iSTART

July 2025

# iSTART iReport

Issue No. 12

# iSTART-TEK Honored with"2025 Outstanding Provider of Automotive-Grade Chips"Award, Highlighting Excellence in the Automotive Electronics Field


June 19, 2025 — iSTART-TEK was honored with the "2025 Outstanding Provider of Automotive-Grade Chips" award at the 3rd AutoSEMI 2025 held in Shanghai. The event was jointly organized by Artisan Event, SAICEC, Shanghai Intelligent Sensor Industrial Park, and the Jiading Integrated Circuit Industry Chain Alliance, bringing together leading enterprises and technical experts in the automotive-grade chip industry.

This award recognizes iSTART-TEK's technical strength in the automotive electronics sector. As an innovative company specializing in EDA tools and IP solutions, iSTART-TEK is among the first to achieve ISO 26262 TCL1 tool confidence certification, providing support for automotive chip development in compliance with ASIL D, the highest functional safety level, helping customers meet their functional safety targets.

iSTART-TEK's product portfolio includes UDA (User-Defined Algorithm), TEC (Test Element Change), Repair, and POT (Power-On Test) functions, significantly enhancing the reliability and test efficiency of automotive chips. In particular, its eFlash test and repair solutions have stood out, helping numerous customers shorten development cycles, improve chip quality, and effectively reduce testing costs.

iSTART-TEK is deeply honored to receive this recognition from the industry. This award not only affirms our technical capabilities but also represents the best acknowledgment of our team's spirit of continuous innovation. Looking ahead, we will remain committed to advancing automotive electronics technologies, further enhancing product capabilities, and working closely with our customers to embrace the future of intelligent vehicles.

# A "New Vaccine" for Chips: iSTART-TEK's Self-Developed UDA for Full-Coverage SRAM Testing

As the U.S. government further expands export restrictions on semiconductor technologies and EDA tools to China, the global chip design industry is facing heightened supply chain risks. In response to this growing geopolitical uncertainty, iSTART-TEK emphasizes that its flagship test algorithm platform, UDA (User-Defined Algorithm), is entirely self-developed, free from dependence on foreign core technologies. This ensures long-term licensing stability and provides a secure, sustainable path for chip design teams navigating both technological and policy shifts.

As semiconductor processes advance toward FinFET, GAA, and other cutting-edge nodes, SRAM defects have begun to "mutate" like viruses, with new fault types such as marginal faults, dynamic faults, and soft errors emerging. Traditional test algorithms like March C are increasingly inadequate, much like outdated vaccines that can no longer fend off evolving threats. To tackle this challenge, iSTART-TEK's UDA platform acts as a flexible vaccine R&D lab, allowing users to mix and match test strategies based on product characteristics and application scenarios. The result is comprehensive fault "immunization" to ensure SRAM stability under any operating condition.

With its graphical user interface and modular design, UDA enables users to design custom test algorithms without the need to write complex code. For instance, to detect leakage defects common in high-temperature environments, specific test elements can be added to ensure these faults are not overlooked, reducing the risk of field failures.

iSTART-TEK further integrates its proprietary TEC (Testing Elements Change) technology. Using just three basic operations (w, r, s), users can flexibly adjust the structure of algorithms across CP and FT stages, boosting defect coverage within limited test time. Combined with both static and dynamic background control strategies, UDA can detect a wide range of complex faults, including SAF, TF, CF, WDF, and DRDF.

Additionally, UDA is fully compatible with iSTART-TEK's in-house EDA tools such as START™ v5 and EZ-BIST, forming a streamlined workflow from algorithm creation to ATE pattern generation, maximizing test automation efficiency while reducing design costs and verification efforts.

As memory quality requirements rise across AI, high-performance computing, edge devices, and automotive systems, iSTART-TEK's UDA platform can quickly generate defect-specific, optimized test programs — much like real-time vaccine responses to viral mutations. This not only improves yield but also reduces downstream RMA and warranty risks, ensuring chip reliability in critical domains such as AI, automotive, and aerospace.

| Feature | Vaccine Principle | SRAM Test Algorithm |
|---|---|---|
| **Design Purpose** | Created to protect the human body from pathogens by simulating or weakening them to "train" the immune system. | Designed to expose and detect potential defects in memory by simulating various operations. |
| **Timing** | Builds immunity before actual infection to prevent catastrophic consequences. | Detects hidden defects before ICs enter the market to prevent functional or reliability failures. |
| **Challenges** | Viruses continue to mutate. | Advanced processes (e.g., FinFET, GAA) introduce new SRAM fault types like marginal, dynamic, and soft errors. |
| **Response Strategy** | Develop different vaccines for specific viruses (e.g., COVID-19, HPV, influenza). | Tailor test operations based on product specs (e.g., high-temp, low-power) to create customized algorithms. |
| **Comprehensive Defense** | Mass vaccination ensures population-wide immunity. | Full-coverage test strategies ensure SRAM functions reliably across all usage conditions (temperature, voltage, and frequency). |

# iSTART-TEK Develops CIM Solutions, Targeting Cybersecurity in the Quantum Era

iSTART-TEK is dedicated to delivering specialized EDA tools and IP for the testing and repair of various types of memory. For licensed clients, we also offer one-stop design services that cover the complete back-end flow.
In recent years, iSTART-TEK has actively invested in the development of Computing-In-Memory (CIM) architectures, redefining the energy efficiency limits of AI computing.

Our SRAM-based CIM architecture under development features 8-bit computing precision, ultra-low power consumption, and high scalability. It is also adaptable to RRAM-based designs to support a wide range of application scenarios.
Facing cybersecurity challenges in the quantum era, iSTART-TEK is among the first to integrate lattice-based cryptography and NTT optimization techniques. By accelerating post-quantum cryptographic algorithms with our CIM architecture, we offer robust and long-lasting protection for smart devices and automotive systems.

Beyond developing SRAM-based CIM, we also provide a dedicated test circuit development environment for CIM. Through innovative memory computing technologies, we empower AI algorithms to run faster, stronger, and more energy-efficient than ever before.

# iSTART-TEK Successfully Achieves ISO/IEC 27001:2022 Information Security Management System Certification

iSTART-TEK, a company specializing in EDA tools and IP solutions for memory test and repair, as well as cloud-based service platforms, iSTART-Cloud, has recently achieved ISO/IEC 27001:2022 certification for its Information Security Management System from the internationally recognized certification body, AFNOR International.

iSTART-TEK's cloud-based EDA service platform, iSTART-Cloud, imposes stringent requirements for information security management. To ensure the security of its member website, in addition to password login, biometric authentication via an app is required. This enhances the security of the member site. Furthermore, through VPN configuration, users can connect from their browser to a secure cloud desktop environment, effectively protecting data from cyberattacks or theft. Regarding file transfer, users can upload files to the cloud and download them locally after the MBIST circuit is completed. This eliminates the need for installation and environment variable setup, providing users with a more flexible and streamlined experience.

ISO/IEC 27001:2022 is a globally recognized standard for information security management, covering critical areas such as risk assessment, access control, data protection, and continuous improvement. By systematically implementing this standard, iSTART-TEK has significantly enhanced its information security policies and management framework, ensuring the confidentiality, integrity, and availability of customer data and business information—thereby effectively safeguarding data security and privacy.

Achieving the ISO/IEC 27001:2022 certification is a strong proof of iSTART-TEK's capabilities in information security management. It also demonstrates the company's commitment to meeting the expectations of customers, partners, and regulatory bodies. With this certification, iSTART-TEK ensures that its information security management systems are robustly enforced and monitored, effectively protecting digital assets from risks such as external threats or internal mismanagement that could lead to data loss, damage, or leakage.

# SRAM Repair with Coexisting Redundancy and Stand-Alone Using START™ v5

With advancing process technologies and the booming development of AI, memory demand has steadily increased. In this context, memories with repair functions have become increasingly important. However, if a memory does not originally include a built-in redundancy block, it cannot be repaired when faults occur and must be discarded. To address this issue, START™ v5 offers a corresponding solution: by leveraging the Stand-Alone feature, redundancy blocks can be generated. These blocks enable fault repair for memories that originally lacked redundancy. Additionally, users can customize the size of the redundancy block to fit specific design requirements.

## Stand-Alone Repair Architecture

As shown in Figure 1, the architecture is similar to the previous MBIST setup, with the key addition of a redundancy block. This block is used to replace faulty SRAM addresses. Through MBIST, SRAM is diagnosed, and the fault information is stored in the TRA. The TCR is used to perform switching; it manages the switch between system and BIST operation. This ensures that during normal system operation, when a faulty address is accessed, the system can still perform repair.

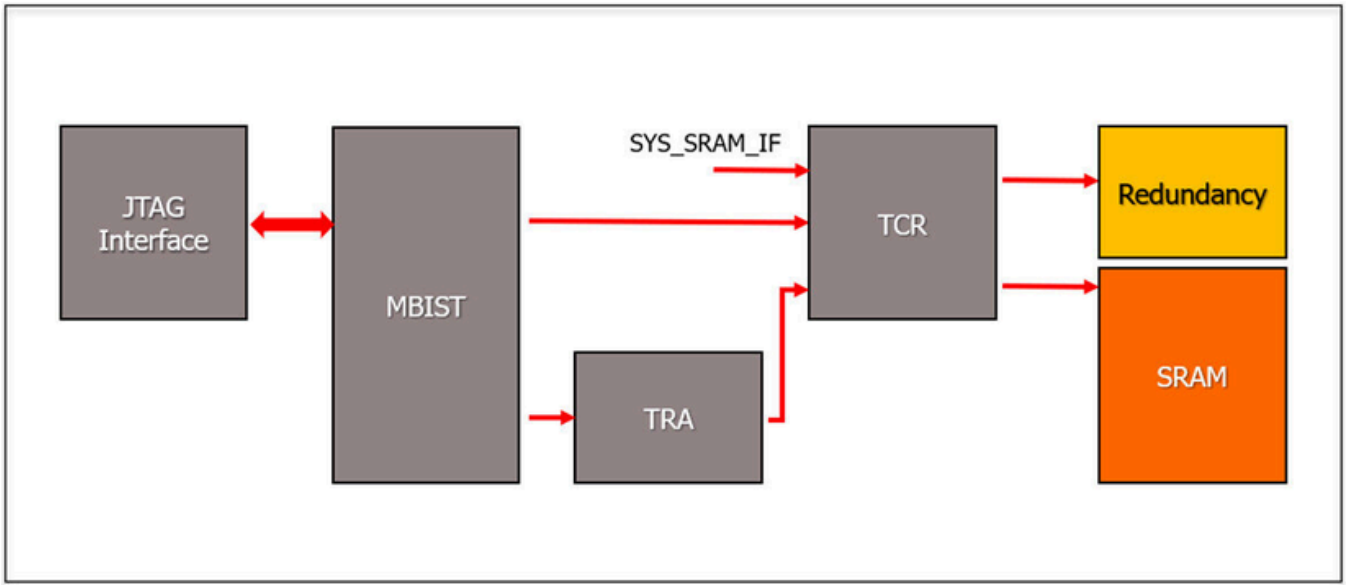



Figure 1 Stand-Alone Repair Architecture

**Tool Setting**

Stand-Alone Repair requires the user to first fill out the rmt (redundancy mapping file), which describes the memory hierarchy for Stand-Alone repair and the corresponding memory repair information. A sample file is shown in Figure 2. If the redundancy memory hierarchy is set to istart, the tool will automatically generate the corresponding redundancy module for that memory, eliminating the need to manually write redundancy circuits.

```
# hierarchy mapping format
# redundancy memory hierarchy(xx.x) = repair memory hierarchy(xx.x)
# ex. top.u_repair1_redundancy = top.u_repair1_ram
istart = top.sp_rpram

# repair memory format
# [memory module name] : redundancy_type = row, redundancy_count = 2(num)
# ex. [SL180_8192X8X4CM32] : redundancy_type = row, redundancy_count = 2
[SL180_8192X8X4CM32] : redundancy_type = row, redundancy_count = 2
```

Figure 2 Example of rmt (redundancy mapping file)

After writing the rmt file, the user must configure the options shown in Figure 3 within the BFL settings file.

```
set redundancy_mapping  = ./redundancy_mapping.rmt
```

Figure 3. BFL Options

**Simulation Method**

The tool will generate the corresponding fault module. Since both regular memory and memory with redundancy will coexist during simulation, the REPAIR definition must be enabled to ensure that the fault module generated by our tool only affects the Stand-Alone memory.

```
`ifdef FAULT
    `ifdef REPAIR
        SRAM
    `else
        SRAM_f
    `endif
`else
    SRAM
`endif
```

```
`ifdef FAULT
    Stand_Alone_SRAM_f
`else
    Stand_Alone_SRAM
`endif
```

Figure 4 Fault Module Definition

Our flow consists of BFL and BII stages, both of which generate the corresponding simulation environment. Simulation commands and results for the BFL stage are shown in Figures 5 and 6, and those for the BII stage are shown in Figures 7 and 8.

```
make controller_name FUNC=tb_INS_RP_f
```

Figure 5 BFL Simulation Command

```
Test Result: Failed!
Repairing and Re-testing
Test Result After Repair: Pass!
```

Figure 6 BFL Simulation Result

```
make integ_name FUNC=tb_f
```

Figure 7 BII Simulation Command

```
-------------- BIST Testing Start -------------- 3000000 ps ps
 Test result of RP_default : Fail!
 Test result of top_default : Pass!
-------------- Test All Result: Failed! -------------- 12953800000 ps ps

-------------- Repairing and Re-testing -------------- 12953800000 ps ps
 Test result of RP_default : Pass!
 Test result of top_default : Pass!
-------------- BIST Test After Repair: Pass! -------------- 25904600000 ps ps
-------------- BIST/BISR Test Result Summary: -------------- 25904600000 ps ps
BIST Testing Start --> Test result: Fail!
Repairing and Re-testing --> Test result: Pass!
```

Figure 8 BII Simulation Result (Soft Repair)

# SRAM Testing Algorithm for Automotive-Grade Chips
# Part 1: Overview of DPPM in Automotive Chips

DPPM (Defective Parts Per Million) is a key metric for measuring the quality and reliability of automotive chips. When a chip is used in a braking system or autonomous driving control unit, even a failure rate of just 1 in a million can lead to irreversible accidents. Therefore, every stage from design, manufacturing, testing to validation must target an ultra-low DPPM.

This episode introduces the DPPM targets during mass production and warranty periods for various types of automotive chips, such as Power ICs, MCUs, and radar sensor ICs. It also explores the real-world quality requirements from Tier 1 suppliers and OEMs, and how international standards—such as AEC-Q100, IATF 16949, and ISO 26262—shape the industry's DPPM management strategies. Through a comprehensive overview of the background and supporting data, this episode aims to help viewers understand the rigor and practical approaches involved in automotive chip quality control.

**Key Points**

- Background and Expectations for DPPM
- Field Return DPPM Expectations
- Reference Standards and Guidelines
- DPPM Targets for Different Chip Types
- DPPM Context and Considerations

▶ **Watch now**

# SRAM Testing Algorithm for Automotive-Grade Chips Part 2: Types of SRAM Failures in Automotive Chips

In automotive applications, SRAM plays a critical role as temporary storage and high-speed buffering. However, it is also exposed to extreme temperature and voltage conditions, making it prone to various potential failures. For automotive-grade chips that need to meet ISO 26262 ASIL-C or ASIL-D requirements, any memory defect could pose a functional safety risk to the system. Therefore, it is crucial to understand and cover all potential SRAM failure types.

These failures can generally be categorized into three groups based on operational behaviors: write operations, read operations, and combined write-read operations.

**Failures Related to Write Operations**

- Stuck-At Fault (SAF): The memory cell cannot be written as 0 or 1, often due to damage in pull-up or pull-down transistors.
- Write Disturb Fault (WDF): Writing to one cell accidentally flips the value of a neighboring cell.
- Access Fault & Open Fault: Abnormal conduction in wordlines or bitlines prevents signals from being properly written.

**Failures Related to Read Operations**

- Stuck-At Fault: Similar to write SAF, but caused by errors in sensing circuits, making the read value consistently incorrect.
- Read Disturb Fault (RDF): The act of reading unexpectedly alters the data in the cell, especially in cells with weak data retention.
- Deceptive Read Destructive Fault (DRDF): The read appears successful, but it has silently corrupted the actual cell content.
- Data Retention Fault (DRF): Data disappears over time, often related to leakage or weak latch strength.

**Failures Triggered by Combined Write-Read Operations**

- Transition Fault (TF): The cell cannot switch from 0 to 1, or from 1 to 0. Alternating write and read operations are required to detect it.
- Dynamic Faults: Failures that only occur after sequences like two writes followed by two reads. Detection requires algorithms like March C- or March SS.

For automotive SoCs, considering their demanding environmental and reliability requirements, all of the above failure types are considered high-risk and must be thoroughly covered. Failures such as WDF, RDF, TF, and DRF become even more severe under high-temperature/high-voltage or low-temperature/low-voltage conditions, making customized test algorithms essential for targeted coverage.

So, how should we address these errors? The answer is to design SRAM testing algorithms tailored to these failure types. By leveraging iSTART-TEK's UDA (User Defined Algorithm) and TEC (Test Element Change) technologies, high-coverage, flexible test sequences can be generated to not only enhance the quality of automotive chips but also meet the functional safety requirements of ASIL-C/D.

▶ **Watch now**

# The Relationship Between Read/Write Operations of SRAM Testing Algorithms and SRAM Defect Types

- Write operations mainly reveal stuck-at faults, write disturb faults, access faults, and open faults.

- Read operations mainly catch stuck-at faults during sensing, read disturb faults, deceptive read destructive faults, and retention faults.

- And combined write-read sequences are used to find transition faults, dynamic faults, and marginal stability issues.

To perform the specific read and write operations mentioned above to detect a wide range of defects, iSTART-TEK's TEC and UDA provide essential support for designing effective SRAM testing algorithms.

UDA is a configurable SRAM testing platform. It enables users to create specific SRAM testing algorithms by executing sequences of write and read operations, and it also supports all kinds of March tests.

TEC, on the other hand, offers flexibility even after CP stages. By using LEGO-based SRAM testing elements, TEC allows users to change and fine-tune testing algorithms whenever needed.

▶ **Watch now**

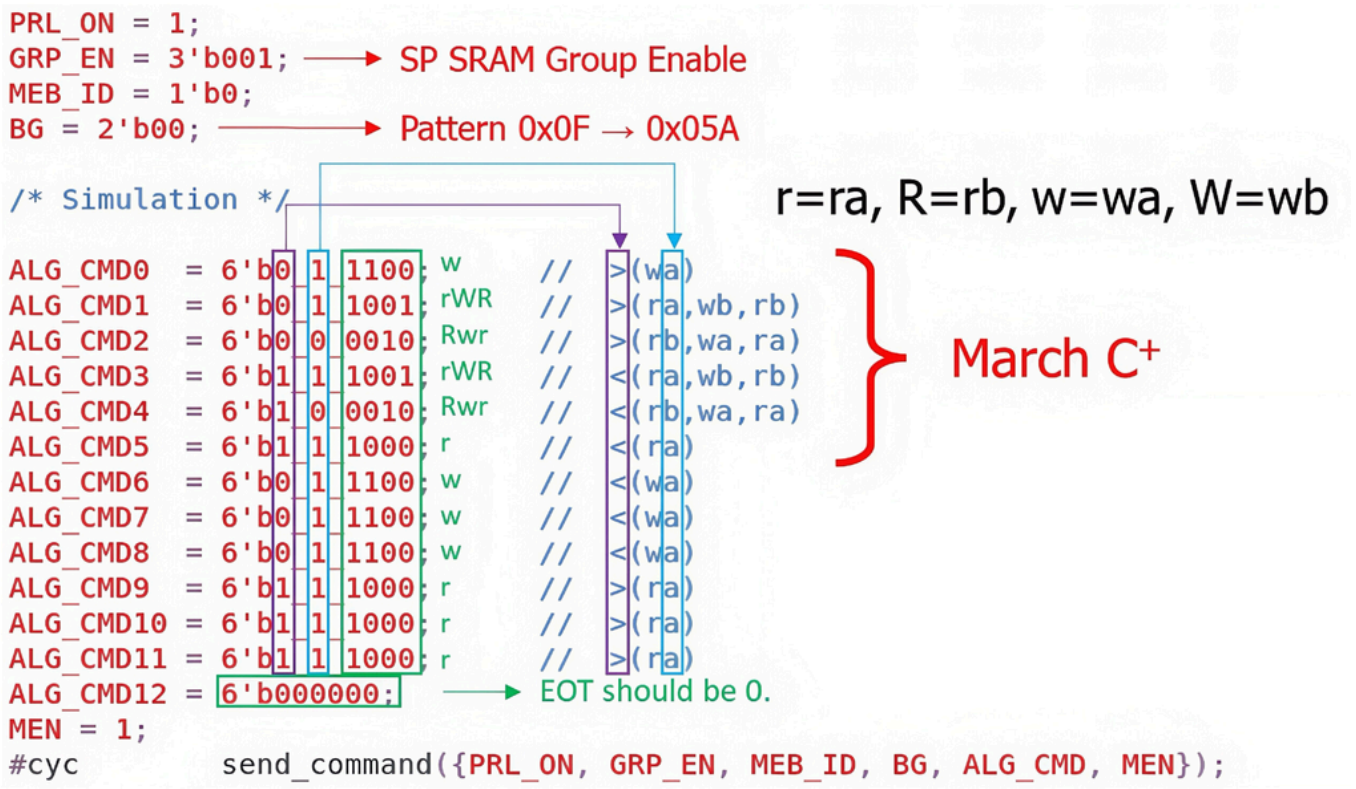
# Testing Elements Change (TEC)

The behavior of traditional algorithms cannot be modified after chip tape-out, which can lead to defects during usage even if the chip has passed the Chip Probe (CP) test and Final Test (FT). Adding new test algorithms at this stage would significantly increase testing time and costs. Therefore, the flexibility and complexity of algorithms have become critical issues.

**Testing Elements Change (TEC)**

iSTART-TEK's Test Element Change (TEC) system, utilizing a Graphical User Interface (GUI), modularizes algorithm behaviors, allowing them to be rearranged and combined into new algorithms. Even if customers do not adopt iSTART-TEK's MBIST circuits, they can retain their original BIST architecture and insert EZ-TEC SRAM BIST IP into the existing circuits. This provides significant convenience and flexibility for customer applications. When users encounter issues in SRAM that cannot be detected by the original MBIST circuits, they can use the EZ-TEC SRAM BIST IP to implement new testing algorithms without altering the SRAM architecture. This effectively increases yield rates.

EZ-TEC SRAM BIST IP is a modularized architecture based on iSTART-TEK's U.S. patent "METHOD FOR GENERATING A MEMORY BUILT-IN SELF-TEST ALGORITHM CIRCUIT." Each element has its corresponding code, which enables the generation of new algorithms. Users only need to prepare four elements to combine and form a common algorithm like the March $C_+$ algorithm.




**Advantages**

- The EZ-TEC SRAM BIST IP can be independent with any MBIST EDA tools, and coexist with the existing memory testing circuits.
- When the original MBIST circuits cannot detect specific memory defects, new algorithms can be generated through element reorganization for re-testing, effectively reducing DPPM (Defective Parts Per Million).
- The Building-Block architecture enables the construction of the most cost-effective circuits.
- Reorganize new algorithms to test critical memories, ensuring comprehensive memory test coverage.
- Easily select memory test algorithm elements, increasing the flexibility and reliability of chip design.

iSTART-TEK's EZ-TEC SRAM BIST IP offers flexible reconfiguration of test algorithms. During the CP/FT stages, test engineers can modify the testing patterns on the machine, thereby enhancing memory test robustness, providing users with significant convenience and flexibility.

**Watch now**

# Impact of BIST & BISR on SoC

## Impact of BIST and BISR on SoC

BIST and BISR significantly influence the functionality of a System on Chip (SoC). For instance, ChatGPT, which is an AI application, relies on advanced CPUs or GPUs for processing, necessitating substantial memory resources to ensure proper operation. After SoCs are fabricated at the wafer manufacturing plant, BIST is utilized for testing, and when memory issues are identified, BISR is employed for remediation. Moreover, AI wafers are produced using cutting-edge processes, which may result in static or dynamic failure issues during manufacturing.

## Usage of BIST and BISR

BIST (Built-In Self-Test) can precisely detect both static and dynamic faults, but it is limited to identifying the defective areas. To transform a faulty wafer into a viable chip, BISR (Built-In Self-Repair) is required to substitute the defective memory with functional redundant memory, thereby restoring the wafer's normal operation.

## Main Advantages of BIST and BISR

iSTART-TEK has nearly 40 patents in the realm of BIST and BISR. The company's BIST and BISR circuits, generated through a variety of high-performance memory testing algorithms, also have the smallest circuit area footprint. Furthermore, customer feedback has confirmed that iSTART-TEK's EDA tools can rapidly produce BIST and BISR circuits across different types of chips, assisting customers in identifying memory defects and effectively enhancing the quality and yield of their SoC.