REDUNDANCY VERIFICATION ANALYSIS

Practice:

Redundancy verification analysis (RVA) is used to verify internal redundancy within electronic assemblies, as well as "cross-strap" redundancy between them, in cost or schedule constrained spacecraft development projects. At the subsystem, assembly, or unit level, it can identify interactions and failure scenarios specific to redundant configurations. RVA tracks a signal from its source to the end of the signal path, through all the subsystems along the way, including software.

Benefits:

RVA verifies the signal level from "end-to-end" that is, it tracks a signal from its source to the end of the signal path, through all the subsystems along the way, including software. The analysis focuses heavily on the verification of internal redundancy. It also verifies the design at the cross-strap interfaces between subsystems, assemblies, and units to reveal single failure points and sneak path sites where redundancy can be compromised. As an added benefit, the approach generates text descriptions and block diagrams that provide a compact, yet high resolution depiction of both the fault protection and the overall functional features of the cross-strapped portions of the design.

RVA goes into more detail than a system-level FMEA, and it extends investigation and knowledge of system performance across subsystems to more fully and accurately express the tolerance of the design to single failures. The most important knowledge gained by a system FMEA is provided by an RVA, and more.

RVA can be initiated at the system block diagram level, and expanded in a detailed fashion as soon as preliminary schematic diagrams of the design are available. Iterations with each release of updated schematics are necessary to assure that fault tolerance is maintained. RVA is consistent with the present NASA emphasis on "faster-better-cheaper" spacecraft design and development; it is:

1. **Faster** because it takes less time than a FMEA to be performed to a level that provides a thorough, accurate coverage of the design implementation,

2. **Better** because it not only accomplishes its primary task of assuring fault tolerance in the design, but also produces a series of block diagrams that exhibit in detail the functionality of the design, and

3. **Cheaper** because it focuses on those areas where redundancy may be compromised, rather than detailing the entire design regardless of obvious block-redundant features.

Programs That Certified Usage:

Mars Global Surveyor

Center to Contact for Information:

Jet Propulsion Laboratory (JPL).

JET
PROPULSION
LABORATORY

REDUNDANCY VERIFICATION ANALYSIS

Implementation Method:

Technical Resource Requirements

Table 1 summarizes the technical resources required to conduct RVA of spacecraft systems.

Resource Requirement		Mandatory	Desireable
Required Technical Experience:	• Electronic engineering and circuit design background.	•	
	• Ability to decipher unfamiliar schematics and attain an understanding of circuit operation.	•	
	• FMEA experience with electronic parts and circuits.	•	
Software Requirements:	• Circuit analysis program (e.g., SPICE).		•
	• Graphics program capable of text and graphics		•
Documentation Requirements:	• Schematics (board and box level as necessary to describe all electrical connections).	•	
	• Interconnect wiring	•	
	• Mechanical layout.		•
	• Parts list.		•
	• Circuit requirements and description.		•

Table 1. Technical Resources Required to Conduct RVA

Documenting the Design-for-Redundancy Concept

The objective of RVA, as applied to the design of a spacecraft system, is to gain sufficient understanding of the function of design elements and their interfaces to verify that no single in-flight failure can compromise more than one signal path among redundant functions or assemblies. The technique requires accurate schematics describing all electrical connections. If mechanical layout documentation is available, RVA can also examine the actual "as built" properties of assemblies.

The schematics and other detailed engineering documentation provide the RVA analyst with a representation of the electrical and physical topology of the circuitry sufficient to identify those design elements that provide for functional redundancy and the ways in which redundant functions are controlled by the system. Working from the schematics and perhaps a circuit description, the analyst isolates the individual electrical circuits that comprise the design, defines their purpose, and identifies all circuit inputs and outputs. From this information, a block diagram may be drafted which

discriminates between redundant functions. Early iterations of the block diagram are typically prepared with pencil and paper; once the principal redundant features are identified, computer graphics software is effective in refining the final product. In this manner, the analyst essentially back-engineers the design to derive a high level representation of the overall design-for-redundancy concept.

The block diagram routinely combines into block representations those parts and circuits that are wholly associated with just one side of the redundant design. More attention is given to:

1. Signals that cross between sides, and

2. Paths and mechanisms that assure survival of one of the two redundant paths in the event of any single failure.

These signals and switches are shown in enough detail that a reviewer may postulate failure modes for the parts and paths and verify that these failures will not inhibit the circuit function from being executed by the redundant side.

Verifying Design Features for a Simple Circuit

Fault tolerance depends on circuitry that either fails gracefully, allowing continued functionality, or is redundant, providing more than one path for a function to achieve its intended purpose. Fault tolerant, non-redundant circuits are possible and are used in modern high-reliability hardware, but they are tricky to design, particularly difficult to verify and test, and are considered uncommon.

Redundancy can be provided by having two or more fully independent strings of equipment, each of which can achieve the mission alone. Such an arrangement has the advantage of simplicity: it is easy to analyze and test, and the probability of mission success is a straightforward reliability calculation.

Parallel independent strings, however, do not provide the degree of fault tolerance that is often required for long, zero-maintenance missions where more that one failure can realistically be expected to occur. Improved reliability can be achieved by introducing interconnections known as “cross strapping” between the strings that allow failures in more than one string to be circumvented using combinations of the subassemblies from each string. Maximum flexibility entails maximum cross-strapping; this must be traded against the difficulties of thorough testing and the single point failure risks associated with frequent commingling of signals from two or more “sides” of the design.

RVA Methodology

A straightforward implementation of typical cross-strapping for a simple circuit appears as Figure 1, which shows one side of a redundant clock divider circuit. Figure 1 can be viewed as a simplified version of the MGS clock divider. The circuit and its companion side are required to provide 2.56

MHz clocks to each side of a downstream redundant subassembly-- in this case, an inertial reference unit. At least one IRU clock must survive any single failure for the mission to succeed.

A 5.12 MHz oscillator input is divided by two and routed both to a local multiplexer and, via a backplane path, to the parallel clock divider on another board. Based on incoming clock selection signals, the multiplexer chooses between the local signal and the one from the other divider. Showing both sides of the design, the RVA block diagram appears as Figure 2.

For a relatively simple circuit design, it may be feasible for the RVA analyst to proceed directly from a logic diagram (Figure 1) to the final block diagram (Figure 2). A more complex design may require several intermediate diagrams, as explained in the next section.

Verification that the design is truly fault tolerant requires attention to three areas: the signal path, the path selection logic, and the power and ground distribution. In the above example, because of the separation of circuit elements on different boards and the use of two oscillators and two power sources, the signal paths and power and grounds are physically independent everywhere except at the multiplexers, where a U1 chip failure or +10V short could compromise both signals if it were not for the R1 series resistors.

The path selection logic is independent in each in-board manifestation, but clock divider fault tolerance relies on the independence of the four select signals, which originate elsewhere. Thus, the selection logic RVA must verify that failures affecting one selection signal (such as the signal beginning to oscillate) will not affect the signals reaching the other side.

Verifying Complex Design Features: the Mars Global Surveyor CIU

MGS is a low cost flight project which makes use of both (1) cross-strapping between redundant sides and (2) autonomous, hardware-based, fault detection and circumvention circuitry contained within a given assembly. The MGS Controls Interface Unit (CIU) contains both of these design elements and is internally redundant at the box level.

CIU Design Features

A higher probability of weaknesses in cross-strapping fault tolerance exists when, either by engineering choice or design constraints, redundancy is implemented on a single board. The clock divider in the MGS spacecraft is provided redundantly on the A4 and A9 circuit boards of the CIU and consists of strings of divider logic chips all working from the 5.12 MHz redundant crystal oscillator (RXO) source provided to each side. The circuit boards also house multiplexers that select the local or opposite side clocks used throughout the spacecraft. These multiplexers typically select either the local on-board clock source or the clock source from the opposite clock divider. In addition, most spacecraft devices requiring clocks are either fully redundant as subassemblies or have two such clocks available, one from each board.

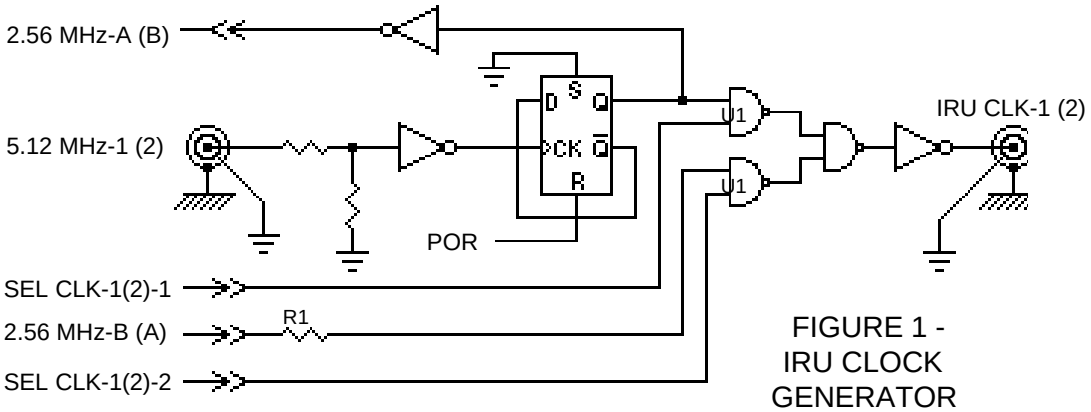


FIGURE 1 - IRU CLOCK GENERATOR

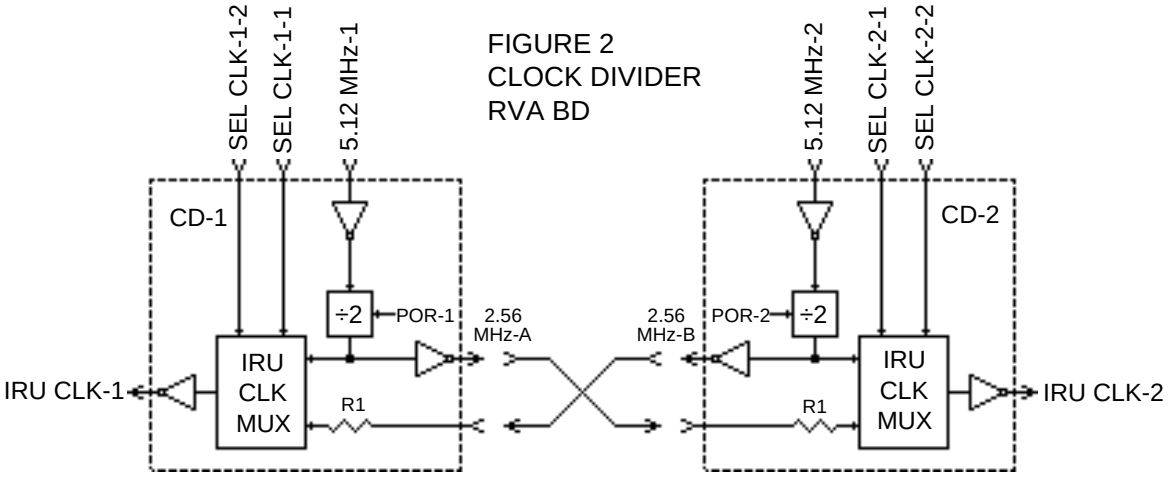


FIGURE 2 CLOCK DIVIDER RVA BD

All multiplexer clock inputs are isolated by a series resistor between the mux and the board connector. Lines that directly leave the board for the other side are also isolated before entering the local mux. This allows for failure of the mux chip where all inputs are shorted to ground or the supply voltage; the isolation resistors assure that the multiplexer on the other board has good clock inputs.

Preparation of the RVA Block Diagram for the CIU Clock Divider

These parts and paths are shown in Figure 3, the redundancy verification block diagram prepared for the clock divider. The MGS clock divider is considerably more complex than the simple circuit illustrated by Figure 1. Instead of proceeding directly to the final RVA block diagram, documentation of these clock divider features as Figure 3 was contingent upon the completion of no fewer than five intermediate diagrams:

Level 1: The process starts with an initial sketch which sorts the circuits identified in the schematics into blocks. Each block represents a circuit function, with the collection of blocks comprising one redundant side of the design. Signal paths internal to the redundant side are shown as interconnections between the blocks. Outputs that leave the clock divider for other parts of the spacecraft exit the top of the sketch, while those going to the redundant side of the clock divider flow to the bottom.

Level 2: The second drawing level produces an initial rendering of one side of the diagram in a graphics program, which is then marked up by hand to reflect an improved understanding of the schematics and circuit interactions.

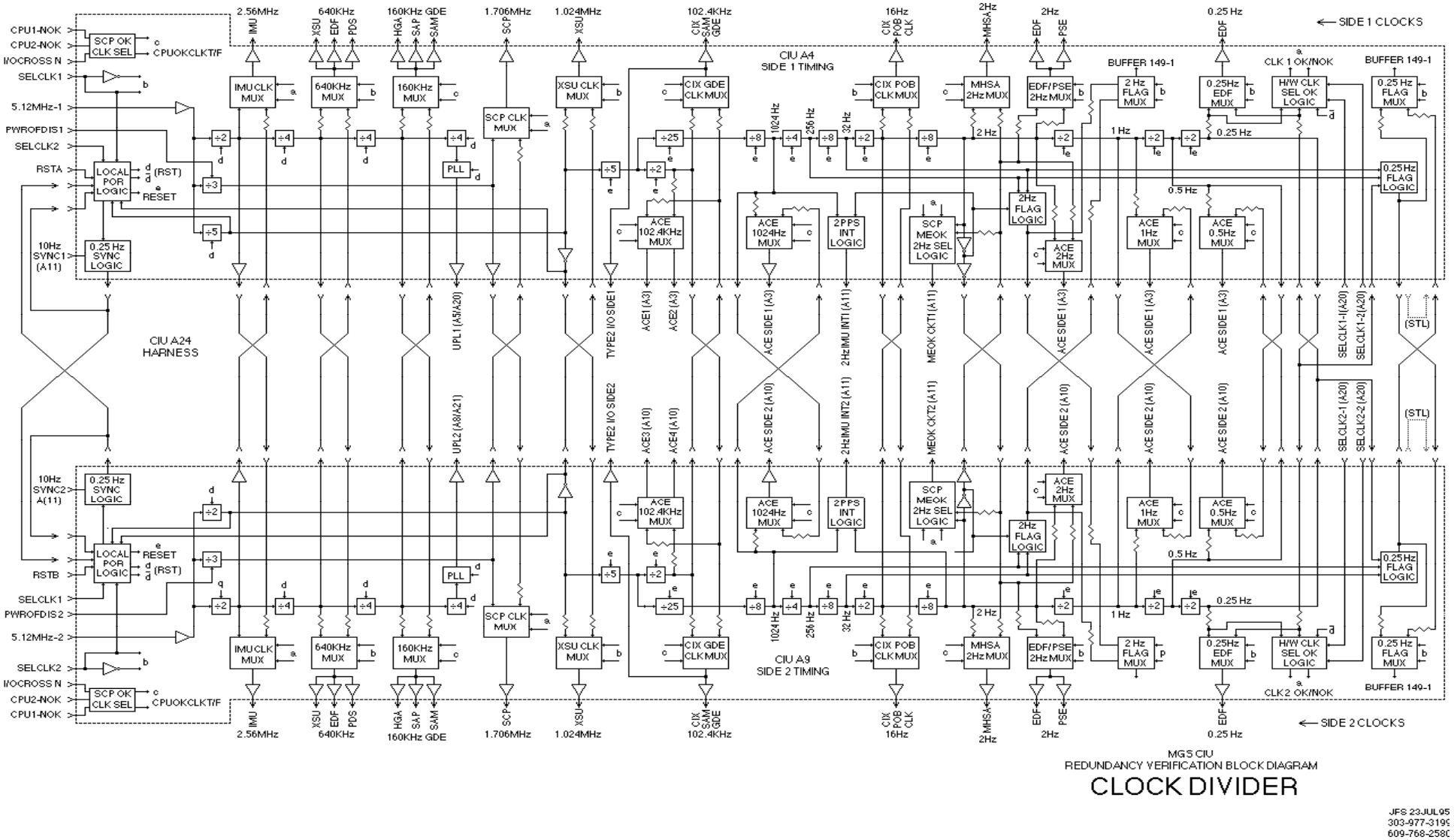
Level 3: Cross-strapped connections between discrete redundant assemblies are identified, and the second side is developed in the diagram.

Level 4: A pin check is executed to verify the backplane interconnections.

Level 5: A preliminary version of Figure 3 is released for review by other individuals familiar with the details of the design.

Following these steps, Figure 3 is released as the final redundancy verification block diagram.

Accompanying the iterative process of preparing these graphics is the generation of a text description of the design reflecting the analyst's understanding of the way it works. In addition to explaining the final diagram, the text serves as an ongoing check on the logic of the analysis, especially when it can be compared to existing descriptions of or specifications for circuit functions. The text description also covers software interactions: this is important



JFS 23JUL95
303-977-3195
609-768-2580

Figure 3

RVA Block Diagram for the MGS CIU Clock Divider (Final)

because the block diagram shows conduits for software instructions without necessarily verifying that the conduits are used properly by the software.

Technical Rationale:

JPL experience in development of the MGS spacecraft suggests that RVA offers a considerable budgetary advantage over traditional, piece-part level FMEA. Although it requires skills similar to those needed by an FMEA analyst, it takes less time to perform. The analysis identifies and focuses on the specific areas of a design that are subject to possible mission-critical failure, while quickly segregating and effectively bypassing those design elements not involved in cross-strapping.

The primary disadvantage of the technique is its reliance on the technical skills of the analyst. Failure modes and effects are postulated and exercised intellectually without a mechanism for cross-checking that all possible modes and effects are covered. This requires of the analyst a high level of technical capability and diligence.

However, RVA produces a product-- the block diagram-- which provides benefits extending beyond redundancy verification. While the results of an FMEA are often inscrutable even in its intended purpose, the RVA block diagrams present functionality data in a graphical form that is easily understood by anyone with a knowledge of circuits. The RVA diagrams for the MGS project were used throughout spacecraft integration and test. They are still in use by ground controllers as an aid in predicting and understanding the behavior of the complex command and data handling equipment aboard MGS.

Impact of Non-Practice:

Future generations of low cost, short duration missions of interplanetary exploration are expected to employ autonomous on-board switching, with fewer opportunities to correct failures by ground control intervention via uplink commands. This will require spacecraft designers to accurately determine the tolerance of redundant configurations to single failure points which may compromise autonomous switching to redundant functions. The established practice of performing FMEA to find these single failure points is laborious, may not show the actual workings of hardware and interfaces, and does not usually reveal software design flaws.

As demonstrated by JPL on the Mars Global Surveyor project, the use of RVA has shown to be consistent with NASA's emphasis on "faster-better-cheaper" spacecraft design and development. Use of traditional alternatives to RVA could present a budget and schedule risk and fail to identify deficiencies in redundant configurations.

Related Practices:

1. *Redundancy Switching Analysis*, Practice No. PD-AP-1315

2. *Failure Modes, Effects And Criticality Analysis (FMECA)*, Practice No. PD-AP-1307

3. *Fault Tolerant Design*, Practice No. PD-ED-1246

References:

1. *Redundancy Techniques for Computing Systems*, edited by Richard H. Wilcox and William C. Mann, Symposium on Redundancy Techniques for Computing Systems (1962: Washington, D.C.)

2. System Reliability Engineering, Gerald H. Sandler, 1963.