



An Architectural Concept for Intrusion Tolerance in Air Traffic Networks

Jeffrey Maddalon

Paul Miner

{jeffrey.m.maddalon, paul.s.miner}@nasa.gov

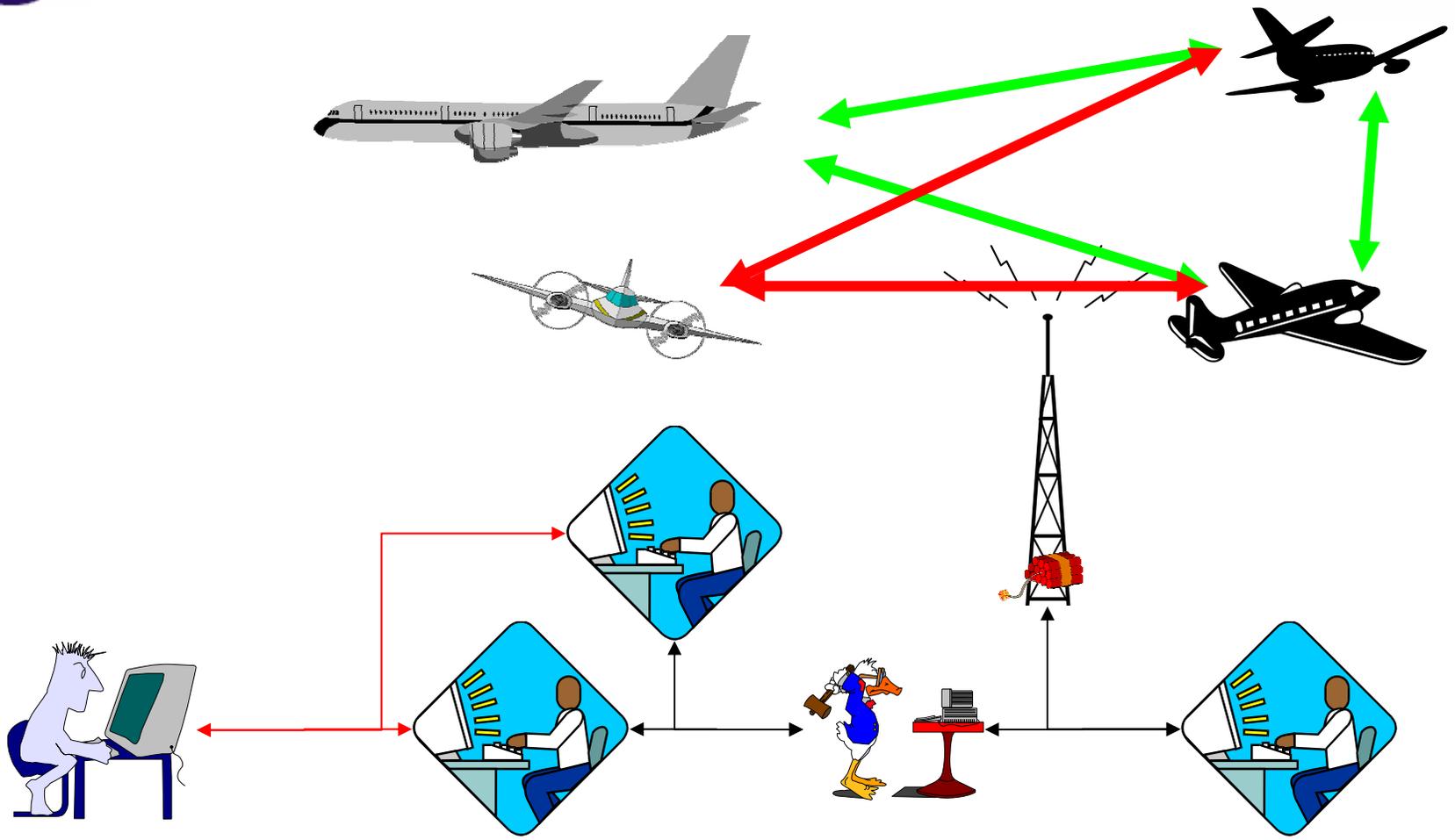
NASA Langley

22 May 2003



Securing reliable communications

- Consider a network that provides safety-critical air traffic management communication
 - controller-controller messages
 - controller-aircraft messages
 - aircraft-aircraft messages
- What vulnerabilities should this network be secured against?
 - core communications hubs may be destroyed (either physically or logically)
 - safety-critical messages may be altered/introduced in transit
 - malicious software for a coordinated attack on the network
 - ?





Desired Security Properties

Confidentiality No unauthorized disclosure of information

Integrity No improper alteration of data

Availability System always completes authorized actions

From Jean-Claude Laprie, *Dependability - Its Attributes, Impairments, and Means*, In Randell, et al. Eds., *Predictably Dependable Computer Systems*, Springer-Verlag, 1995

System Protection Goals

Attackers look for the weakest link, so not just strong barriers, but ...

strong barriers *and* redundancy





Intrusion Tolerance

- Ability to preserve Availability and Integrity, in presence of bounded number of compromised network nodes
- A compromised node may exhibit
 - Crashed (unable to deliver any service)
 - Unable to deliver timely service (e.g. Denial of Service)
 - Uniformly corrupted data (consistent misinformation)
 - Arbitrary behavior (includes malicious human-directed behavior)



Fault-Tolerance (FT) and Intrusion Tolerance (InT)

- Worst case scenario in FT is arbitrary behavior
 - identical to worst case for InT
- Easily detectable failures (crash, omission) are similar in both domains
- Failure modes are comparable, but fault arrival rates are not
 - In FT, we require independence of failure
 - exponential fault arrival rate
 - multiple fault scenarios are rare
 - In InT, we expect coordinated attack
 - potential for simultaneous arrival of multiple faults



What is SPIDER?

- A family of fault-tolerant architectures
 - Scalable Processor-Independent Design for Electromagnetic Resilience (SPIDER)
- A system built using SPIDER protocols can continue to operate with
 - arbitrary malicious failures
 - many easy-to-detect failures
 - multiple simultaneous failures

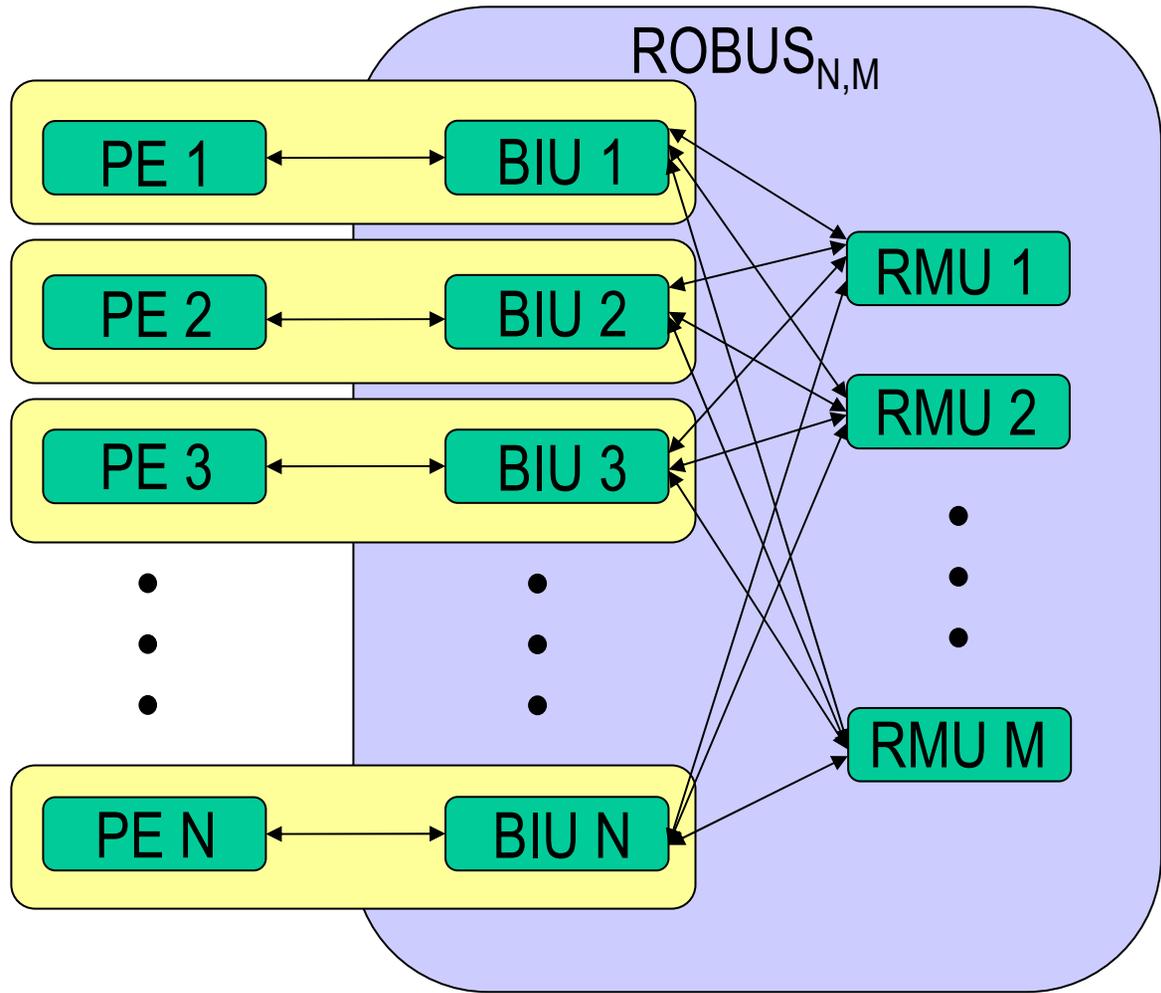


SPIDER Architecture

- N simplex general purpose Processing Elements (PEs) logically connected via a Reliable Optical BUS (ROBUS)
- A ROBUS is an ultra-reliable unit providing basic fault-tolerant services
- A ROBUS is implemented as a special purpose fault-tolerant device
 - ROBUS contains no software



ROBUS Topology





SPIDER Fault Tolerance

- **ROBUS Guarantees**
 - All processors attached to a good port will observe identical message streams
 - All processors attached to a good port will be synchronized within a bounded amount of time
 - All processors attached to a good port will have correct and consistent diagnostic information
- **From these guarantees SPIDER can provide**
 - Interactive Consistency (Distributed Agreement)
 - Distributed Diagnosis
 - Clock Synchronization



Intrusion Tolerance and SPIDER

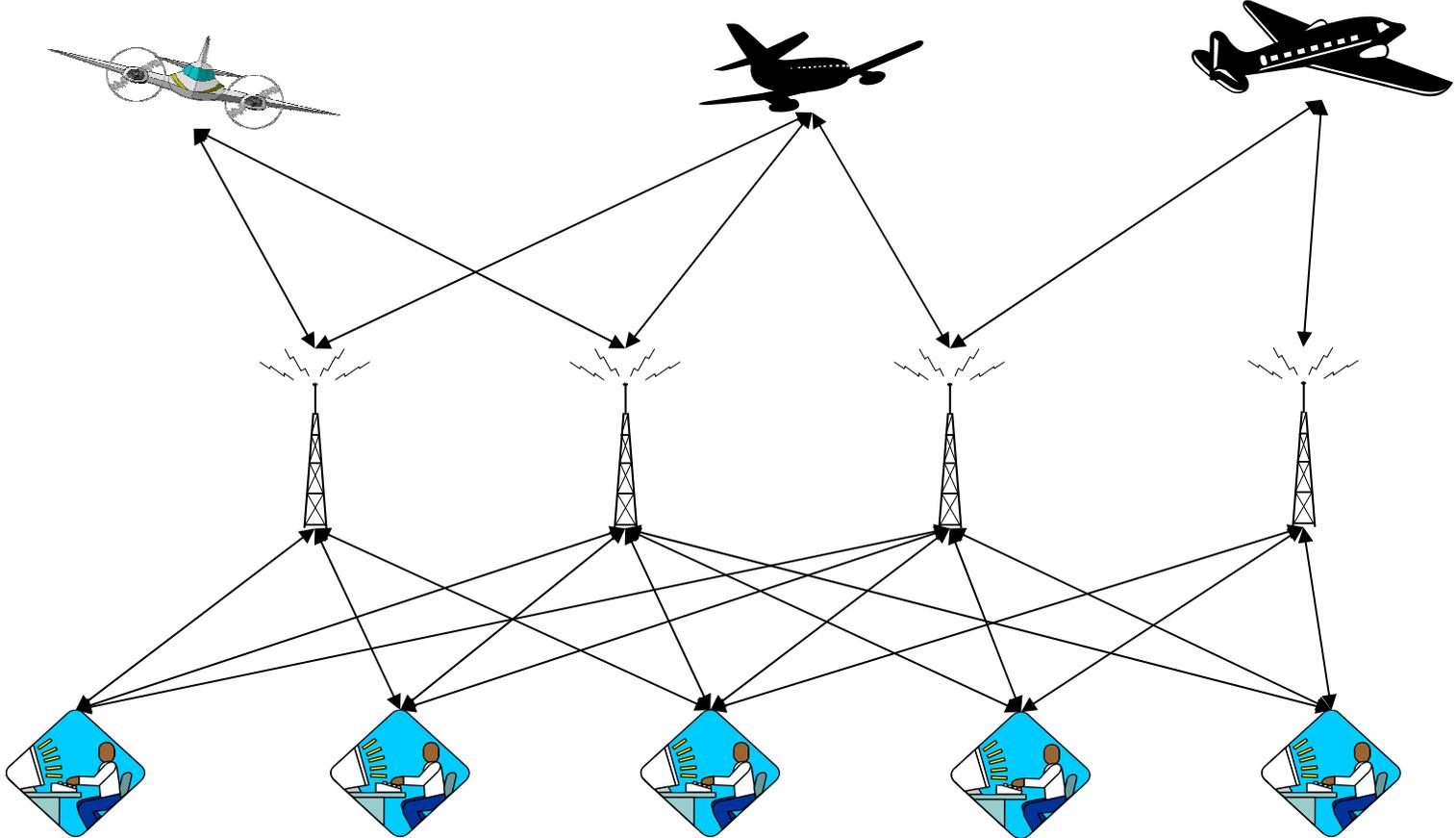
- With enough good (not compromised) nodes, we can still provide service
- Standard versions of fault tolerant protocols that can withstand a bounded number of faulty nodes
 - deemed too expensive in both time and space to be of practical use
 - variant of SPIDER protocols might provide cost-effective Intrusion Tolerance
- Fault arrival rates are different between fault tolerant and intrusion tolerant systems
 - SPIDER architecture designed for multiple active faults



Arbitrary Network Structures?

- ROBUS can use a distributed implementation (not necessarily optical)
- Can generalize the bus-oriented structure to establish an intrusion tolerant version of classical network topologies
 - Rings
 - Hub and Spoke
 - For any particular network topology, there is a corresponding intrusion tolerant topology (at cost of adding redundant links and nodes, and ensuring independence of failure)
- Many existing network structures may include sub-networks capable of supporting this idea

Network Concept





Formal Verification

- Sound concepts with poor designs can result in security issues
- A poor design of these protocols could cause security problems

Solution: formal verification

- SPIDER fault tolerance properties have been formally verified
- We expect any modifications to provide intrusion tolerance will also be formally verified.



Summary

- Intrusion resilience vs. Intrusion tolerance
- Techniques from fault tolerance used to achieve intrusion tolerance
- The SPIDER fault tolerant architecture may be adapted for intrusion tolerance