Paper 120
6th USA/EUROPE Air Traffic Management R&D Seminar
Baltimore, Maryland, USA
June 27-30, 2005

SAFETY ANALYSIS FOR ADVANCED SEPARATION CONCEPTS

John W. Andrews and Jerry D. Welch
MIT Lincoln Laboratory

Heinz Erzberger
NASA Ames Research Center

***This work is sponsored by NASA Ames under Air Force Contract #FA8721-05-C-0002. Opinions, interpretations, recommendations, and conclusions are those of the author and are not necessarily endorsed by the United States Government.**

Capacity Goal and Safety Questions

Goal:

Use advanced techniques to handle traffic at 2 or 3 times the current density.

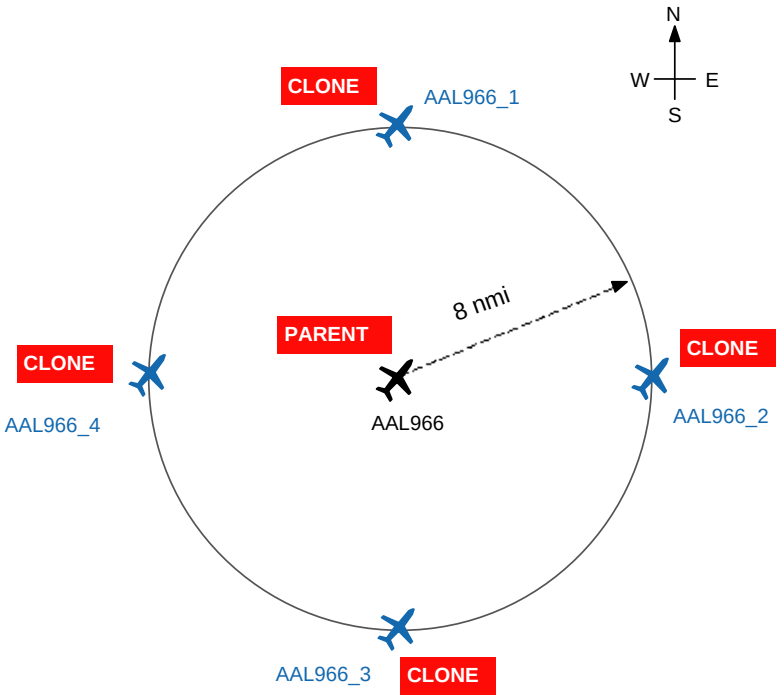
Safety Questions:

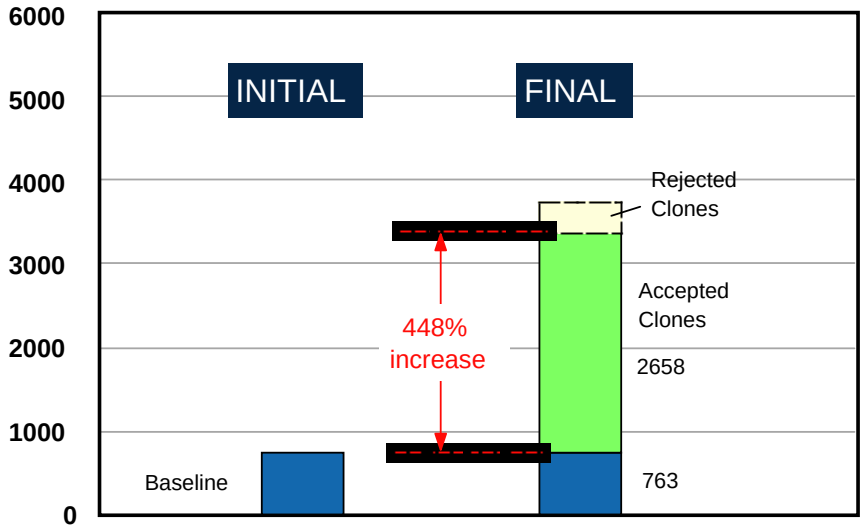
- **Can the required level of safety be attained?**
- **What are the priorities for safety research?**

The System Outage Conundrum

Since automation can fail, how can traffic density be increased beyond the density that can be safely handled *without* automation?

Cloning Experiment



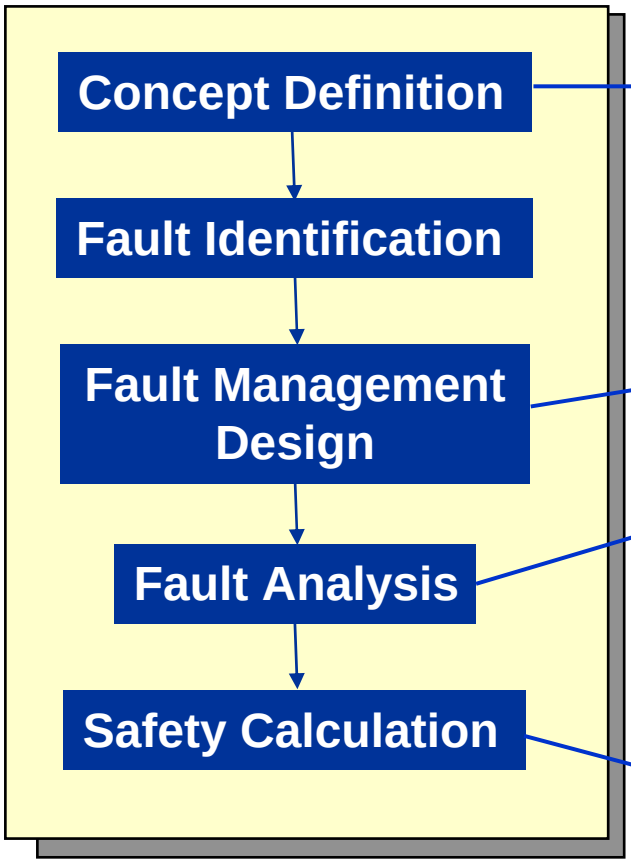


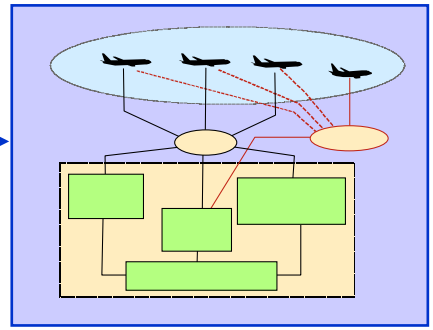
- *87% of clones were acceptable.*

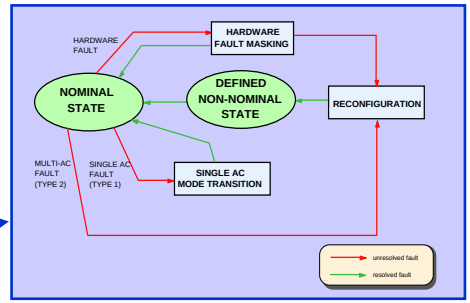
Conclusion: A sufficient number of conflict-free trajectories can be found despite the increased traffic density.

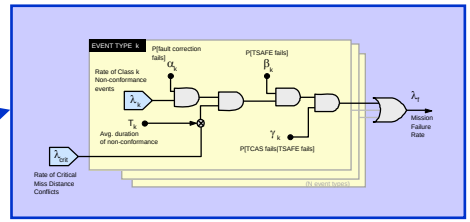
Ref: Andrews, J.W. "Capacity Benefits of the Automated Airspace Concept (AAC)", 42PM-AATT-0014, M.I.T. Lincoln Laboratory, 17 August 2001

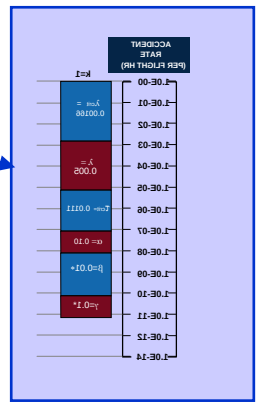
Safety Assessment for AAC



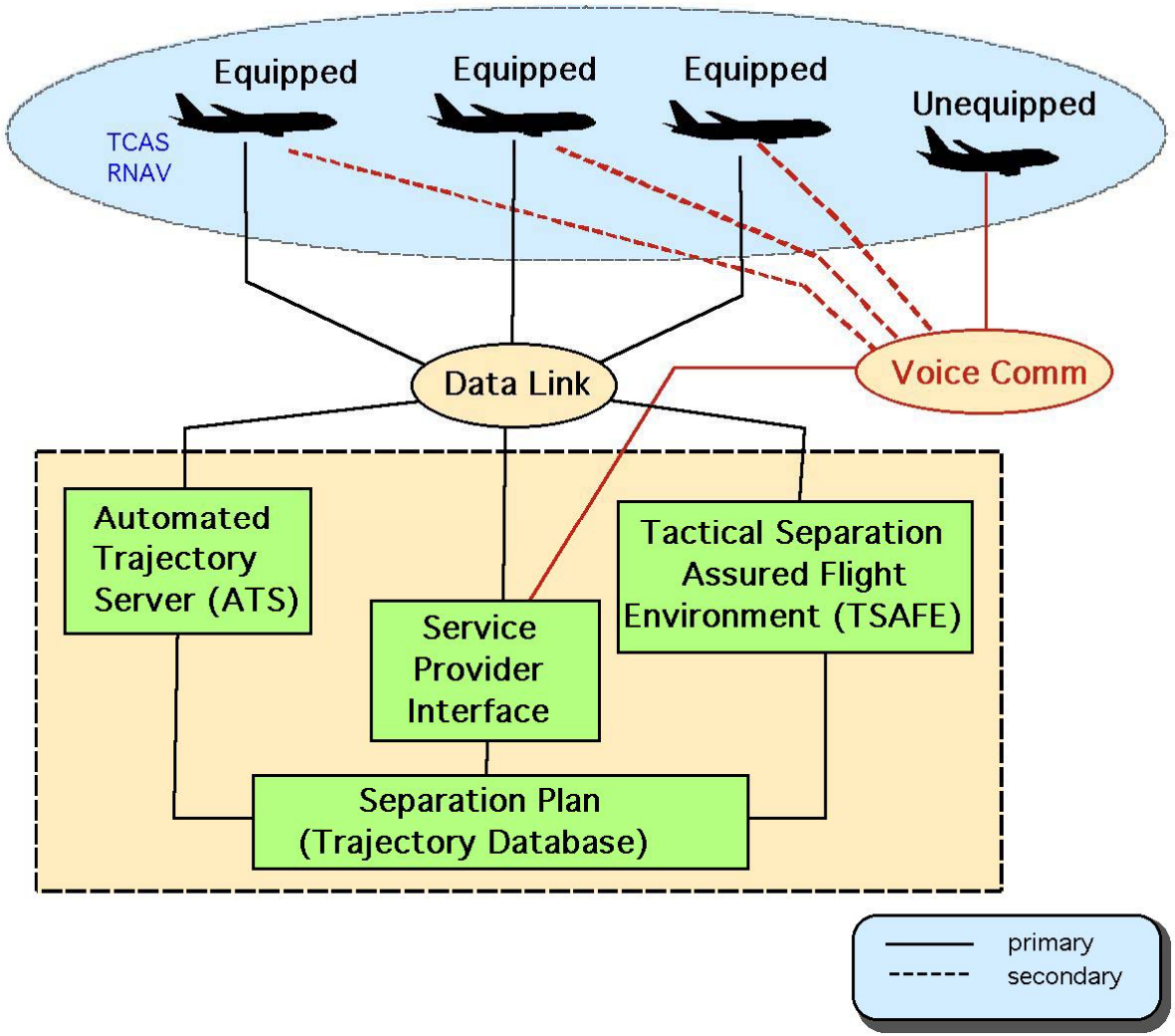








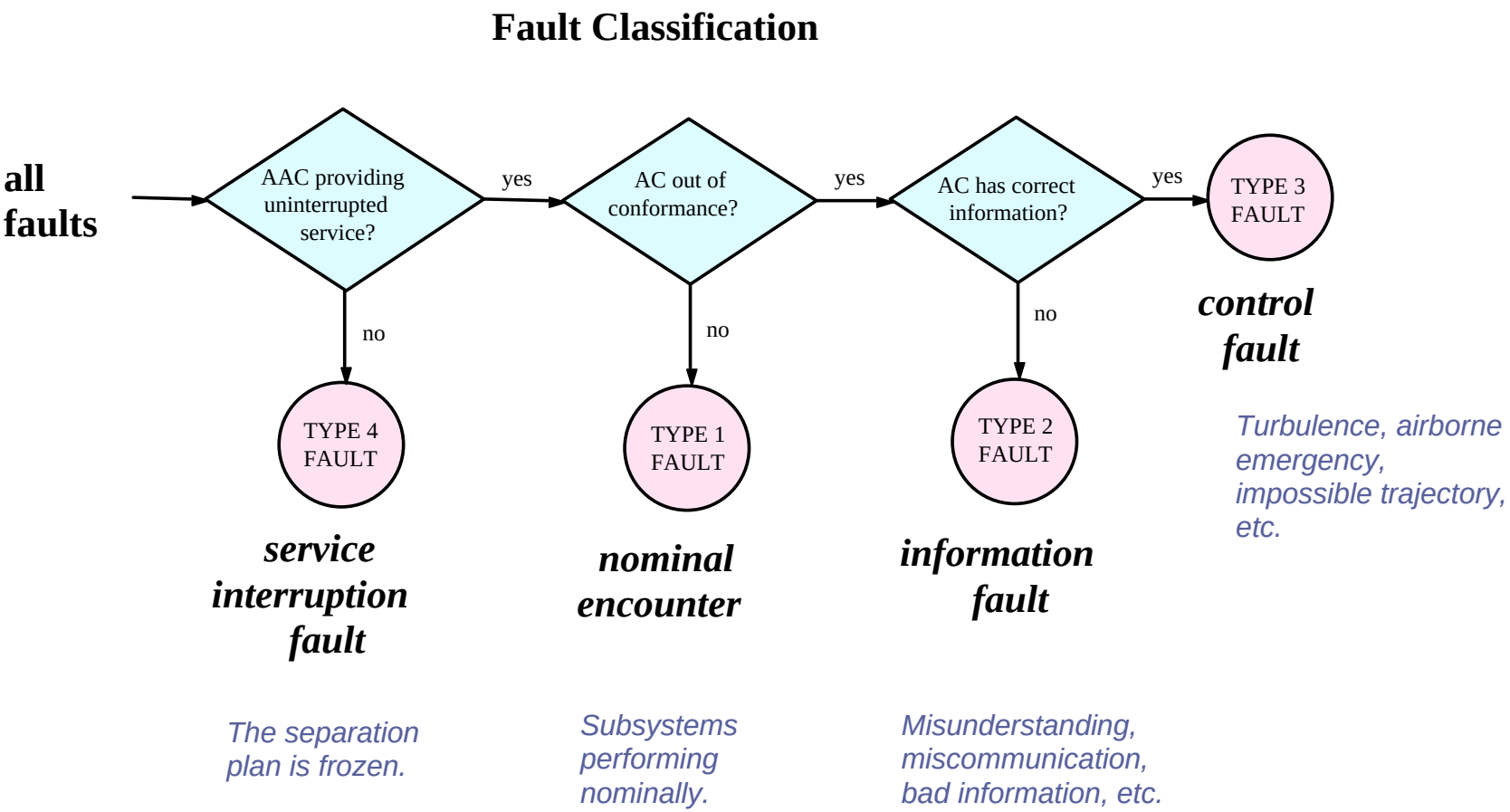
Advanced Airspace Concept



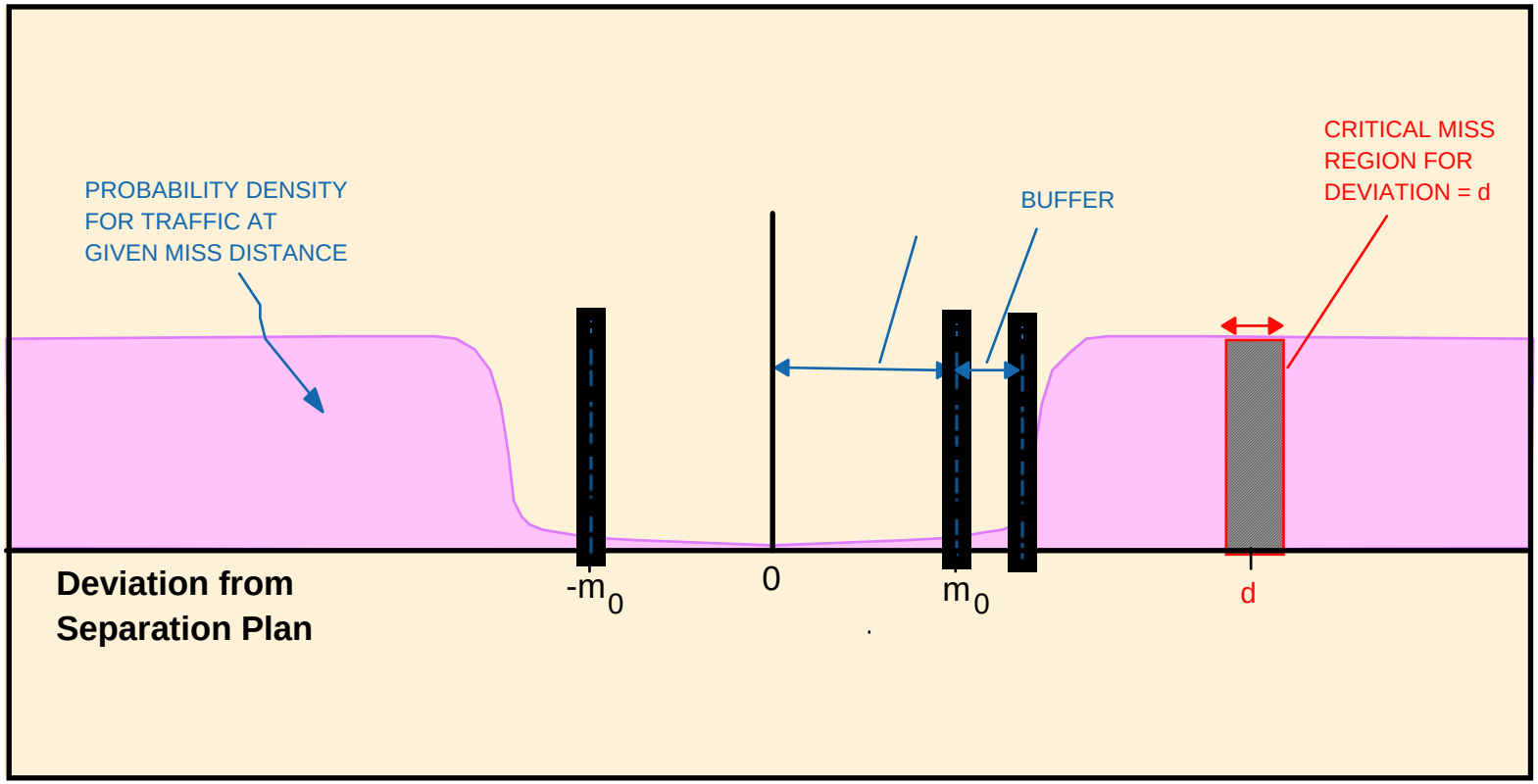
Key Operating Principles

- No update process is allowed to compromise the safety of the Separation Plan.
- The Separation Plan is rapidly and easily modified to accommodate user requests or to optimize itself in response to new data.
- The Separation Plan is available for inspection.

Four Types of Faults

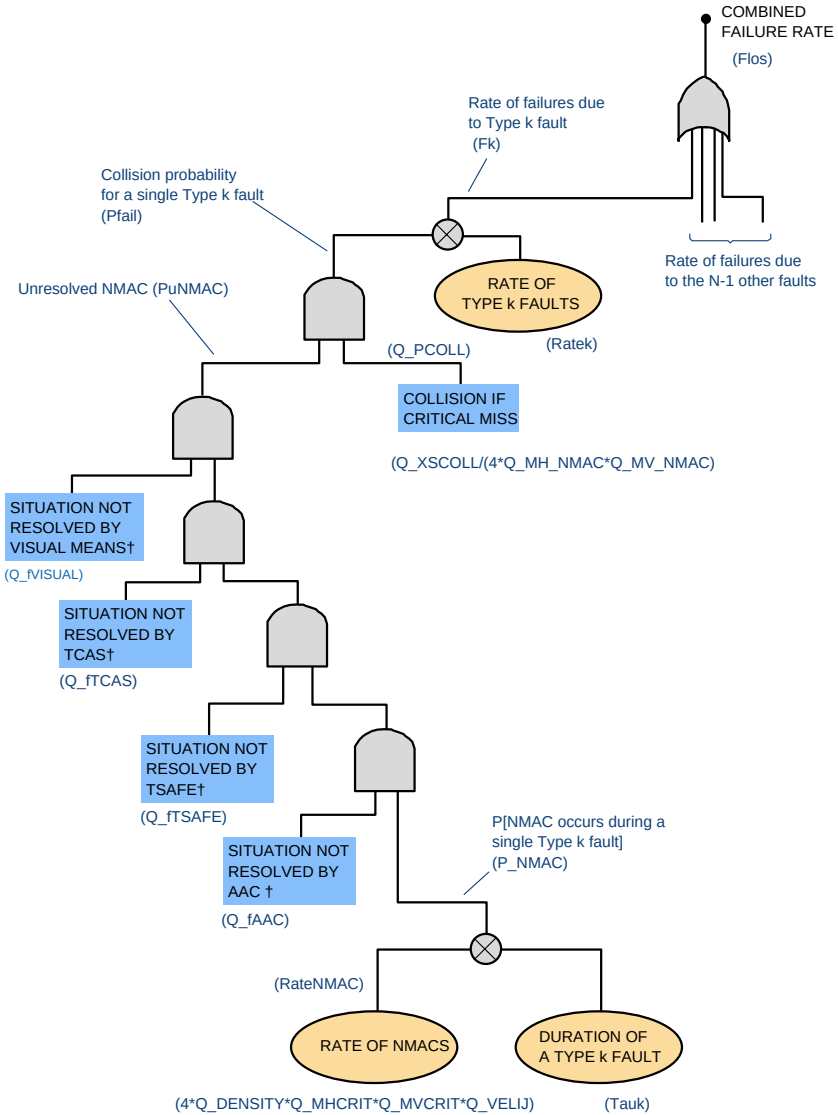


Risk Model for Non-Conformance



Modeling Approach: Non-conformance exposes aircraft to critical miss encounters for a certain time period (until restoration of conformance)

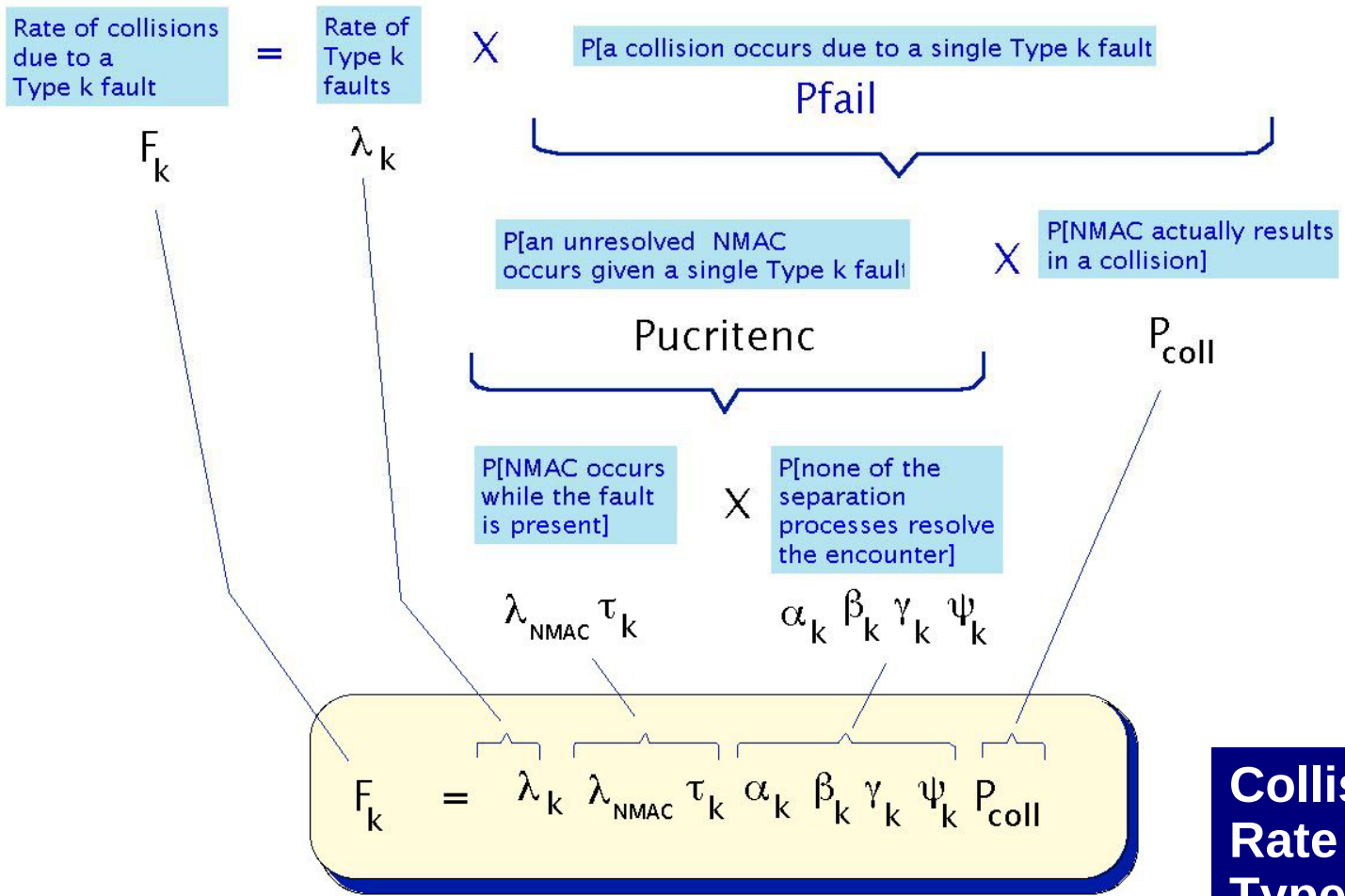
Fault Tree Analysis



- **A fault tree analysis allows the risk from each fault to be estimated.**

- **Probabilities are estimated from**
  - **historical statistics**
  - **ACASA safety model (for TCAS II in Europe)**
  - **postulated AAC design goals**

Risk Calculation



Collision Rate due to Type k Fault

NMAC = Near Mid-Air Collision (500 ft. lateral/100 ft. vertica

Type 4 Fault: Service Interruption

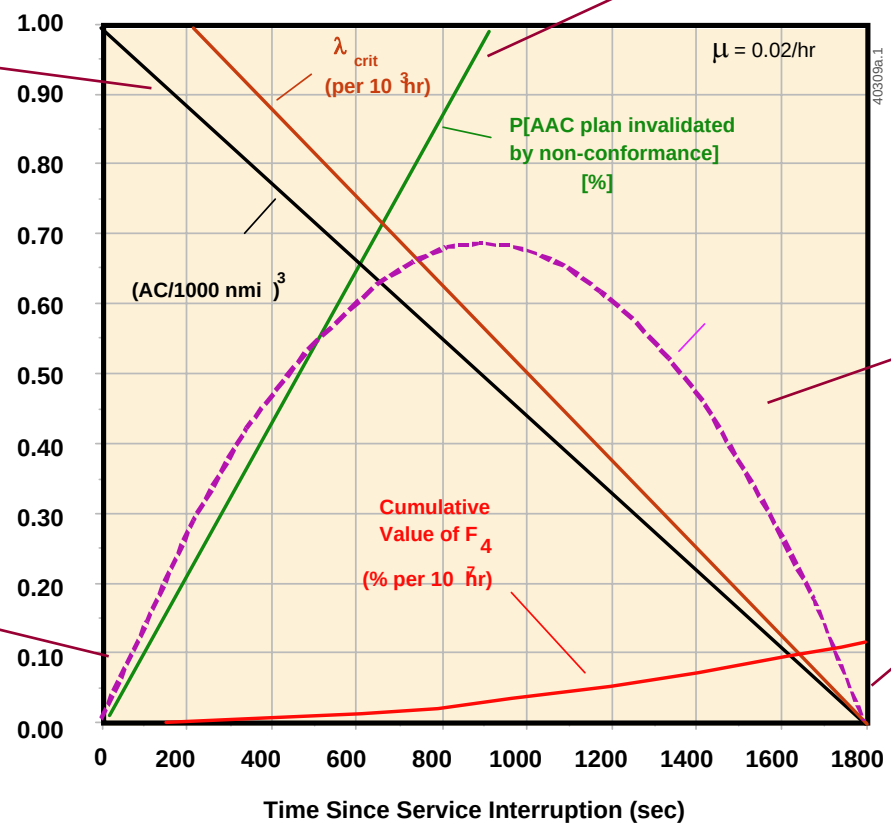
Key Assumptions

- AAC service is terminated for all aircraft in the supersector.
- No other aircraft are allowed to enter the sector.
- Aircraft have been given conflict-free trajectories to the point of exit from the sector.
- Aircraft attempt to follow the trajectory in effect at the time of the service interruption.
- Once an aircraft loses conformance, it never regains it.
- Service is not restored until after the sector is cleared of traffic.

Dynamics of a Type 4 Fault

The probability of lost conformance increases with time.

Traffic density within the sector decreases

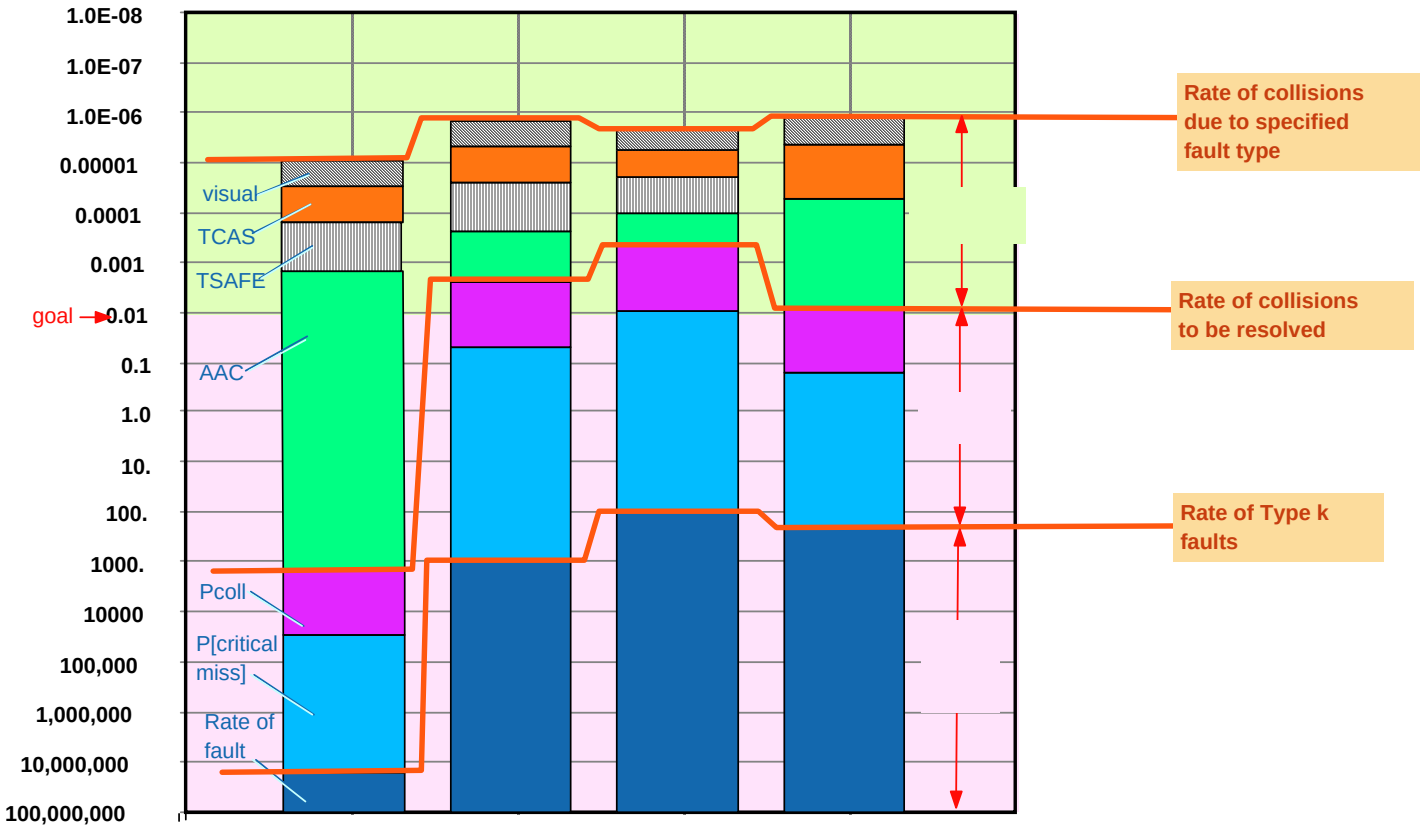


The rate of collision peaks near the mid-point of the risk period.

Risk is zero initially since AC are coasting on the original plan.

Risk is zero at end since sector has been cleared of traffic.

Safety Assessment



AAC Design Features for Safety
(Mature AAC)

- Fully specified trajectories (4D)
- Secure Plan Transmission (via data link)
- Independent safety monitors for Separation Plan
- Onboard conformance assurance
- TSAFE
- Rapid replanning
- Fully cognizant back-up
- Conflict-free extension to active trajectory segment
- Mature safety management system

Safety Advantages of AAC

- **Reliable communication of the separation plan**
  - Datalink is orders of magnitude more reliable than voice communication of clearances.
- **Plan can be validated by independent monitors**
  - Not possible if plan is in the mind of a sector controller
- **Conflict-free planning horizon increased by factor of four or five**
  - Outages pose less immediate risks than in current system.
- **Tactical separation back-up (TSAFE) built upon full knowledge of intent of traffic**
  - TCAS has no intent information.
- **System-wide fault detection and reporting**
  - Goal: Every failure is detected, reported, and analyzed to enable effective system safety management.

Conclusions

- **Fault-based analysis is useful in assessing the safety of advanced concepts.**
- **With appropriate designs, concepts such as the Advanced Airspace Concept have significant *safety advantages* over conventional control.**
- **The four fault types analyzed so far do not appear to prevent satisfaction of the ICAO level-of-safety requirement**

The End

Thank You!