SoC Reliability Features in the FlexNoC Resilience Package

A complementary IP package for use with Arteris FlexNoC IP

Jonah Probell
Senior Solutions Architect
Arteris Inc.
Campbell, CA USA
jonah.probell@arteris.com

Benoit de Lescure
Director of Application Engineering
Arteris Inc.
Campbell, CA USA
benoit.delescure@arteris.com

***Abstract*—This document describes the need for end-to-end data and control protection in Systems-on-Chip (SoC) and describes features in the Arteris FlexNoC Resilience Package that implement this protection.**

I. Introduction

Digital integrated circuits can fail in various ways. Physical damage in the field or undetected manufacturing defects can cause short, open wires, or destroyed logic gates. Transient electrical problems can cause glitches on power supplies or clock nets that cause logic transitions to be missed or repeated. Soft errors due to alpha particles, cosmic rays, and thermal neutrons can cause logic values of small transistors to change. Logic design bugs, missed by verification, can cause chip malfunctions. Designing a resilient network-on-chip requires covering all of them.

Currently developed systems-on-chip for safety-related applications in the automotive, industrial and medical markets use CPU cores like the ARM Cortex-R5 and Cortex-R7 processors. These types of CPU core IP implement techniques like ECC and parity data protection, dual-core lockstep (DCLS) redundancy, duplicated internal memories, safety checkers, and built-in self-tests (BIST). However, this CPU-only approach neglects to provide end-to-end protection from initiator to target. End-to-end protection can only be provided by implementing resilience features in the on-chip interconnect.

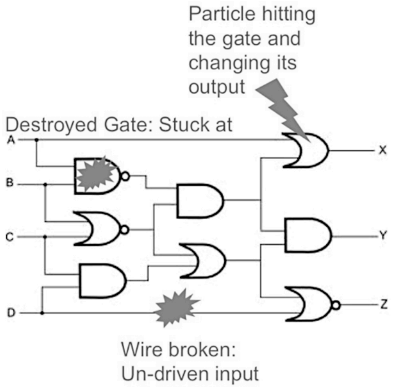
Particle hitting the gate and changing its output
Destroyed Gate: Stuck at
A
B
C
D
X
Y
Z
Wire broken: Un-driven input

Figure 1. Sources of Errors in Digital Logic

II. On-Chip Interconnect Fabric Safety Features

The following is a list of features that, combined, provide end-to-end protection of data within a system-on-chip.

A. ARM® Cortex®-R5/R7 Processor Port Checking

The ARM Cortex-R5 and R7 offer redundancy at the CPU AXI interface. To create a fully resilient system, it is necessary for the interconnect fabric of a chip to support these special interface capabilities. FlexNoC performs generation and termination of all CPU command redundancy, with support for 32 and 64 bit AXI interfaces and odd or even parity. This includes data ECC, which can be terminated and generated within the NoC, or transported to destination using byte-level ECC.

A. Custom Transport Protection

While data ECC generation and termination is supported at IP socket interfaces, an end-to-end resilience strategy requires packet transport protection. FlexNoC can pass ECC information through the NoC between socket interfaces. Alternatively, FlexNoC can generate custom data payload and control ECC in packet-generating units and detect or correct errors in packet-consuming units. The amount of redundancy per data byte is configurable based on the cost and resilience requirements of the chip.

Packet headers are also protected by parity that is checked and generated within all units that modify packet headers.

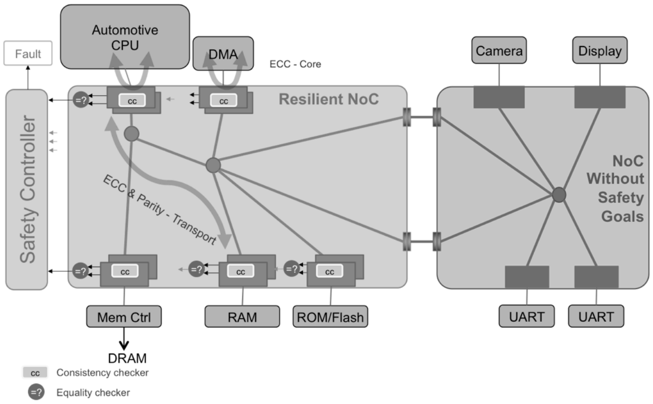

Figure 2. ECC Generation in the CPU Core or at the Fabric Edge

B. Packet Validity Checking

Packet validity is checked in all units that modify or consume packets, particularly the interface units at the edge of the NoC. This allows the detection of bad routing and word deletion/duplication.

C. Transaction Timeout

Target-side timeout in network interface units detects unresponsive target IP failures and ensures that they do not block the NoC. Initiator-side timeout in network interface units detects transport packet deletion, bad routing, or failures of stuck arbiters or targets. Timeout is detected per transaction using a pre-scaled counter to minimized hardware cost and power consumption.

D. Control Register Parity Checking

Control registers can be configured to use parity in order to detect and report any single bit soft error. Registers should be read by software after each write to confirm the correct value.

E. Unit Duplication And Comparison

Hardware duplication enables detection of complex failures and is often required to meet the ISO 26262 ASIL C and D safety integrity levels. FlexNoC supports the duplication of all units that modify packets, including network interface units. The duplicate late copy of the hardware runs with a cycle delay and is compared to state of the early copy. The delay avoids common faults due to transient clock or power glitches. Each unit has separate clock and reset inputs, and the checker uses separate independent clock gating.

Checkers also support a BIST mode in which patterns are run through the delay registers to detect stuck-at faults in the comparison logic, providing means to validate the checker after reset.

F. Fault Controller

All of the resilience features of FlexNoC can report faults. Faults are synchronized across clock domains and gathered in a fault controller unit. The fault controller generates maskable CPU interrupts and identifies fault sources. The fault controller is software-visible. It reports both BIST and mission mode faults, and controls in which mode the checkers are working.

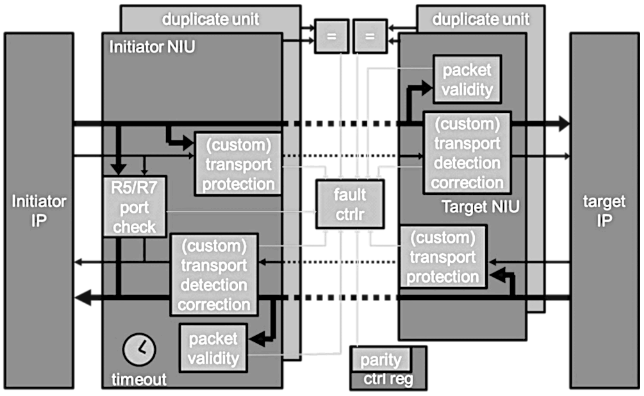

FIGURE 3. RESILIENT SOC FABRIC WITH INTEGRATED FAULT CONTROLLER

III. CONCLUSION

To be resilient to the numerous possible failure modes of chips, a resilient NoC must address many disparate aspects of its design. Arteris FlexNoC with its companion FlexNoC Resilience Package solves the resilience challenge from every angle, providing the reliable NoC technology needed for the chips serving the most critical applications. Arteris is the only source for resilient NoC IP, and a dependable partner for the world's most demanding chip design teams.