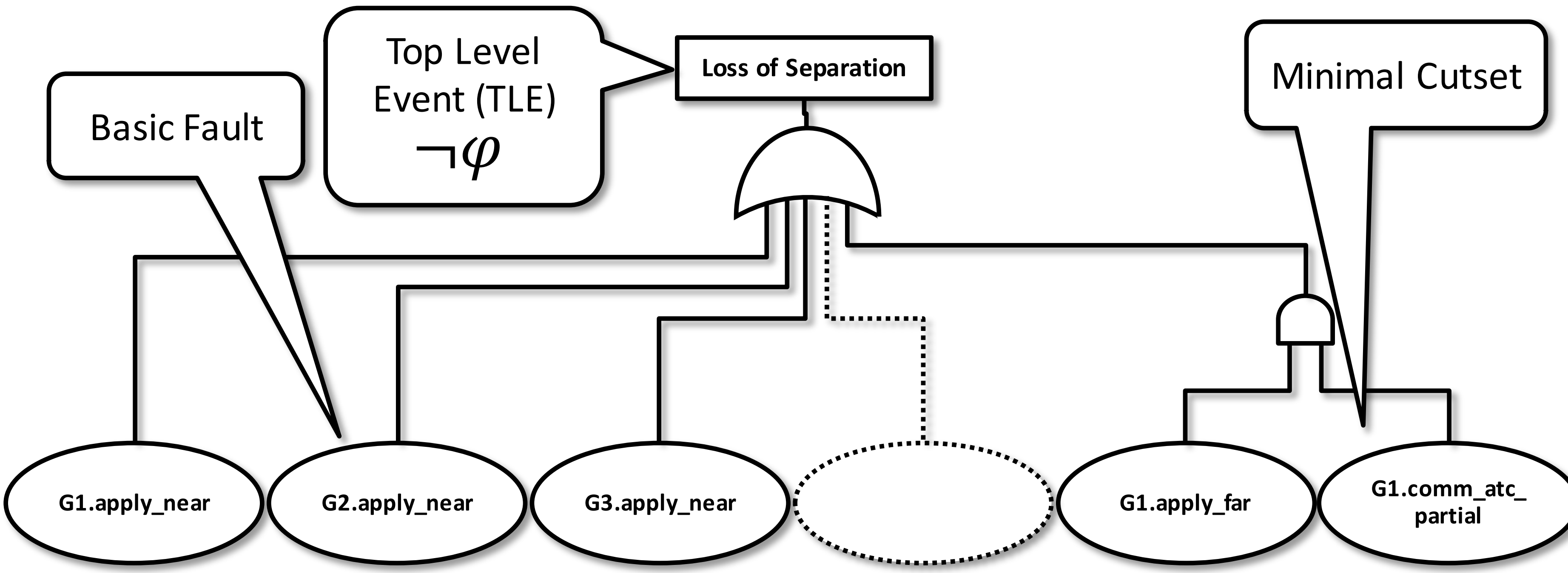
It is not possible to reach a Loss of Separation. φ

$$\delta(\mathcal{F}) : \mathcal{M}_{[\mathcal{F}]} \not\models \varphi$$

All possible assignments to ***F*** such that ***M*** does not satisfy **φ**

Fault Tree

Formal Safety Assessment: Fault Tree Analysis



- Fault Tree Analysis as **Minimal Cutsets Computation** [Bozzano et al. CAV15] via xSAP
- CS={f_1,…,f_n} is a cutset of M, φ if there exists a counterexample π of $\mathrm{M} \vDash \varphi$ that triggers f_1,…,f_n
- A Cutset CS is Minimal iff $\forall\, CS' \subset CS$, CS' is not a cutset of M, φ

Formal Validation, Verification, and Safety Assessment Process

- Formal Requirements and Model Validation
  - Outcome: positive results for all checks
- Formal Model Verification
  - Outcome: table where the cell i,j expresses whether the configuration i satisfies or not the property j.
- Formal Safety Assessment
  - Outcome: a Fault Tree for each pair of configuration, property… **How do we compare them?**

Formal Safety Assessment: Minimal Cutsets Comparison

MCS Cardinality	3GSEPs-1SSEP (M1)		2GSEPs-2SSEPs (M2)		…
	GFar	¬GFar	GFar	¬GFar	
0	0	0	0	0	…
1	5	5	5	5	
2	12	15	12	16	
3	33	24	35	23	
…	…		…		…

- Impact on the "Loss of Separation" when varying the sharing of GSEPs Far intentions (GFar):
  - Same number of single point of failure (5)
  - While double failure increases (¬GFar), triple failures decreases

Formal Safety Assessment: Minimal Cutsets Comparison

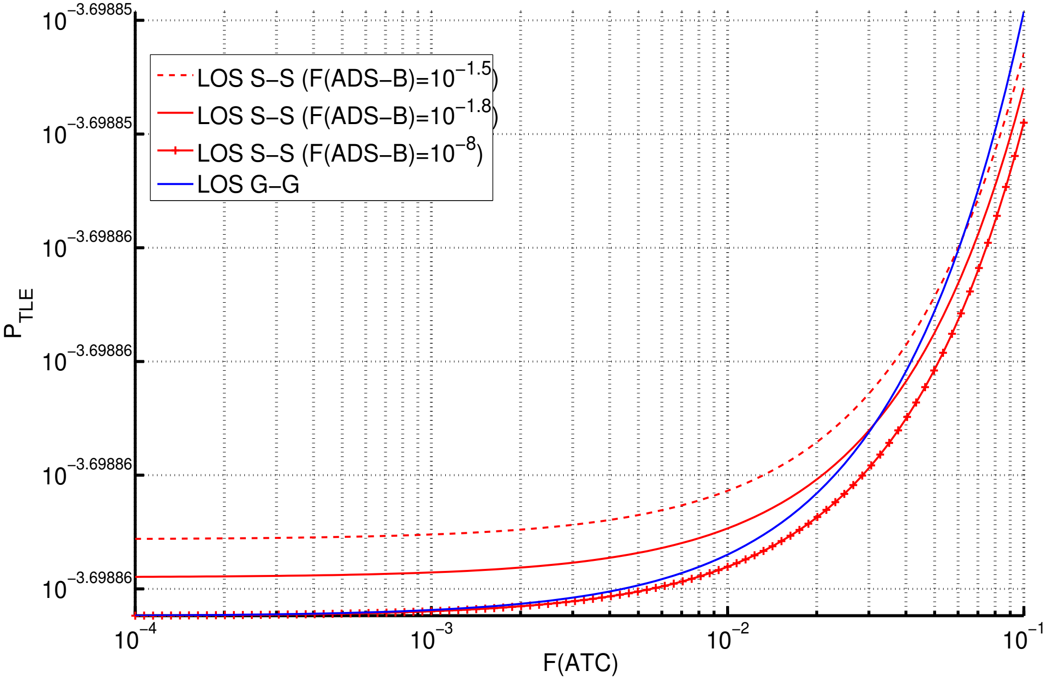
- Analyze set relations between Minimal Cutsets i.e., MCS are set of set of faults

- Compare the MCS with TLE as “LoS between SSEP and GSEP” varying GSEP-Far (GF) information sharing:
  - $\mathbf{MCS_{\neg GF}}$ = {<…>, {F_{ATC}}}
    F_{ATC} = G.F_comm_ATC_tot, S.F_comm_ATC_tot
  - $\mathbf{MCS_{GF}}$ = {<…>, {F_{ATC}, ATC.F_mid_res},
    {F_{ATC}, ATC.F_far_res},
    {F_{ATC}, G.F_comm_adsb},
    {F_{ATC}, S.cdr.F_future_resolve, S.cdr.F_resolve_detection}

Formal Safety Assessment: Reliability Function Evaluation

- Set relation over Minimal Cutsets might be inconclusive i.e., two sets can be incomparable
- From **Minimal Cutsets** to **Reliability Function** (P(TLE) : $\mathbb{R}^n \mapsto \mathbb{R}$) [Bozzano et al. ICECCS15], assuming no faults dependency
- Analyze under which condition one Reliability Function dominates the others

Formal Safety Assessment: Reliability Function Evaluation



- Loss of Separation between SSEPs and GSEPs as TLE, varying P(failure ATC) and P(failure ADS-B). Other probability of failures are fixed
- Still conceptual design, thus numerical values are not yet defined

Conclusion and Future Works

Conclusion

- Modeling of a **real-world case study**, from a **conceptual** architecture description
- Application and tailoring of a comprehensive **Formal Validation, Verification, and Safety Assessment** process to evaluate different functional allocations
- Collaboration with "Flight Dynamics, Trajectory and Controls Branch” of NASA Ames to **support decision making**

Future Works

- Extend the modeling to cope with the whole set of Functional Allocations and Scenarios i.e., **> 1600**
- Integration with **Compositional Modeling and Verification**
- Evaluation of **overlapped supervision** i.e., with more than one ATC
- Analysis of the impact of **Unmanned Autonomous Systems**

Thank you!

Comparing Different Functional Allocations in Automated Air Traffic Control Design

- *Modeling with Conflict Areas and Time Windows*
- *Formal Validation and Verification, controlled and uncontrolled system*
- *Safety analysis via minimal cutsets and reliability function computation*
- Website: https://es-static.fbk.eu/projects/nasa-aac/

Cristian Mattarei - mattarei@fbk.eu