The Concept of a Software-Free Resilience Infrastructure for Cyber-Physical Systems

Algirdas Avizienis
Distinguished Professor Emeritus, UCLA and
Rector Emeritus, Vytautas Magnus University, Lithuania

IFIP WG 10.4 Meeting, Queenstown, New Zealand
January 26-30, 2017

The Evolution of the Means for Dependability

· ***First Generation:***

Hardware error detection, then human response - ILLIAC 1 diagnostics, etc.

· ***Following Generations:***

The human is replaced by OS software and service processors SP.
Probably the first SP was the *Test and Repair Processor TARP* in the *JPL Self-Testing And -Repairing (STAR)* computer, proposed in 1962, demonstrated and patented by NASA in 1969.

·

The Goal of my Invention

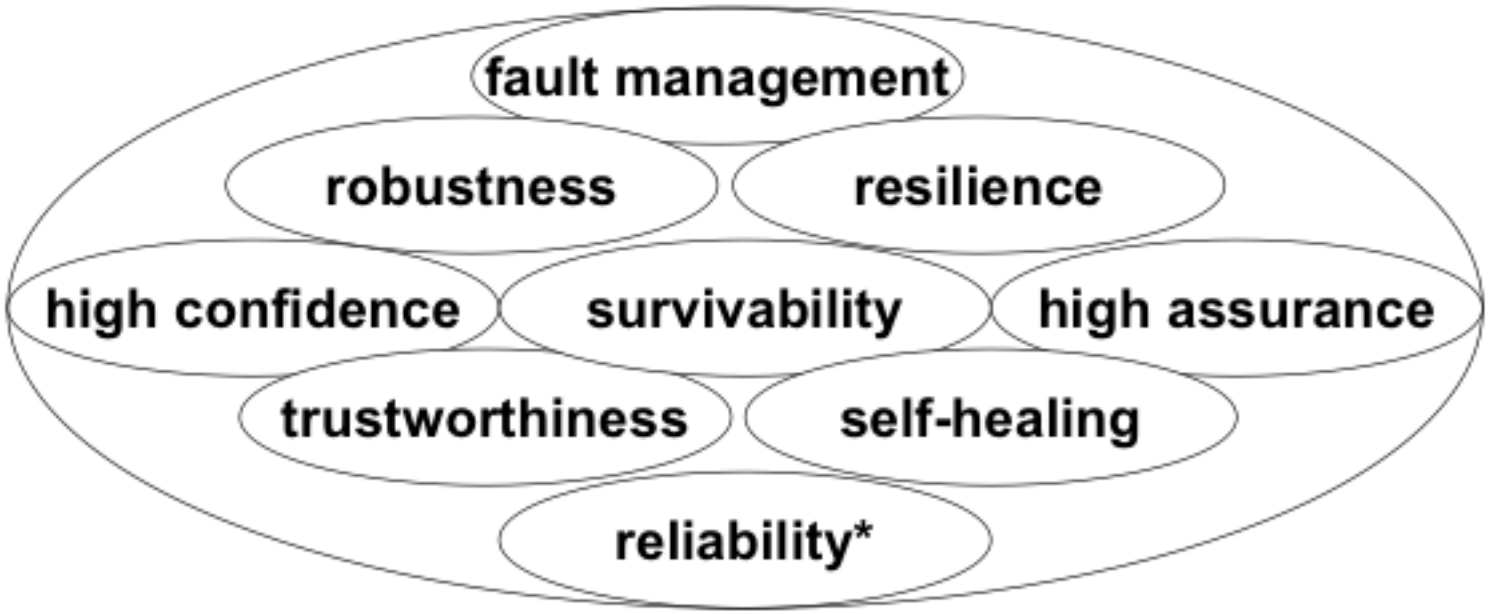
Use only hardware and firmware to provide a ***Resilience Infrastructure RI*** that complements the software and other fault tolerance capabilities of a ***Client*** system.

Make the ***RI*** fully fault-tolerant by using mature and well known hardware fault tolerance techniques, as used in

the JPL-STAR, FTMP, Stratus, August, and other fault tolerant computers.

Our Field's Objective: deliver expected service under adverse circumstances

Beside ***dependability*** *we have* ***top concepts:***



***used as a top concept, not as an attribute of dependability**

The Quantitative Definition of Dependability

The ***dependability*** (of a system)
is the ability to avoid service failures that are
(1) more frequent, and
(2) more severe
than is acceptable (to the user)

The Dependability Specification

1. Maximum Acceptable Frequency of Service Failures
2. Maximum Acceptable Severity of Service Failures:
   (a) Maximum Duration of a Service Outage
   (b) Unacceptable Modes of Service Failure
3. Fault Classes to Be Tolerated
4. Properties of the Use Environment

Resilience as defined by J.-C. Laprie
in "From Dependability to Resilience", *Proc. DSN 2008, supplemental volume, Anchorage, AL, June 2008*

supplemental volume, Anchorage, AL, June 2008.

"*Resilience* is the persistence of dependability when facing changes."

There are *3 dimensions of changes:*

1. their ***nature***: *functional, environmental, technological* (hardware and software)

2. their ***prospect:*** *foreseen* (new software versions), *foreseeable* (new hardware), *unforeseen* (new types of threats, new fault classes, etc.)

3. their ***timing***: *short term* (seconds to hours), *medium term* (hours to months, as in new versioning or reconfigurations), *long term* (months to years, as in merger of airline or banking information systems, or in military coalitions)

The Definition of Resilience Used Here

- ***Nature*** of Change - functional, environmental and technological
- ***Prospect*** of Change - unforeseen only, that is: beyond the

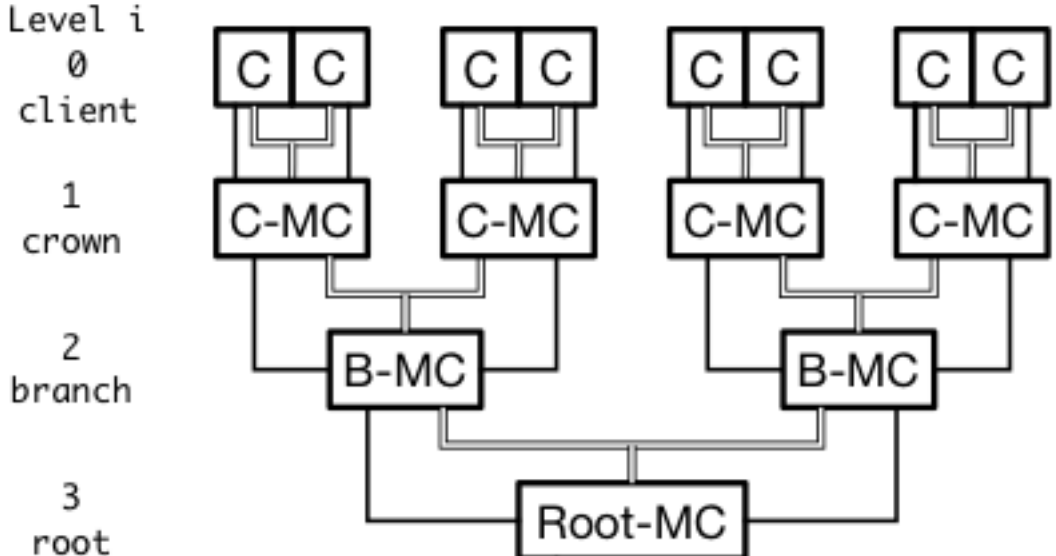
original dependability specification of the Client system

- ***Timing*** of Change - short term only: nanoseconds to seconds

★ ***Resilience*** is the *persistence of dependability* when the Client system is affected by *unforeseen short-term changes* in its *function* (unknown design faults, vulnerabilities, physical damage, etc.), its *environment* (excessive radiation, large temperature changes, etc.), and its *hardware and software* (fault classes outside the Client's dependability specification).

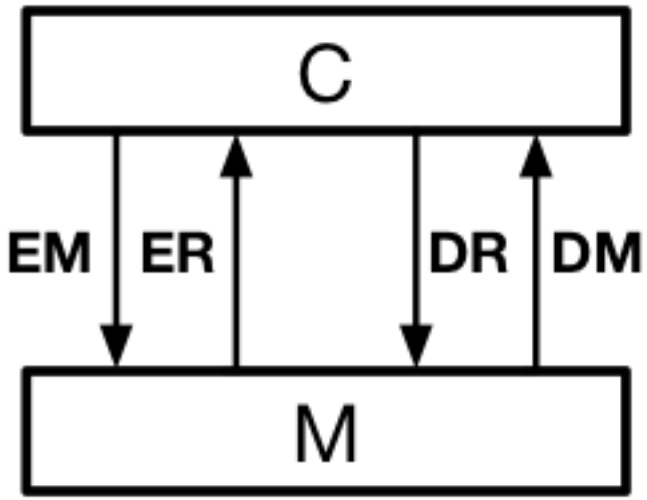
Properties of Resilience Infrastructure RI

(1) the *RI* is a ***tree structure*** of Monitor Clusters MC connected to Client modules C to form the RI-tree.



Properties of Resilience Infrastructure RI

(2) the RI is ***separate*** from Client system. Only connections are Error Messages EM and Data Requests DR from Client modules C and Client-specified Error Responses ER and Data Messages DM from the Monitor M of RI to C.



Properties of Resilience Infrastructure RI

(3) the RI is ***generic*** - it supports any Client System that can issue EM and DR and receive ER and DM that are specified by Client designers.

(4) the RI is ***self-protecting*** - it uses well-known hardware and firmware fault tolerance techniques. RI contains no software and does not need any external assistance for fault tolerance.

The Client System

- A Cyber Physical System

- A Cyber-Physical System
- Replaceable C-Modules with f-t. Infrastructure Port and physical boundaries
- External Power On-Off Control of each C-module

The Monitor Module M

- The Crown Monitor C-M is connected to the I-Port of a C-Module
- The Branch Monitor B-M is connected to the I-Port of another Crown or Branch Monitor

Monitor

- The Root Monitor Root-M is located at the bottom of the Monitor Tree and holds the Survival Module S

The Manager

- An external Entity authorized to access Root-Monitor Data and (if specified by the Client's owner) to issue commands to the Monitor modules and the Client modules

An Elementary RI: the Fault Tolerance Path

- Two f.-t. inputs (EM): Heartbeat of C and Power Status of C
- Two f.-t. outputs (ER): Restart C and C-Power On/ Off switch control
- Two functions: (1) replace failed C-module, (2) Client Power Off/On for catastrophic events.
-

An Enhanced RI: the Fault Tolerance Path

Tolerance Path

- The Client supplies to the M a ROM with responses ER(i) for inputs EM(i) for i= 1,…,n
- The ROM may be exchanged as requirements for for values of ER(i) change.

An Elementary RI: the Data Path

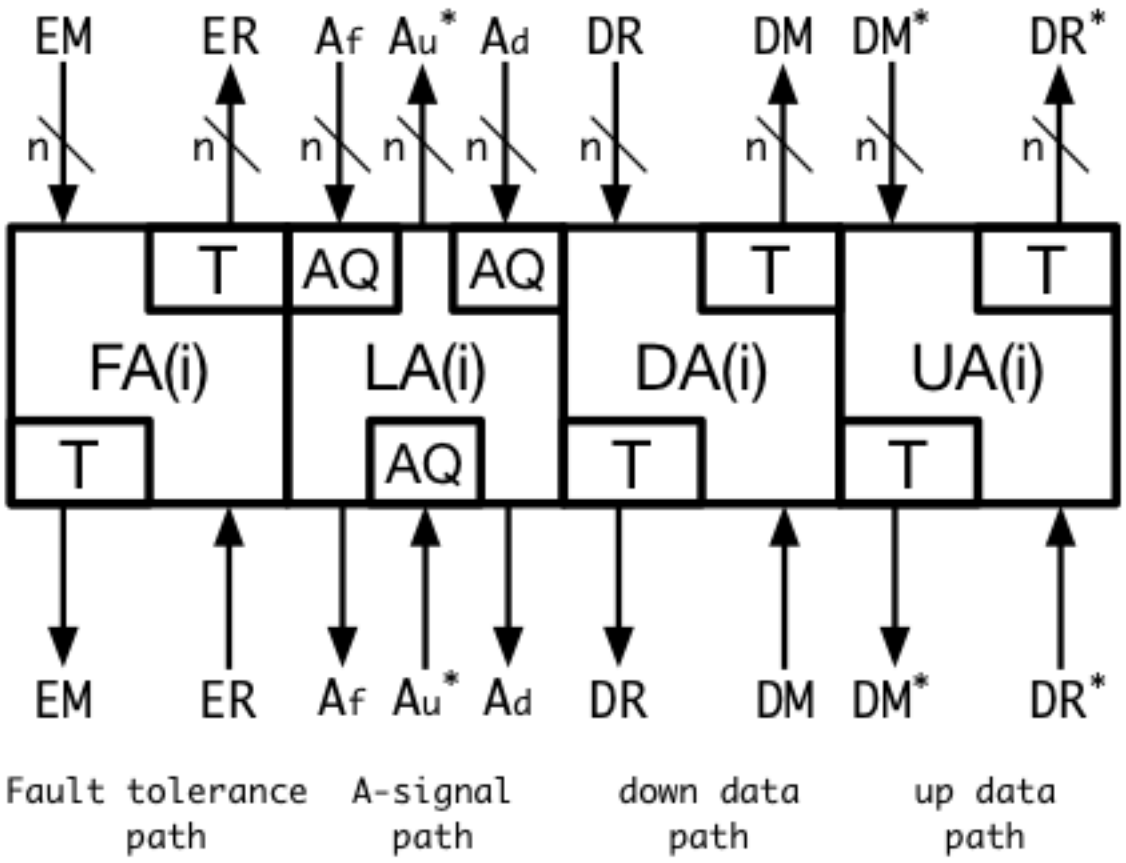
- The C-Module sends data with a

specific service request, for example - execute a majority vote, or an N-version decision algorithm, etc.

An Enhanced RI: the Data Path

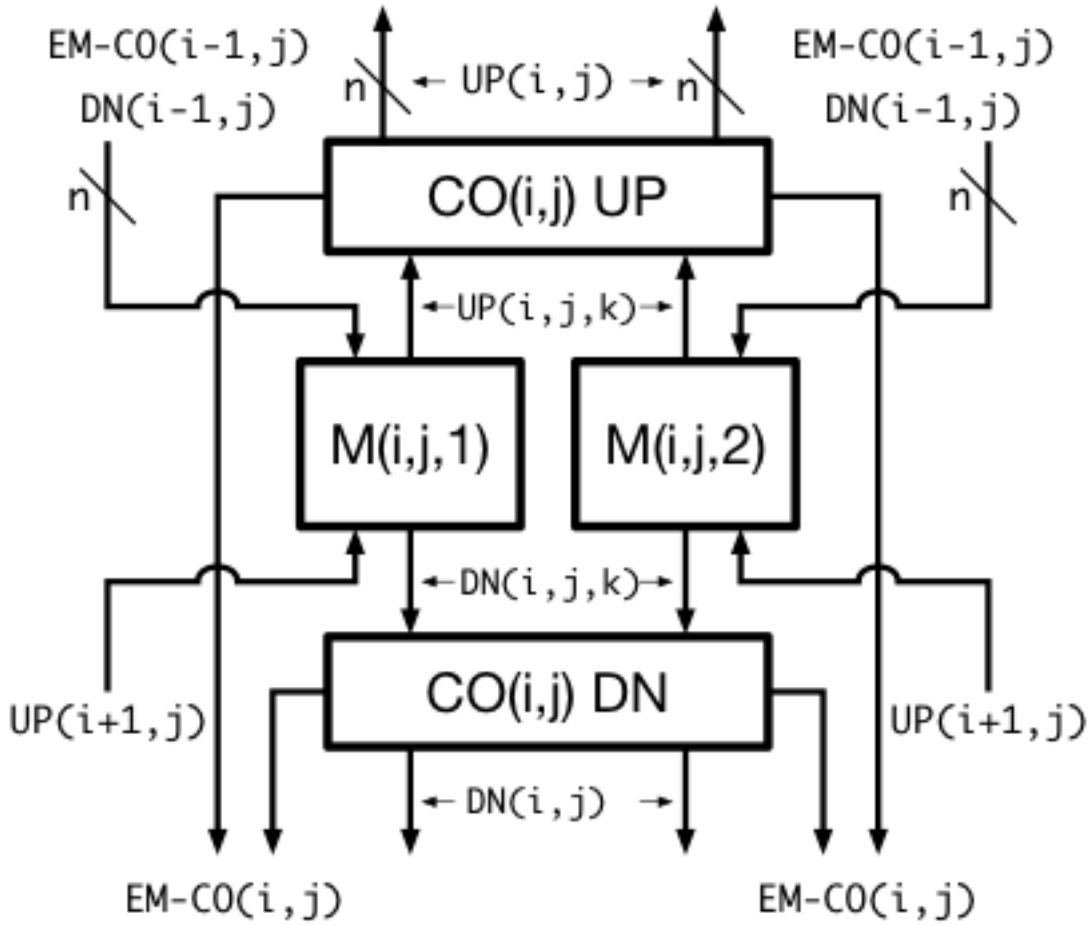
- The Data Path also includes fault-tolerant messaging between any pair of C-Modules and between the Manager (via the Root-Monitor) and any C-module

Functional Structure of one Monitor M(i)



Cluster MC(i,i) implemented as a Self-

Checking Pair of Monitors M(i,j,k)

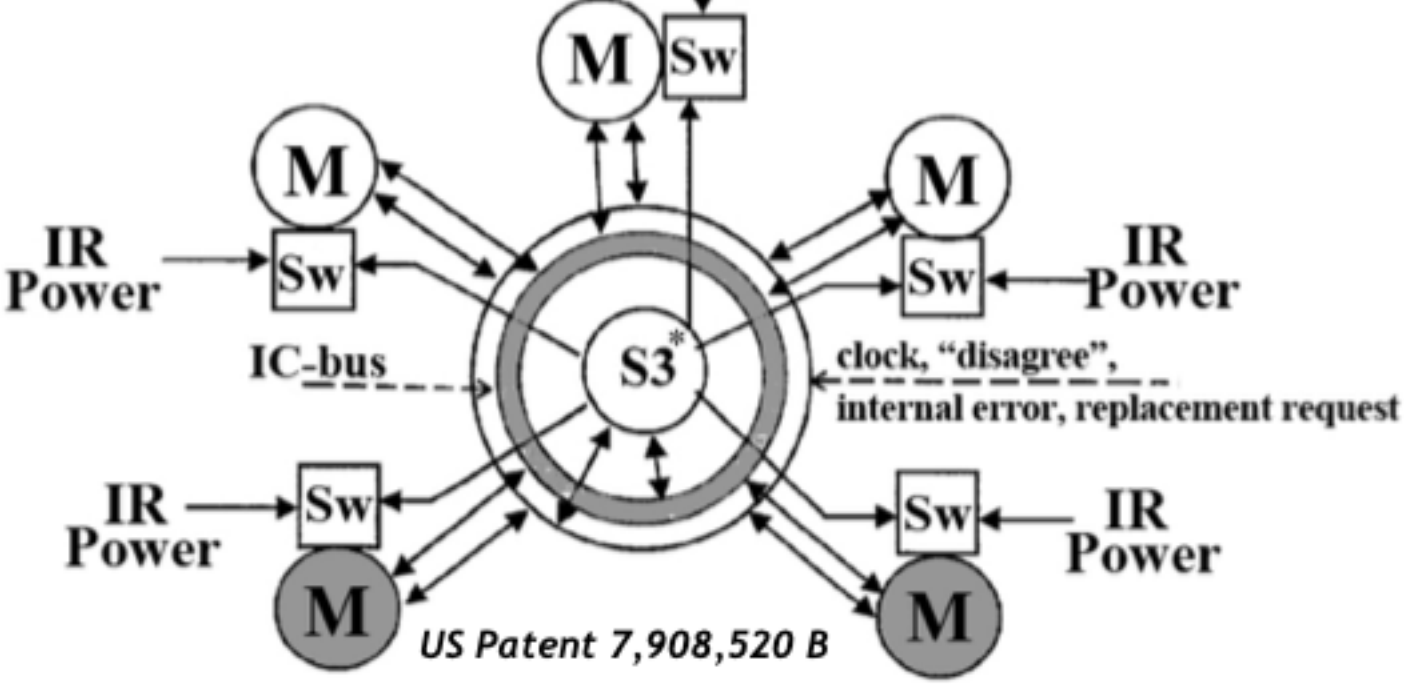


The M-Cluster Root-MC

TMR with two spares and degradation

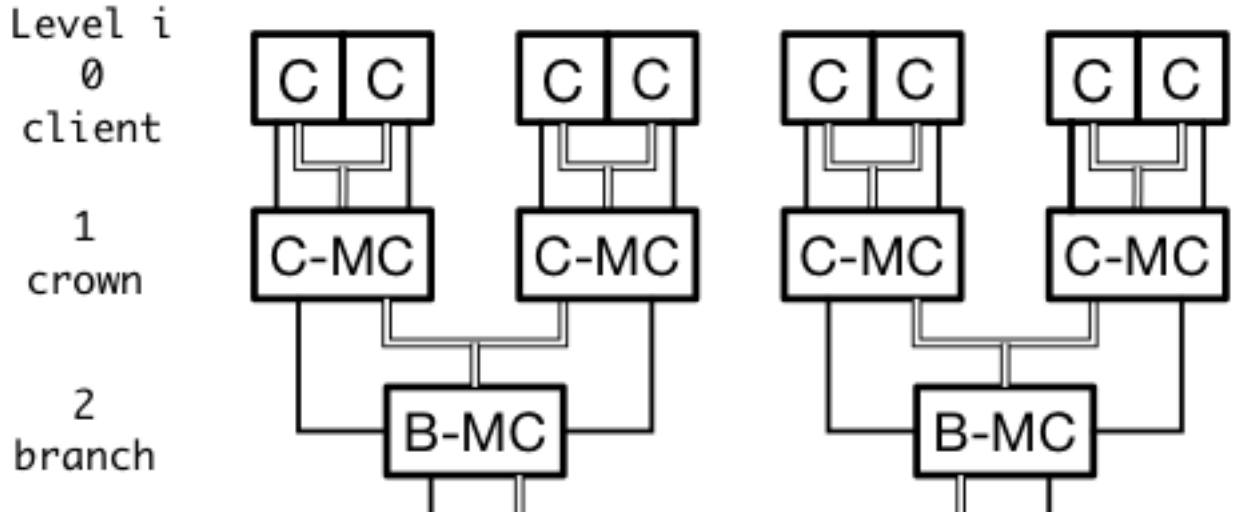
S3 is the Survival Module Cluster*

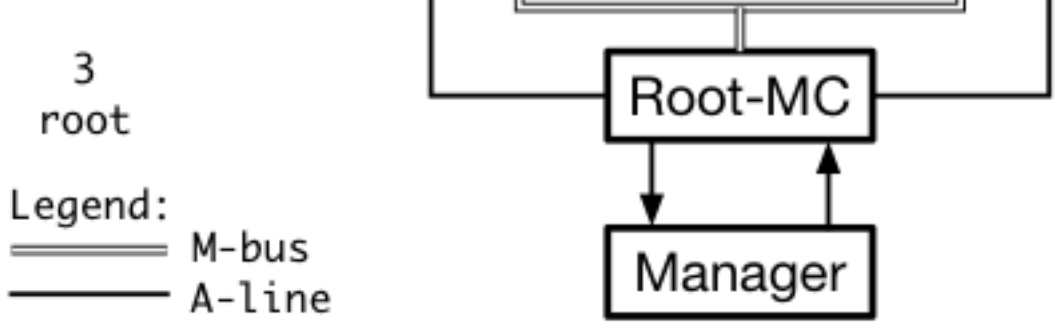
IR Power



Properties of Resilience Infrastructure RI

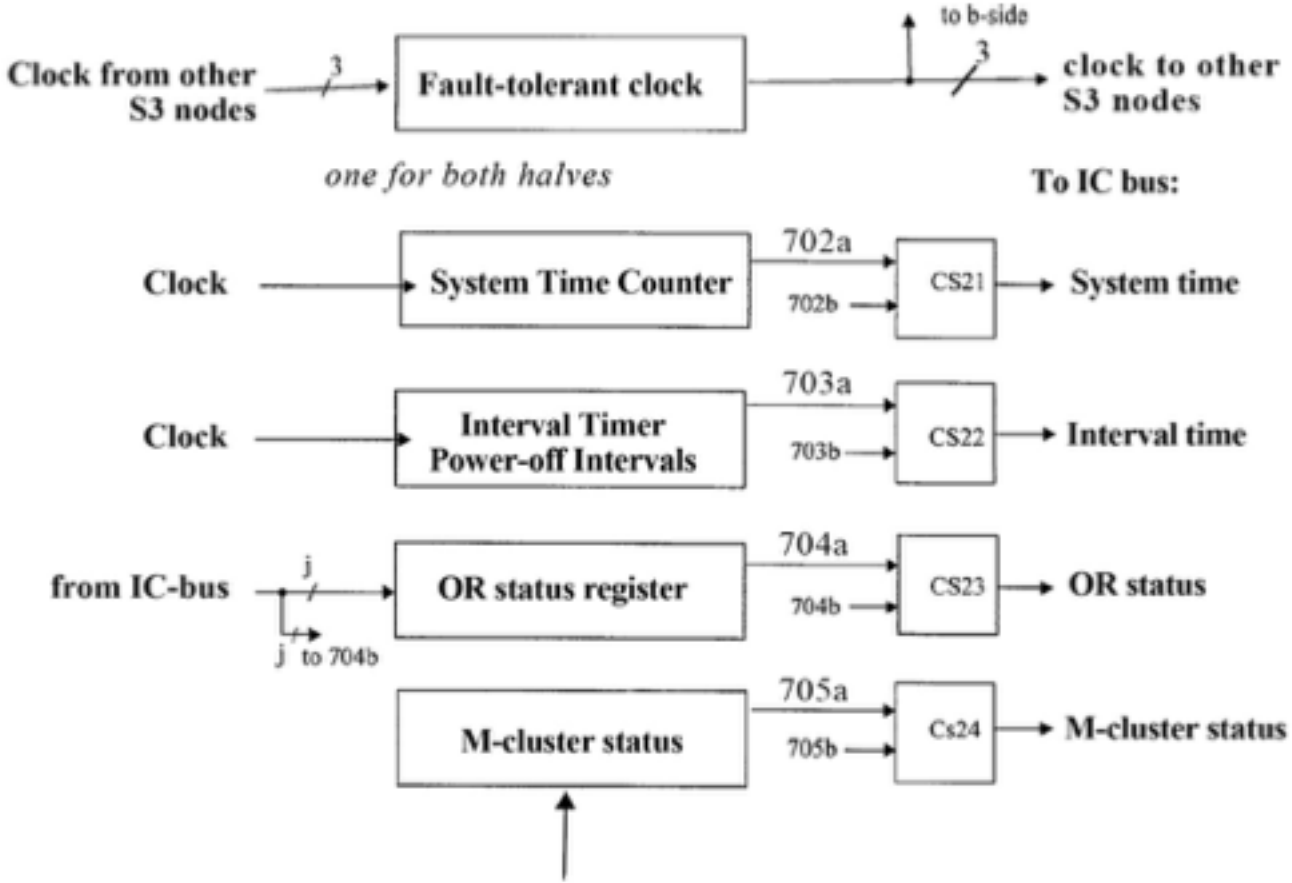
(1) the *RI* is a ***tree structure*** of Monitor Clusters MC connected to Client modules C to form the RI-tree.



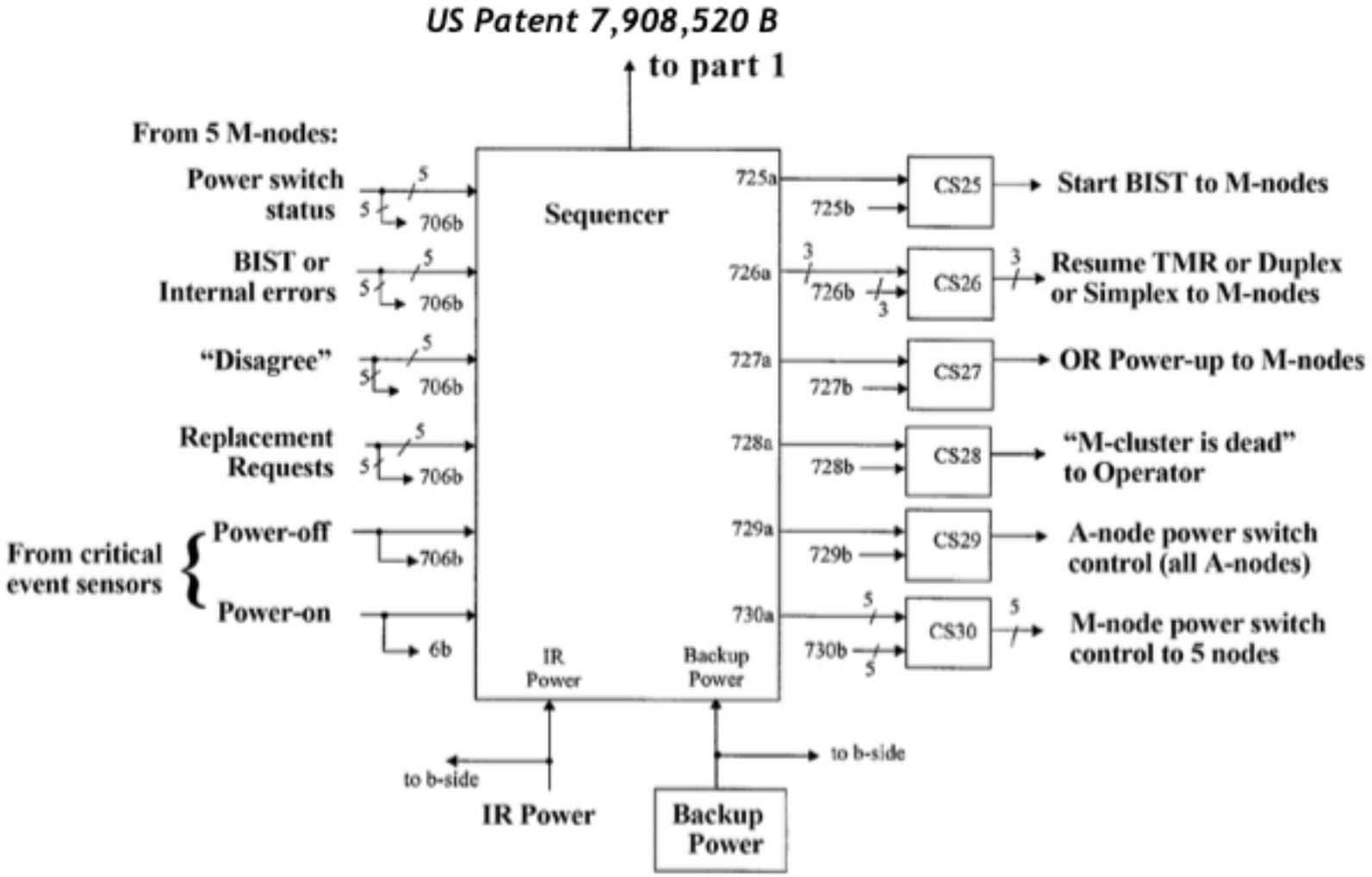


One Half of Survival Module S (Part 1)

US Patent 7,908,520 B



One Half of Survival Module S (Part 2)



In Conclusion: Will the RI Be Used ?

- ***NO:*** Legacy favors software command of recovery !

- ***YES:*** a new software-free “last line of defense” will be needed in cyber-physical systems of the future !!!
- Our favorite application of the RI - the spaceship for human visit to Mars and the habitation on Mars

We hope that it will happen !

- Algirdas, Rimas, and Audrius Avizienis