

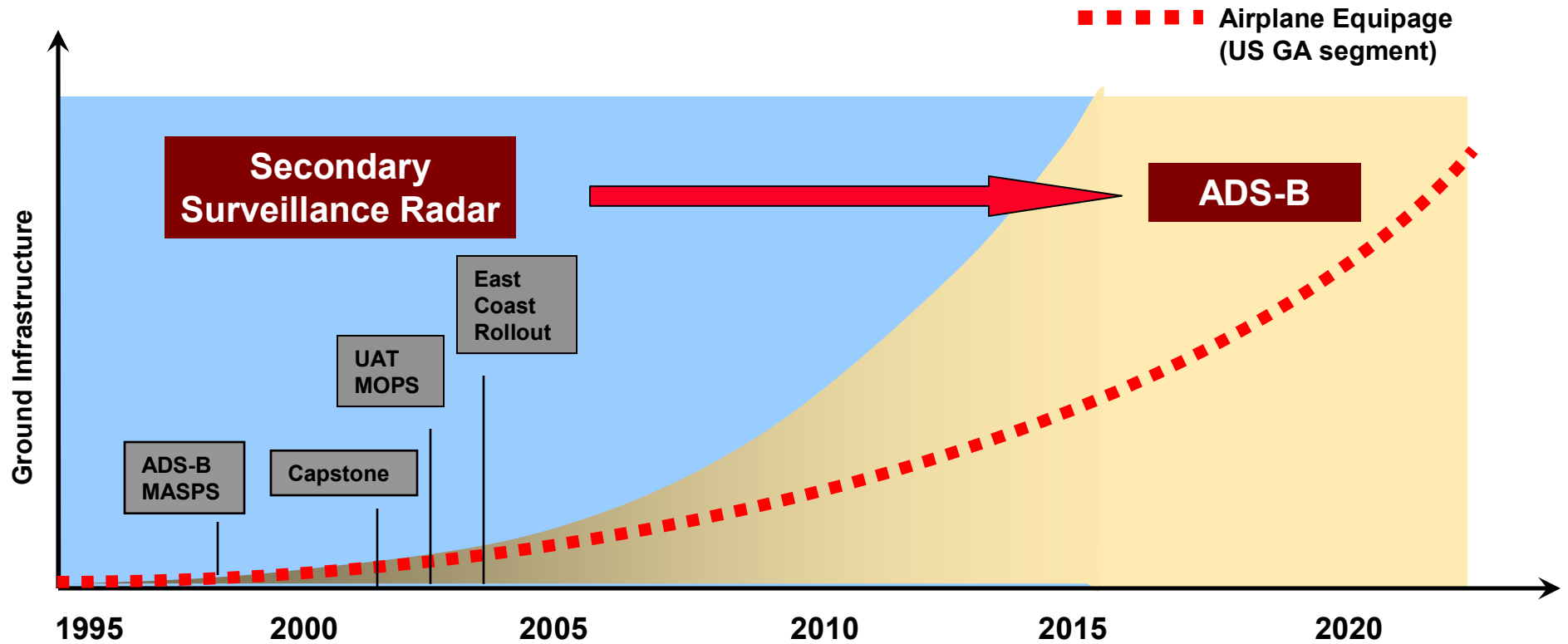
Enhanced ADS-B

Cooperative Research and Demonstration Project

NASA Glenn and Sensis Corporation

Ken Samuelson, Principal Investigator

Aviation Surveillance Projection



Consideration of ADS-B Enhancements is motivated by Surveillance Technology Trends

Overview - Enhanced ADS-B Project

Objective: Explore protocol enhancements that enable a more robust datalink

Desirable characteristics

- **Securable**
- **Transactional**
- **Sufficient effective bandwidth**

Constraints

- **Minimize impact on existing standards**
- **Preserve fundamental openness of ADS-B**

Focusing on ADS-B UAT

UAT has the greatest potential for growth of the ADS-B links

FIS capability

Project Approach

□ Phase 1: Enhancements that provide selective security features within existing MASPS constraints

- Authentication***
- Encryption of message fields***

Using Washington DC ADIZ as a representative Special Use Airspace (SUA)

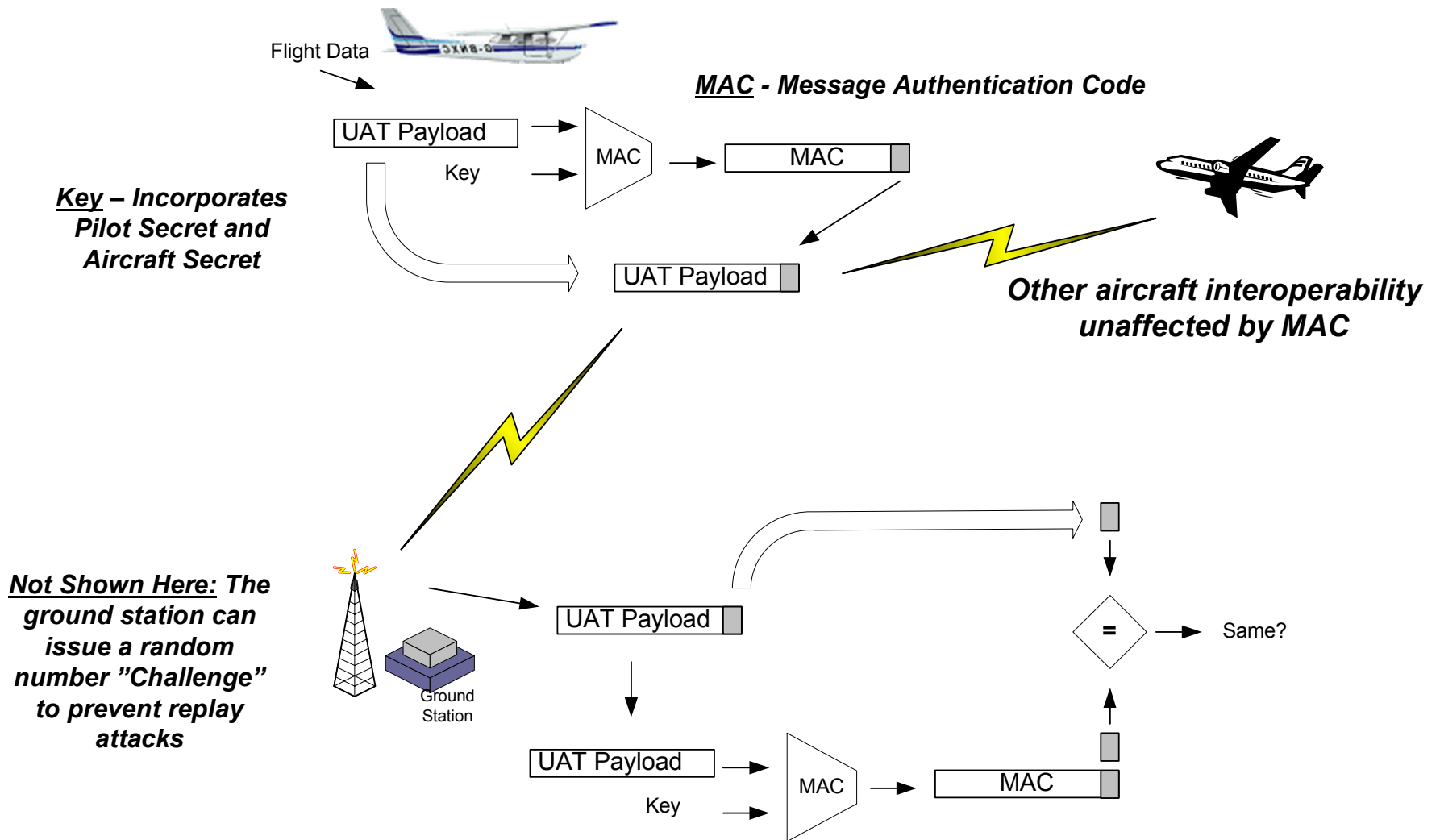
□ Phase 2: Enhancing capacity for additional applications including transactional link

- Changes to access protocol***
- Changes to the modulation scheme***

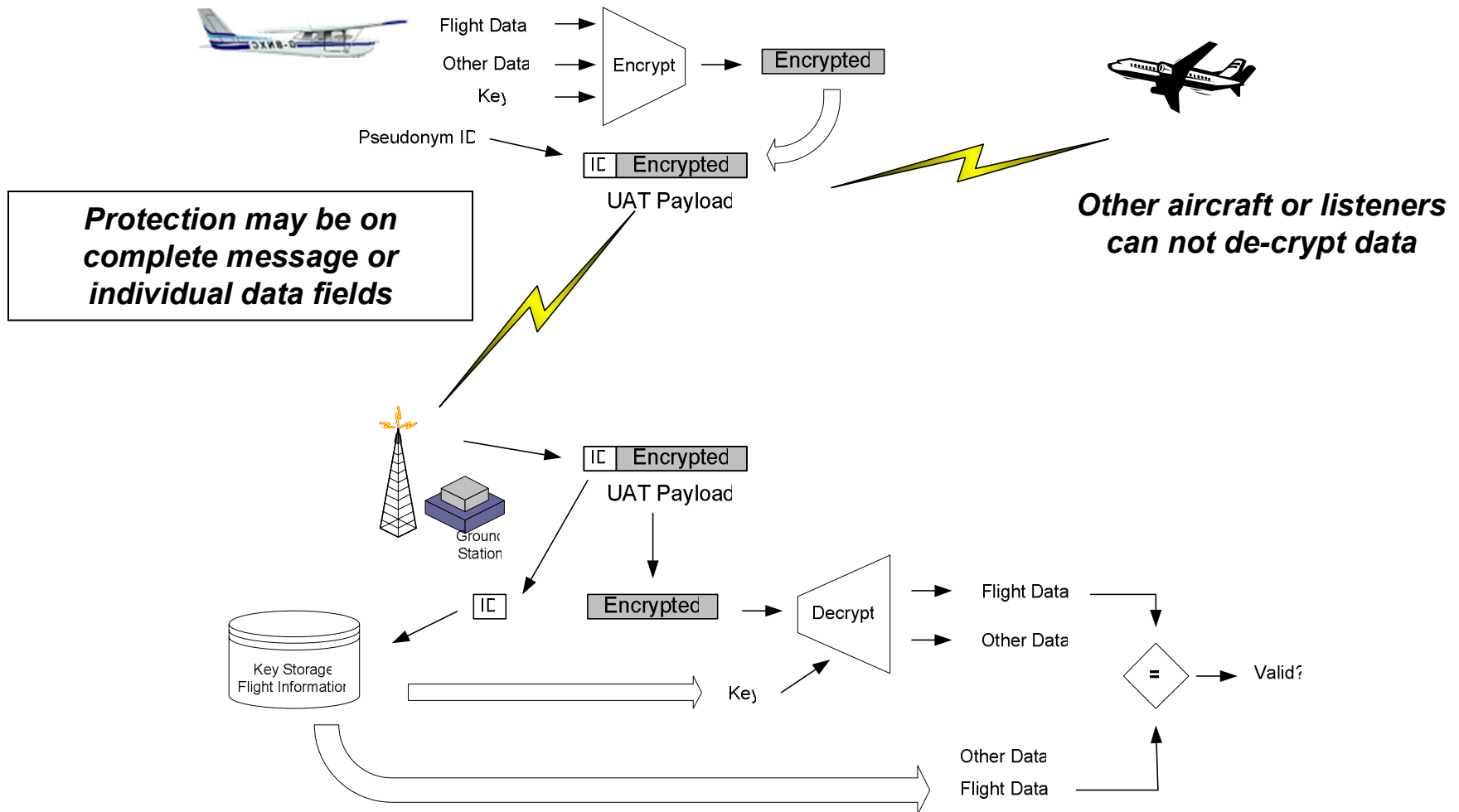
Security Enhancements Technical Approach

- 1. Investigate and demonstrate a selectable, secure data link by providing aircraft information message authentication signature**
 - **Enables automated, verifiable, authentication of aircraft Information**
 - *Aircraft ID, Pilot ID, Cargo Certification, etc.*
- 2. Investigate and demonstrate a selectable, secure data link by providing ground station information message authentication signature**
 - **Enables aircraft verification of ground message data**
 - *FIS, TIS, Rebroadcast, Flight Plan authorization data, etc.*
- 3. Investigate and demonstrate encryption for selective hiding of certain pieces of aircraft information on the data link**
 - **Enables message data hiding**
 - **Enabled by ground key exchange**
 - **Investigating: airborne key exchange, requires increased capacity through modulation and/ or access protocol changes on data link**
- 4. Investigate and demonstrate capability for secure data link transactions between air/ ground**
 - **Provide bandwidth and security such that secure transactions between individual pilot and ground are possible**

Authentication Construction and Comparison



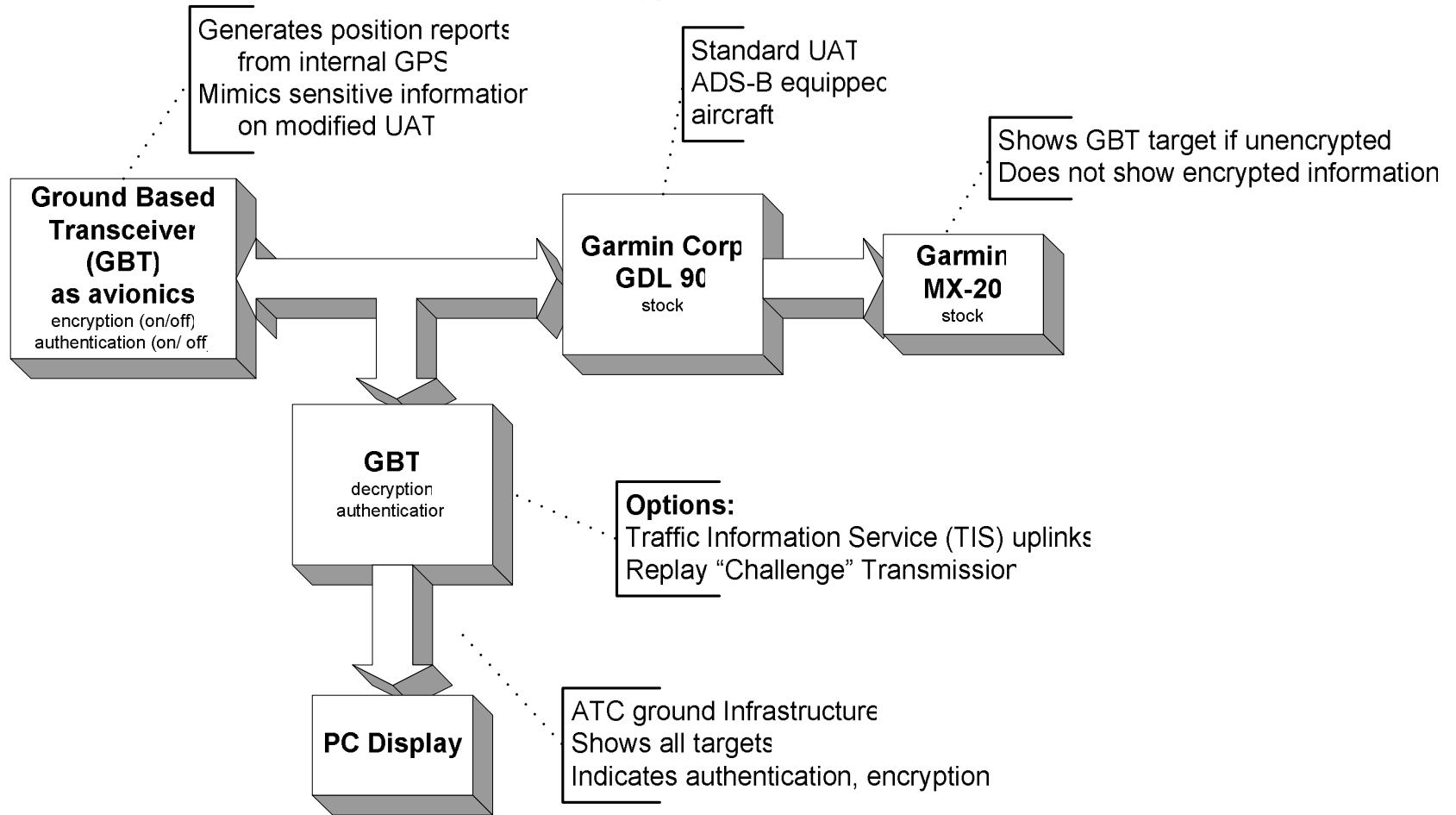
Message Content Protection



Enhanced ADS-B Test System

-- Generates Authentication information

-- Encrypts information



**System is Operational Today at Sensis;
Demo here at ACAST**

Phase 2: Access Protocol Changes

Currently:

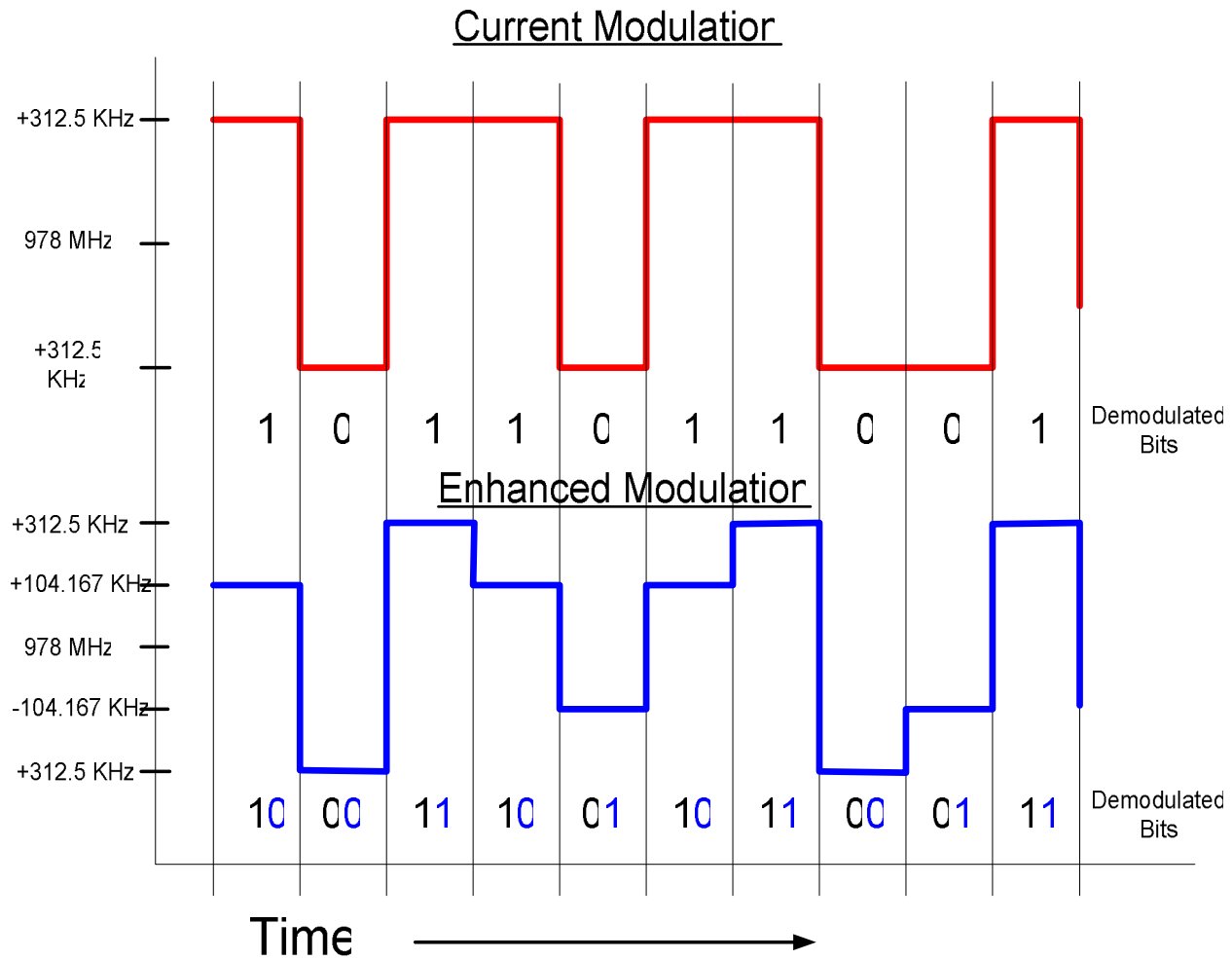
- Randomly selected time slot by individual aircraft

Investigating:

- Aircraft Self organizing system
- Ground assigned

Goal: Reducing Message Collisions

Modulation Enhancements



Program Schedule

