System Safety

Normalization of Deviance

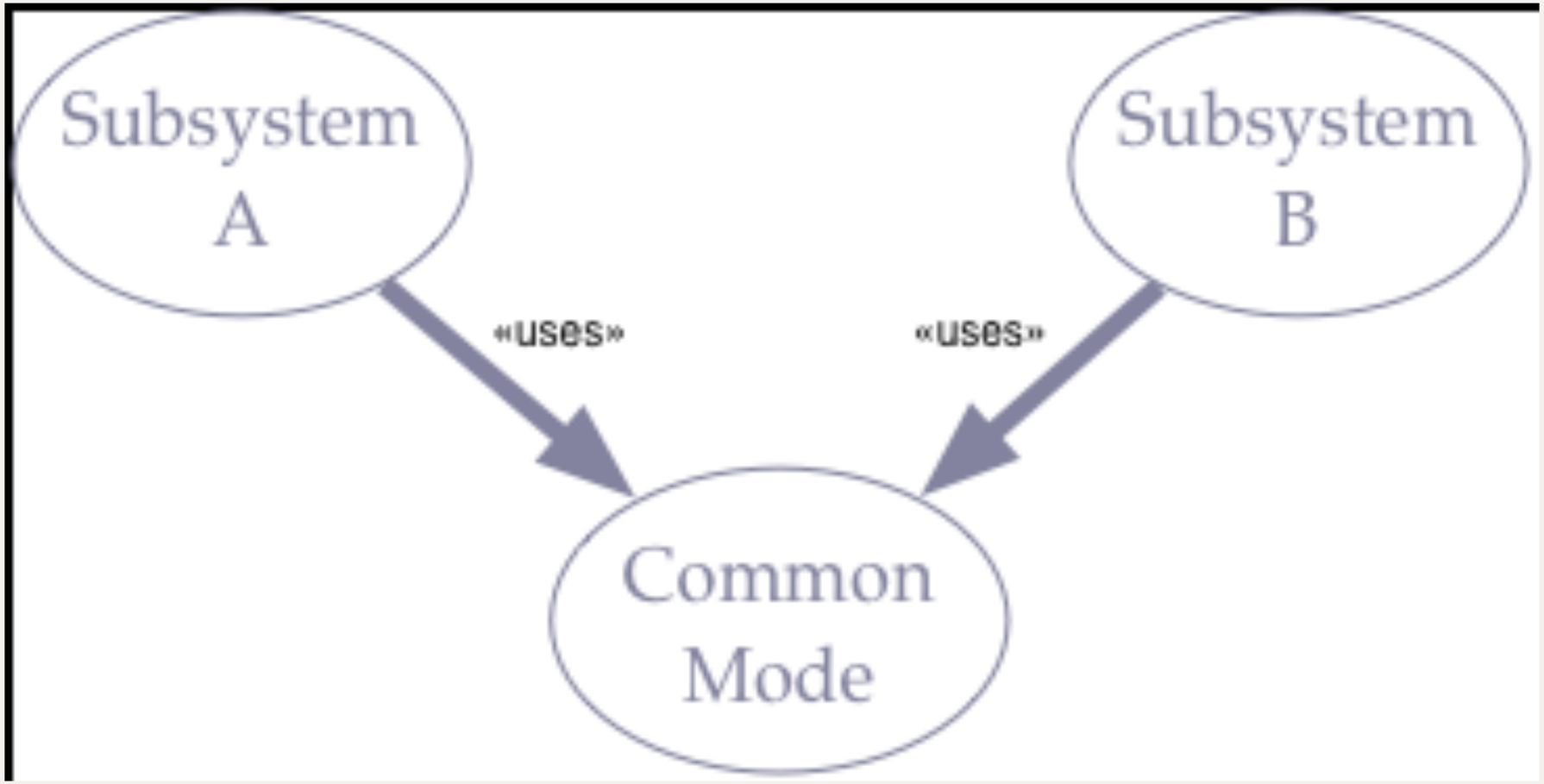
"We did it last time and nothing bad happened."

Failure-inducing Technology

- Dynamic coupling
- Continuous flow
- Non-linear responses
- Production pressure
- Ambiguous or confusing signals to operators
- Operators are under-trained or have mental model mismatch

Coupling

Common Mode Failures

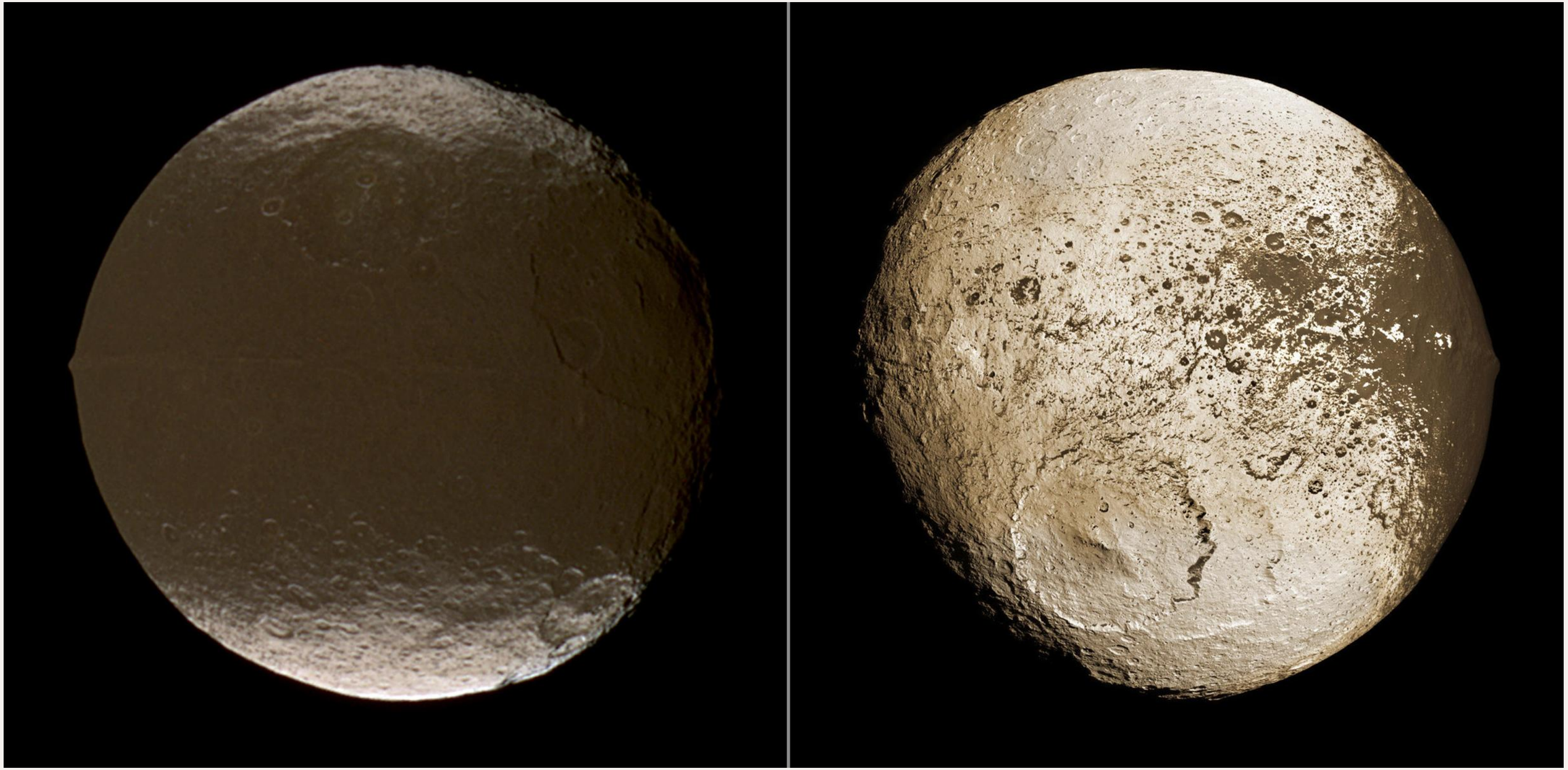


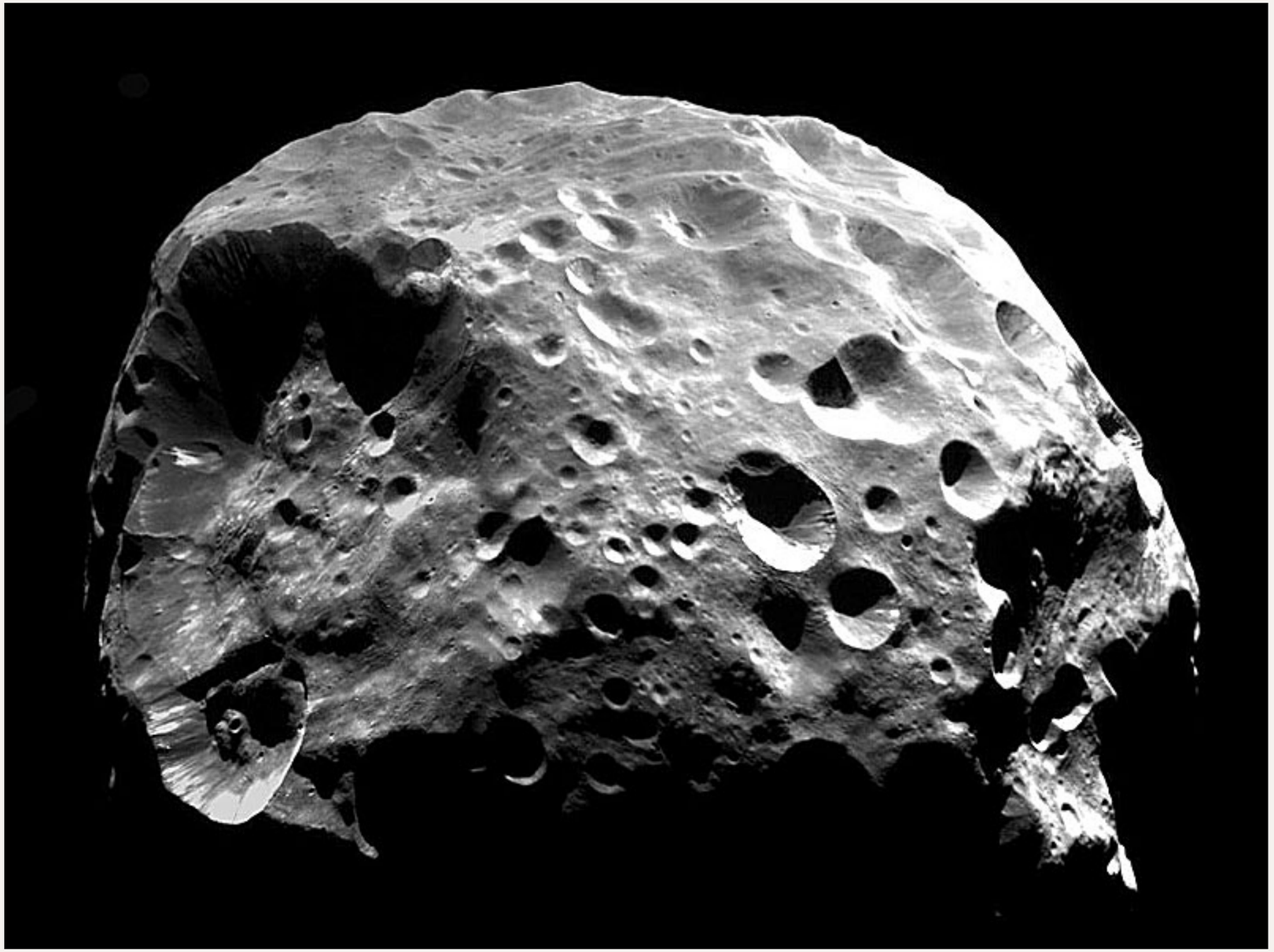
Coffee and Airplanes

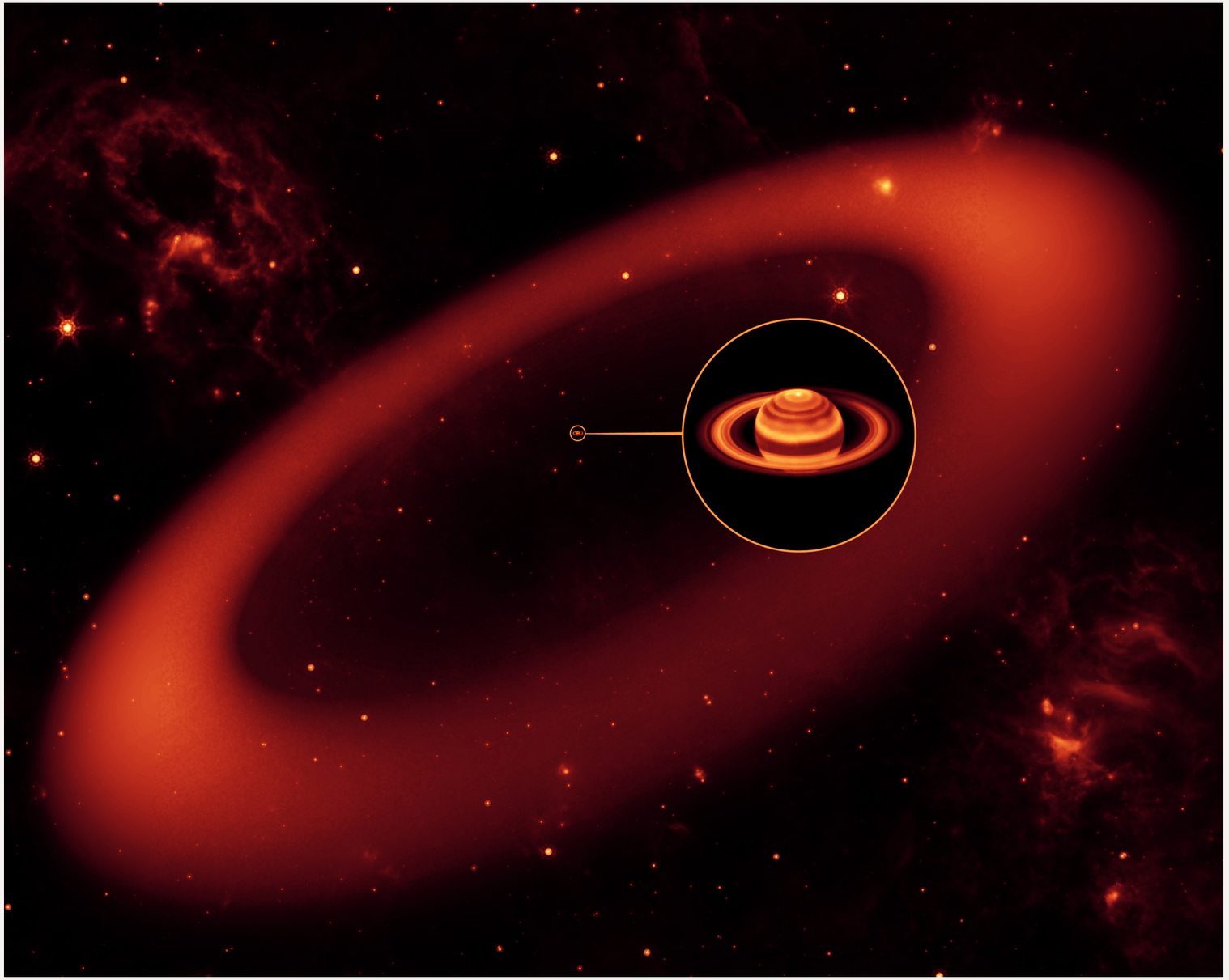
- UA940, Jan 2011 - Pilot spills coffee into communication equipment. Triggers "hijack alert" emergency code. Plane diverted, lands safely.
- Possibly apocryphal - Coffee leak into common bulkhead causes electrical short in hydraulics control. Plane crashes.
- Air New England, June 1979 - Coffee and Danish pastry implicated. Pilot suffered from hypertension and hypoglycemia.

Pervasiveness of Coupling

A brief aside about coupling: Iapetus and Phoebe







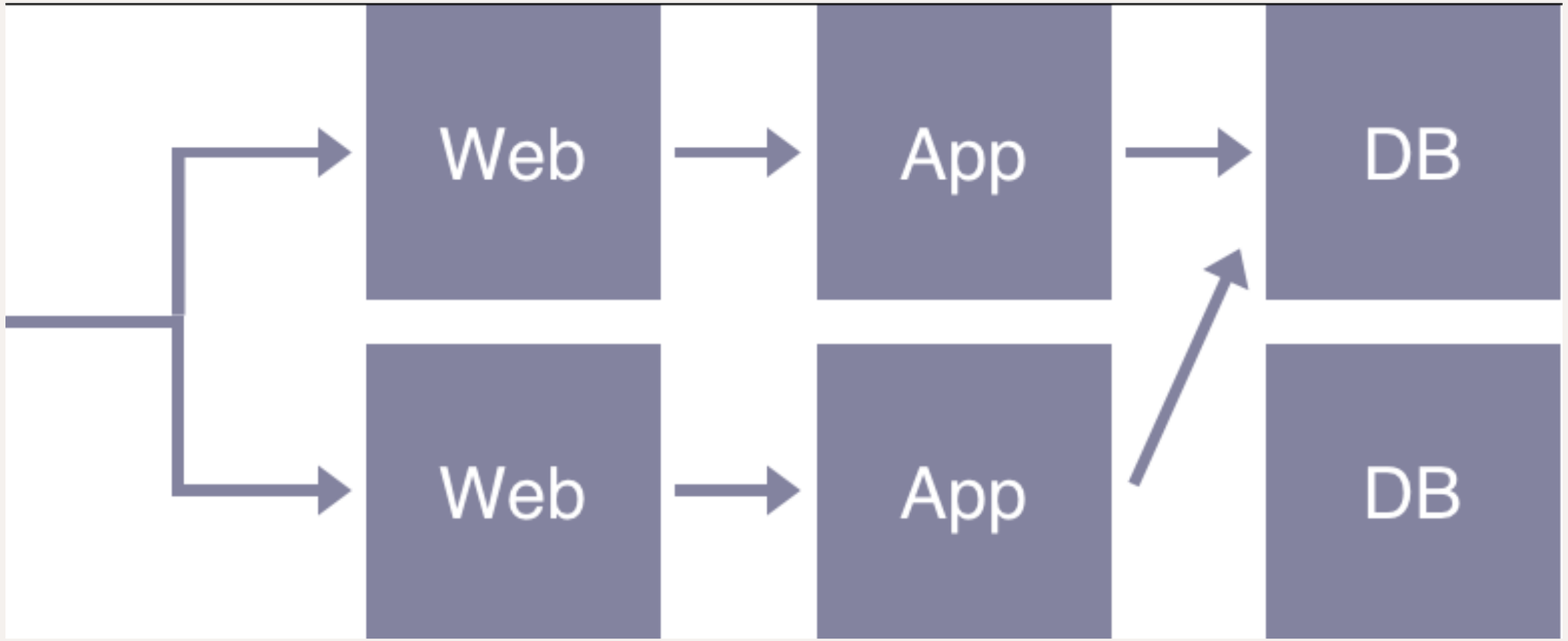
Everything is coupled to everything

- Ambient temperature
- Ambient atmosphere
- Electromagnetic field
- Gravity
- Non-local quantum effects

Surprises

- Sudden change in strength/correlation
- Factors coupled to external environment
- Nonlinearity

Exercise: Six Pack



What kind of couplings reduce independence?

Coupling in Software Systems

1. Load sharing
2. Shared infrastructure
3. Shared services
4. Application code
5. Assumptions about data model and usage

Drift Into Failure

- Long term buildup of energy
- Gradual erosion of safety barriers
- Increasing production and management pressures
- Diluted or diffused accountability

Examples of Drift

- Space Shuttle Challenger - launch temperature
- Space Shuttle Columbia - debris impact
- Aberfan, South Wales - coal mine tip
- Union Carbide plant - Bhopal, India
- DC-9/MD-80 - stabilizer trim screw

DC-9/MD-80

Maintenance Interval changes by year

1965 - 300 flight hours
1985 - 700 flight hours
1987 - 1000 flight hours
1991 - 1200 flight hours
1994 - 1600 flight hours
1996 - 8 months, ~2550 flight hours

Union Carbide - Bhopal, India

- 2 December 1984
- Union Carbide pesticide plant
- Water entered overloaded tank, causing reaction
- Tank reached 200C, pressure unknown but high
- 30 tons of methyl isocyanate released into atmosphere
- Over 8,000 dead, 30,000+ injured for life

Buildup before failure

- Negligence in safety equipment
- Tank alarms inoperative for 4 years
- Gas scrubbers inoperative for 5 months
- Tank pressure gauge malfunctioning

High Reliability Organizations

- Safety is the primary objective
- Decentralized decision-making
- Culture of reliability, peer reinforcement, management emphasis
- Continuous training and simulations
- Learn from successes and near-misses
- Blameless post-mortems

Circuit Breaker

- Sever part of the system
- To save the rest

Governor

- Limit rate of dangerous actions

Hysteresis

- Scale up quickly
- Scale down slowly

Shock Absorbers

- Fail fast
- Bulkheads
- Circuit breakers
- Load shedding

Assist Operators

- Humane logs
- Unambiguous displays
- Self-describing systems

Dry Run

- The `--not-really` flag

Game Day

- Practice release, launch, hurricane, plague

Chaos Engineering

- Techniques to surface systemic problems
- Use randomness
- Apply stresses
- Create faults

© 2016-2017 Michael Nygard