

AEC WORKSHOP | OCTOBER 14, 2026

Leveraging Functional Safety Analysis for Quality and Reliability

Failure Knowledge from Safety Analysis: An Input to Test and Qualification

Melissa Uribe

micron

Melissa Uribe — SMTS, Functional Safety & Cybersecurity

QUALITY & RELIABILITY and AUTOMOTIVE ENGINEERING

2007 – 2019

**Senior Manager — QRA and
Automotive Engineering**

Aligned Micron qualification flows to
AEC and drove continuous quality
improvements for automotive product

AEC ACTIVE MEMBER

2016 – present

**Micron's lead AEC technical
representative**

Active involvement in committees to
provide and negotiate content for
automotive qualification specifications
and quality requirements

FUNCTIONAL SAFETY

2019 – present

**Senior Member Technical Staff —
Functional Safety**

Owns random hardware analysis and
dependent fault analysis to enable
Functional Safety compliance for
Micron products

Consistent focus : manifestation of internal device faults as customer-observable failures.

Qualification practice, AEC requirements development and functional safety analysis each address that question from a different direction.

Fault grading: stimulating the circuitry, and making the result observable

Per AEC-Q100-007, fault simulation measures the effectiveness of a defined, ordered set of input test vectors at detecting a specified set of modeled faults in the device under test. For each considered fault location, a fault is injected and a circuit simulation is executed to determine whether the observed values differ from the behavior of a good circuit.

1

Fault is stimulated

The test vectors must drive the node so that the modeled fault produces a value different from the good circuit.

2

Fault effect is propagated to device output

The difference created at that node must travel through the surrounding logic to a primary output of the device.

3

Primary output is observed on the tester for the expected logic value

The tester must sample that output and compare it against an expected logic value that the fault would change.

So why are we talking about safety analysis in a discussion about fault grading?

Because safety analysis — Failure Mode, Effects and Diagnostic Analysis (FMEDA) — builds the layer of failure knowledge that connects internal fault behavior to externally observable effects. That is the same connection on which production test and qualification readouts depend.

Quality eliminates defects; safety eliminates uncertainty

QUALITY & RELIABILITY

A measure of excellence or a state of being free from defects, deficiencies and significant variations.

To improve quality — eliminate the source of defects.

Optimizes for: low fail rate and defect prevention

FUNCTIONAL SAFETY

Absence of risk due to hazards caused by the failure of electronic systems during operation.

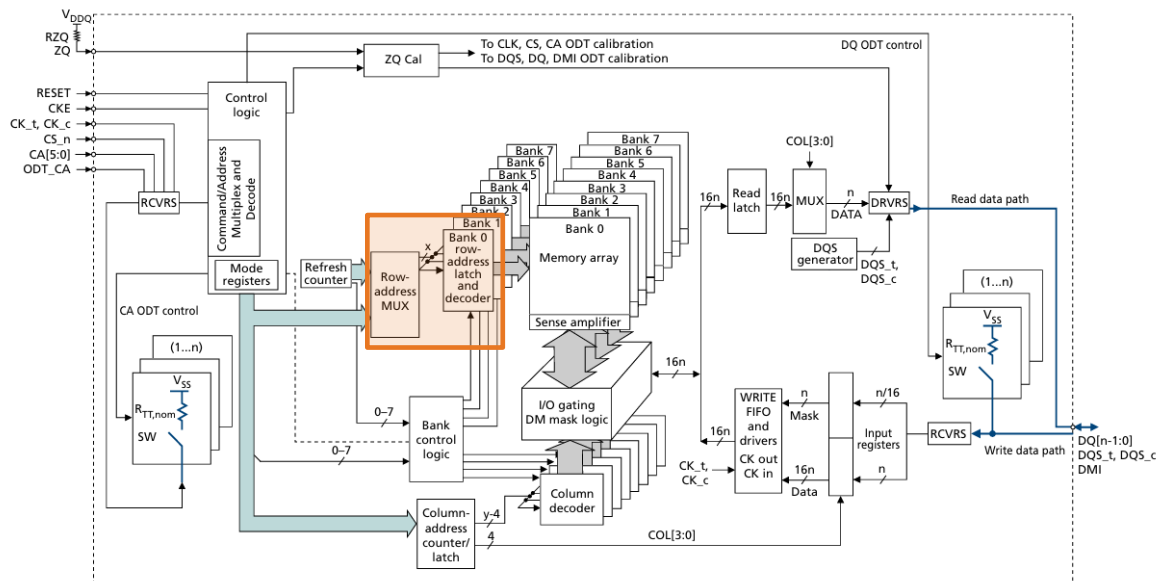
To improve safety — detect faults and control failure.

Optimizes for: failure observability and control in operation

A car pulled over to the side of the road may not be considered “good quality” — but it is a “safe car”

For safety, risk is reduced by detection of faults — not only, and perhaps not even, by prevention.

Row address decoder



The analysis that follows establishes the intended function of the row address decoder, the failure modes associated with that function, and their resulting manifestation at the device boundary. Observable top-level failure modes are documented. Faults are documented even with no history in monitors or RMA.

EXAMPLE 1

Row address decoder observable failure modes

THE FUNCTION OF THIS BLOCK

Take the incoming row address and activate exactly one word line — the one addressed — for the duration of the access, then release it in step with the sense sequence.

WAYS IT CAN FAIL TO PERFORM THAT FUNCTION

Activates nothing

The addressed word line is not selected

Activates more than one

Several word lines are driven at the same time

Activates the wrong one

A word line is selected, but not the one addressed

Activates at the wrong time

Turn-on or release mistimed against the sense sequence

HOST OBSERVATION

No row selected,
wrong activation timing

Data corruption

Multiple rows selected

Data corruption

Wrong row selected

Wrong data

In addition, the safety analysis quantifies the probability of each observed failure.

Confirm the expected data cannot mask the fault

NOT SUFFICIENT

A single repetitive pattern — the same value at every address

- The same value is written to every address
- A decode fault sends the read to a different address
- That address holds the same value
- Data compares correct — recorded as a pass

GOOD

A non-repetitive pattern — checkerboard or better

- Neighbouring locations hold different values
- A decode fault sends the read to a different address
- The value often differs from the one expected
- Many decode faults become visible — but not all

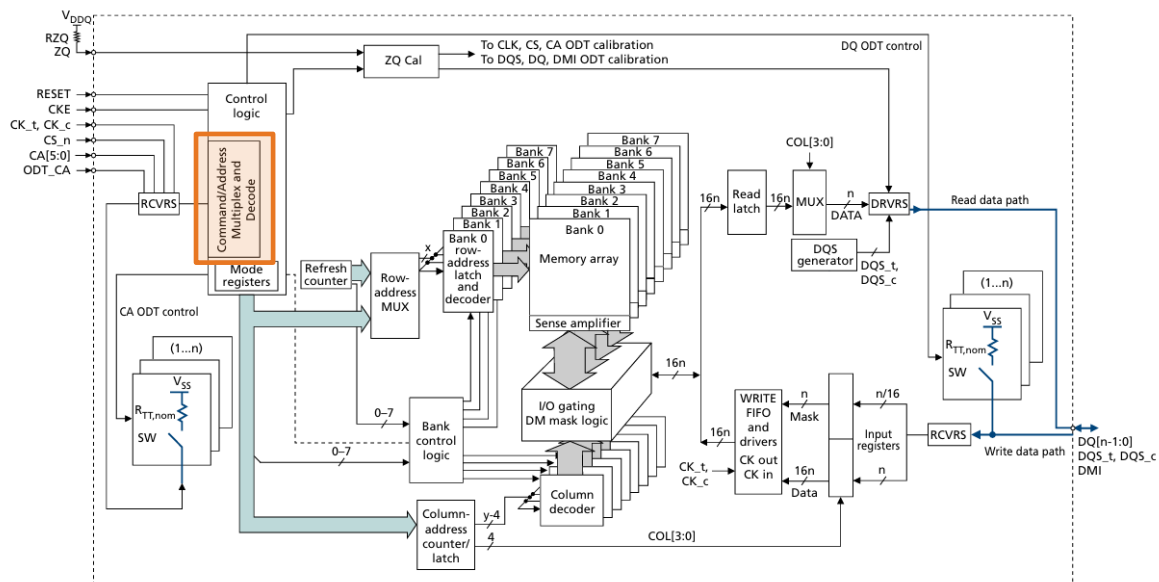
BEST

A pattern that encodes its own address

- Stored content is a function of the address
- A decode fault sends the read to a different address
- The value can never match the one expected
- Every such fault is observable and classifiable

Verifying that every cell can hold a one and a zero validates cell storage but says nothing about address fidelity.

Command and address decode



The analysis that follows establishes the intended function of the command and address decode path, the failure modes associated with that function, and their resulting manifestation at the device boundary. Observable top-level failure modes are documented. Faults are documented even with no history in monitors or RMA.

EXAMPLE 2

Command and address decode observable failure modes

THE FUNCTION OF THIS BLOCK

Decode the incoming command and address — determine which operation the device is to perform and on which location — and launch that operation in step with the requested sequence.

WAYS IT CAN FAIL TO PERFORM THAT FUNCTION

Decodes no command

The requested operation is not performed

Decodes the wrong command

A different operation runs than the one issued

Determines wrong address

The requested operation runs on the wrong location

Decodes command too late

The operation launches out of step with the requested sequence

HOST OBSERVATION, DURING READ

No command,
Late command

No data driven (all-0)

Wrong command

No data driven (all-0)

Wrong address

Wrong data

In addition, the safety analysis quantifies the probability of each observed failure.

Confirm the expected data does not match a default

NOT SUFFICIENT — ALL-ZERO EXPECTED DATA

- All zeros are written to the addresses under test
- A command decode fault means the read is never executed
- The bus is never driven — the host samples all zeros (due to ground termination)
- **Data compares correct — recorded as a pass**

BEST — NON-ZERO EXPECTED DATA

- Non-zero data is written to the addresses under test
- The same command decode fault means the read is never executed
- The bus is never driven — the host samples all zeros (due to ground termination)
- **All zeros cannot match — recorded as a fail**

Nothing in the returned word distinguishes “the device read zeros” from “the device never performed the read.” An all-zero result is the signature of a command that did not execute since the device is ground terminated, and it is only distinguishable if the expected data makes zero an impossible answer.

Quantified failure modes direct where test and design effort pays off

THE QUANTIFIED VIEW

FMEDA does not just list how the device can fail — it determines the probability on each failure mode, so the failure modes can be prioritized against one another instead of all being treated as equally important.

Direct effort to the biggest impacts on user

The quantified failure modes show which faults are most likely to reach the user as a visible failure, so attention goes to the modes that carry real exposure.

Show where added capability is worth the cost

The same numbers identify where additional test coverage, DFT capability, or an architectural enhancement would deliver the greatest return.

Identify internal indicators to improve observability

FMEDA documents the internal detection and error indicators that signal a failure. Test can read those indicators to gain coverage on faults that are otherwise difficult to observe.

Focus on observability

1

Build a failure mode list block by block

If your FuSa office has an FMEDA, start from it. If not, reason block by block as a safety analysis — what is the function of the block, how can it fail to perform that function, and what would the host observe for that failure mode.

2

Determine what is required to observe each mode

For each failure mode, consider whether a specific test pattern or requirement is needed to make it observable. Check the default output cannot mask the fault, and consider internal fault detectors.

3

Identify fault grading improvements

Use the quantification in the safety analysis to identify and prioritise observability gaps, then feed them into test coverage and fault grading improvements.



Thank you