Safe Chip, Safe Trip: Ensuring Safety in Automotive Chip

Clara Chen, Will Lin
Mediatek

Safe Chip, Safe Trip: Ensuring Safety in Automotive Chip

Clara Chen, Will Lin
Mediatek

Outline

- Introduction
- Challenges in Automotive Chip Design
- Safety introduction
- Implementation with safety file
- Experimental Results
- Conclusion

Introduction

Introduction

- As advanced driver-assistance systems (ADAS) become increasingly prevalent, the transition towards autonomous driving is becoming unstoppable.

- Automotive chips serve as a critical component of ADAS, playing a key role in the evolution of autonomous driving technology.

- Since vehicles have direct impact on human safety, the reliability and safety of automotive chips are of paramount importance.

Challenges in Automotive Chip Design

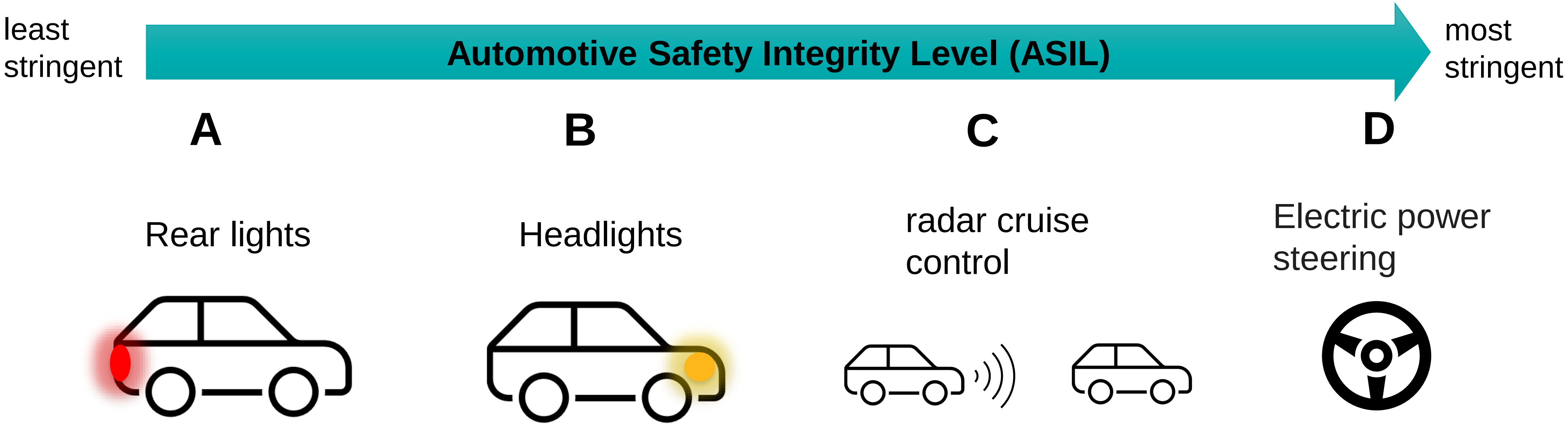
Challenges in Automotive Chip Design

- To develop an automotive chip, we face the following challenges:
  - **Error detection:** Lack of diagnostic information makes it difficult to identify faults and failures.
  - **Error correction:** In the event of a malfunction, there are no corrective measures available.
  - **Function failure avoidance**: Fault on even a small number of components, or possibly just single one, can result in functional failure.
- It is imperative to incorporate additional safety considerations to address these challenges and ensure the reliability and safety of automotive chips.

Safety Introduction

Safety Standard of Automotive Products

- Automotive chips must comply with ISO 26262, which is a functional safety standard for automotive electronic systems.
- Automotive Safety Integrity Levels (ASIL) of ISO26262 define various risk levels, and different automotive components have varying ASIL level requirements.



least stringent

Automotive Safety Integrity Level (ASIL)

most stringent

A

Rear lights

B

Headlights

C

radar cruise control

D

Electric power steering

Safety Mechanism Introduction (1/4)

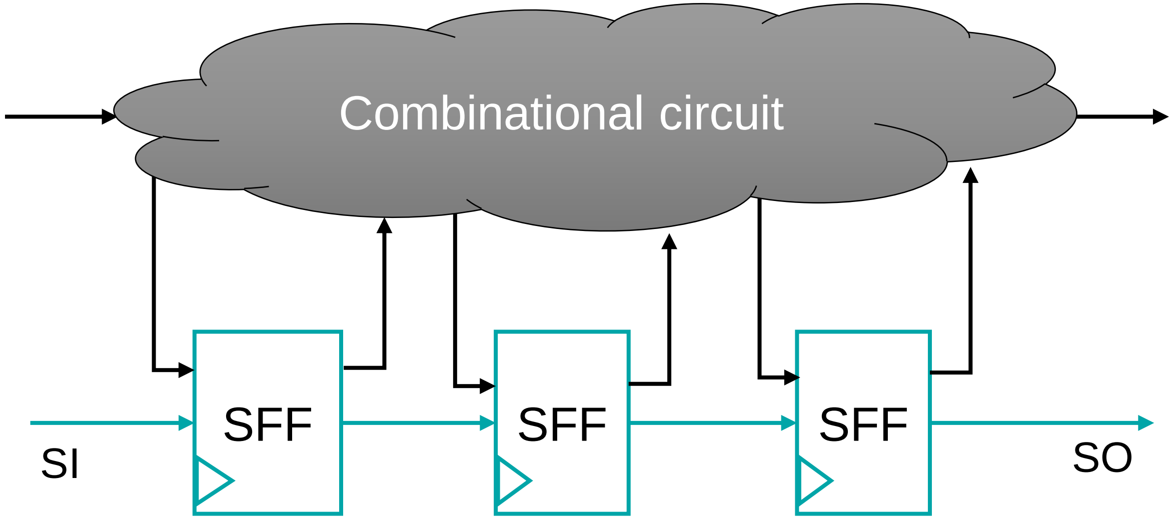
- The following SM (safety mechanism) can improve safety, each targeting specific safety challenges.

	Scan Chain	BIST	ECC	FFSM	DCLS	TMR
Error detection	✓	✓	✓	✓	✓	✓
Error correction	×	×	✓	✓	×	✓
Function failure avoidance	×	✓	△	✓	✓	△

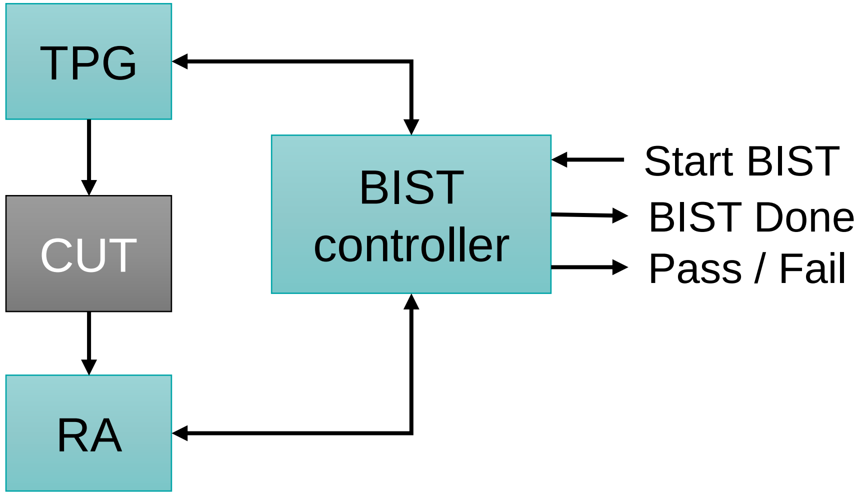
- To achieve the required ASIL level, the combination of SMs can be determined through FMEDA (Failure Mode, Effects, and Diagnostic Analysis).

Safety Mechanism Introduction (2/4)

- **Scan Chain:** Able to externally detect faults in sequential circuits.
  - Convert FF into SFF (scan FF) and stitch them together.
  - Data can be shifted in SFF from SI (scan-in) and shifted out to SO (scan-out).

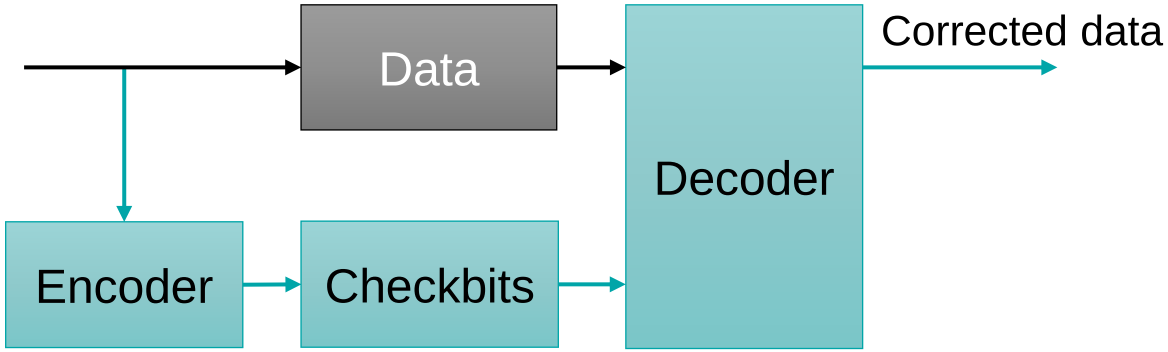


- **BIST (Built-In Self-Test):** Capable of self-testing on the device without relying on ATE (Automatic Test Equipment).
  - For the CUT (circuit under test), it adds BIST controller, TPG (Test Pattern Generator) and RA (Response Analyzer).

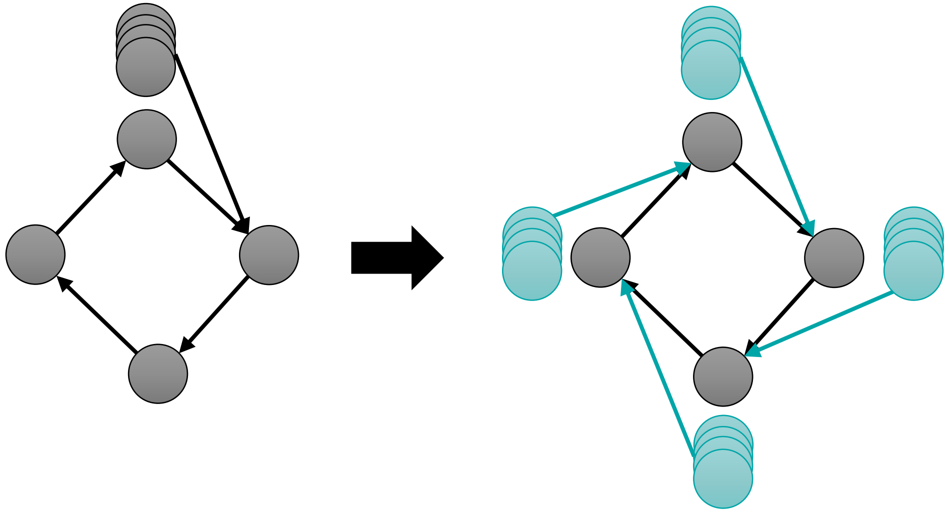


Safety Mechanism Introduction (3/4)

- **ECC (Error Correction Code):** An SEU (Single-Event Upsets) error occurred in a group of register can be detected and corrected.
  - Add additional check bits, and corresponding encoder and decoder.

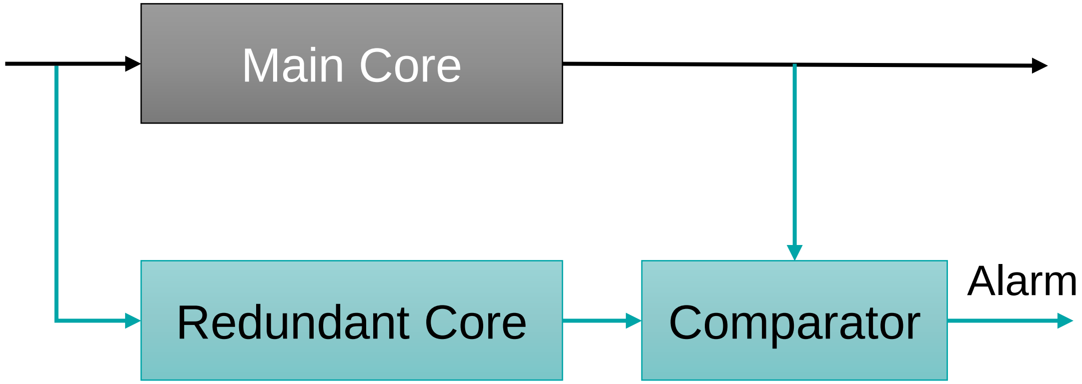


- **FFSM (Failsafe Finite State Machines):** When 1~2 SEUs occur on the state code, FSM can still operate normally.
  - Re-encode state machine with Hamming distance 2 or 3 and create dummy states.
  - Upon entering the duplicated dummy state, the FSM will recover and maintain correct functionality.

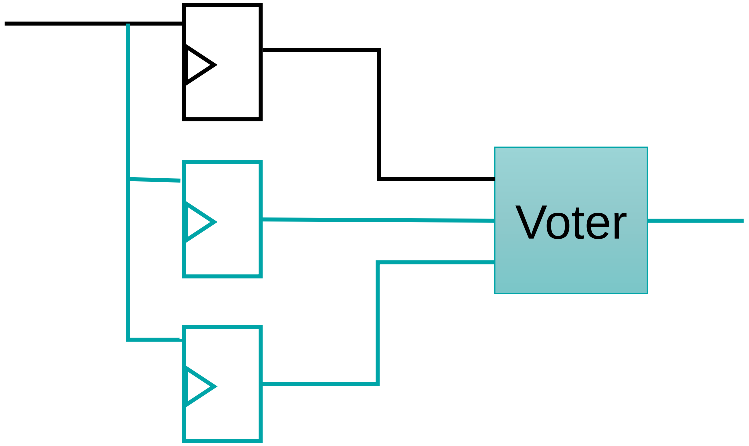


Safety Mechanism Introduction (4/4)

- **DCLS (Dual Core Lock Step):** Trigger fault alarm during critical core malfunctions.
  - Create a duplicate core with the same functionality as the main core and a comparator.
  - When main and redundant core is not in sync, error signal will be triggered.



- **TMR (Triple Modular Redundancy):** Able to detect errors and perform corrections when a single register malfunctions.
  - Consist of a critical register, 2 clone registers and a voter.
  - The output is decided through majority voting; hence, the circuit self-corrects when an error occurs on a single register.



Implementation With Safety File

SM Implementation in Synthesis Stage

- Since SM (Safety Mechanism) involves extra components and safety-related logical/physical requirements, SM implementation is required at synthesis stage.

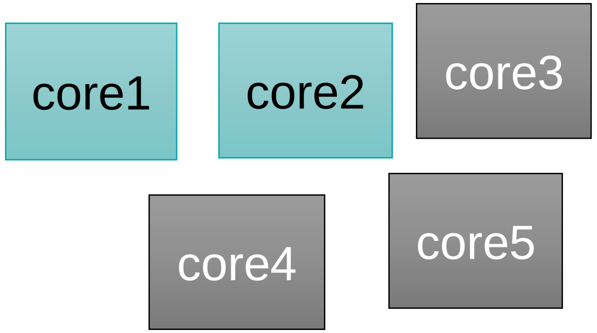
- Since DCLS and TMR are new SMs, implementation of them will face several challenges:
  - Safety-critical components identification
  - Logical/physical safety rule implementation
  - Cross-stage safety content delivery

- To address the above challenge, we use safety file SSF (Safety Specification Format), which is R2G safety solution of Synopsys.

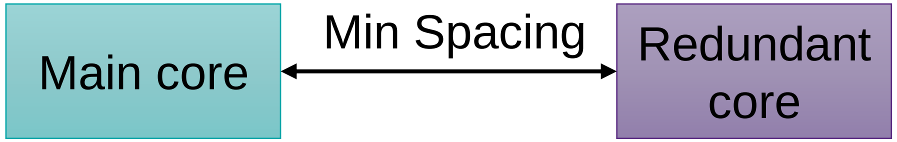
SSF supported safety requirements (1/2)

- **Dual Core Lock Step (DCLS):**

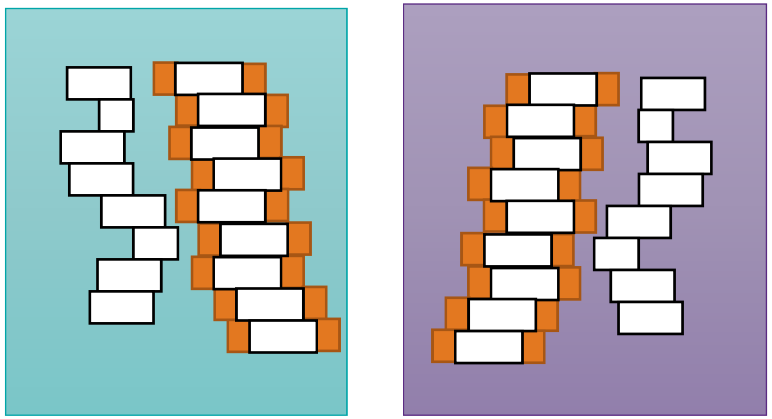
Safety Core Identification



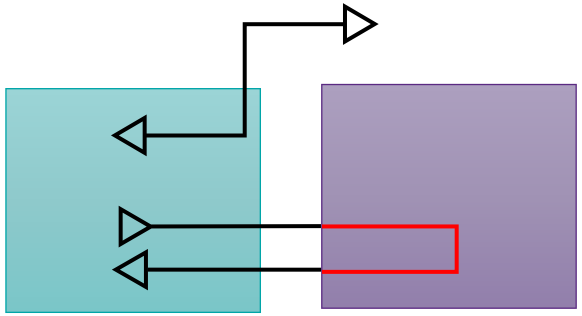
Placement Separation



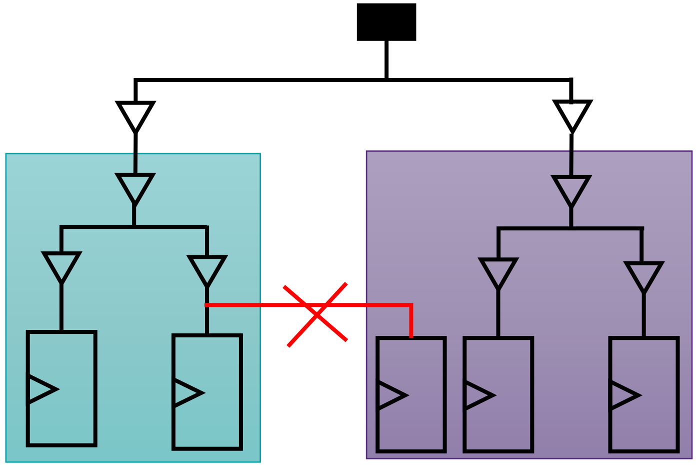
Safety Core Isolation



Routing Separation



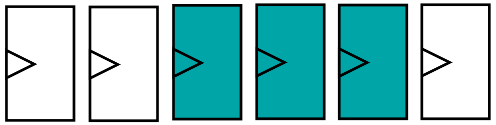
Clock Isolation



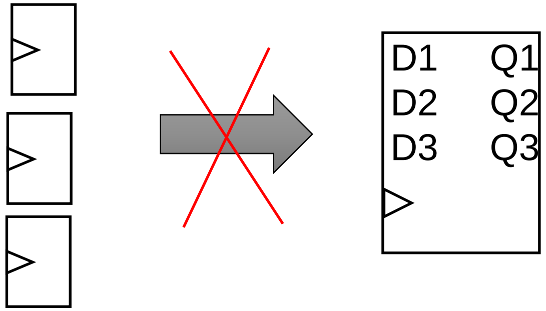
SSF supported safety requirements (2/2)

- **Triple Modular Redundancy (TMR):**

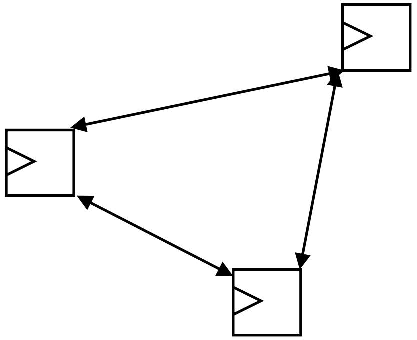
Safety Register Identification



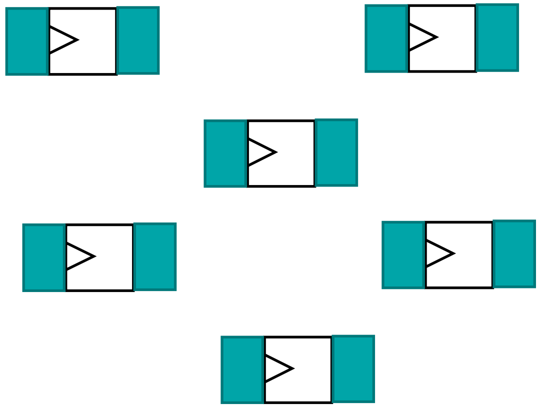
Optimization Restrictions



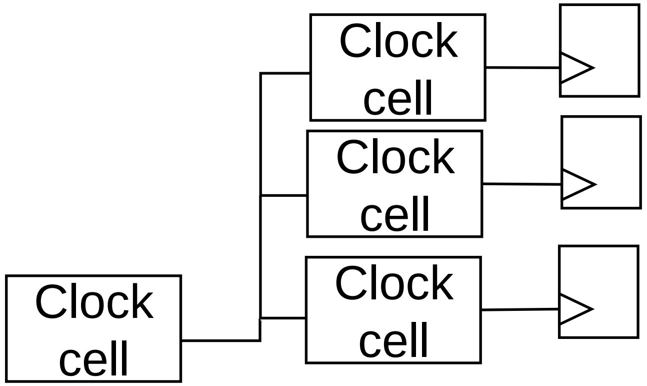
Safety Register Separation



Safety Register Isolation

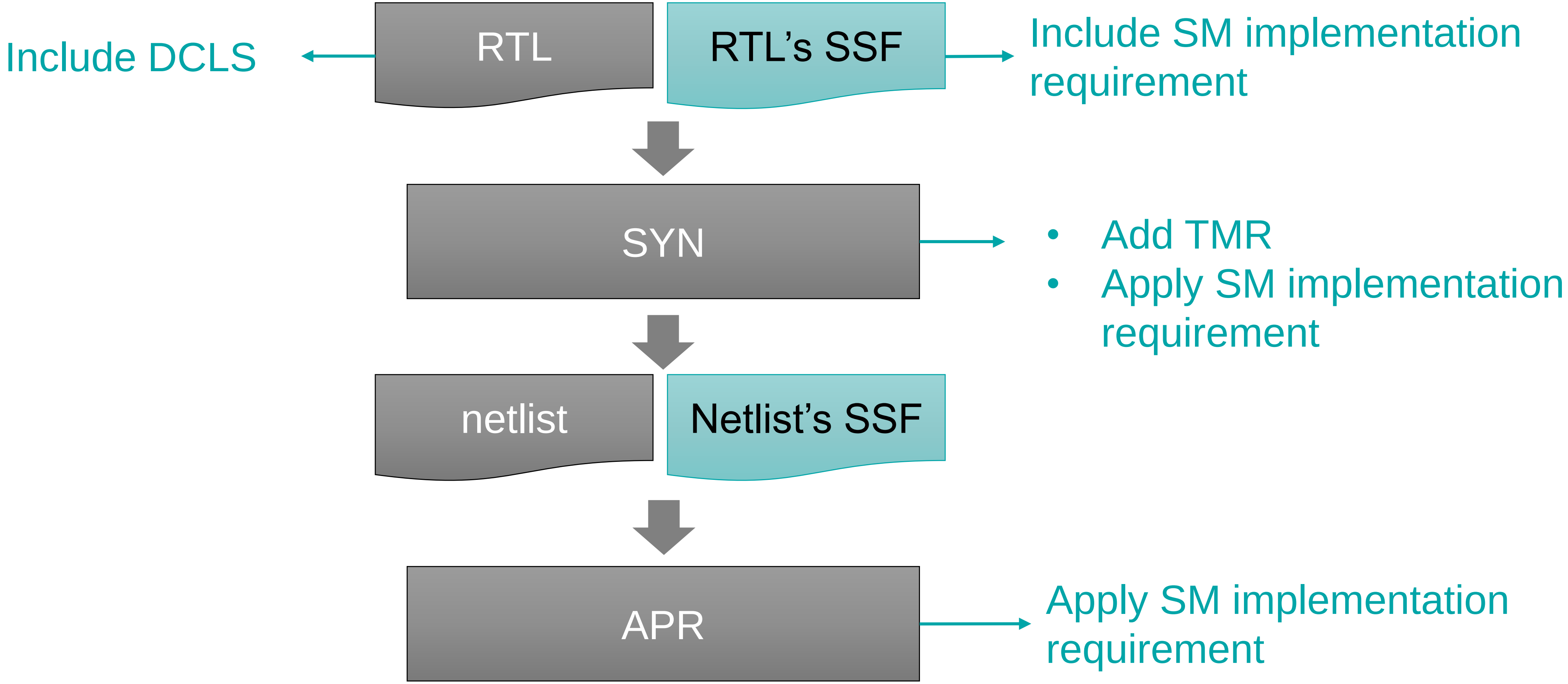


Clock isolation



Proposed: SSF R2G Flow

- SSF delivers SM related content and requirement to FusionCompiler.



Include DCLS

RTL

RTL’s SSF

Include SM implementation requirement

SYN

- Add TMR
- Apply SM implementation requirement

netlist

Netlist’s SSF

APR

Apply SM implementation requirement

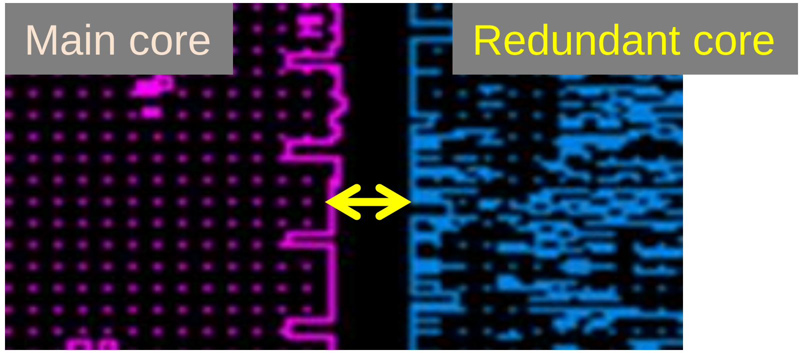
Experimental Results

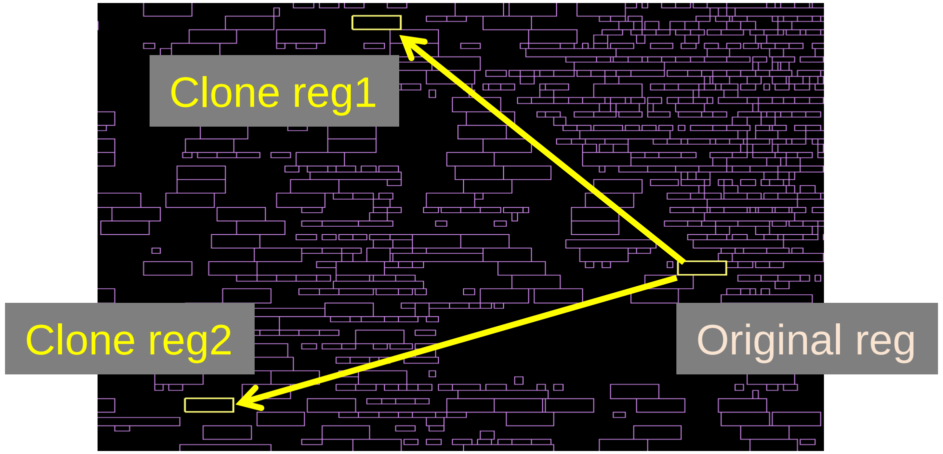
Experimental Results (1/2)

- To assess the impact of SM, the table on the right shows the PPA change of the module that has DCLS applied and includes TMR.
  - While DCLS will cause the area and power to double, the timing and congestion could remain unaffected.
  - Enhancing safety may require trade-offs in PPA.

PPA	Trend
Area	2X
Power	2X
Timing	Same
Congestion	Same

- SM can be implemented by giving SSF.
  - DCLS: 2 cores can be separated
  - TMR: 2 additional registers can be successfully duplicated, and 3 registers can be separated





Experimental Results (2/2)

- Through safety report generated by FusionCompiler, we can review safety violations:

Category	Rule	Content
Placement separation	SR-007	Insufficient distance between registers of a TMR group.
	SR-123	Insufficient distance between cells from two different cores of a DCLS group.
Clock isolation	SR-011	No buffer on split pin.
	SR-016	Common pin/port driving multiple split pins.
TAP isolation	SR-281	TMR register misses marked compliant tap cells.

  - Placement separation: need to review the DCLS/TMR physical setting
  - Clock & TAP isolation: no need to address these violations in synthesis stage and should be solved in APR stage
  - Safety requirements are not resolved all at once but are implemented across various stages.

Conclusion

Conclusion

- To address the safety requirements for automotive chips, this work incorporates new safety mechanism, DCLS and TMR, into chip designs.

- Safety mechanism implementation enhance safety
  - DCLS can trigger an alert during a critical core failure
  - TMR enables fault detection and correction in the event of an error in a single register

- Experimental results demonstrate that this approach can successfully implement DCLS and TMR through the SSF, thereby ensuring the chip's safety.

MEDIATEK snug

THANK YOU

Our Technology, **Your Innovation**™