Survivability:
What Is It and
What Can It Be Used For?

John C. Knight

Department of Computer Science
University of Virginia

Joint Work With Colleagues

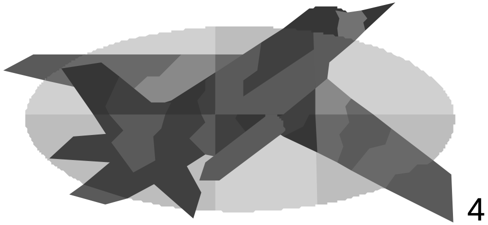
- University of Virginia:
  - Elisabeth Strunk
  - Kevin Sullivan
- University of Colorado:
  - Alexander Wolf
  - Dennis Heimbigner
- University of California, Davis:
  - Premkumar Devanbu
- Thanks to our funding sources: DARPA & NASA

Survivability

What Is It?

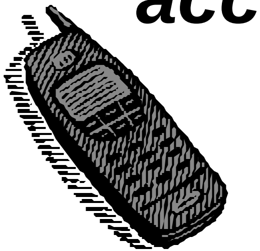
Aircraft Survivability

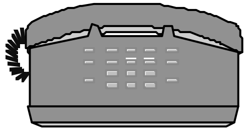
- "Aircraft combat survivability is the capability of an aircraft to avoid and/or withstand a man-made hostile environment. It can be measured by the probability the aircraft survives an encounter with the environment, P_S." (Note circularity!)
- Goal here is to get aircraft safely to the ground



Telecommunications Survivability

- “A property of a system, subsystem, equipment, process, or procedure that provides a defined ***degree of assurance*** that the named entity will continue to function during and after a natural or man-made disturbance; e.g., nuclear burst. Note: For a given application, survivability must be qualified by specifying the ***range of conditions*** over which the entity will survive, the ***minimum acceptable level of post-disturbance functionality,*** and ***the maximum acceptable outage duration***.”





What Is Survivability?

- Common, useful notion in other disciplines
- Frequently used term in information systems:
  - Systems are often described as ***survivable***
  - Sometimes used as a synonym for ***security***
- Is it useful for information systems?
- Actually, “yes”, wide applicability
- Need a precise definition so that we know what we are trying to achieve

What Is Survivability?

Dependability is always a tradeoff

Preservation of function vs. cost of construction

Survivability is such a tradeoff.

It pays explicit attention to alternate function and system value

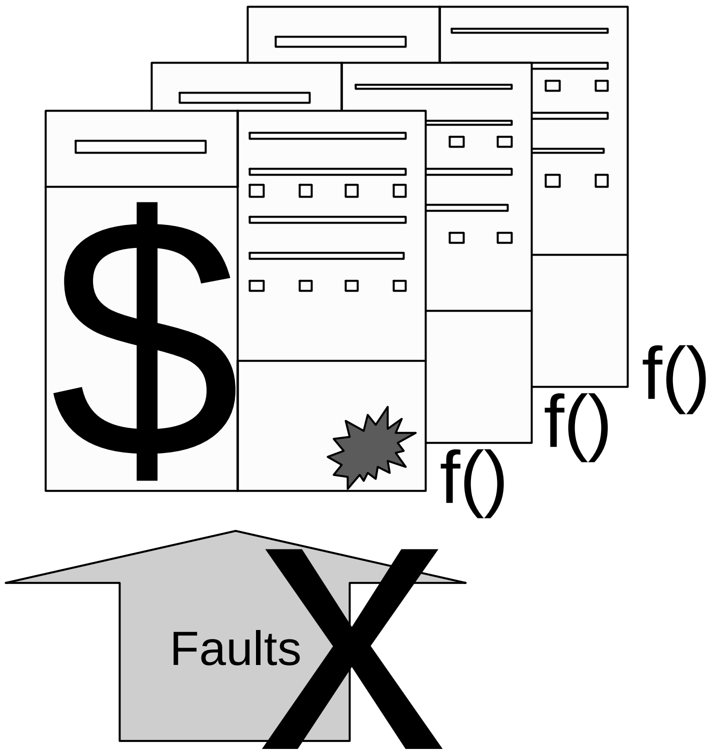
What Is Survivability?

- ***Explicit decision*** to:
    - Not mask certain faults
    - Not avoid/remove certain faults
- ***Explicit decision*** by system stakeholders to accept alternate functionality if errors do occur
- Why?
    - Adequate masking is too expensive
    - Adequate avoidance/removal is infeasible

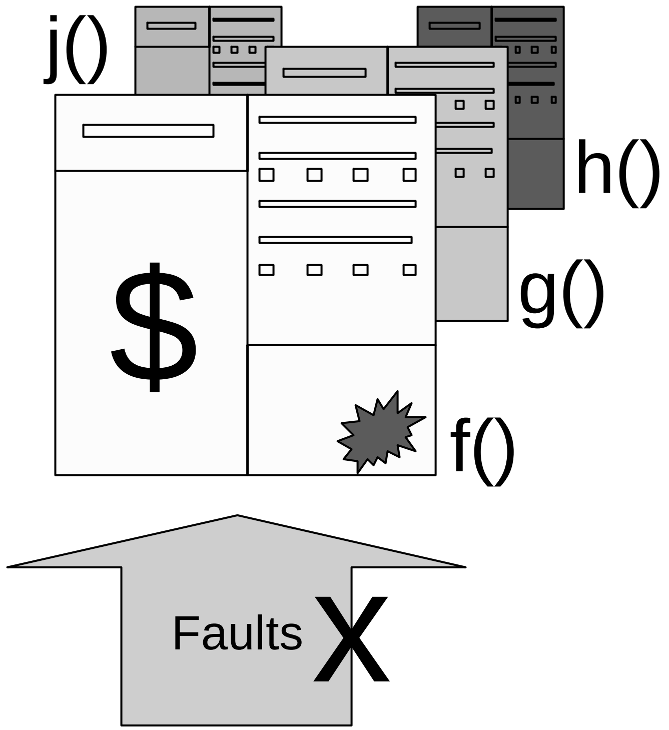
  } Common cases
- Note: This is not graceful degradation

What Is Survivability?

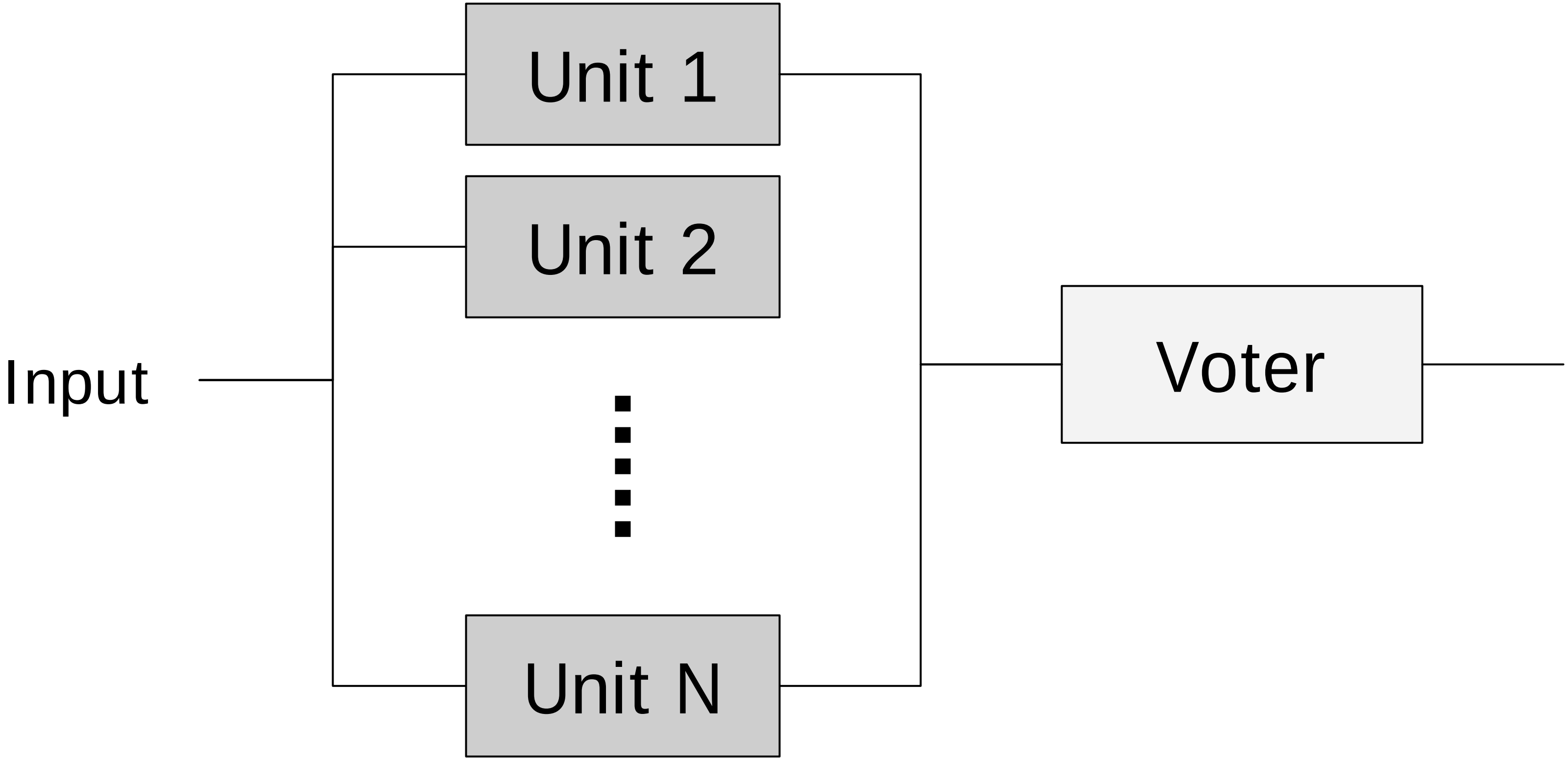
Reliability, Availability



Survivability



N Modular Redundancy (NMR)



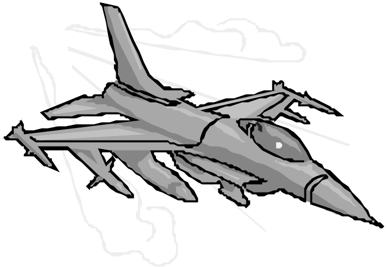
- To what extent can redundancy be applied?

Computer System Survivability

- Other types of system, ***no*** meaningful options

Keep
person
alive

Get
aircraft
"home"



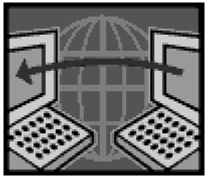
- Computer systems, ***meaningful*** options:
  - □ Continued service depends on user requirements
  - □ Which service has greatest ***value***
  - □ ***Value is a function of state***

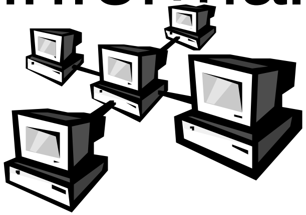
Computer System Survivability

- Ellison et al proposed a definition:

  “Survivability is the ability of a network computing system to provide essential services in the presence of attacks and failures, and recover full services in a timely manner”

- Good start, but informal and incomplete



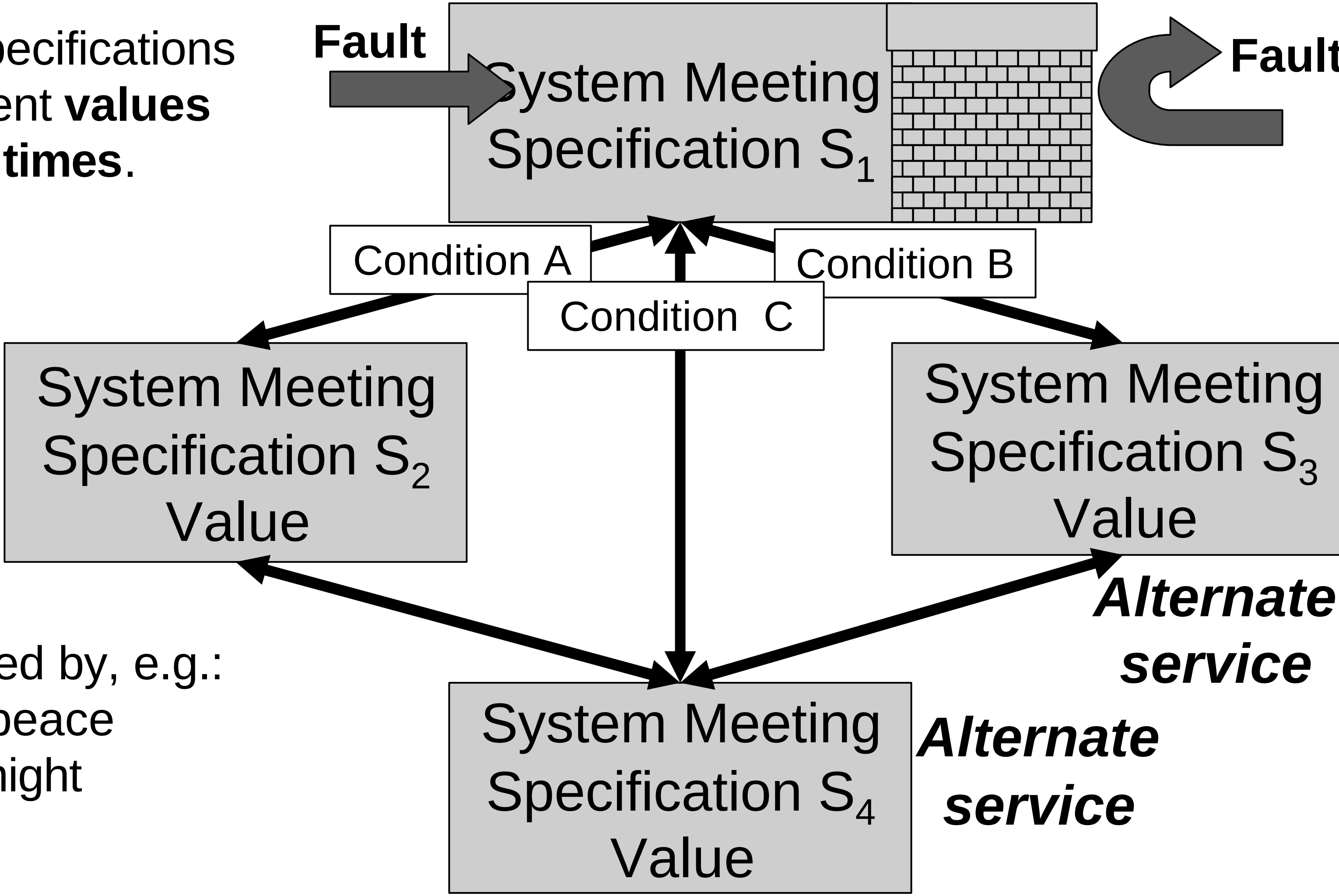


Informal Notion of Survivability

- *Essential* services:
  - Which services are essential?
- *Attacks* and *failures*:
  - What attacks?
  - What failures?
- How will we know if we achieve survivability?
- How will a system’s owners know what they can expect?

Survivability Concept

Different specifications have different **values** at different **times**.



Fault

System Meeting Specification S_1

Fault

Condition A

Condition B

Condition C

Alternate service

System Meeting Specification S_2 Value

System Meeting Specification S_3 Value

Alternate service

System Meeting Specification S_4 Value

Alternate service

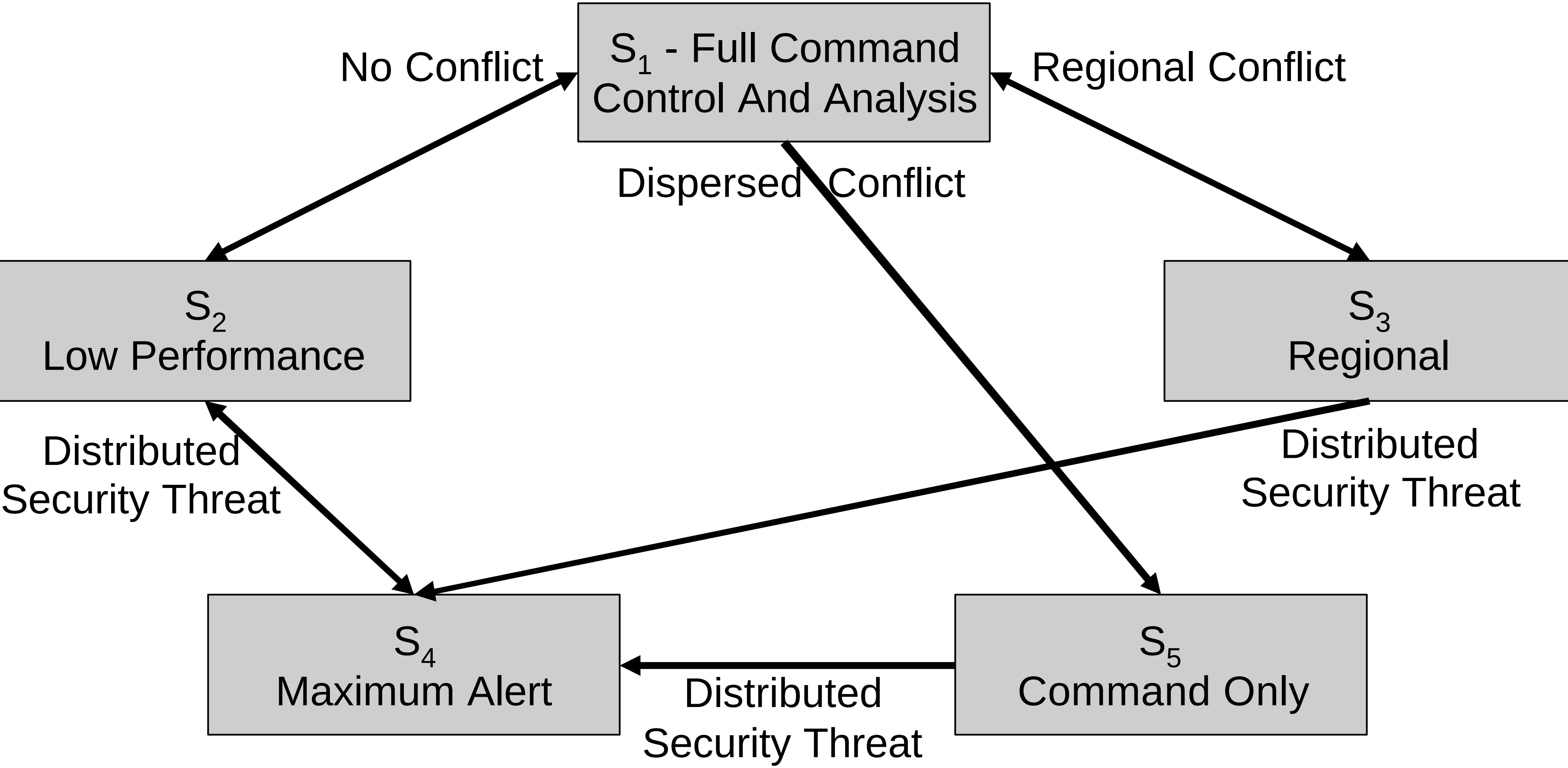
Value affected by, e.g.:

- War vs. peace
- Day vs. night
- Etc.

Survivability Concepts

- Acceptable services:
  - What functionalities are ***acceptable*** to users?
- Service value:
  - What are the ***values*** of the various functionalities?
  - How is the value affected by state changes in the operating environment?
- Service transitions:
  - What ***transitions*** between functionalities are valid?
- Operating environment:
  - What factors in the ***environment*** affect value?

An Example—A C^3 System


S1 - Full Command Control And Analysis
No Conflict
Regional Conflict
Dispersed Conflict
S2 Low Performance
S3 Regional
Distributed Security Threat
Distributed Security Threat
S4 Maximum Alert
S5 Command Only
Distributed Security Threat

More Rigorously (In Part)

- Definition:

  A system is survivable if it meets its survivability specification

- A survivability specification is a six-tuple:
  - A set of specifications of acceptable forms of service
  - A function from the set of services to the set of values that each service can have
  - The set of valid transitions between acceptable forms of service
  - Probability that acceptable service will be provided
  - The relevant environmental factors and their values
  - The relevant combinations of environmental factor values

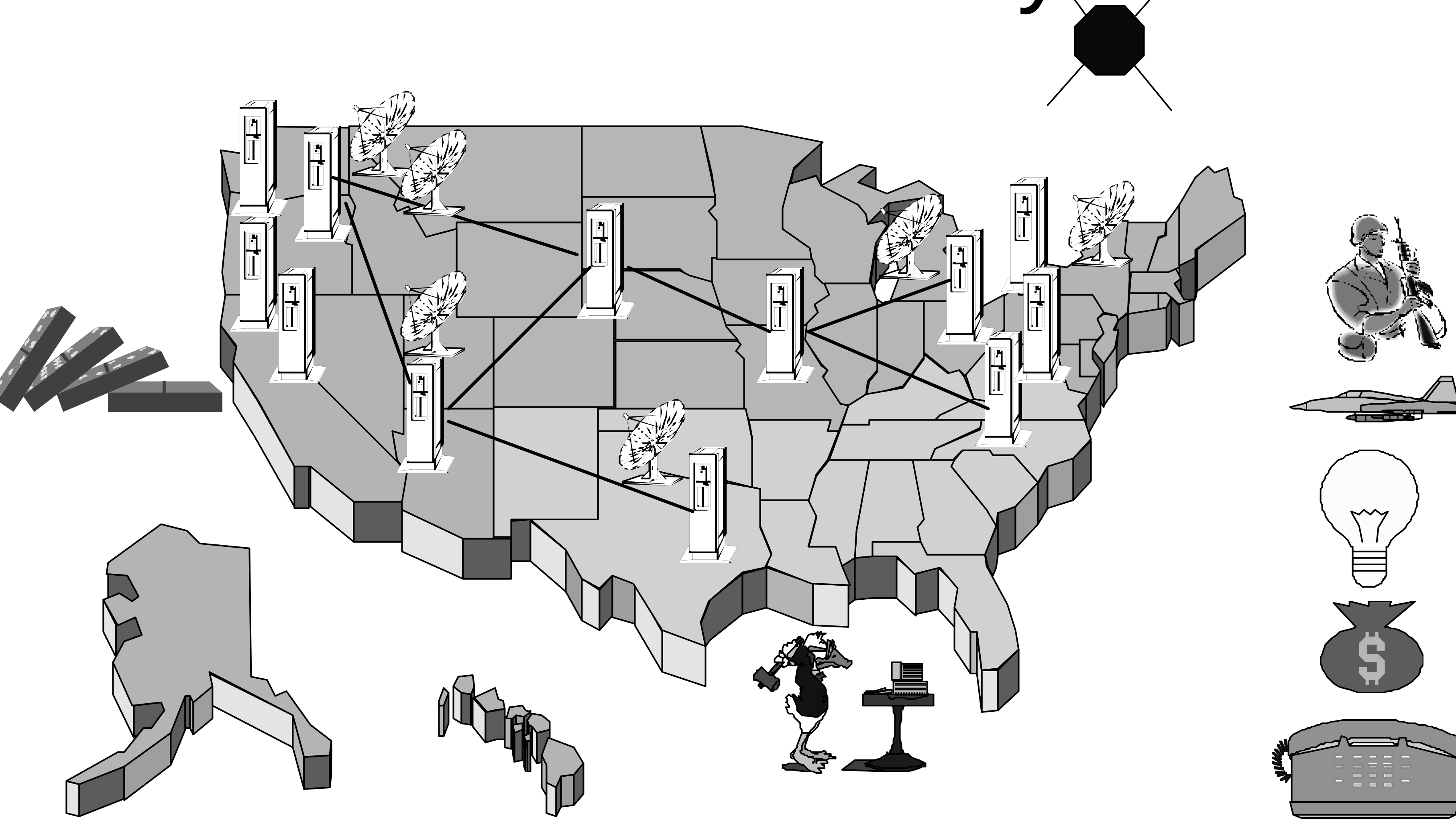
Service Level

- *Acceptable service* does not mean *preferred service*
- Preferred service should be supplied “most” of the time
- Engineering to meet “most” means that “most” must be included in system specification
- Defined as probabilities that specifications will meet their dependability requirements

Survivability

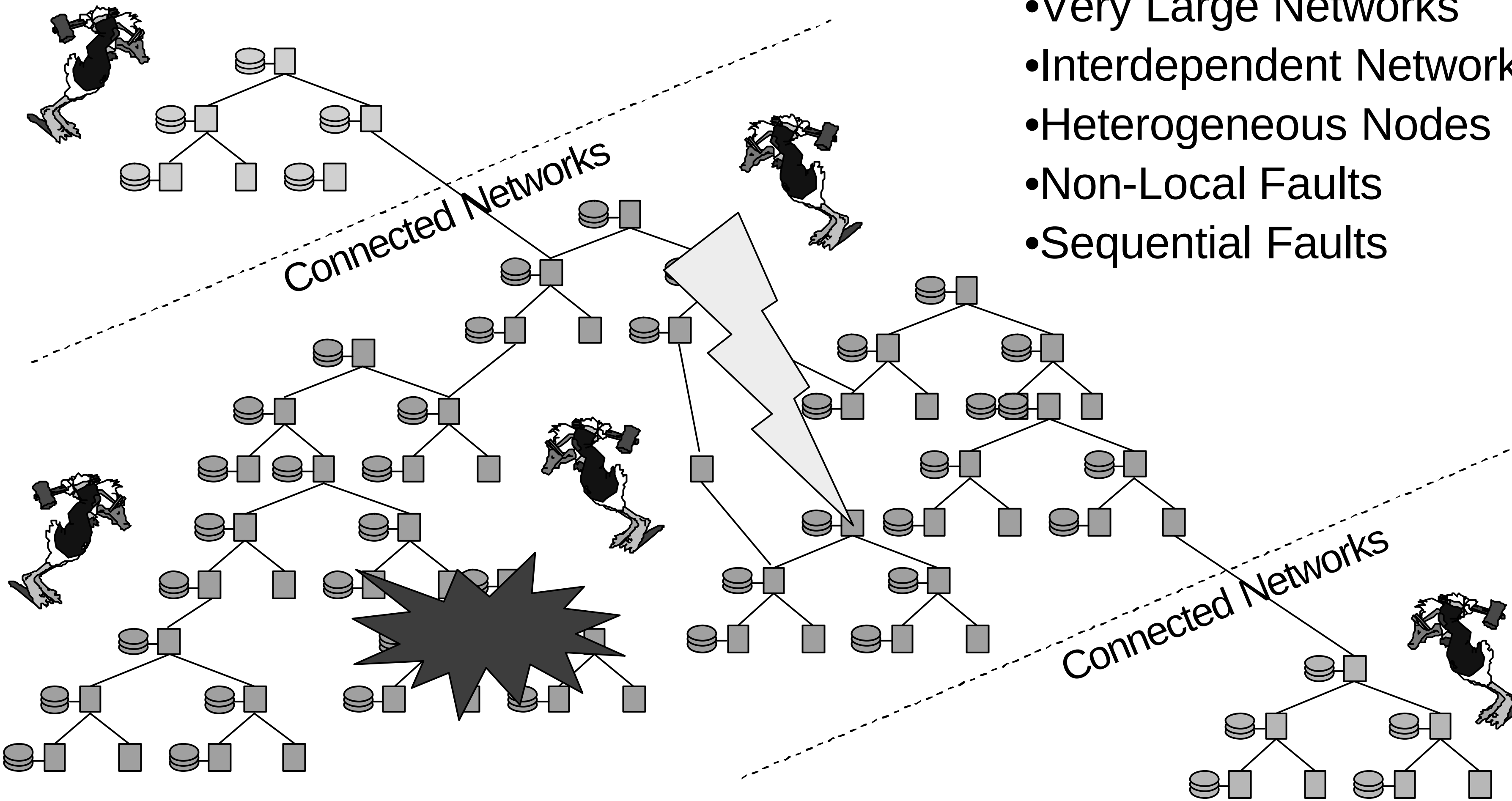
For Systems Where The Alternatives Are Too Expensive

Critical Information Systems

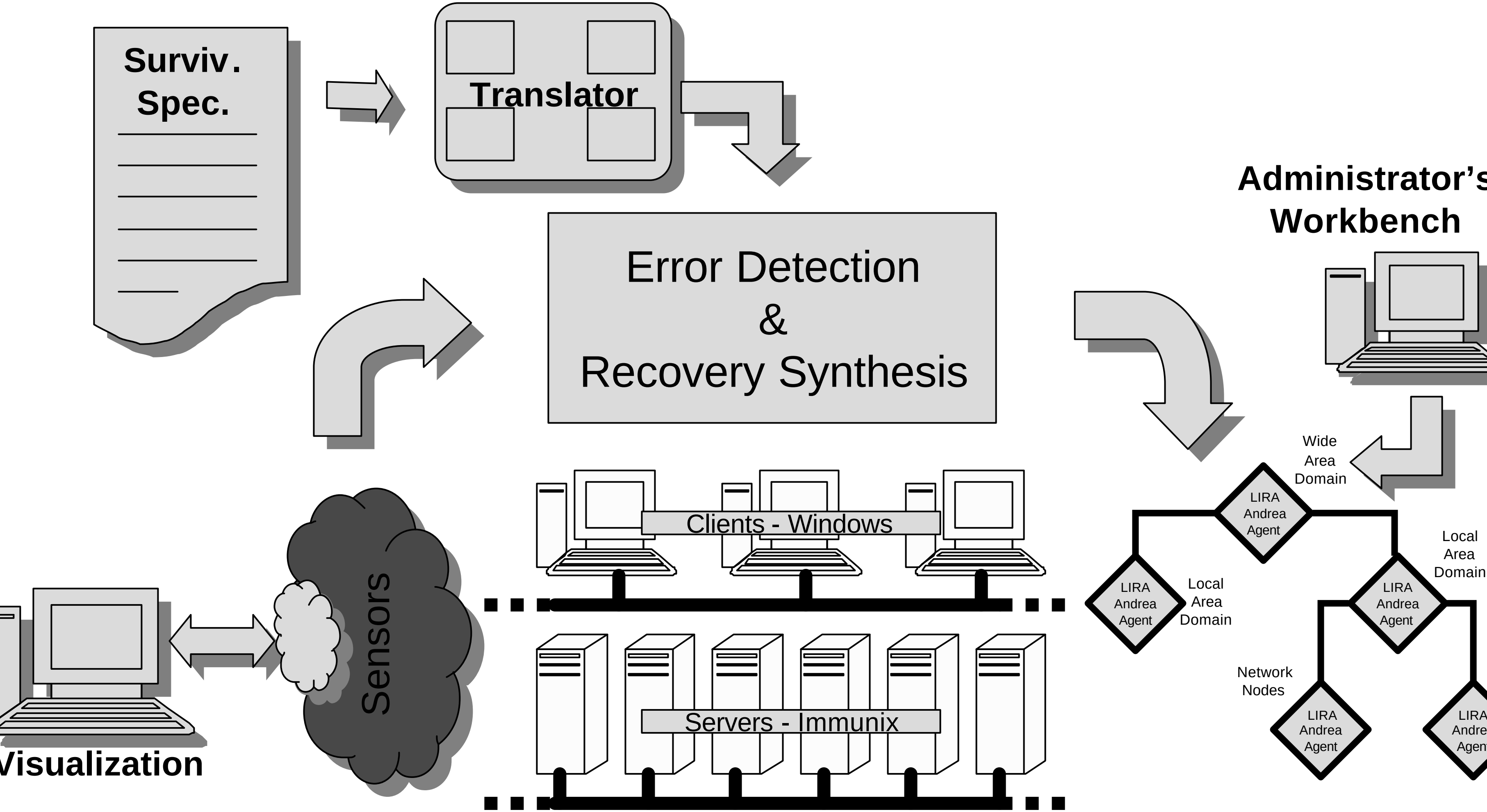


Faults In Information Systems

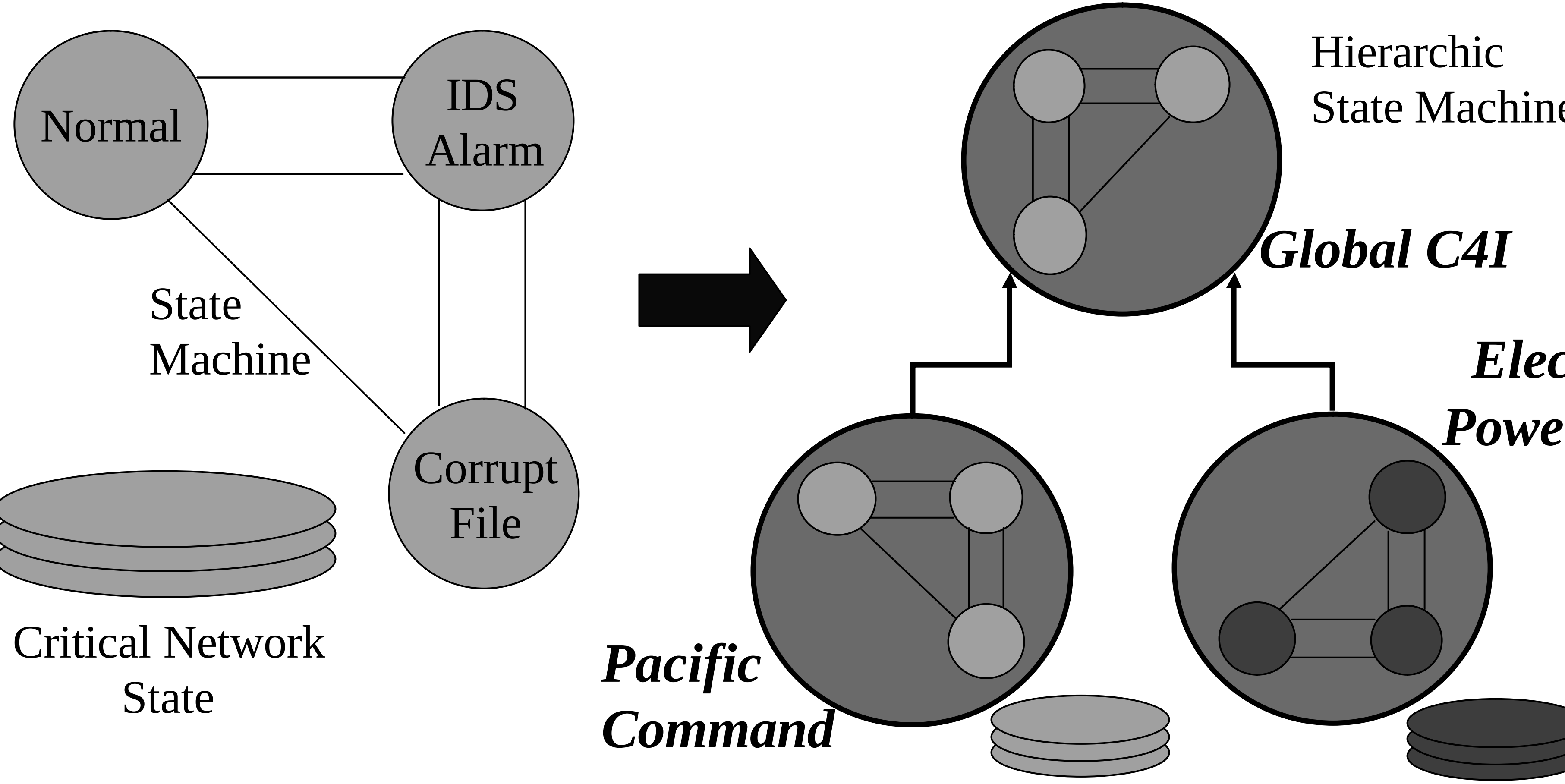
- Very Large Networks
- Interdependent Network
- Heterogeneous Nodes
- Non-Local Faults
- Sequential Faults



Willow Reactive Control Mechanism



Error Detection
Via Hierarchic State Machines



Normal

IDS Alarm

Corrupt File

State Machine

Critical Network State

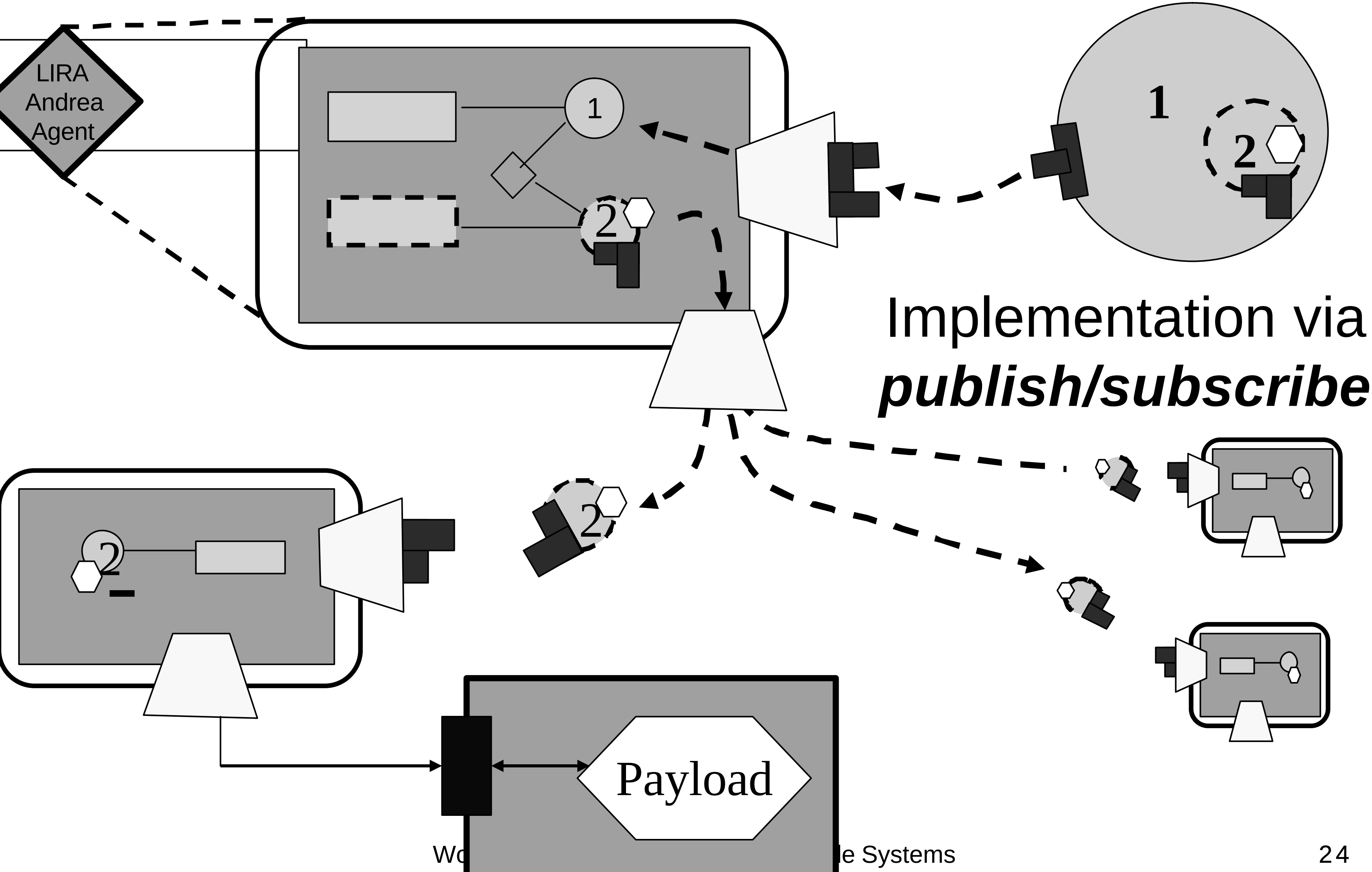
Hierarchic State Machine

Global C4I

Elec Powe

Pacific Command

Control Via Selective Notification



Implementation via ***publish/subscribe***

Survivability

For Systems Where The Alternatives Are Infeasible

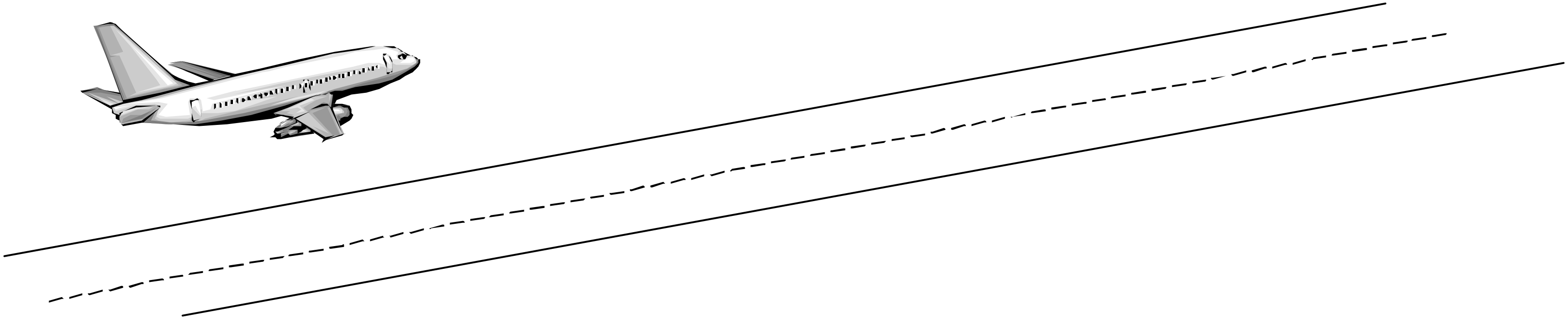
Safety-Critical Systems

- How reliable do safety-critical systems have to be?
- Ultra reliable, of course. They are safety-critical by definition!
- Regulating agencies agree, e.g. FAA:
  - “Failure conditions which would prevent continued safe flight and landing must be extremely improbable. “Extremely improbable”, corresponds to a failure rate of 10^{-9} per hour of operation.”

Safety-Critical Systems

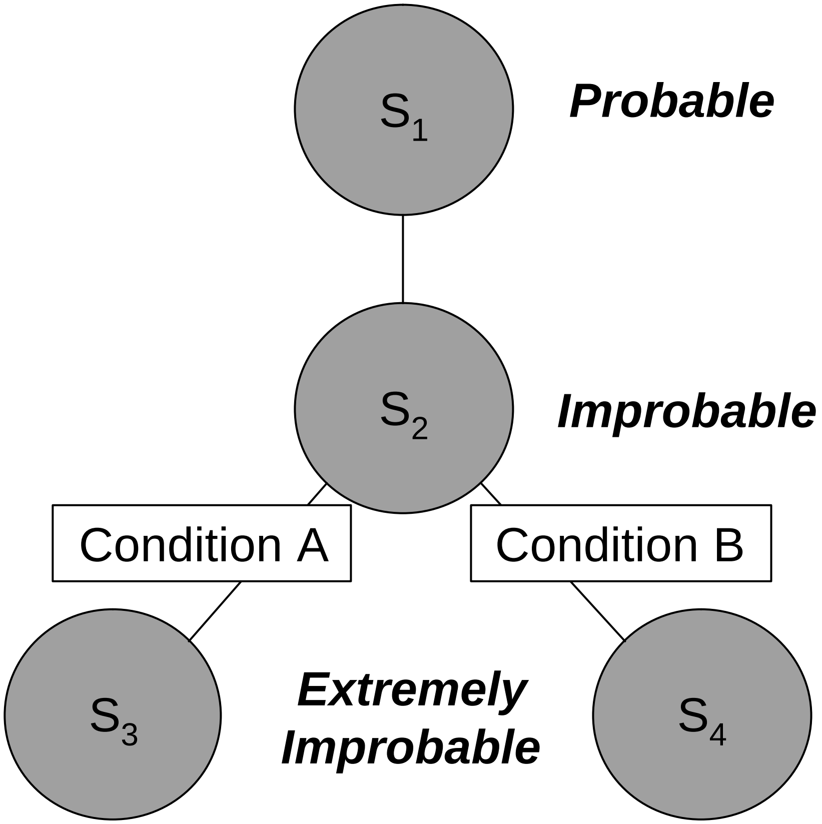
- Numbers such as the FAA’s are essentially impossible to demonstrate
- Some (most?) functionality in safety-critical systems does not need to be reliable, it needs to be *fail-stop* with ultra high dependability
- Would survivability be an option for safety-critical systems to achieve dependability goals? (Proposed by others, e.g., Sha)

Example—An Automatic Landing System



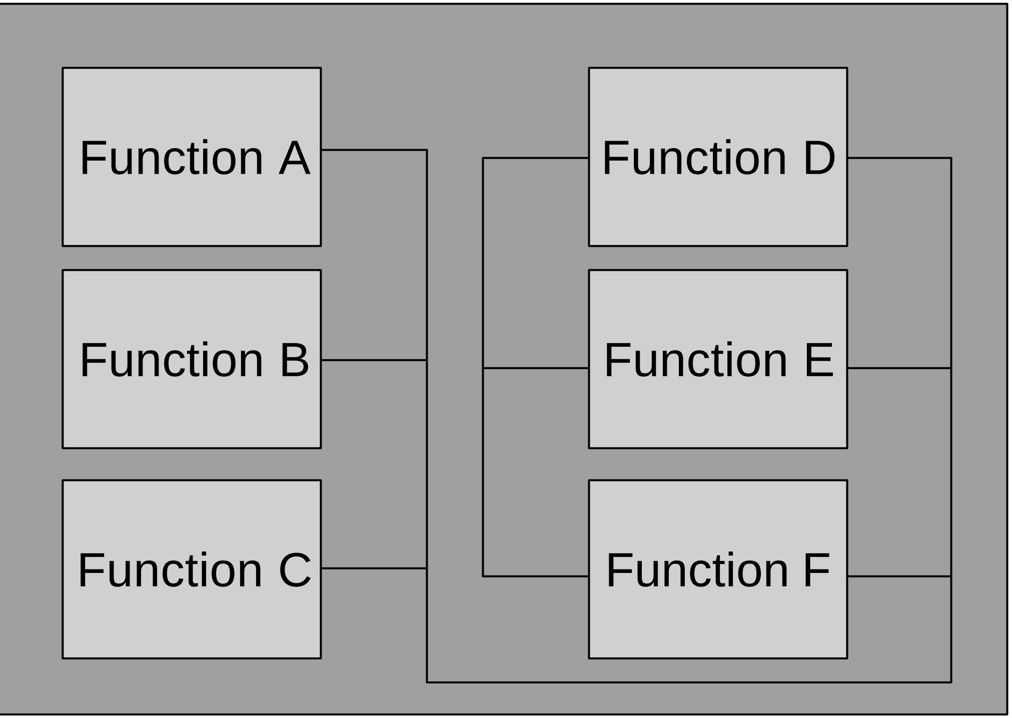
- Criticality and preferred functionality of ALS functionality depends on circumstances:
  - Cruise, above/below threshold height
  - Pilot alarm vs. go around, vs. basic landing function
- In many ways, the requirement is precisely survivability

Survivability For Ultra Dependability



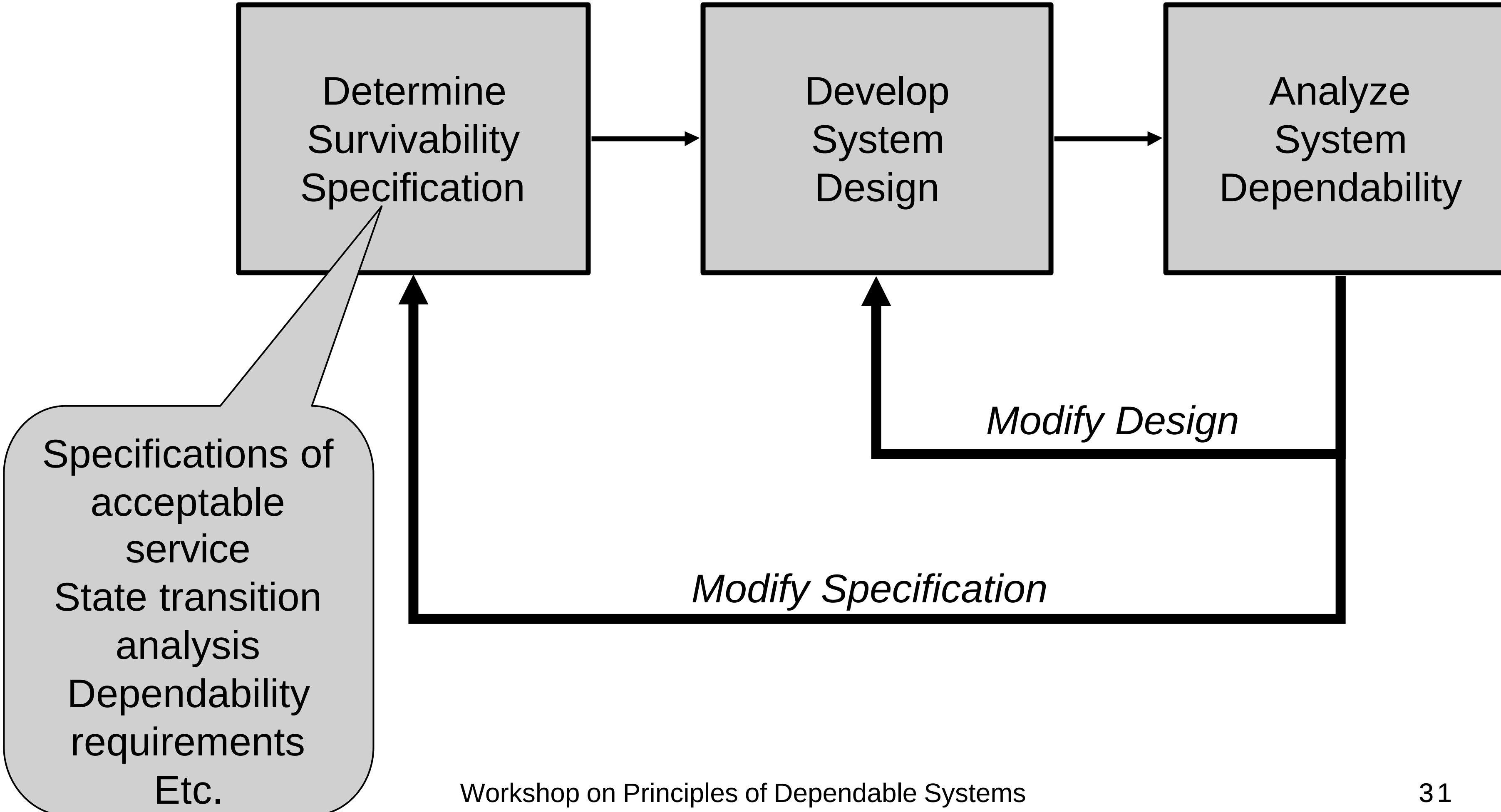
- Prescribed failure semantics
- Guaranteed transition state properties
- Bounded time to transition state
- Bounded transition time
- Bounded time value calculation
- Etc.

Integrated Modular Avionics



- Dozens of functions on same platform
- Interdependent functionality
- Isolation has been a primary concern
- What about functional dependence?
- Survivability:
  - □ Overall
  - □ Components

Engineering a Survivable System


Determine Survivability Specification
Develop System Design
Analyze System Dependability
Modify Design
Modify Specification
Specifications of acceptable service
State transition analysis
Dependability requirements
Etc.

Conclusions

- Survivability is a useful notion
  - It is a tradeoff between cost, value, and desired dependability
- To be applied, we need a precise definition, we have developed one
- Application in critical networked applications is evolving
- Application to safety-critical systems seems like a reasonable direction

Questions?

Contact Information

John C. Knight
Department of Computer Science
University of Virginia

knight@cs.virginia.edu
http://www.cs.virginia.edu/knight