Presented to:

56th Annual Fuze Conference

National Defense Industrial Association

Baltimore, MD

CRC – 16 Check on Flash Based Logic Devices in the Implementation of Safety Features

TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

16 May 2012

Presented by:

Anthony C. Steele II

Electronics Engineer

U.S. Army Aviation and Missile Research, Development, and Engineering Center

Acknowledgements

- Bob Hubal, Fuze Division, FPAT METC, ARDEC
- AMRDEC:
  - Wayne Eads (Dynetics, Inc)
  - Daniel Pitts
  - Shannon Haataja

CRC Background

- **Appendix A.2 of the FESWG "Technical Manual For The Use Of Logic Devices" specifies:**
  - ***"For devices relying on charged-based memory to implement a Safety Feature (SF), a method of validating the integrity of the memory shall be performed prior to executing the safety function"***

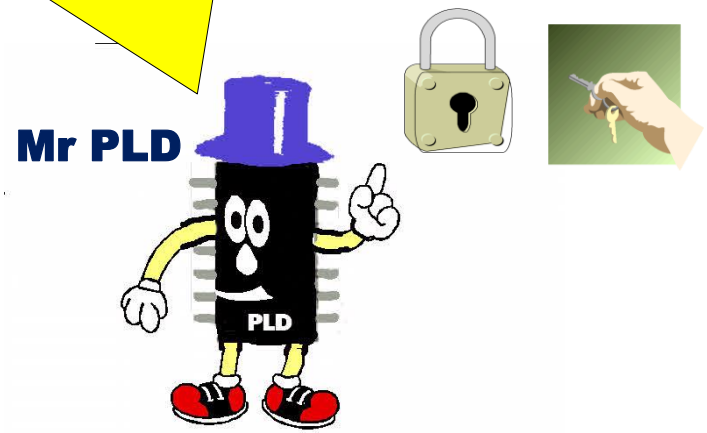
- **The AMRDEC ESAD design uses a CRC-16 algorithm to verify the integrity of the microcontroller code. The ESAD computes the CRC-16 result and compares it to a known-good value stored externally to the microcontroller.**

- **Failure of the CRC-16 check in the ESAD will disable the 3.3 Volt regulator used by the ESAD including the microcontroller.**

Memory Check Concept (Hubal Key)

Fuze Safety Critical Functions Locked in here.

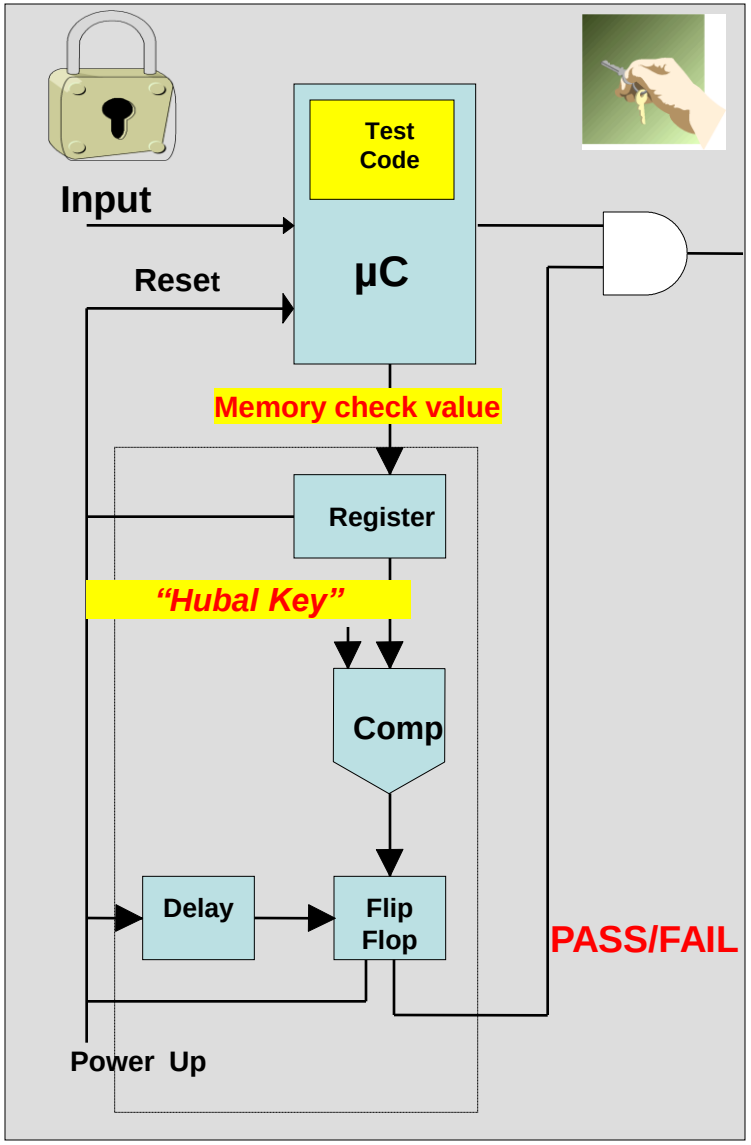
Now what was that combination again??



1	1	0	0	1	0	1	1	0	0	1	1	0	0	1

- PLD has to derive the right combination based on checking it's memory.
- This value is not resident in memory
- The memory check is robust and the value is unlikely to be generated by mistake.

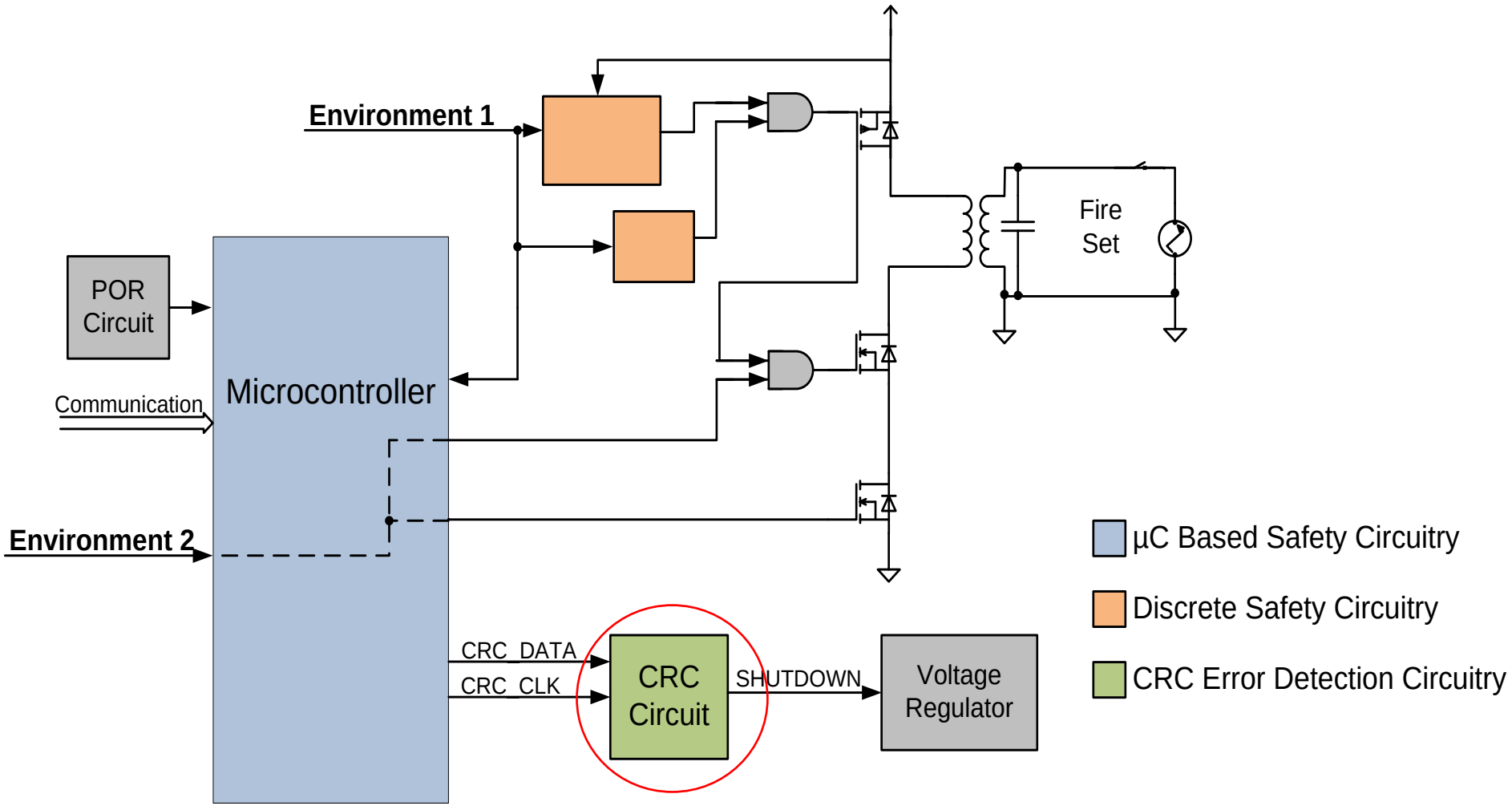
Hubal Key Diagram



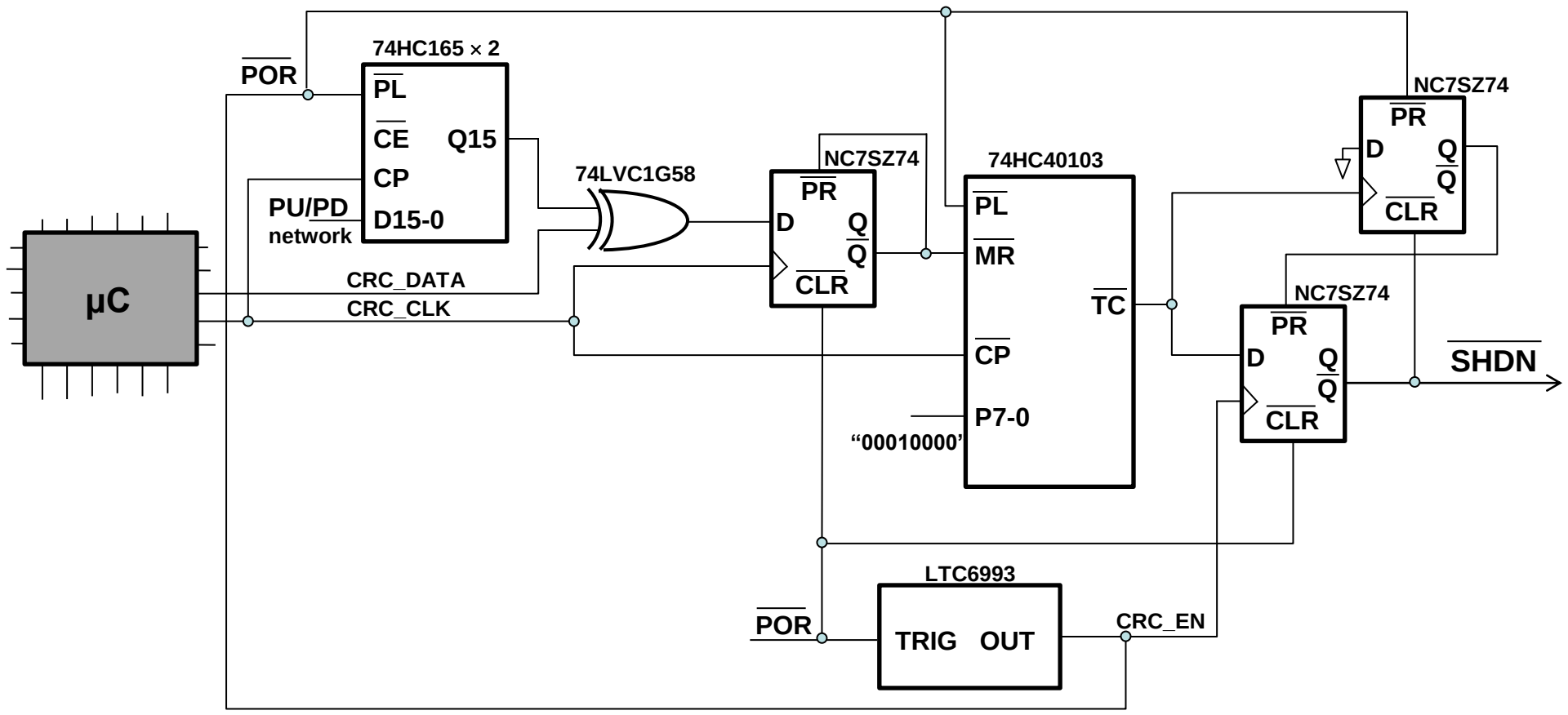
Purpose:

- Checks program memory against an external "coded word" (a.k.a. key).
- Re-programmability feature shall be defeated robustly (Service-review required).
- Hubal Key acts only as a check for the integrity of EPROM/EEPROM/Flash memory.
- Hubal Key does not check hardware or processing functions.
- Lines between µC and Hubal Key are dedicated and shall not be used for any other purposes, including monitoring.
- Memory integrity check shall be run upon the application of power and at the start of all arming processes.

Notional Fuze Architecture

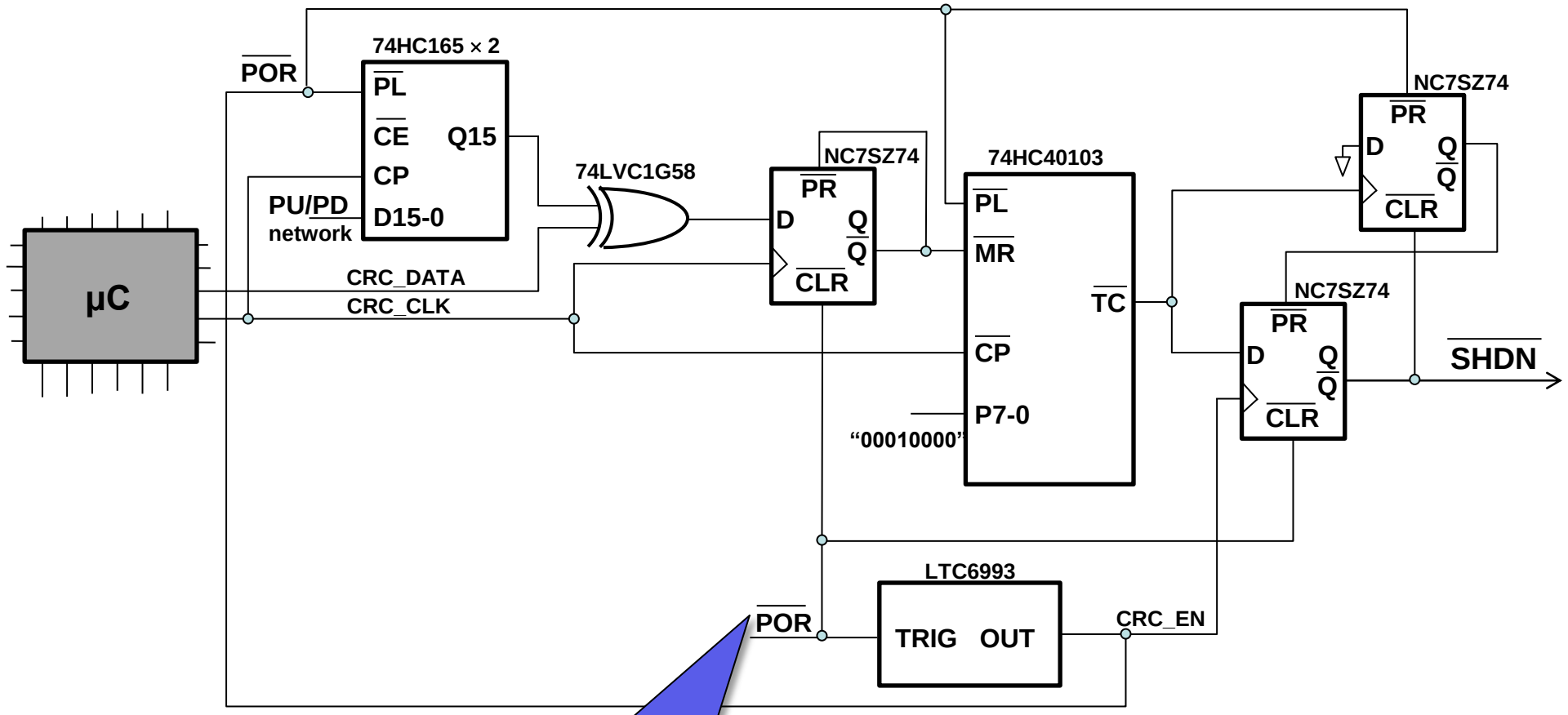


CRC Verification



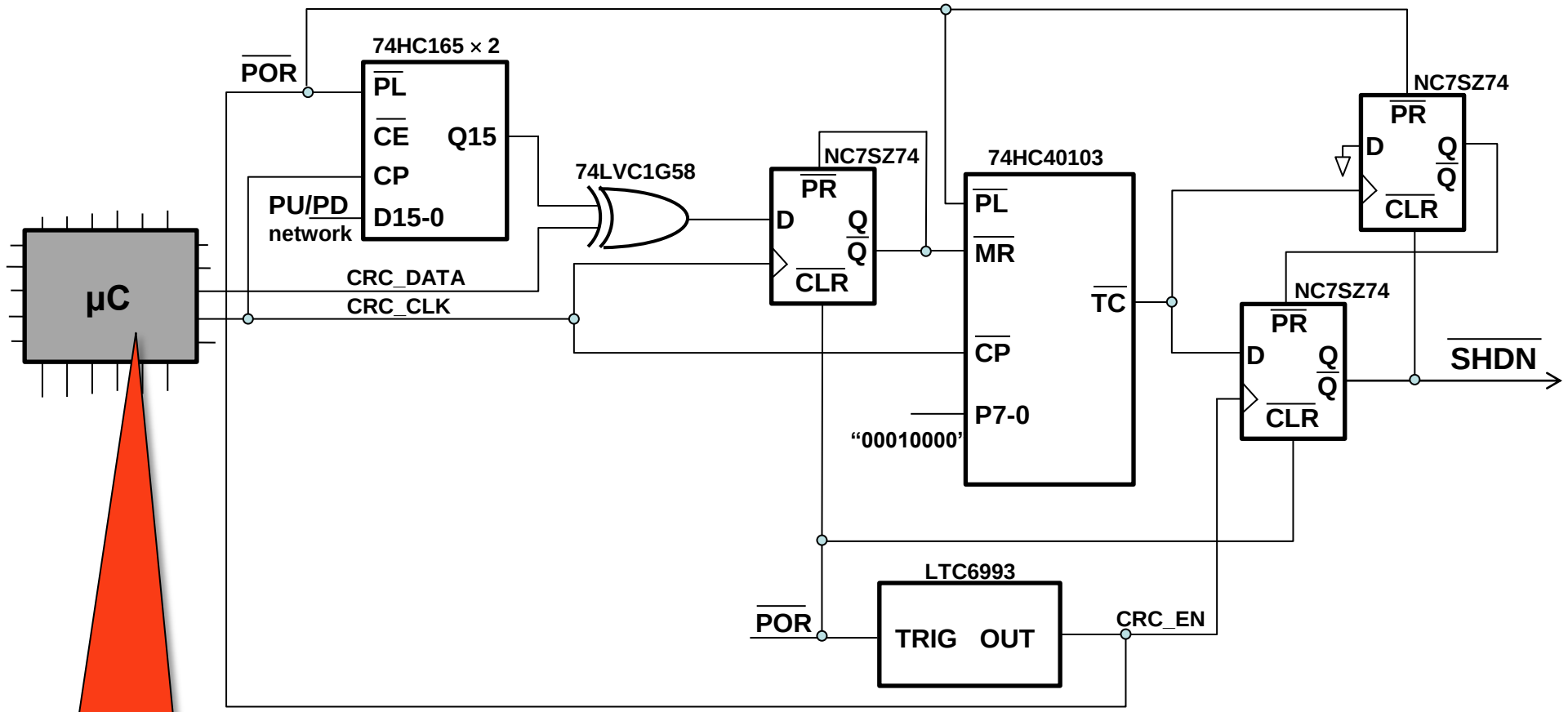
Failure of CRC verification results in shut down of 3.3 volt regulator used by the ESAD including the µC.

CRC Verification



POR starts 1-shot timer and initializes shift register, flip-flops and counter.

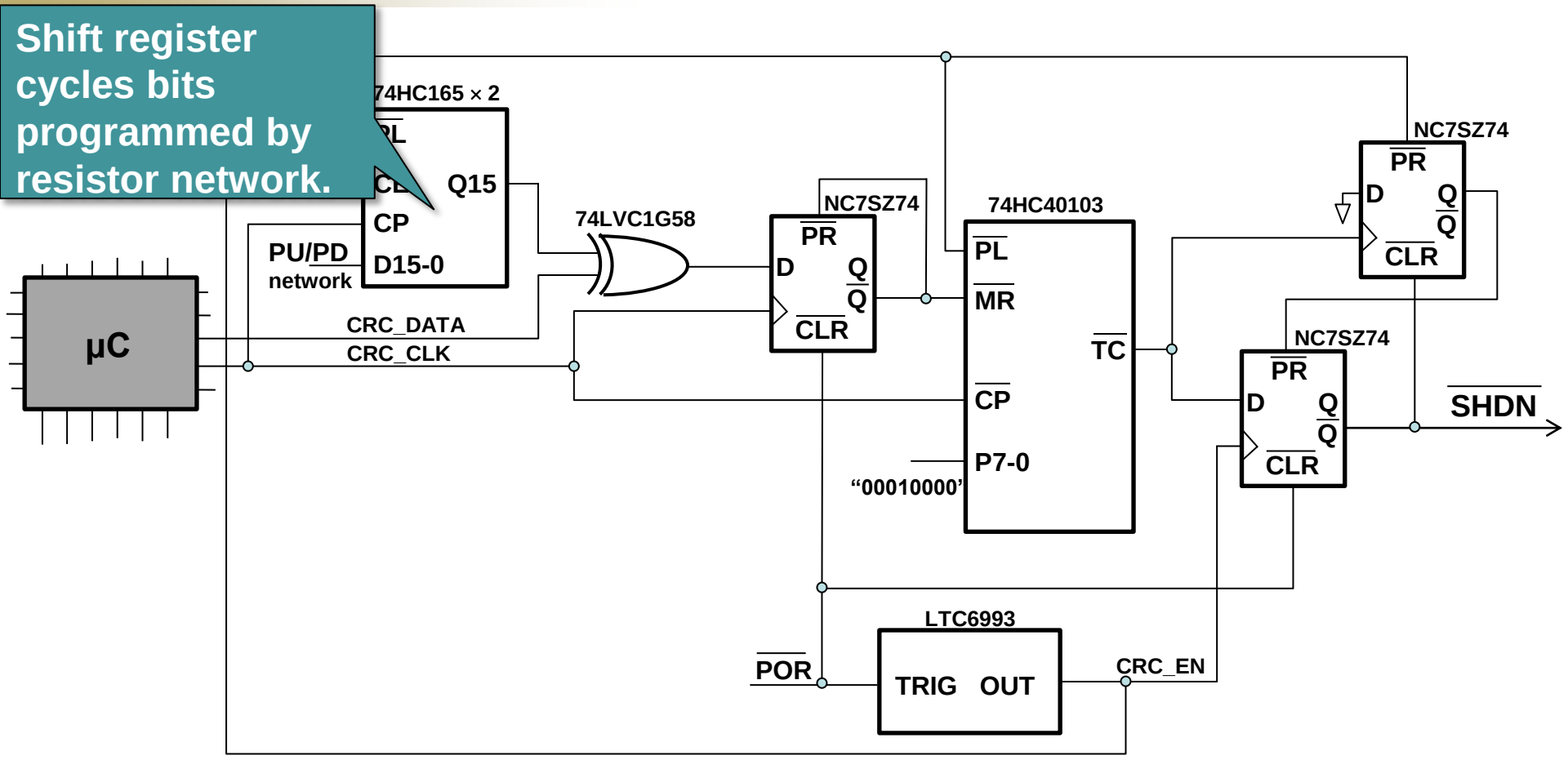
CRC Verification



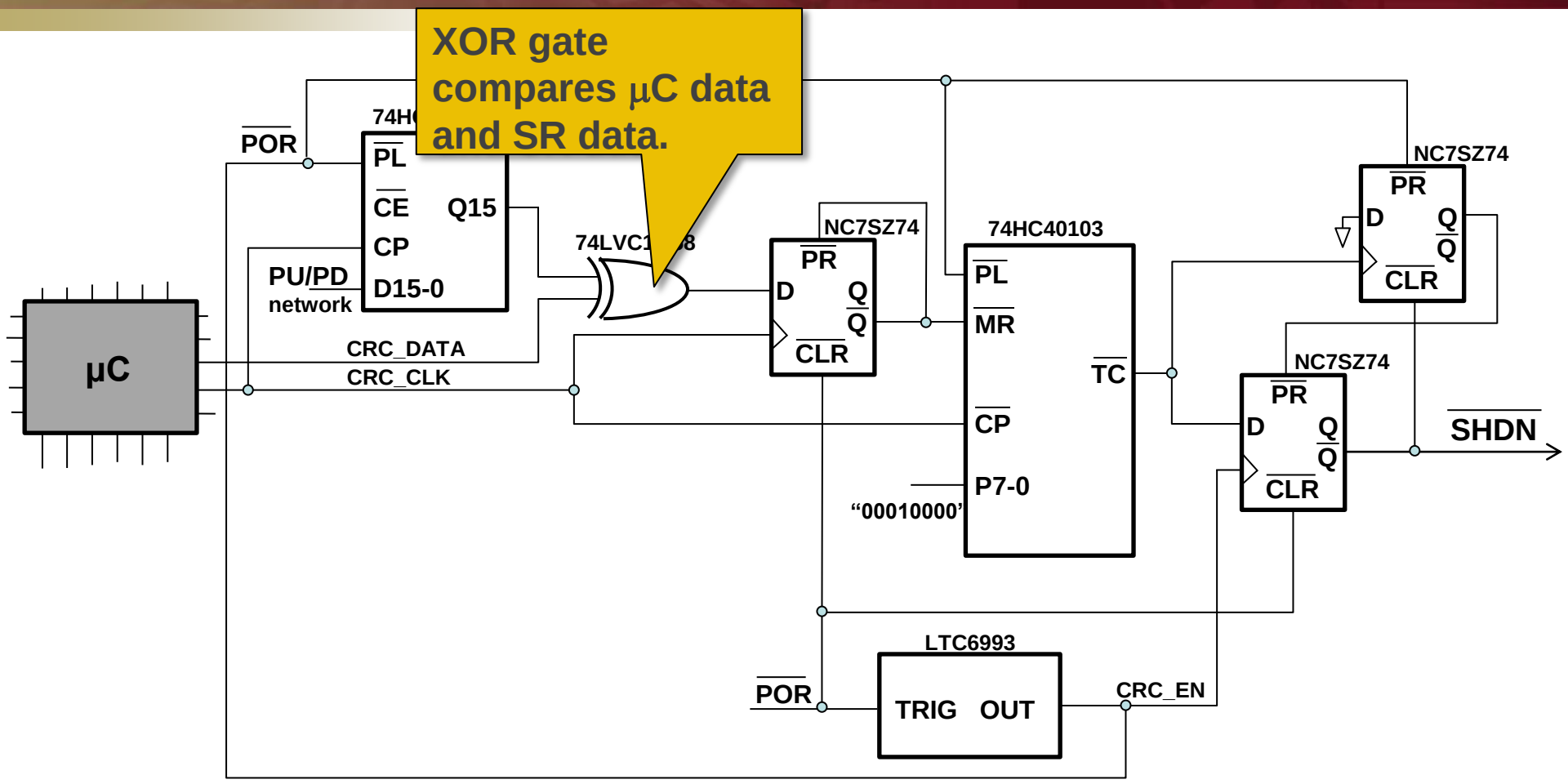
Microcontroller issues CRC data and clock pulses.

CRC Verification

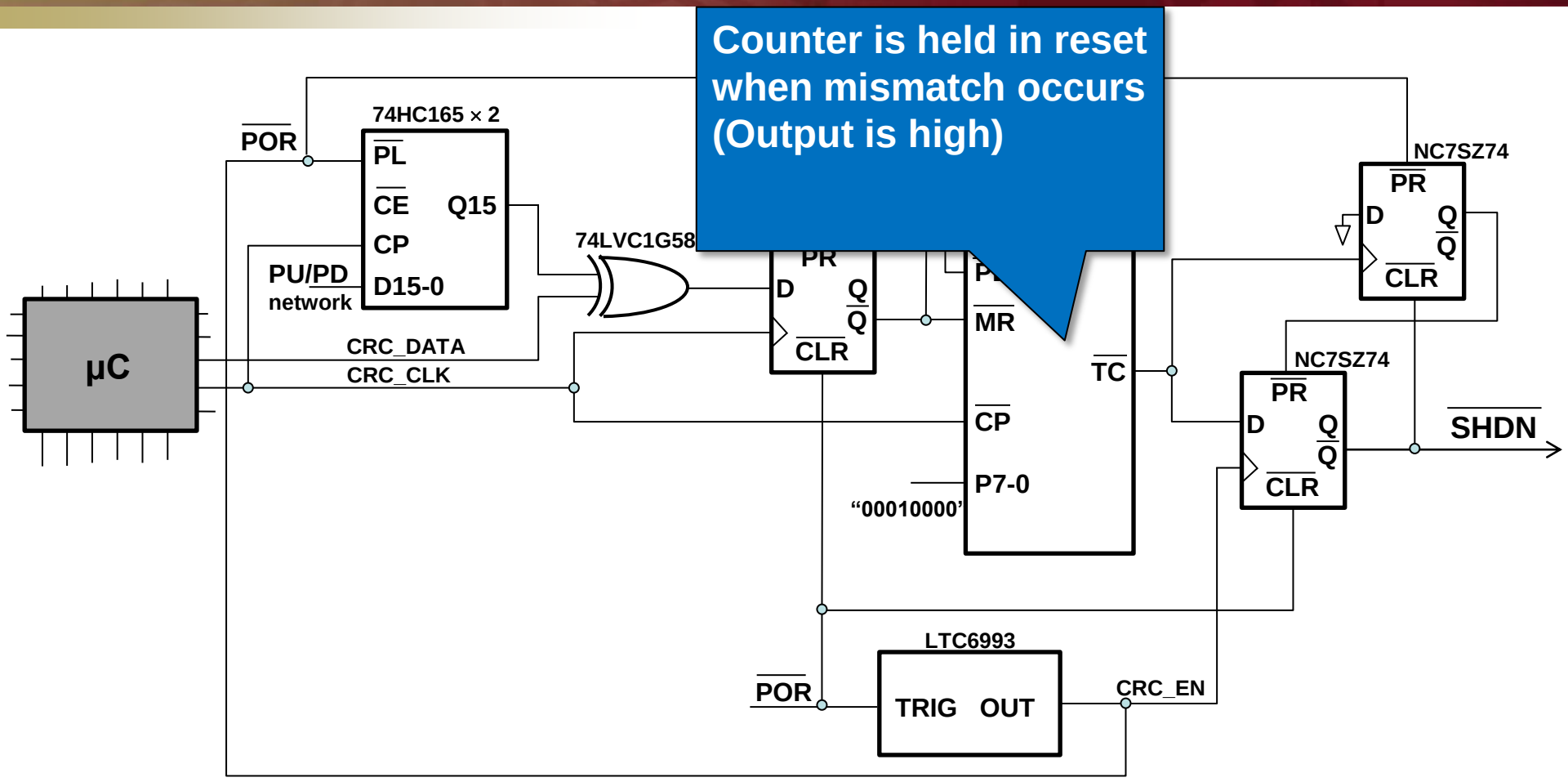
Shift register cycles bits programmed by resistor network.



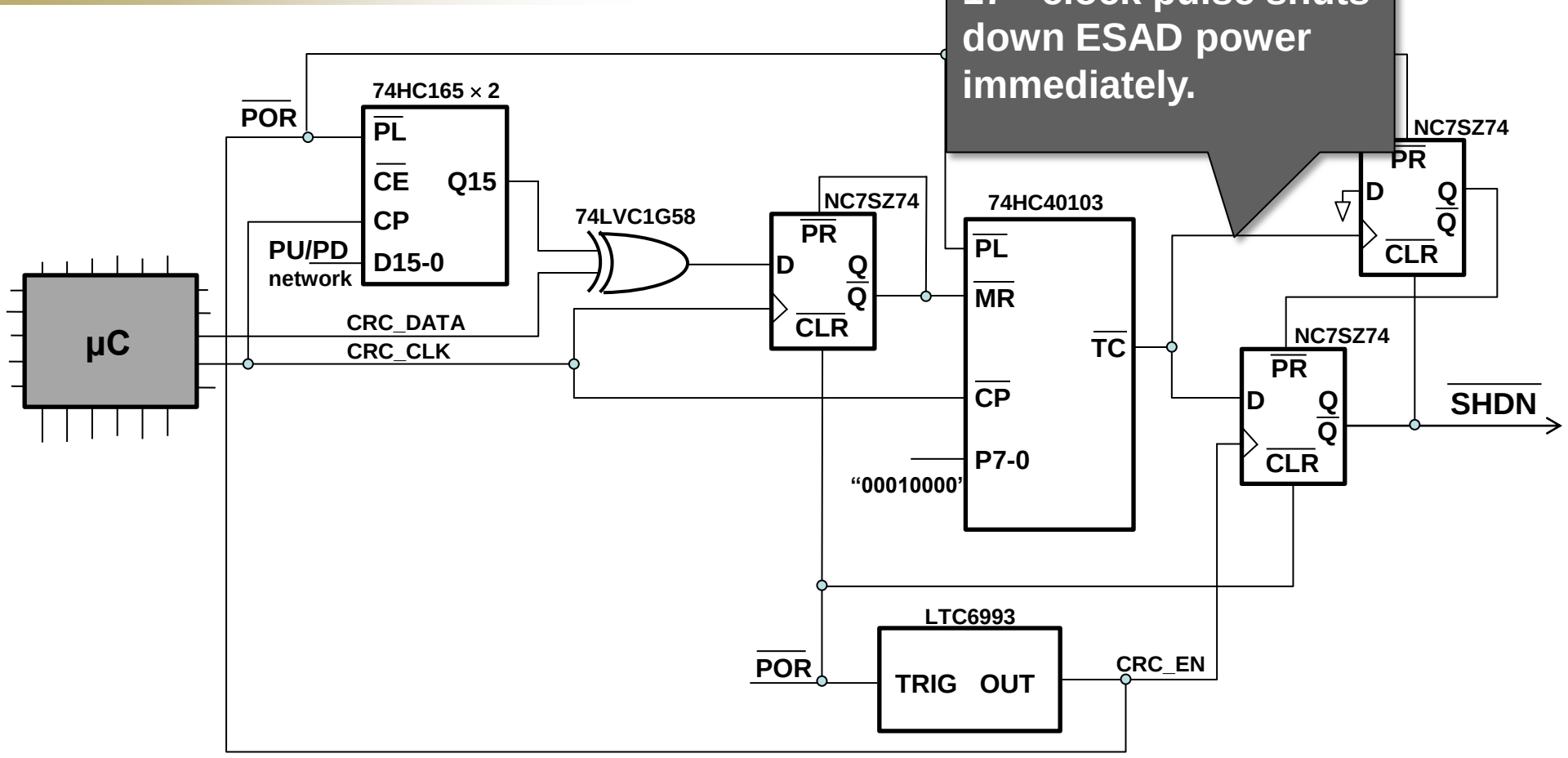
CRC Verification



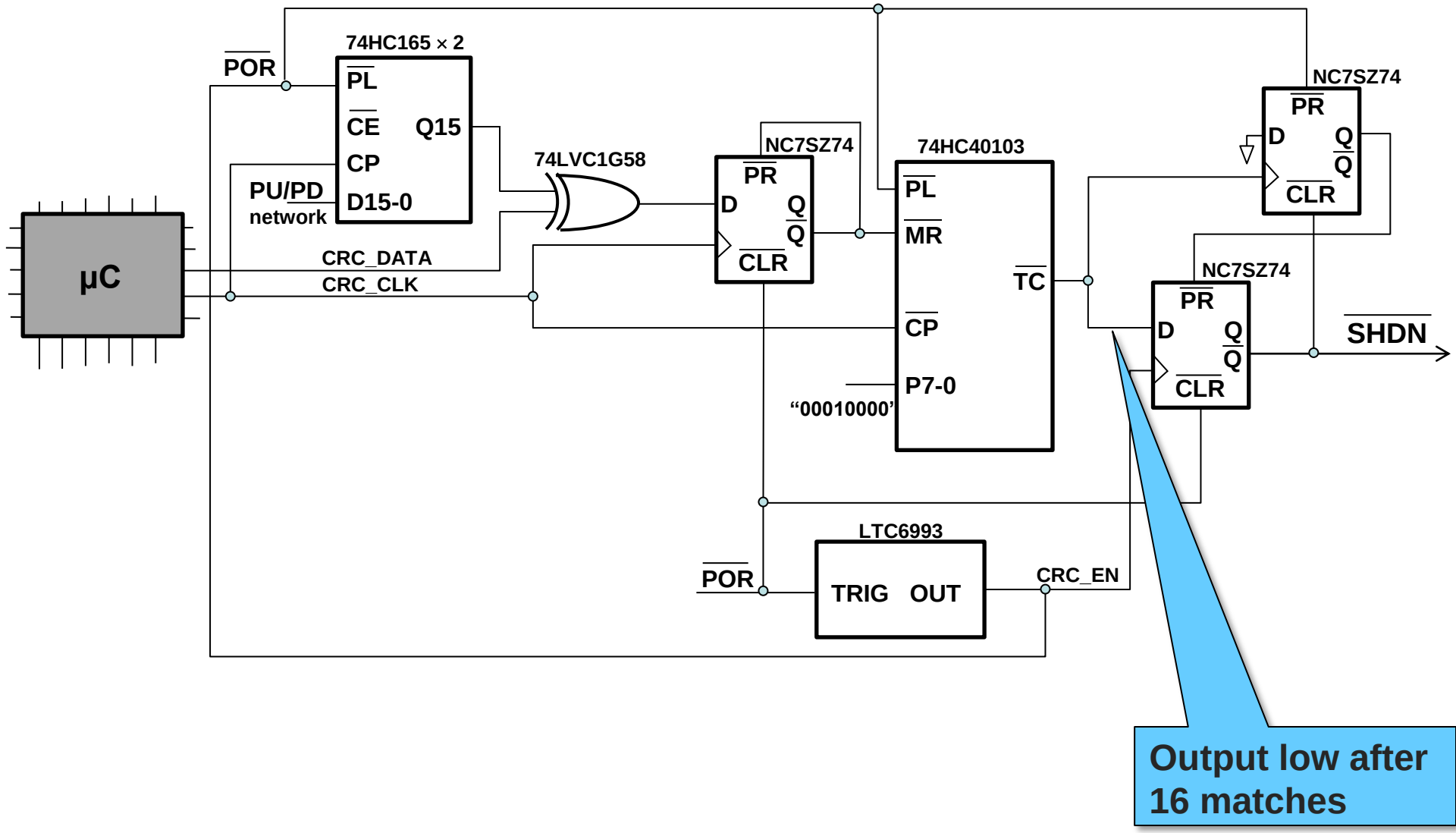
CRC Verification



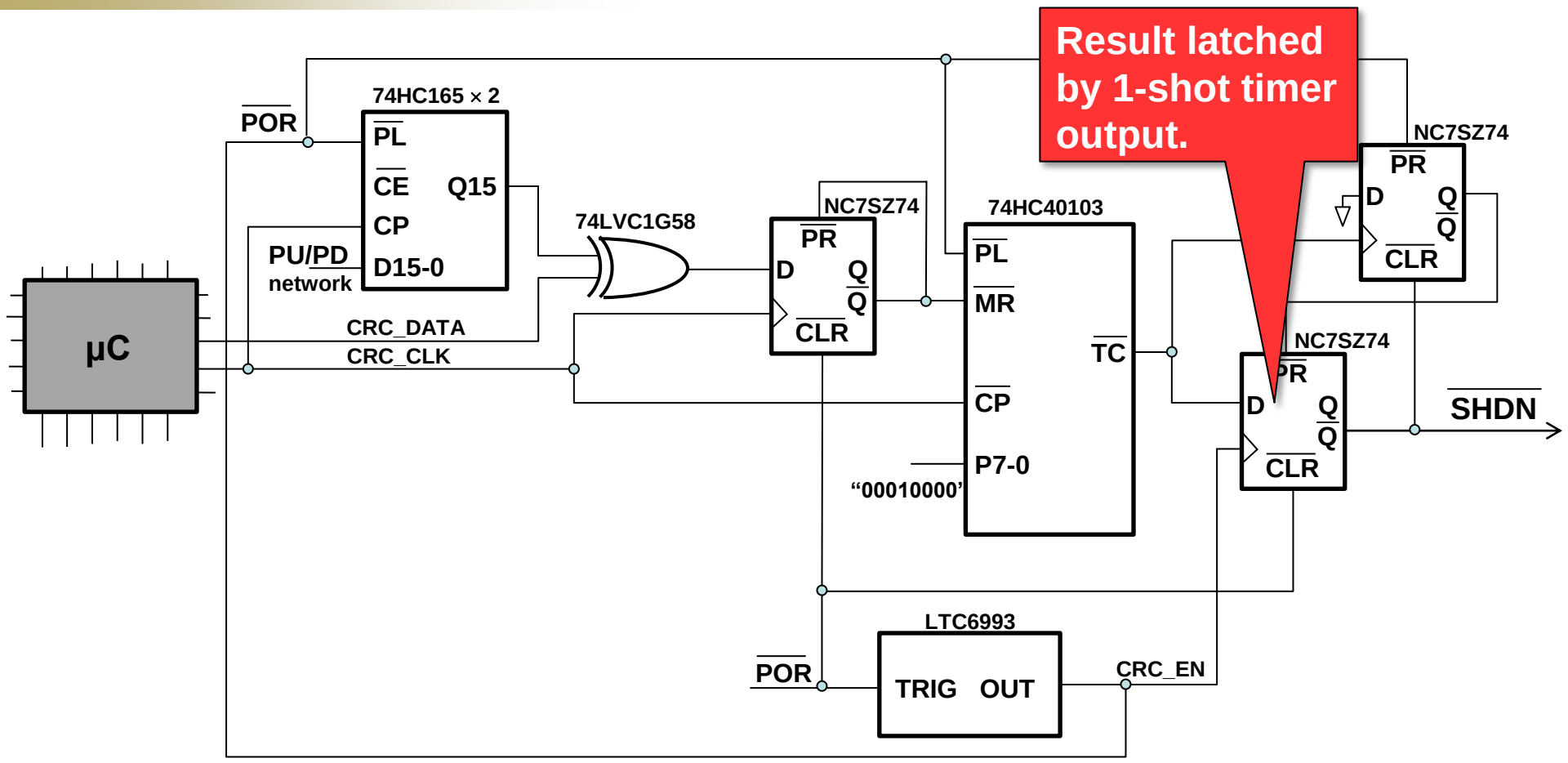
CRC Verification



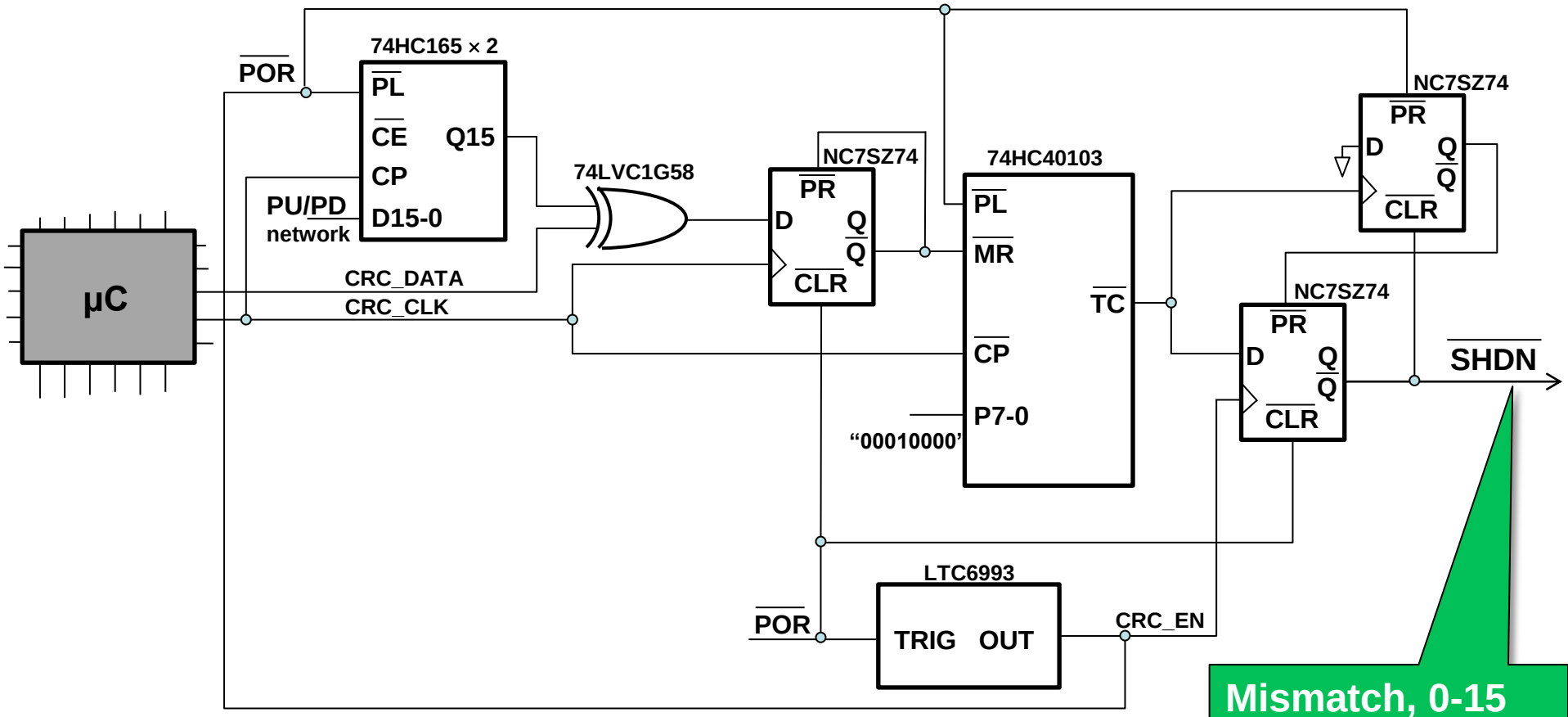
CRC Verification



CRC Verification



CRC Verification

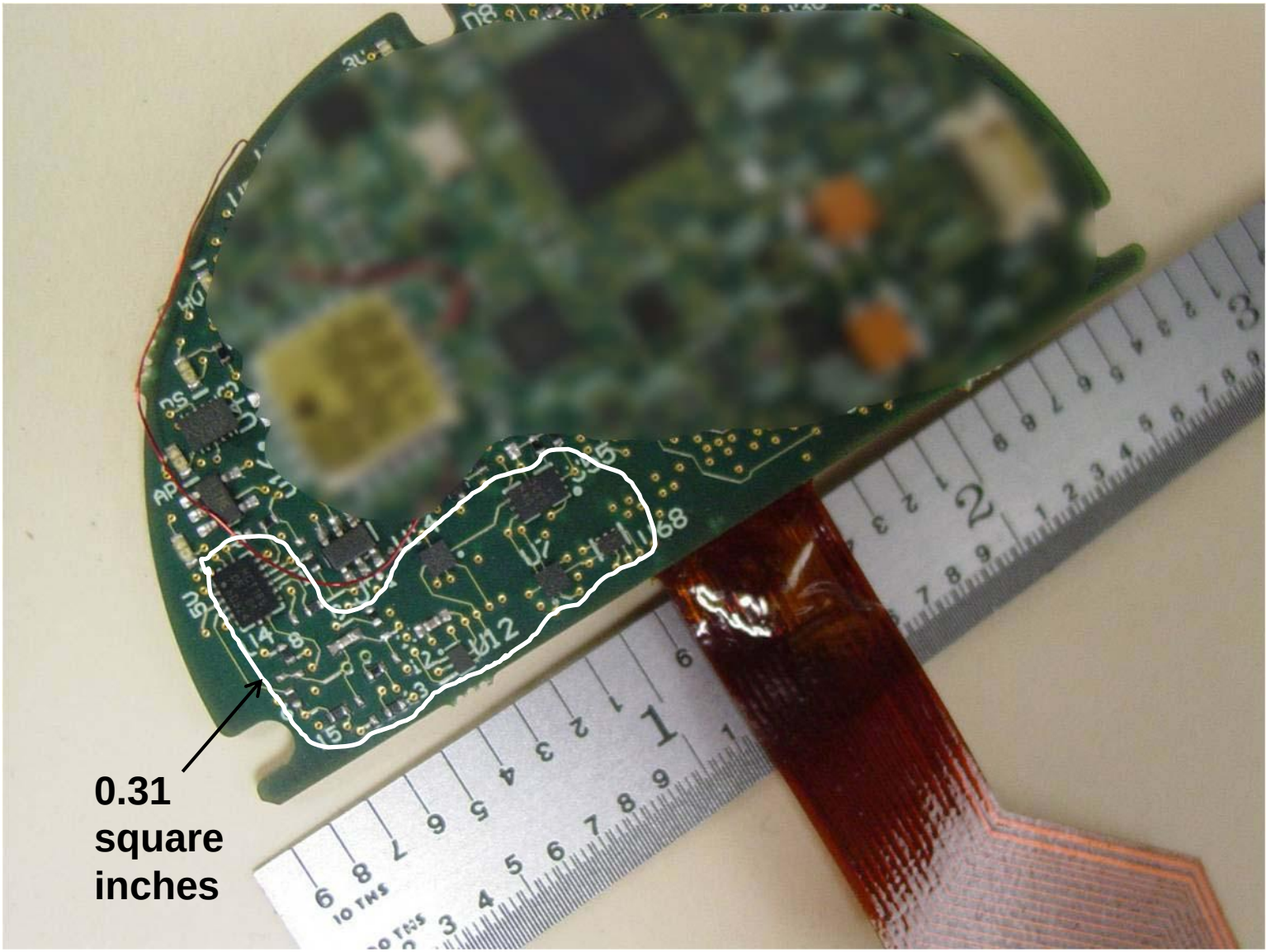


Mismatch, 0-15 clock pulses, or 17+ matches shut down ESAD power.

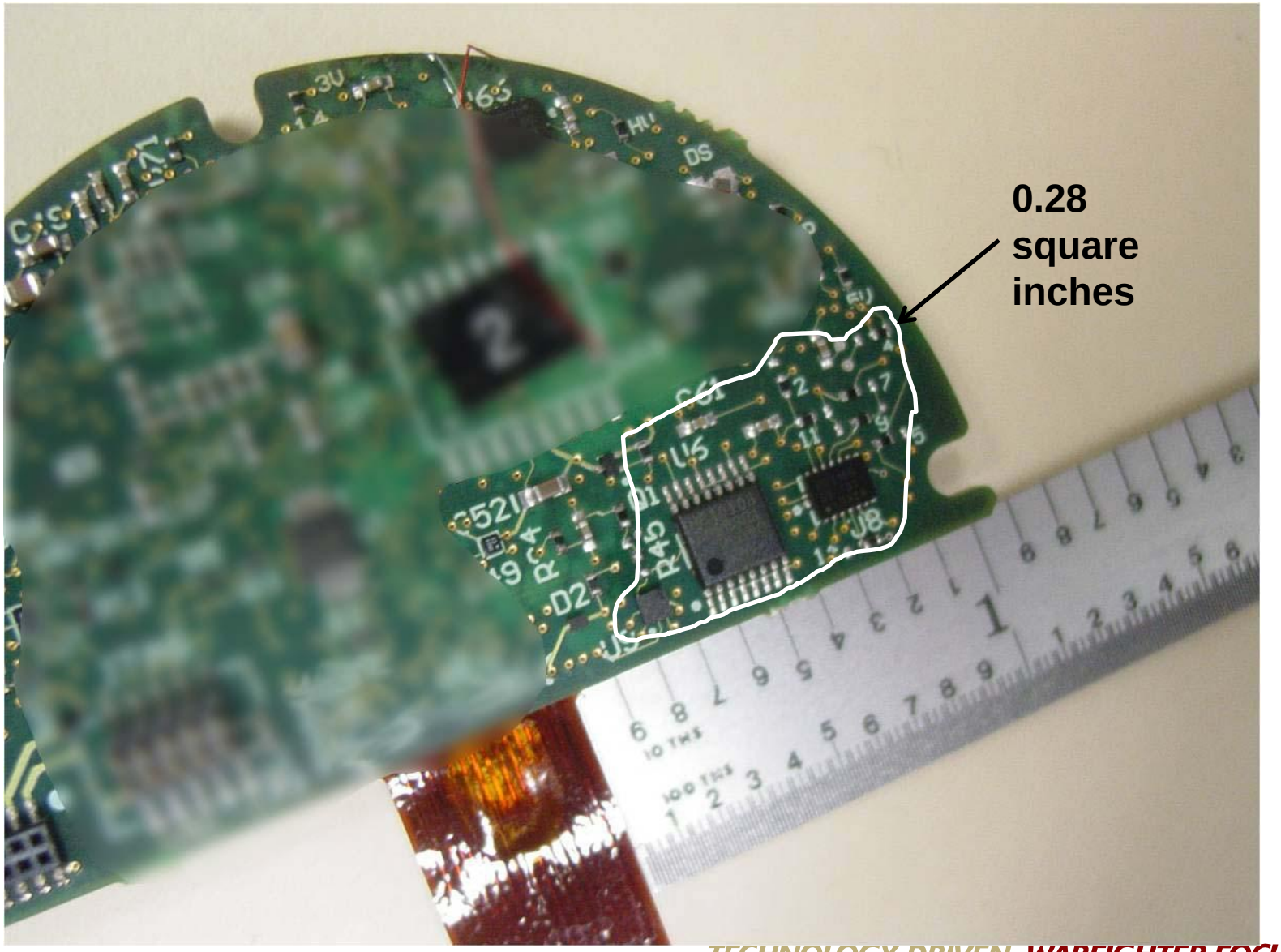
CRC Error Detection

Output Mode	Result
No pulses	Counter output (TC) remains high. 1-shot timer latches SHDN low (Power down).
1 match	Counter output (TC) remains high. 1-shot timer latches SHDN low (Power down).
1 mismatch	Counter output (TC) remains high. 1-shot timer latches SHDN low (Power down).
4 matches, 2 mismatches and 10 matches	Counter output (TC) remains high. 1-shot timer latches SHDN low (Power down).
6 matches, 2 mismatches and 10 matches	Counter output (TC) remains high. 1-shot timer latches SHDN low (Power down).
1 mismatch, 16 matches	Counter output (TC) remains high. 1-shot timer latches SHDN low (Power down).
16 matches, 1 mismatch	Counter output (TC) goes low on 16th match then high, forcing SHDN low (Power down).
18 matches	Counter output (TC) goes low on 16th match then high, forcing SHDN low (Power down).
16 matches	**Output of counter is set low and remains low. Power stays on.**

CRC Locations on Board



CRC Location on Board



Additional Information

- Time required to perform CRC
  - Approximately 300ms to calculate
  - Approximately 160µs to output
- Major components
  - Two 8-bit shift registers
  - 8-bit counter
  - 1-shot timer
  - flip-flops
  - XOR gate
  - PU/PD resistor network
- Future Development:
  - Replace shift registers with I^2C buffer
  - Fewer components and less board real-estate

Presenter contact information:

Anthony C. Steele II
US Army Research, Development, and Engineering Command (RDECOM)
Aviation & Missile Research, Development, and Engineering Center (AMRDEC)
Redstone Arsenal, Alabama, USA
(256) 842-1980
anthony.c.steele@us.army.mil