2023 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION

UNITED STATES

SAN JOSE, CA, USA
FEBRUARY 27-MARCH 2, 2023

Is Your System’s Security preserved? Verification of Security IP integration

Predrag Nikolic, Verification engineer, Veriest Solutions

Veriest

accellera SYSTEMS INITIATIVE

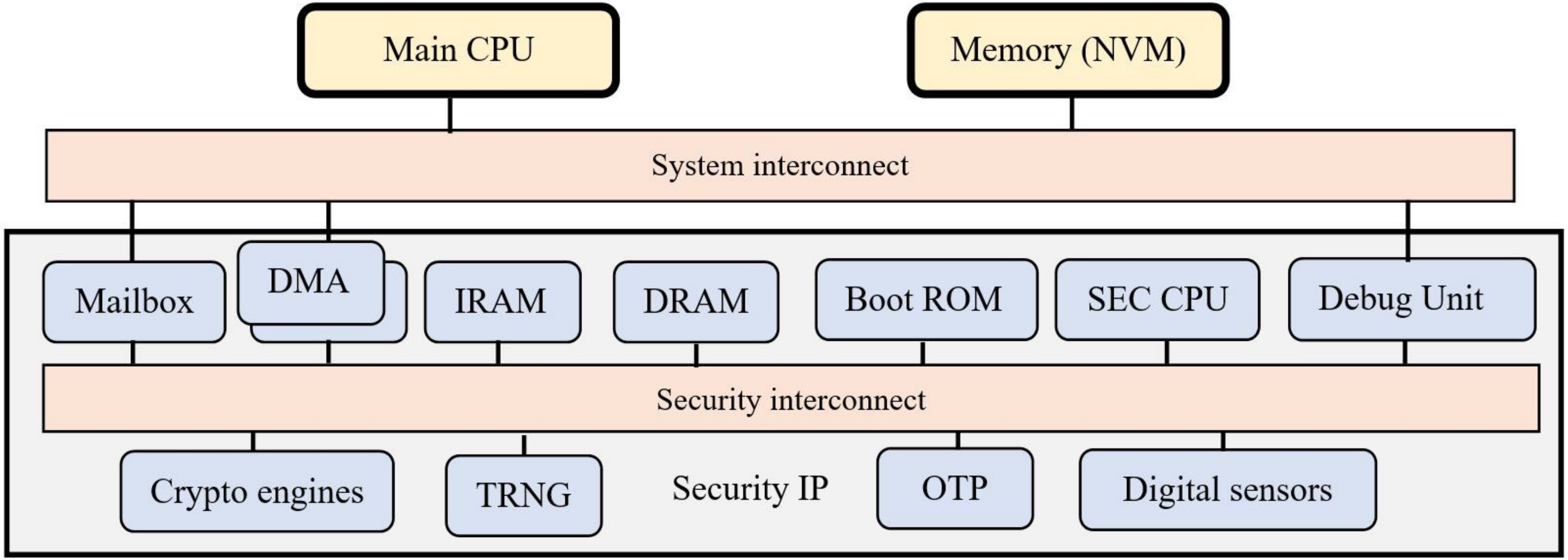
Agenda

- Introduction
- Security System overview
- Test plan
- Boot flows
- Tests
- RTL bugs
- Conclusions

Introduction

- What is the role of Security system in SoC?
- How does Security system provide the service?
- Block level verification provided by vendor
- Why do we need to verify correct integration?
- Approach used in this paper – gaps detection

Security System overview



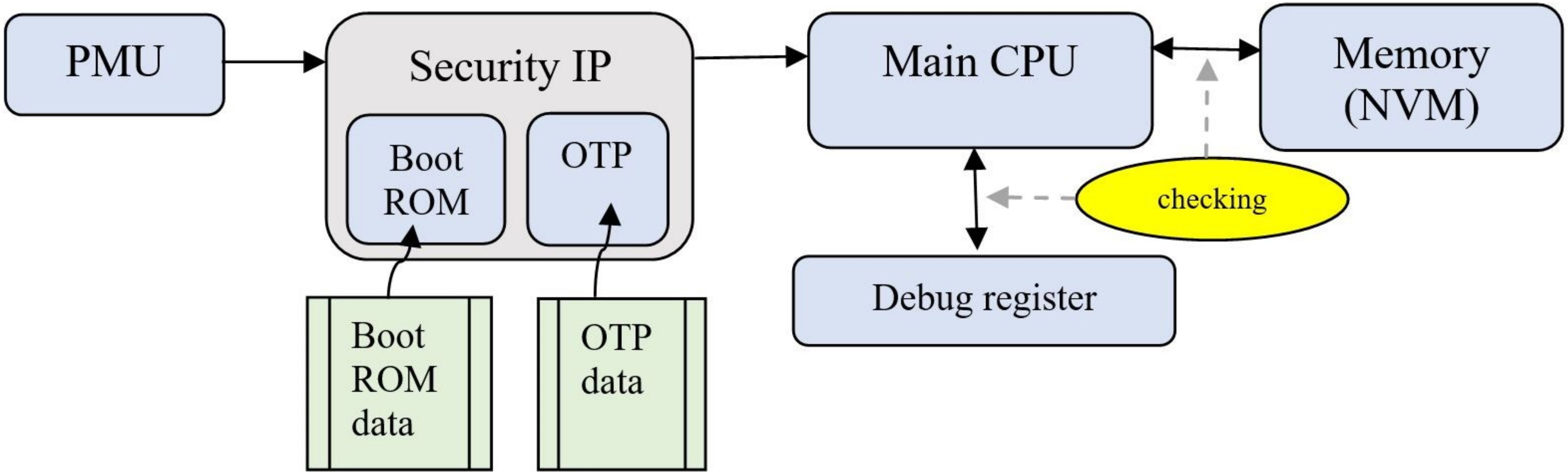
Test plan

Test name	Description
non_secure_boot_test	Complete scenario for Non-secure boot.
secure_boot_test	Complete scenario for Secure boot.
trng_test	TRNG service request
crypto_service_test	Crypto service request
debug_inf_non_secure_test	Scenarios for accessing Debug blocks in Non-secure mode
debug_inf_secure_test	Scenarios for accessing Debug blocks in Secure mode
hw_alarm_interrupts_test	Scenarios for setting HW alarm and interrupts
performance_path_1_test	Performance test for verification of the one critical path.

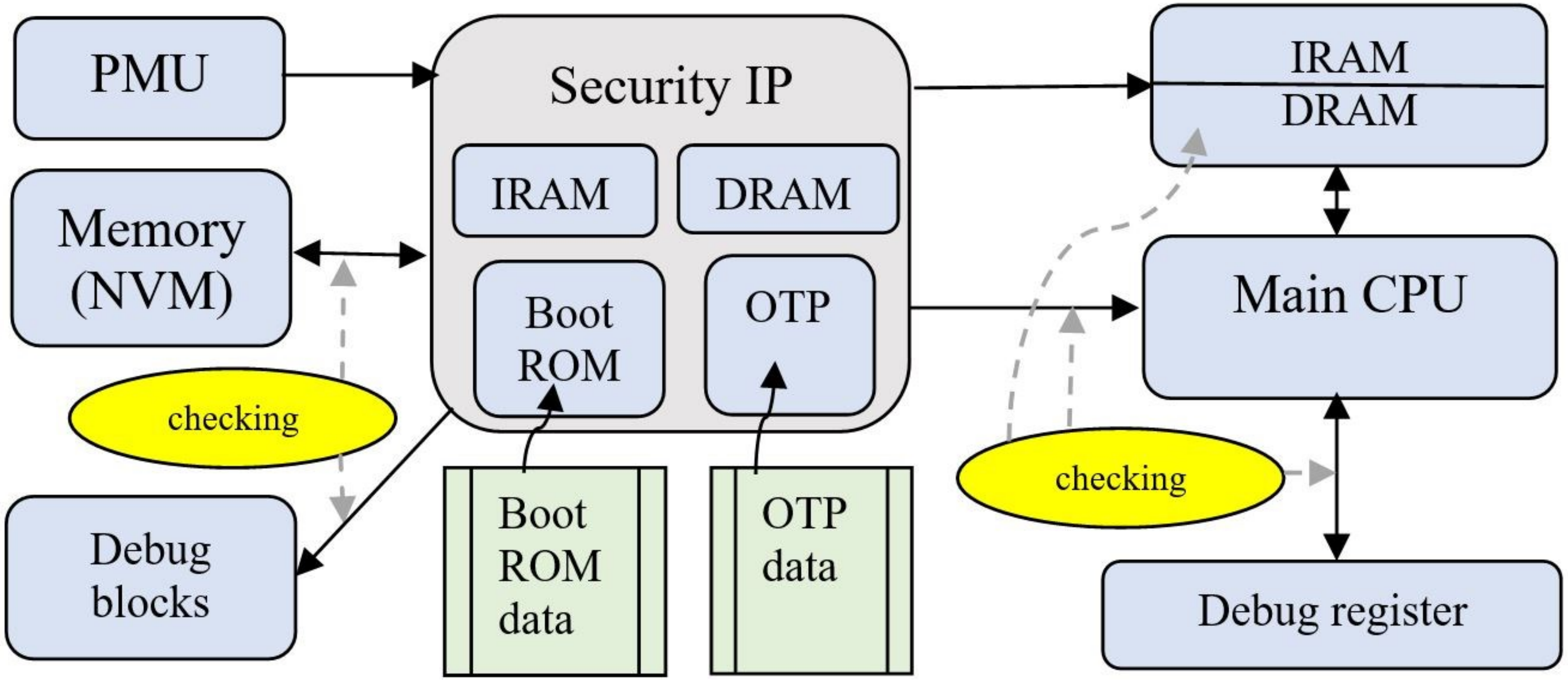
Boot flows

- Security IP is involved in power-up sequence
- IP provider cannot generate boot ROM data
- Usage of place-holder functions
- Non-secure and Secure modes of operation

Tests (1): non-secure boot

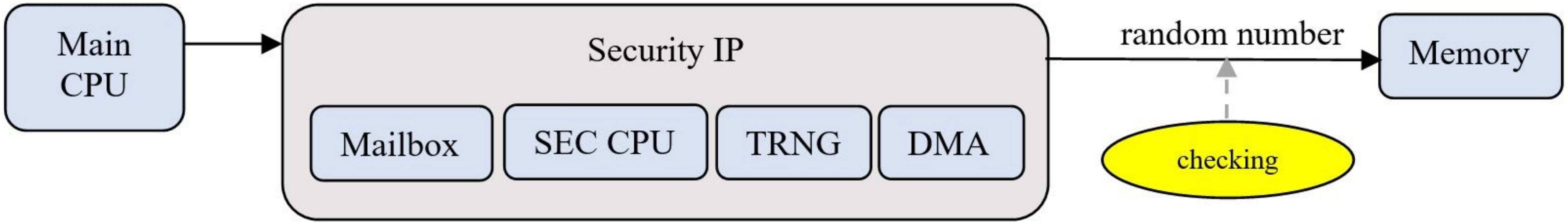


Tests (2): secure boot



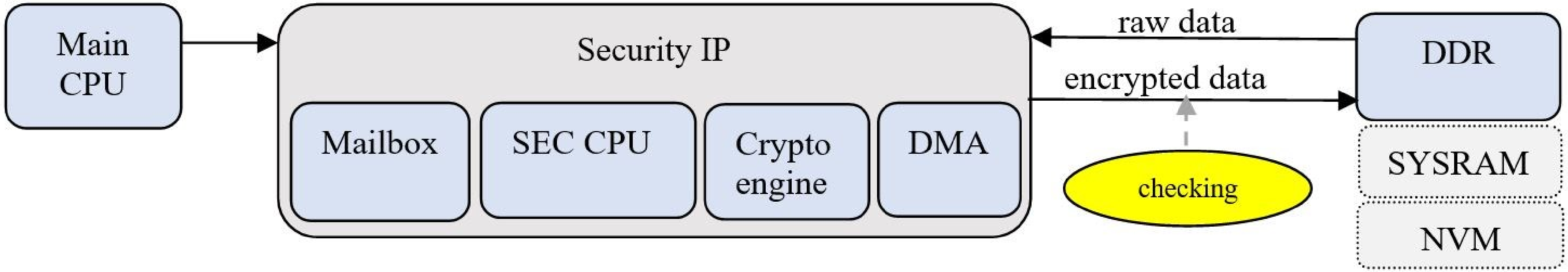
Tests (3): TRNG

- Communication between Security IP and the rest of SoC
- Usage of provided set of instructions



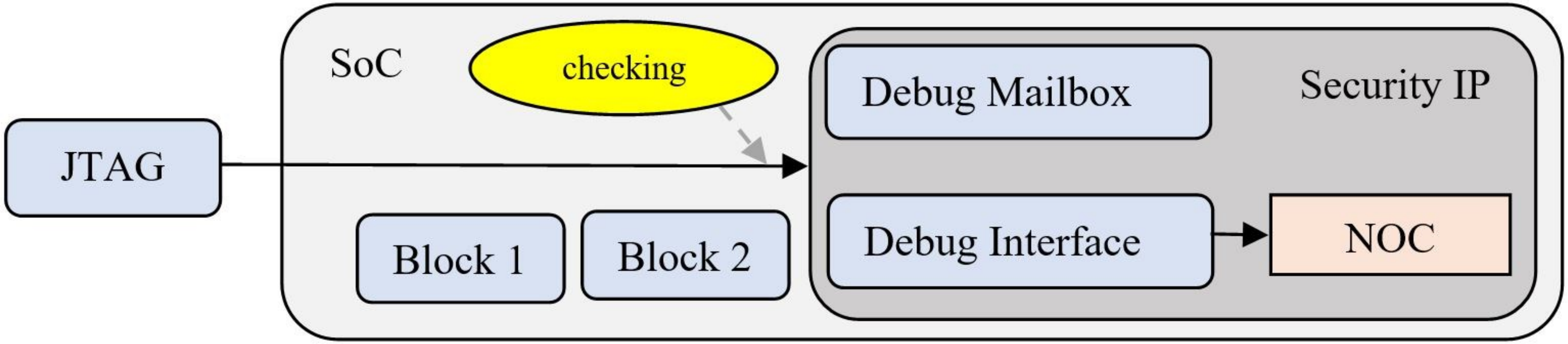
Tests (4): Crypto service

- More complex than TRNG
- Usage of crypto engines



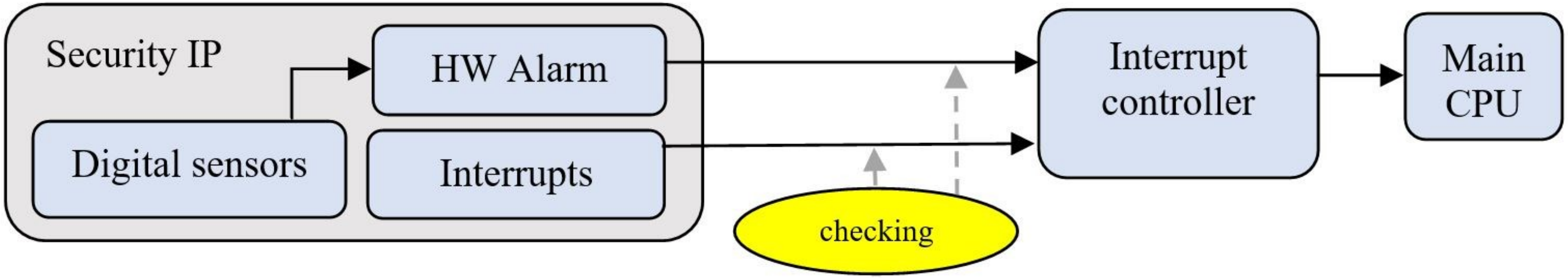
Tests (5): Debug interface

- Check for all modes of operation
- Access complete memory space



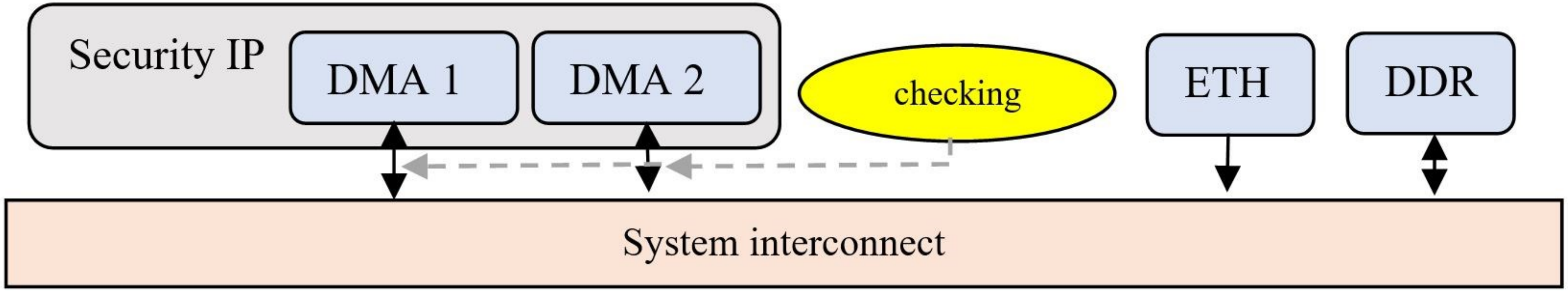
Tests (6): HW alarms and interrupts

- Inject faults and errors to trigger alarms and interrupts



Tests (7): Performance preservation

- Test the performance on all paths



RTL bugs

Bug location	Description
PMU flow	**Issues**: The order of transactions execution and timings were wrong. **Example**: PMU sequence did not provide the clock and took main CPU out of reset on time - before Security IP tried to enable it. **Result**: the SoC was stuck.
Security IP timeout	**Issue**: Duration of the Boot ROM flow was underestimated, therefore the timeout expired before the Boot flow was done. **Result**: the SoC considered Security IP “dead” and started the fallback sequence.
AXI connectivity	**Issue**: ID port was internally made too narrow. **Result**: corrupted transfers.
SPI debug port	**Issue**: The port was locked by Security IP, but transactions still propagated inside. **Result**: Potential gateway for pirates.

Conclusions

- Verification of Security IP is complex task
- Method: gaps detection
  - Compact and effective
  - Minimal set of tests
  - Usage of standard tools and methodologies

Questions?