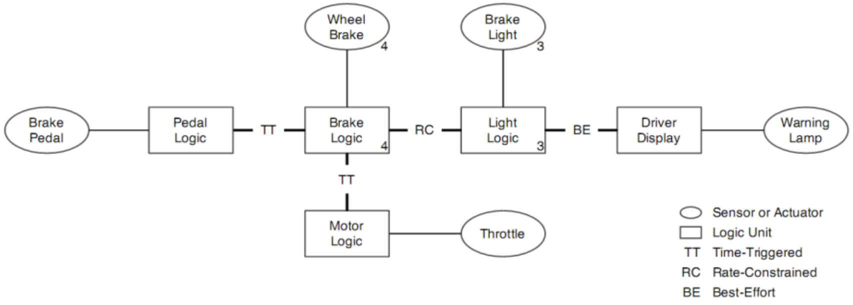
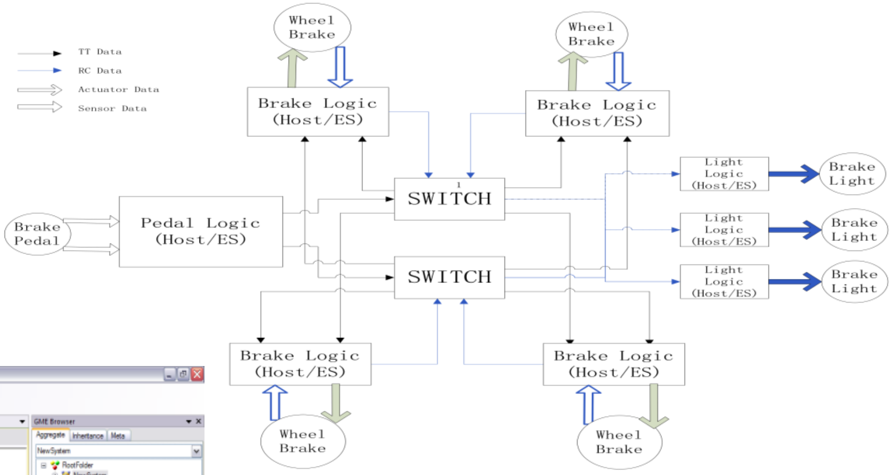
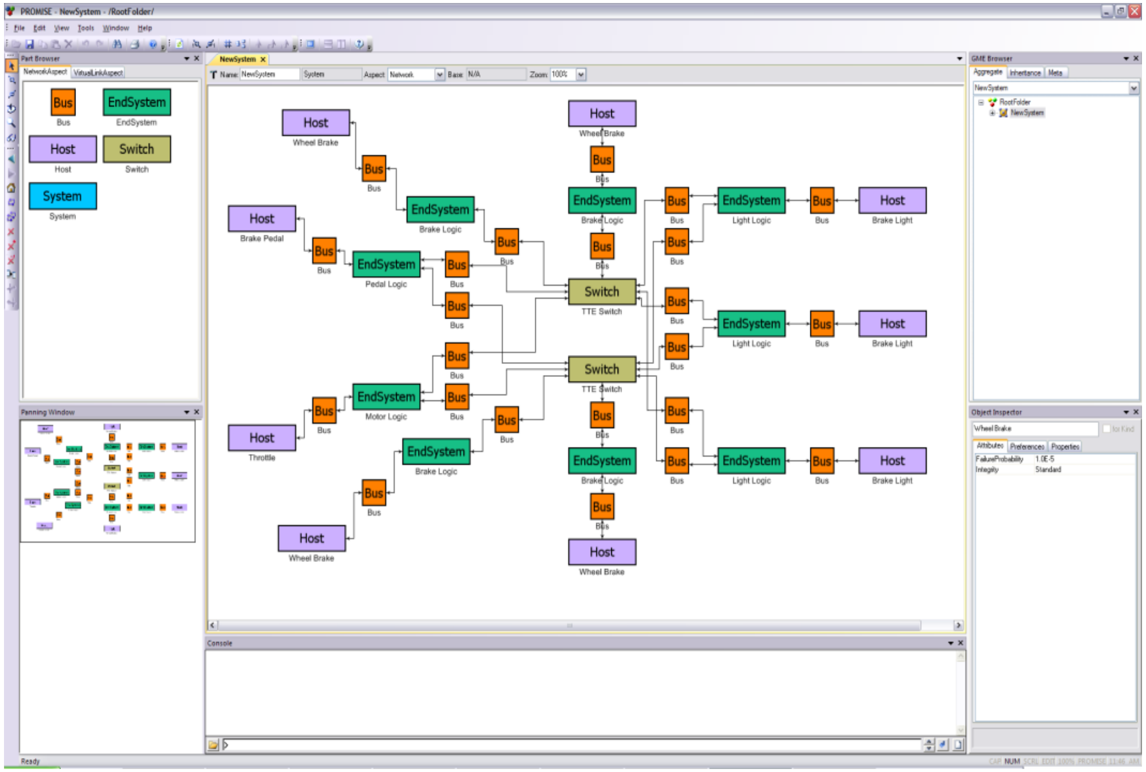
Fault Modeling Considerations for ADSL in AFFIRM

Example of a Complete System Specification End to End







Name: NewSystem System Aspect: Network Base: N/A Zoom: 100%

GME Browser: NewSystem

Object Inspector: Wheel Brake

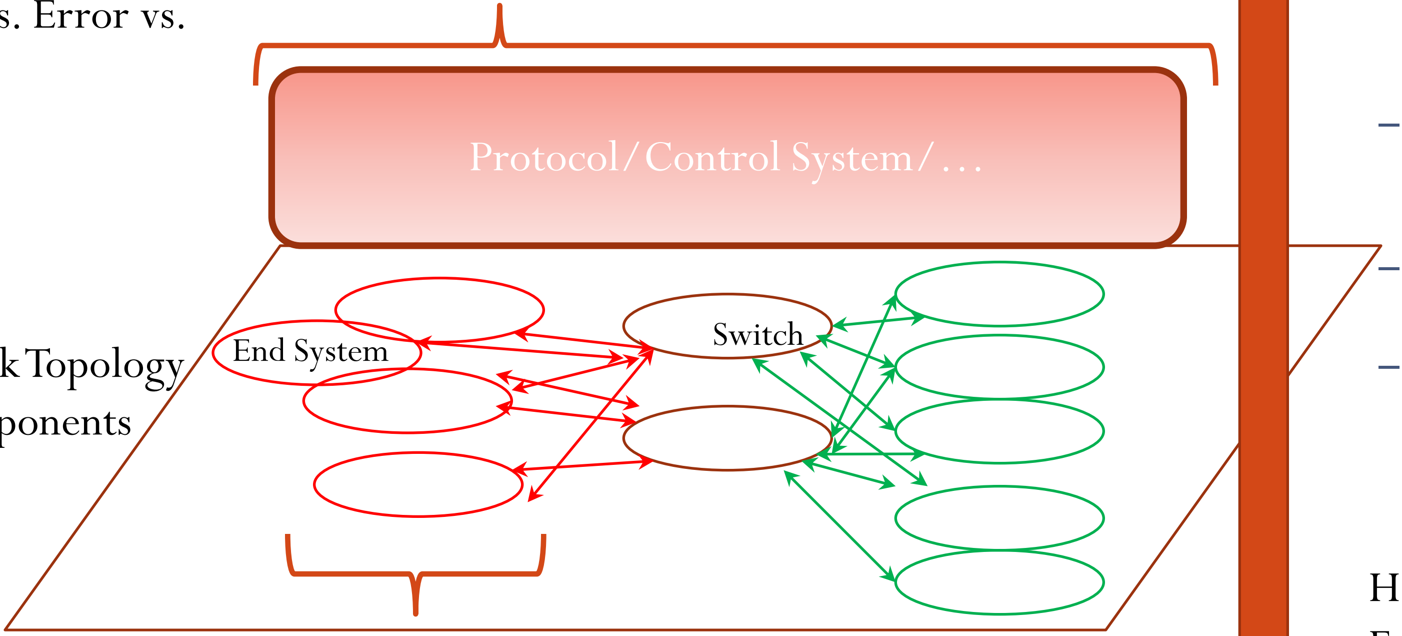
FailureProbability	1.0E-5
Integrity	Standard

Hybrid Faults Modeling: Global vs. Local Faults

No distinction in slides between Faults vs. Error vs. Failure

Global Faults (describes faults on relationship two or more nodes) at System Level

- **Symmetric**
- **Asymmetric (Byzantine)**
- **…**



Network Topology of Components

Local Node/Component Faults

- **Omission**
- **Commission (babbling)**
- **Untimely (late, early, sequence,..)**
- **Invalid Value (semantic, syntactic,..)**
- **Invalid Behavior/Protocol (e.g. Failure of Fault Handling of detection, protection etc)**
- **….**

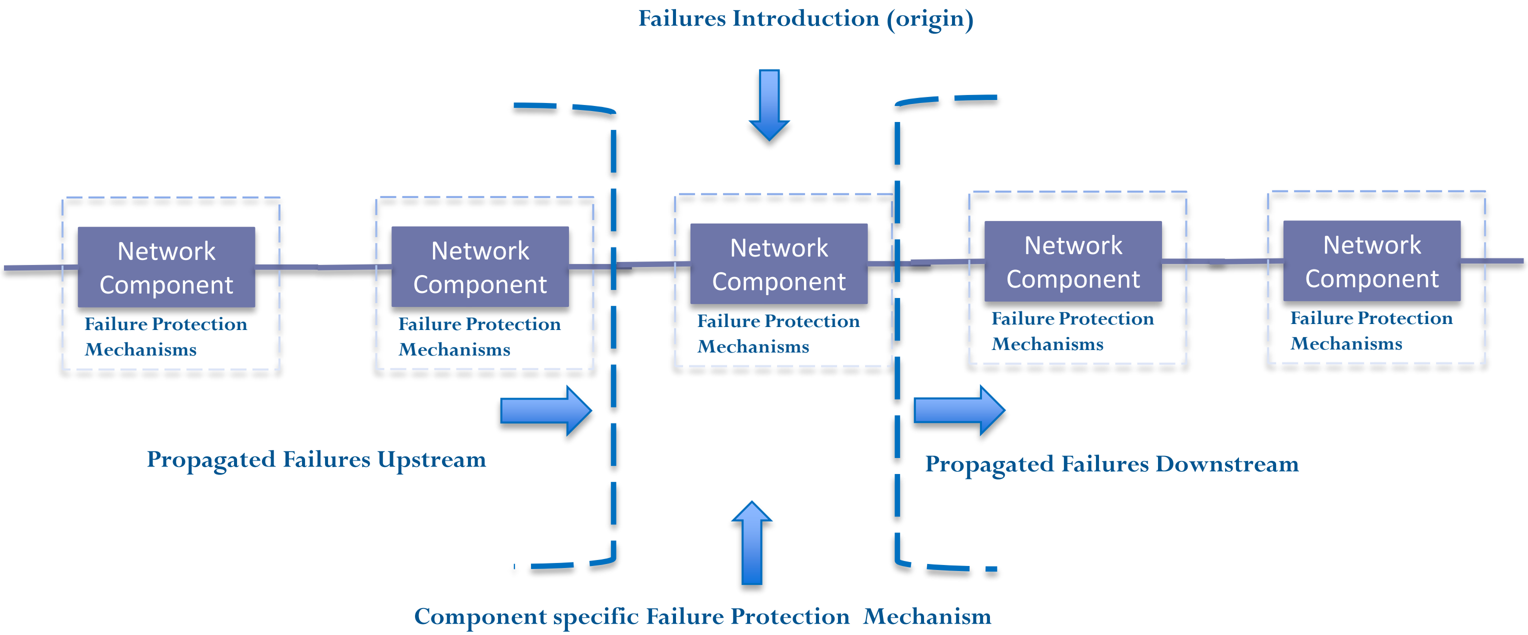
Fault Space Constraints & Assumptions

- **# of Faults**
- **Validity and Propagation fault Assumption**
- **Agreement Generation Fault Assumption**
- **Independence Assumption**
- **Degree of maliciousness**

↓

Helps Synthesize Faults SAL, PVS models In AFFIRM

Horizontal Propagation of Faults


Failures Introduction (origin)
Network Component
Failure Protection Mechanisms
Network Component
Failure Protection Mechanisms
Network Component
Failure Protection Mechanisms
Network Component
Failure Protection Mechanisms
Network Component
Failure Protection Mechanisms
Propagated Failures Upstream
Propagated Failures Downstream
Component specific Failure Protection Mechanism

Failure Protection Mechanism

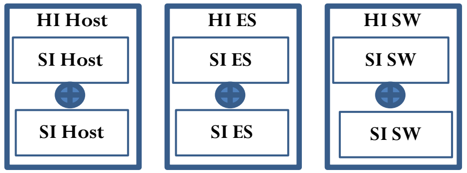
Different for SPIDER, TTP, TTE, AFDX, SAFEBUS etc

Horizontal Propagation of Faults though Topology of network components

Faults introduced/propagated from upstream transforms to another fault based on Protection Mechanisms e.g. Commission -> Omission if bandwidth check implemented as protection mechanism in a component

Vertical Composition of Faults

Vertical Composition of Faults from Local Component Faults to Global Faults at System Level



Self checking components

Legend:

SI: Standard Integrity

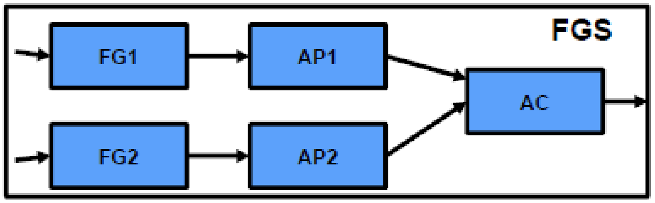
HI: High Integrity

SW: Switch

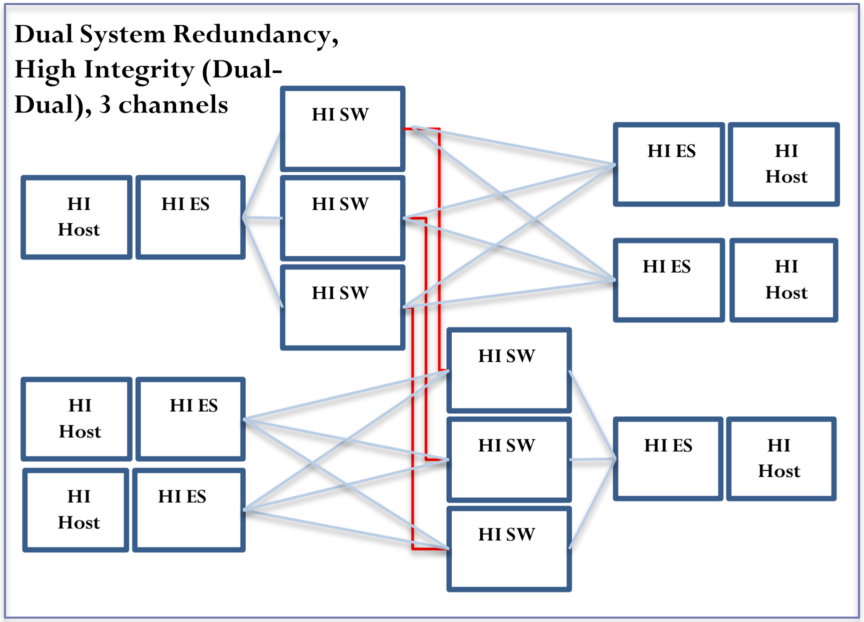
ES: End System

⊕ : High Integrity Check

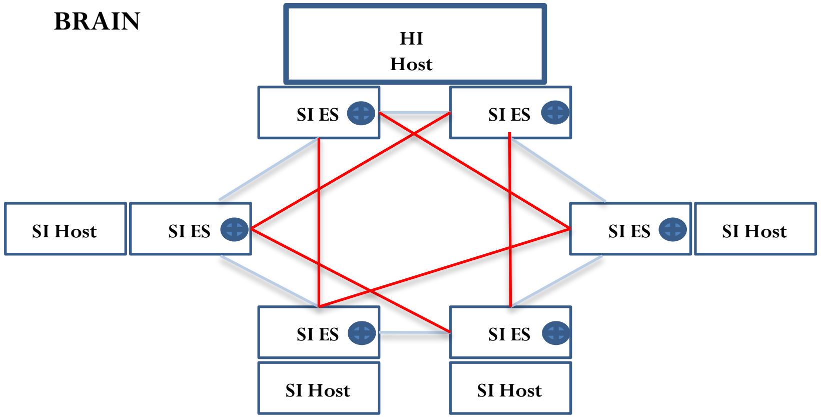
Dual redundant flight guidance system: Redundant Flight Guidance (FG) and Auto Pilot (AP) channel



Dual System Redundancy, High Integrity (Dual-Dual), 3 channels



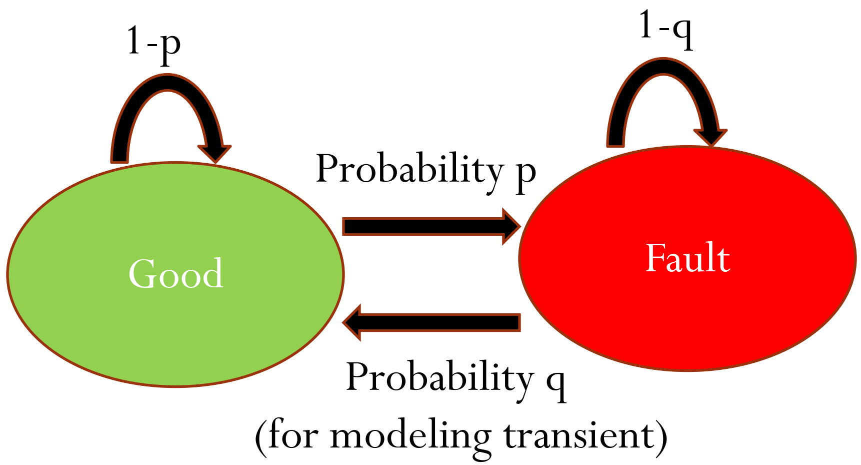
BRAIN



Pair of "adjacent" SI ES's acts as a High Integrity Pair "Comparison" logic is over frames from direct link (blue) vs skip link (red) and over frames arriving at receiver (clockwise vs counter-clockwise)

Fault Behavior

- Permanent Fault vs. Transient Fault at each Component
- Probabilities need to be specified
- Fault Duration how to specify?
- Role of Repair – related issue of maintenance intervention which essentially replenishes the "probabilities" for analyzing aircraft wide failure likelihoods so level A/B/C aircraft hazard likelihood are limited to smaller than $10^{-9}/10^{-7}/10^{-5}$ failures/flight hour respectively


1-p
1-q
Probability p
Good
Fault
Probability q
(for modeling transient)