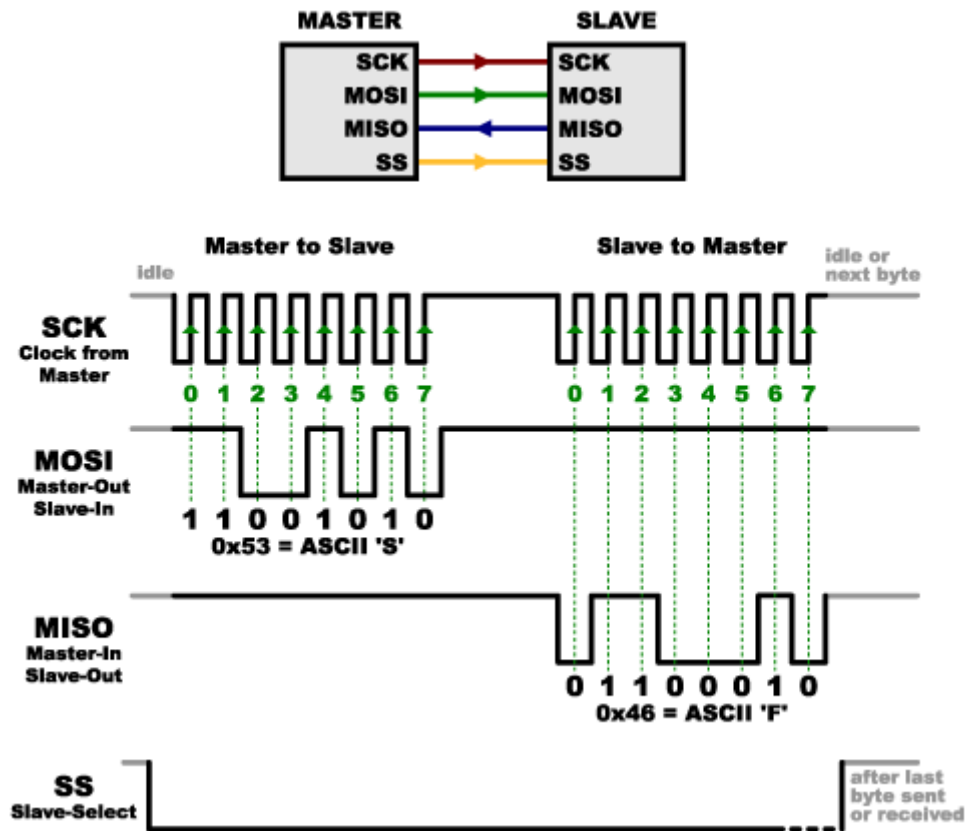**JTAG**

★ Joshua Tree Art Gallery
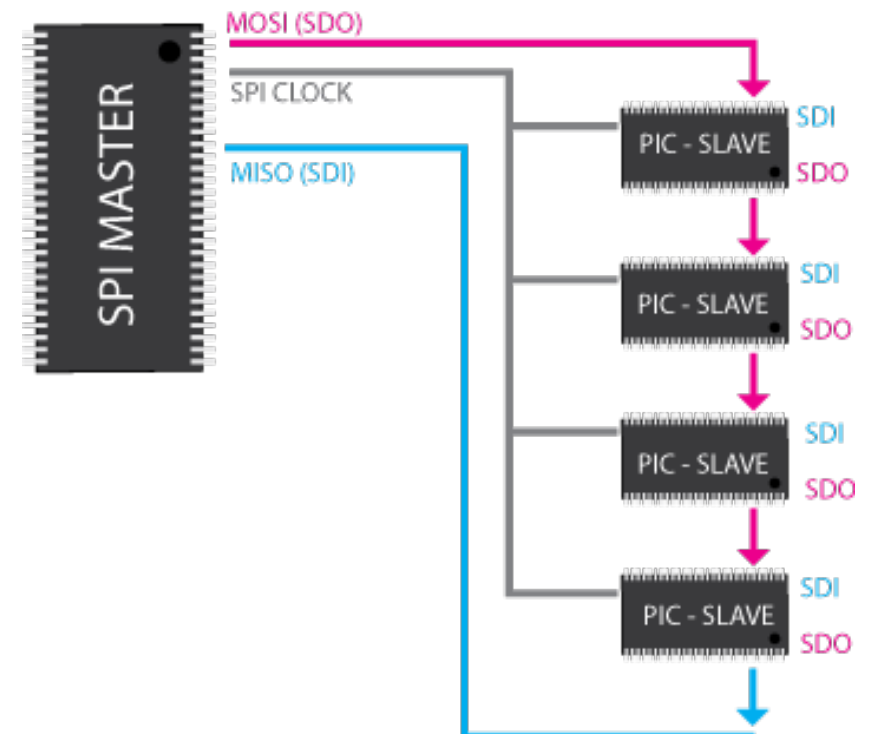
JTAG protocol

- *"It's I2C for testing"*

- Popular transport layer for boundary-scan, debugging, etc

- ...but not limited to this.

SPI

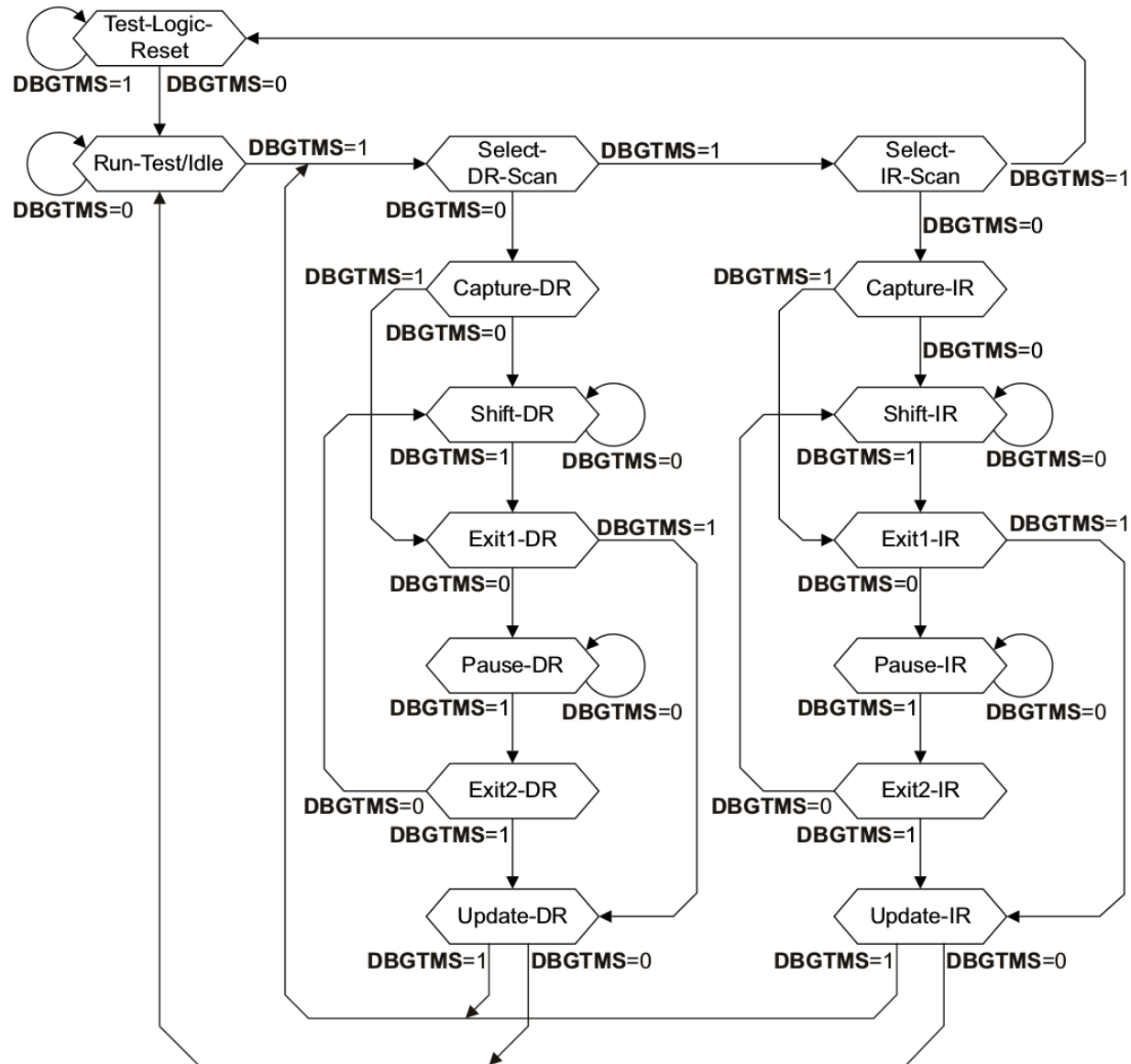## Signalling:

Daisy chaining:

JTAG: a *reconfigurable* daisy chain.

- **One or more slave systems in the scan chain**
  - **TAPs (Test Access Ports)**
- **Each slave has multiple register options**
  - **Instruction register** *(fixed bit-length, but same for all ICs)*
  - **Data register** *(variable bit-length, based on instruction)*
  - More **versatile**, better **performance** for complex systems
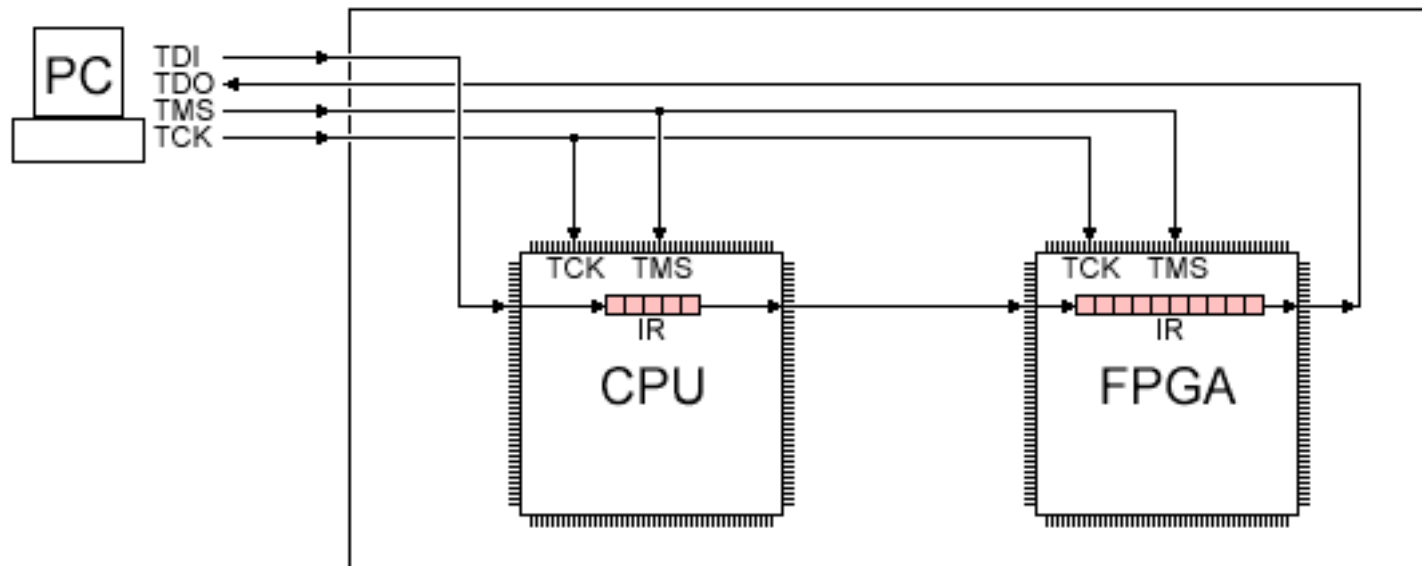
How? the TMS signal

Types of instructions

Mandatory:

- **BYPASS** (1-bit DR) ← *standardized instruction code*
- **EXTEST** (write access to device pins)
- **SAMPLE/PRELOAD** (read access to device pins)

Other:

- **IDCODE** (32-bit DR)
  - Not mandatory, but often supported
  - DR value identifies the TAP
  - If supported, IDCODE data register is the default connected data register after reset (allows scan-chain discovery)
- **Other instructions are TAP-specific – usually allow some kind of data access**
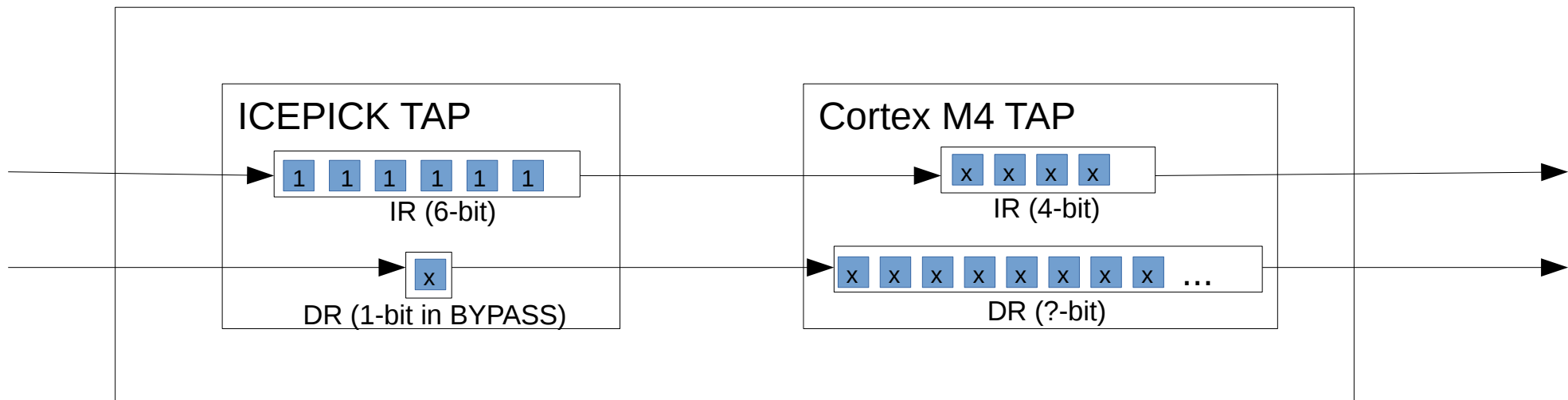
Example: CC3200 SoC

1.2 Architecture Overview

The building blocks of CC3200 system-on-chip are shown in Figure 1-1
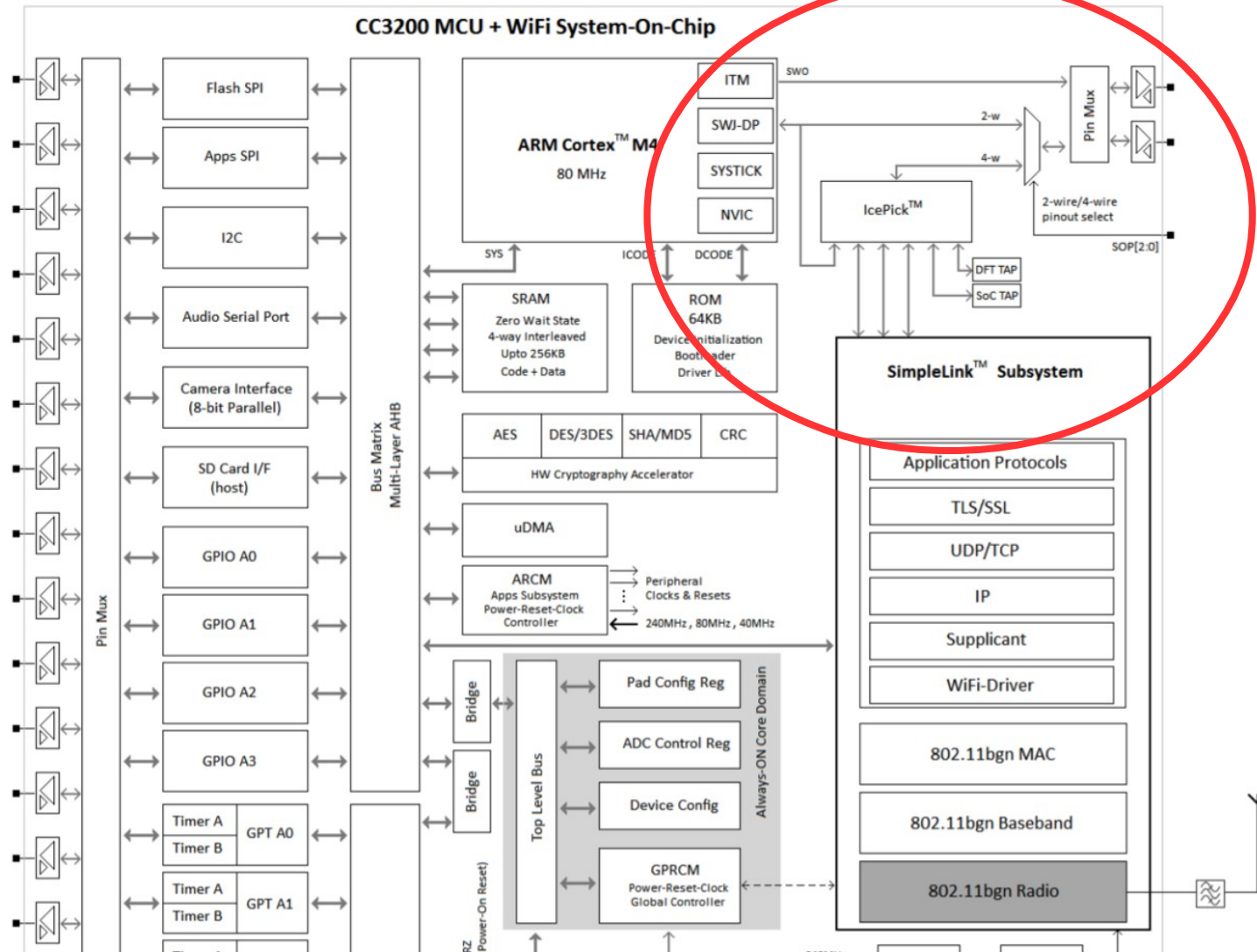
Example: CC3200 SoC

- By default, only one TAP: TI's "ICEPICK" router.
  - Can be configured to add various SoC internal TAPs to the scan chain.
  - Generic documentation available, CC3200-specific configuration found in OpenOCD
- Only internal TAP explicitly specified in the public datasheet is that of the user ARM Cortex M4 core.
  - Presumably others for pin access, testing features, access to the Wi-Fi core, etc.

- Debugging TAP scan chain configuration for CC3200:

ICEPICK TAP

`1 1 1 1 1 1`
IR (6-bit)

`x`
DR (1-bit in BYPASS)

Cortex M4 TAP

`x x x x`
IR (4-bit)

`x x x x x x x x` ...
DR (?-bit)

Example: CC3200 SoC

Q: So once we have access to the ARM core's TAP, what do we do?

- A: we need read a whole bunch of stuff first.

  - ARMv7-M Architecture Reference Manual

  - ARM Debug Interface v5 Specification

  - ARM Cortex M4 Technical Reference Manual

Example: CC3200 SoC

Cortex M4 TAP
(same in all ARMv7-M
family processors)

MEM-AP
(same in all ARMv7-M
family processors)

access to "AP's"
via an address-based
access protocol

Memory-mapped debug registers
(Cortex M4-specific)

access to memory
via a another address-
based access protocol

System memory access
(Cortex M4-specific)

(other AP's)