Reverse engineering AT32UC3A's JTAG

LSE Summer Week 2014

Pierre Surply

EPITA 2016

Jul 19, 2014

On-Chip Debug

Figure: AVR Dragon

```
avr32gdbproxy -e "avrdragon" -a ":4242"
```

JTAG

- Join Test Action Group
- Published in April 1990
- IEEE 1149.1
- Standard Test Access Port and Boundary-Scan Architecture

JTAG pins

- TCK : Test Clock
- TMS : Test Mode Select
- TDI : Test Data Input
- TDO : Test Data Output
- TRST : Test Reset

Registers

- Instruction Registers
- Data Registers:
  - `IDCODE`
  - `BYPASS`
  - `BSR`

JTAG Block Diagram

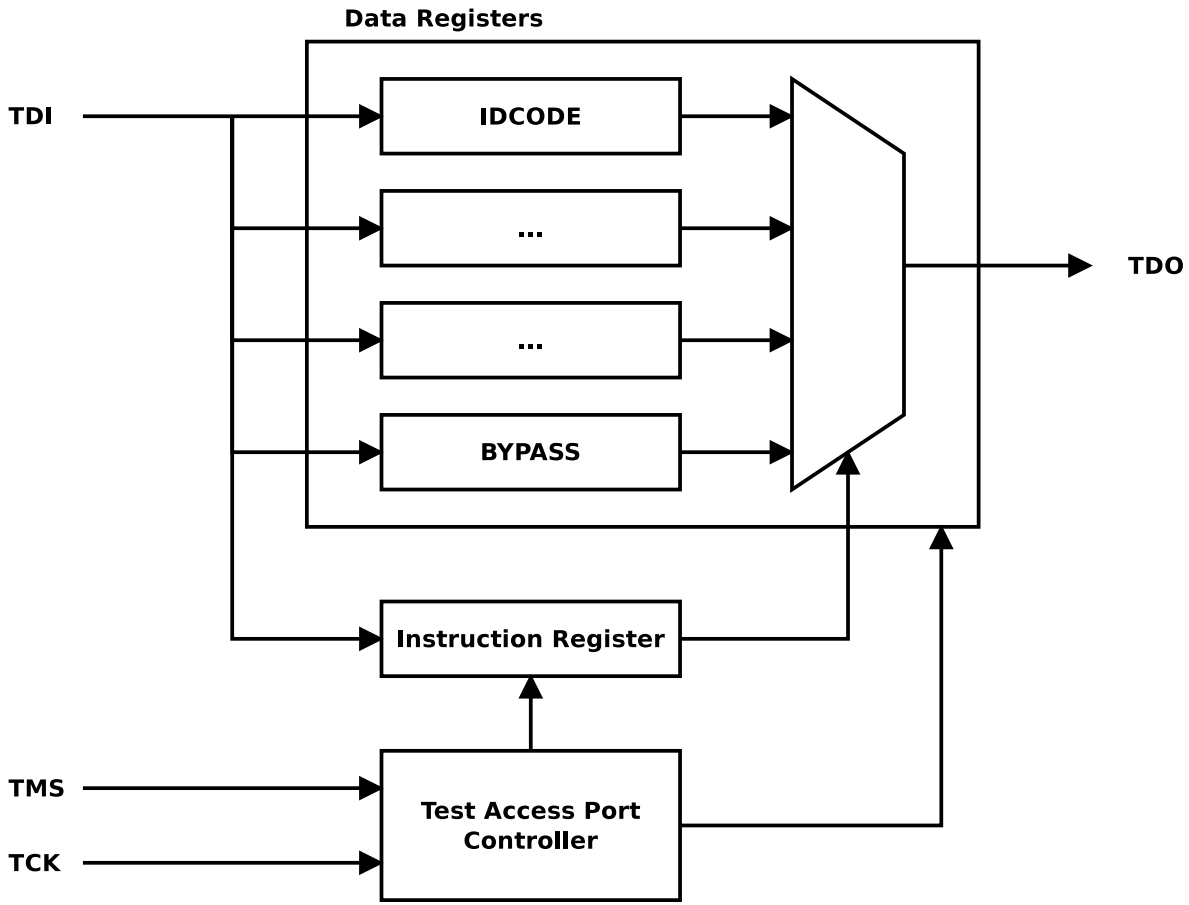


Figure: JTAG Block Diagram

Shift Register

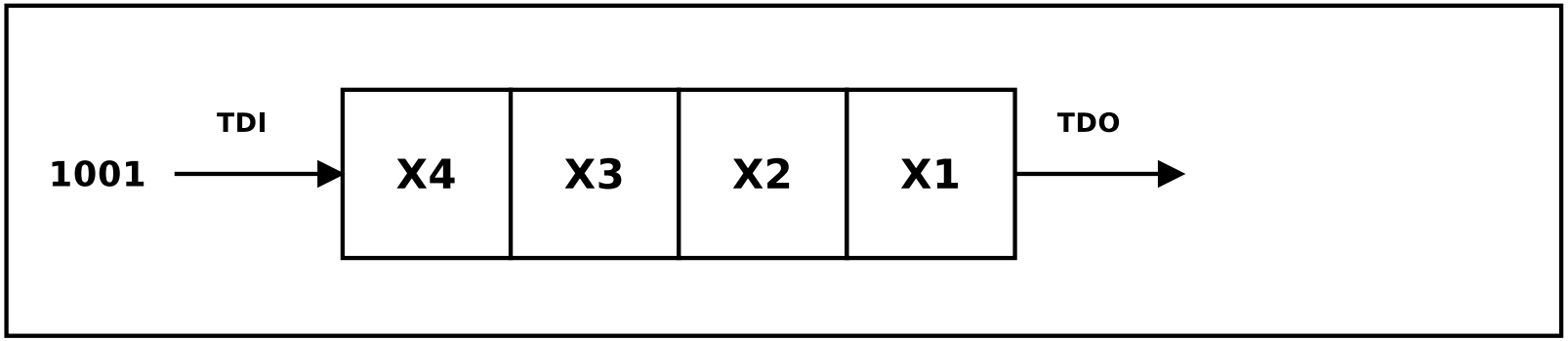


Figure: Shift Register (1/5)

Shift Register

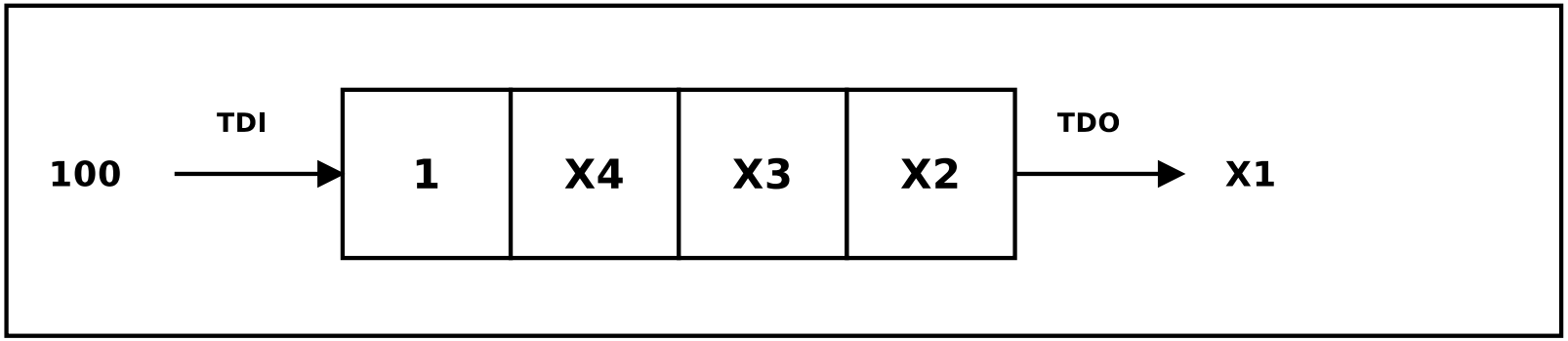


Figure: Shift Register (2/5)

Shift Register

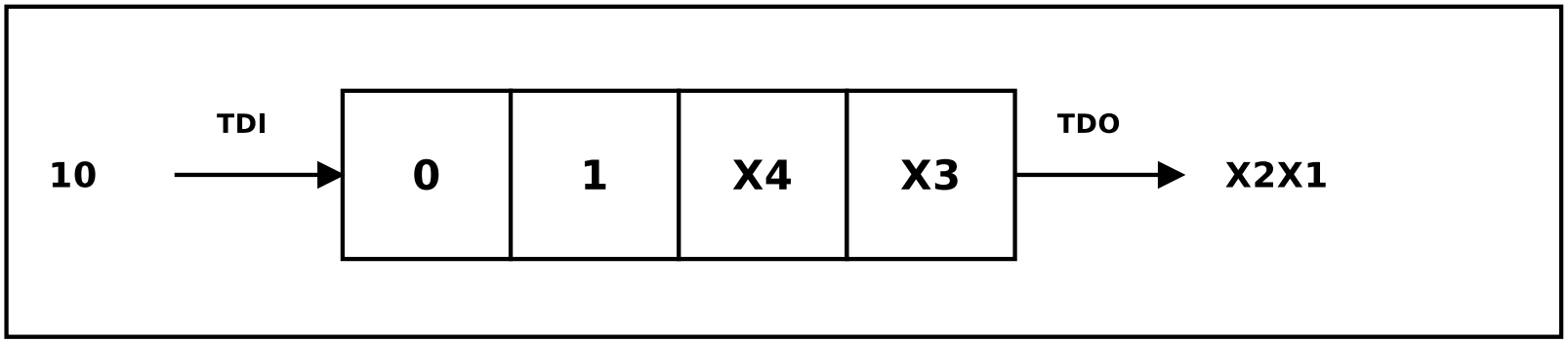


Figure: Shift Register (3/5)

Shift Register

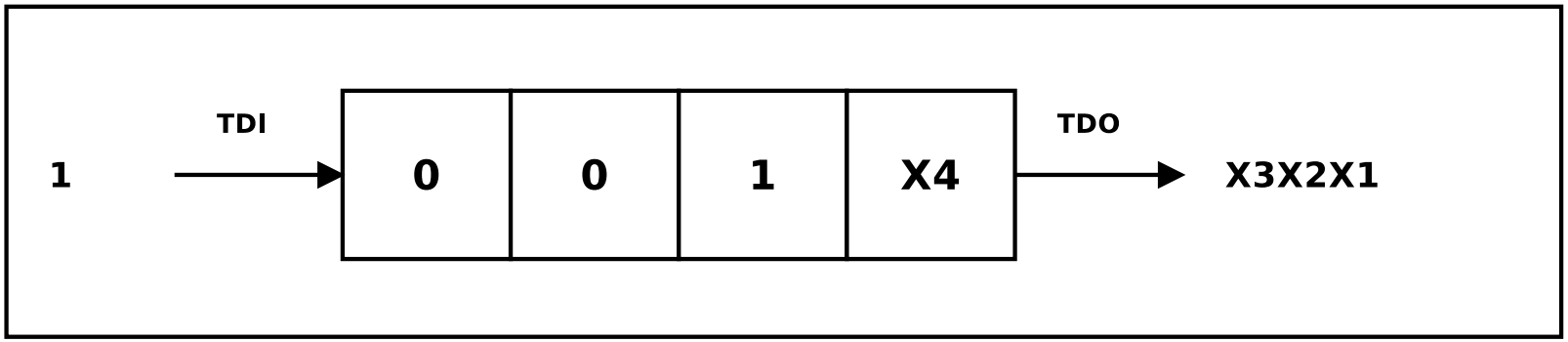


Figure: Shift Register (4/5)

Shift Register

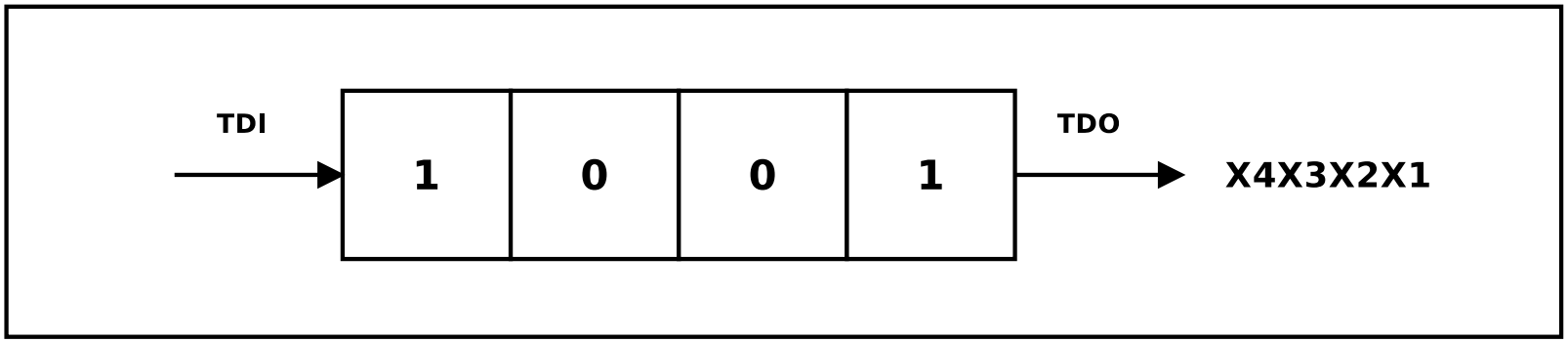
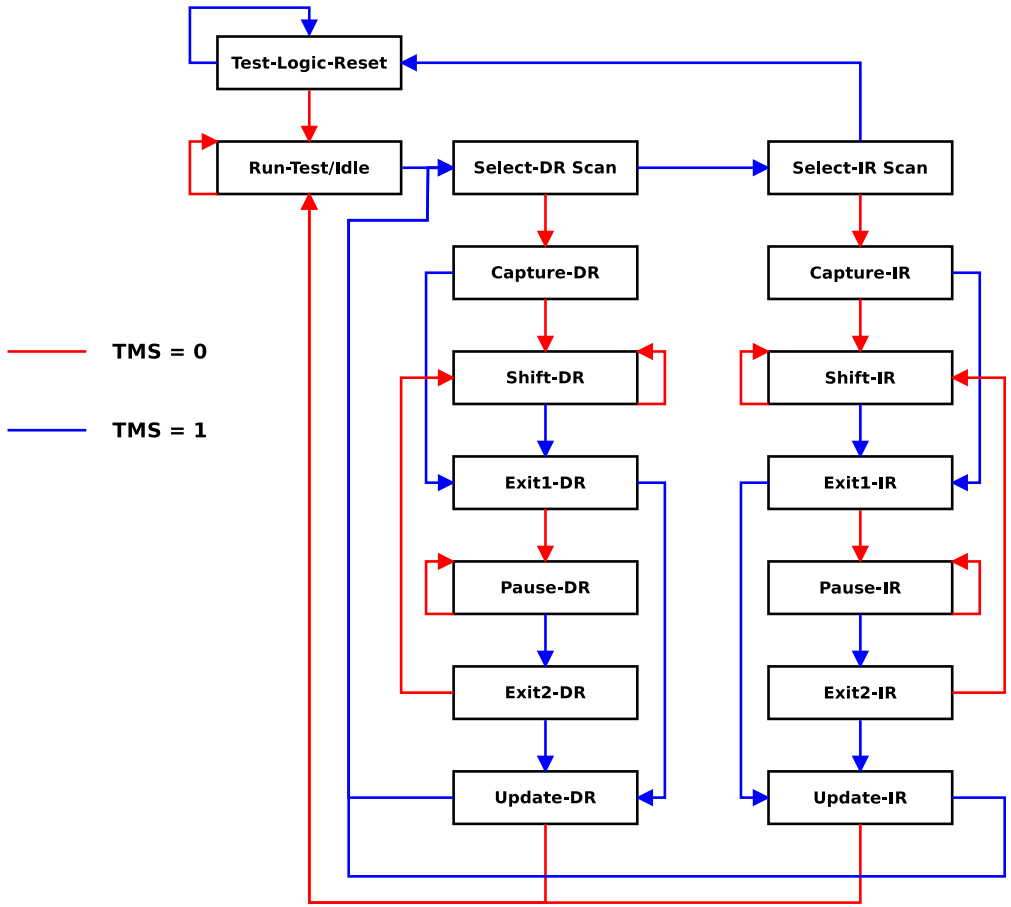


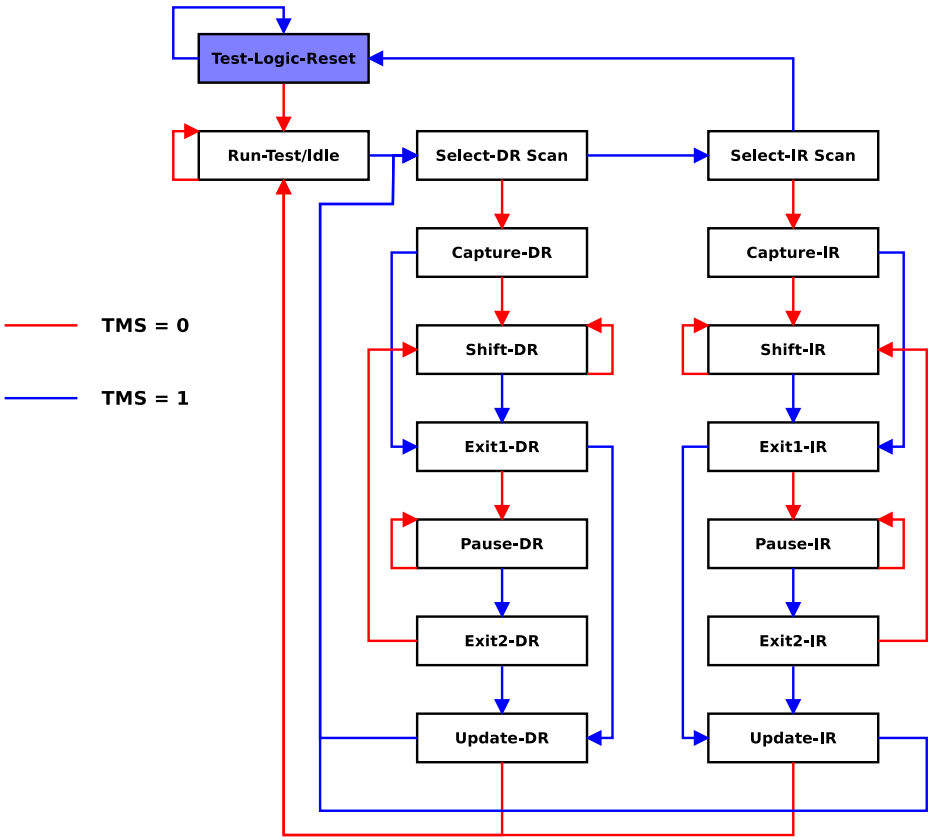
Figure: Shift Register (5/5)

TAP Controller State Machine



- DR: Data Register
- IR: Instruction Register

TAP Controller State Machine



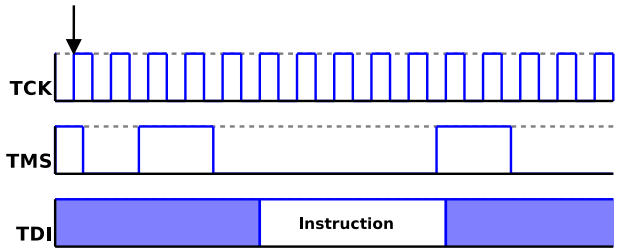


Figure: TAP Controller Example (1/13)

TAP Controller State Machine

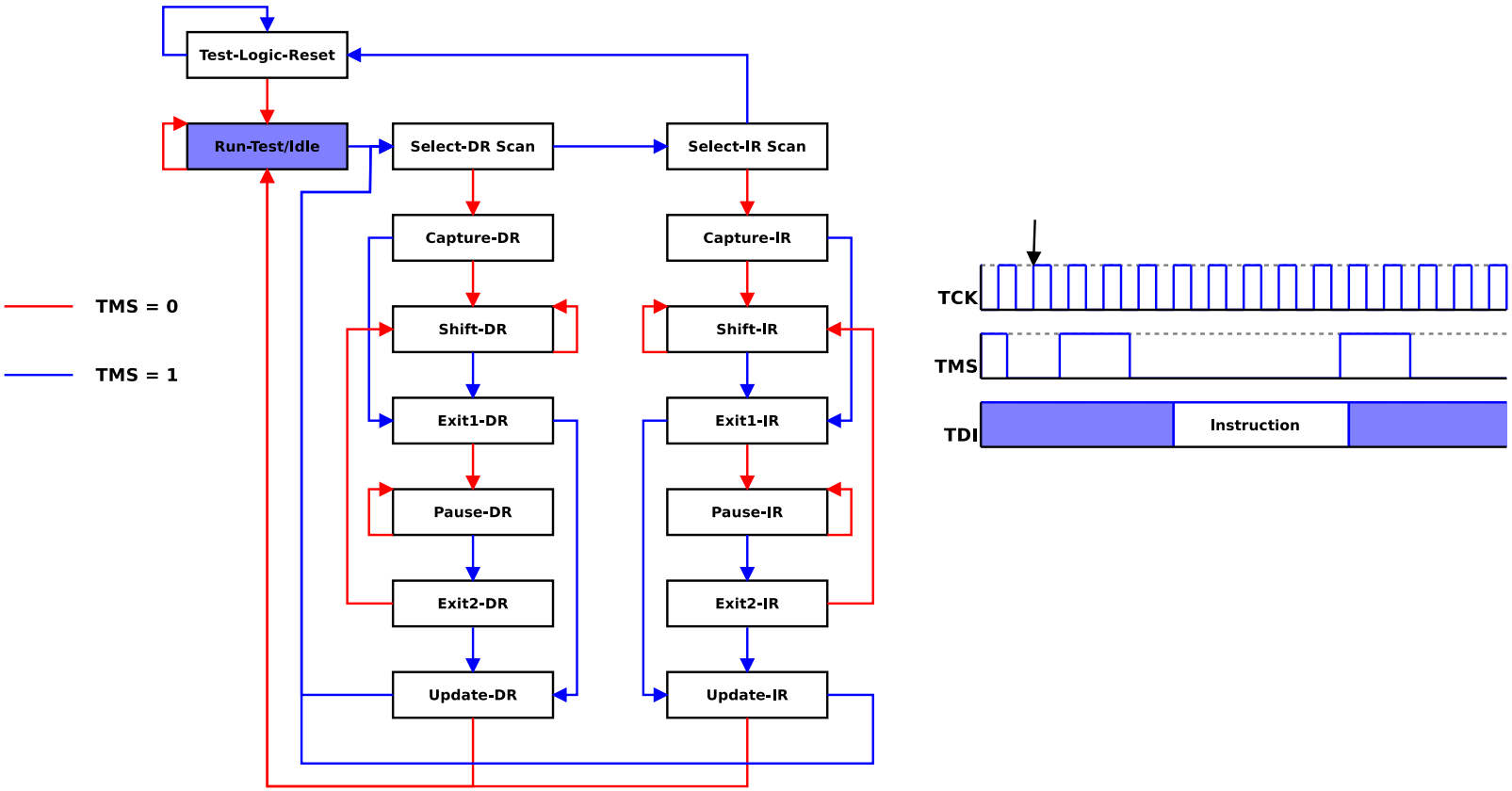
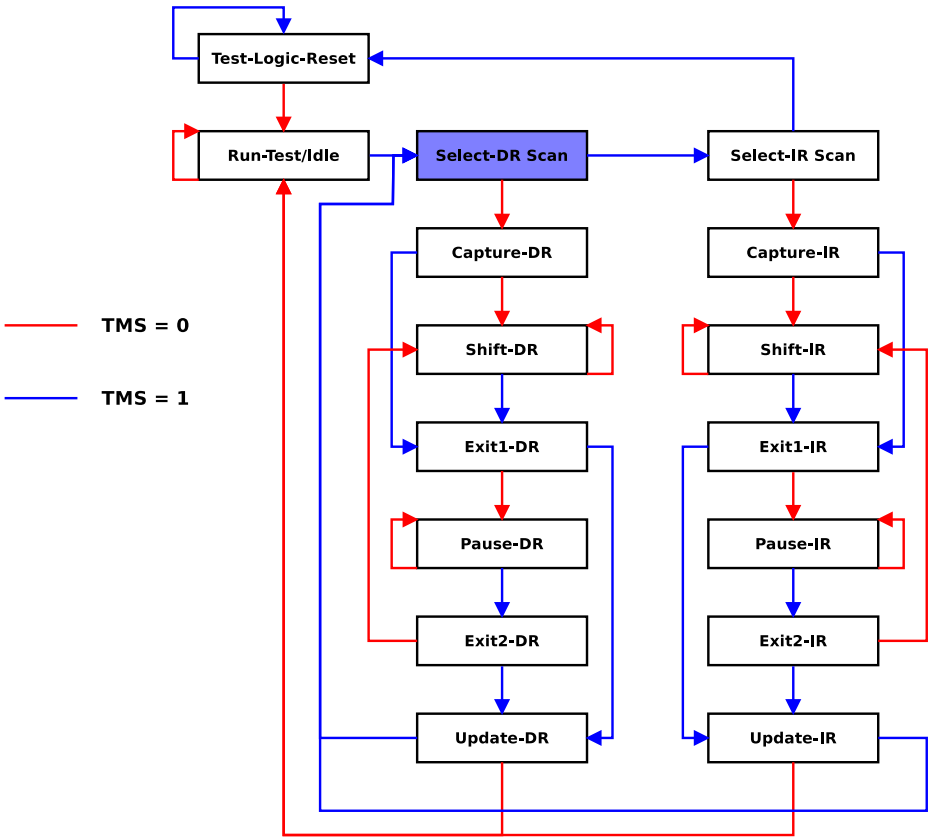


Figure: TAP Controller Example (2/13)

TAP Controller State Machine



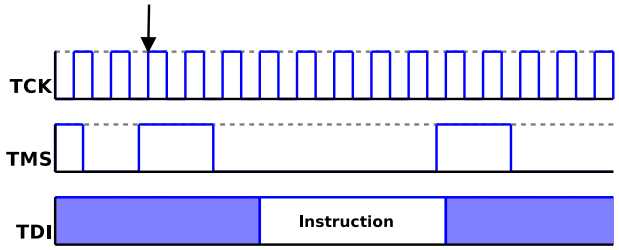
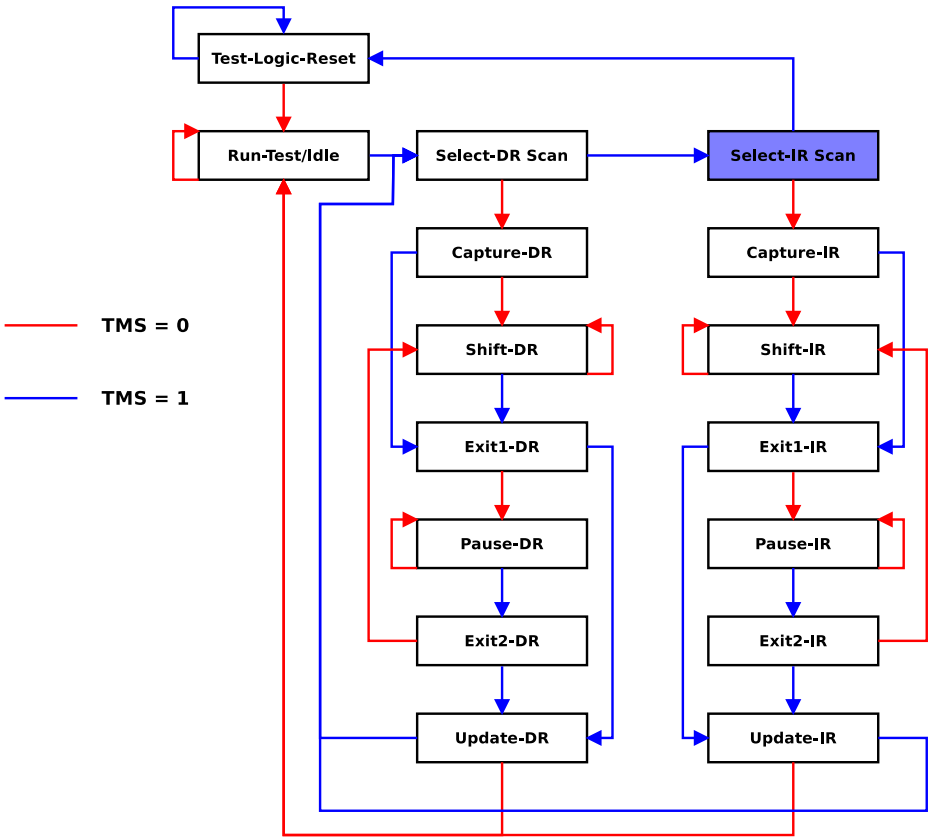


Figure: TAP Controller Example (3/13)

TAP Controller State Machine



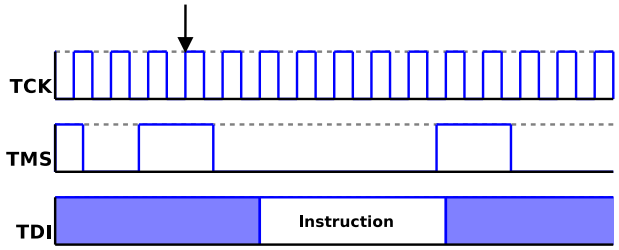


Figure: TAP Controller Example (4/13)

TAP Controller State Machine

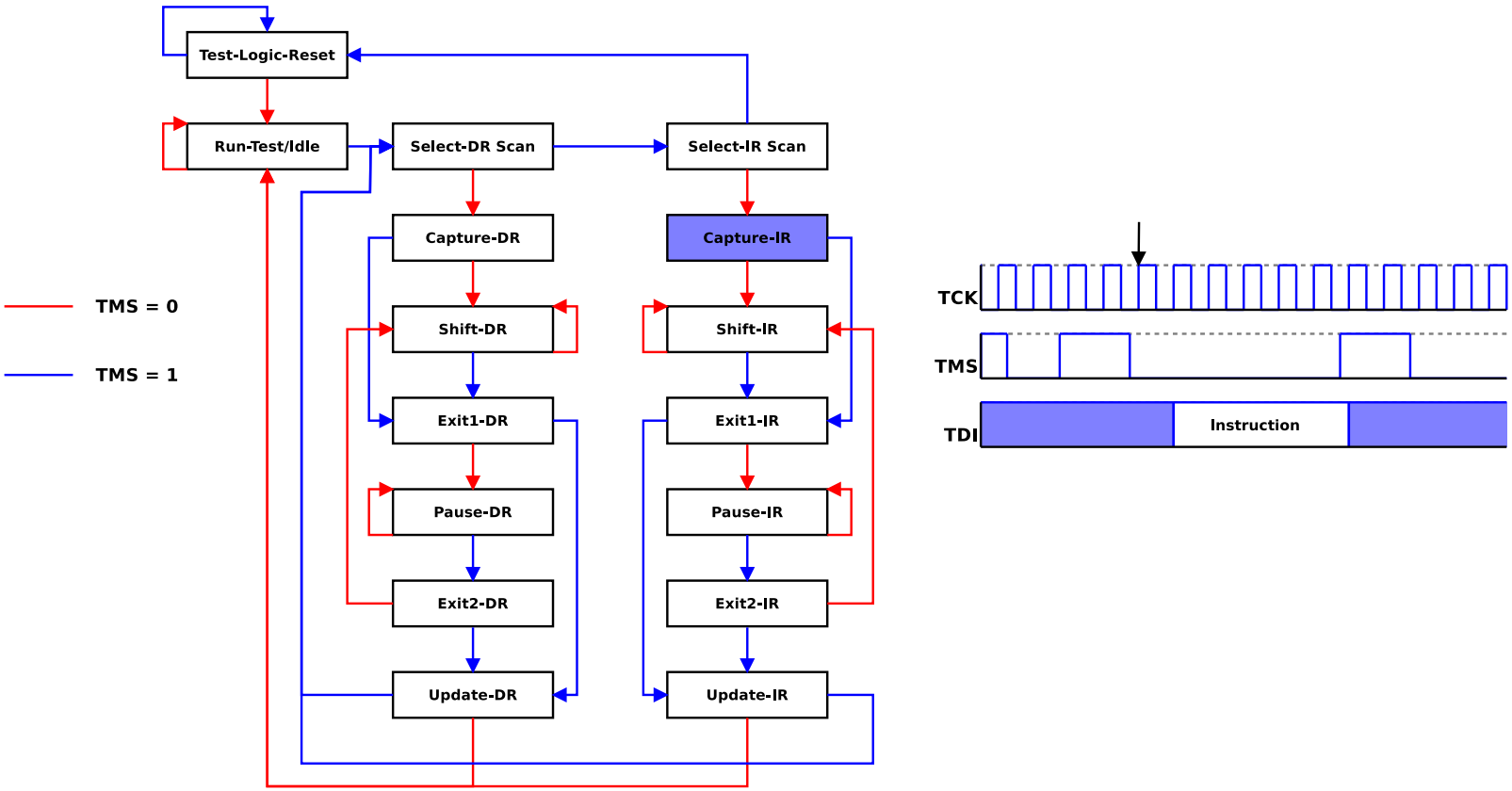


Figure: TAP Controller Example (5/13)

TAP Controller State Machine

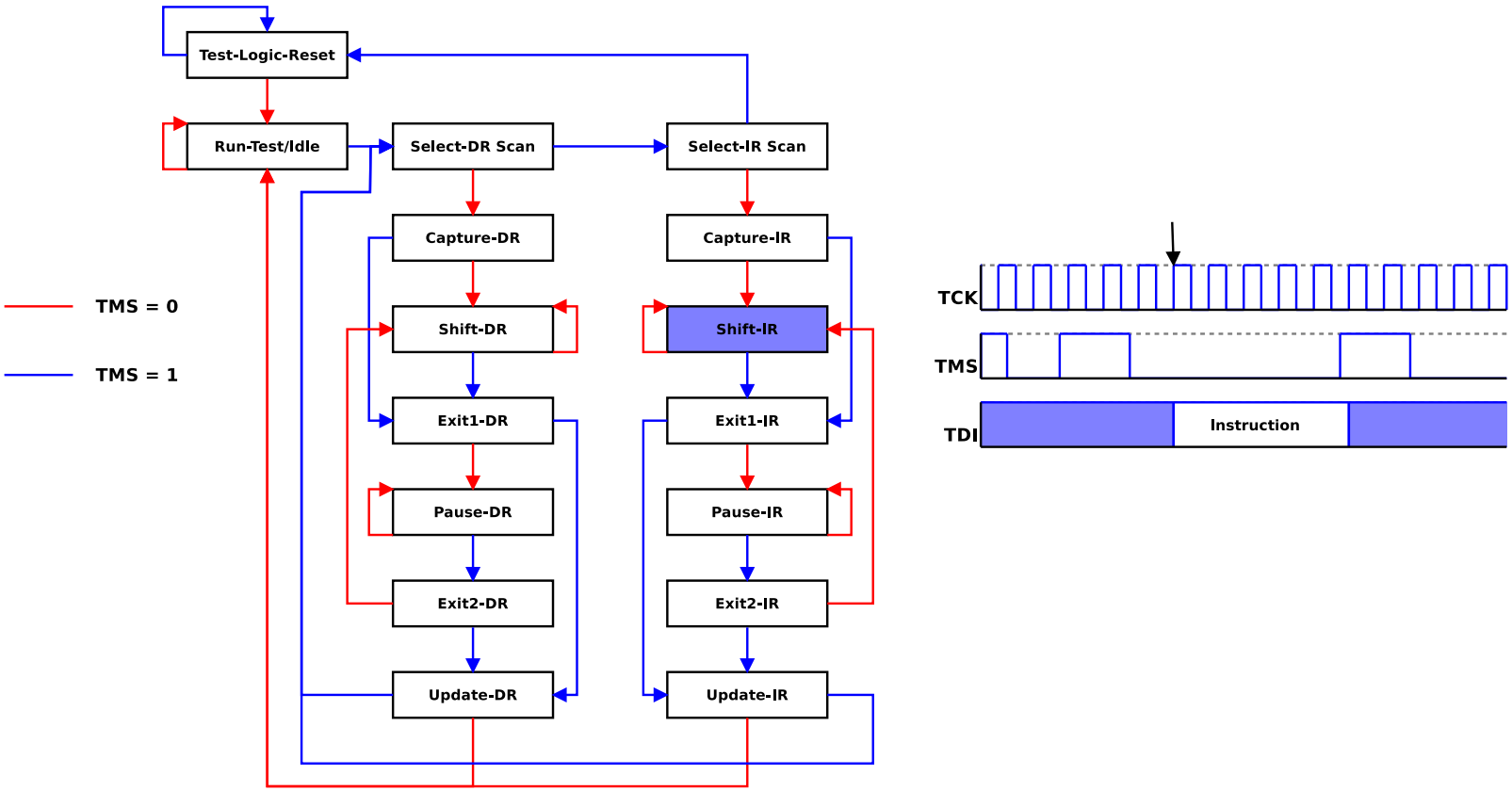


Figure: TAP Controller Example (6/13)

TAP Controller State Machine

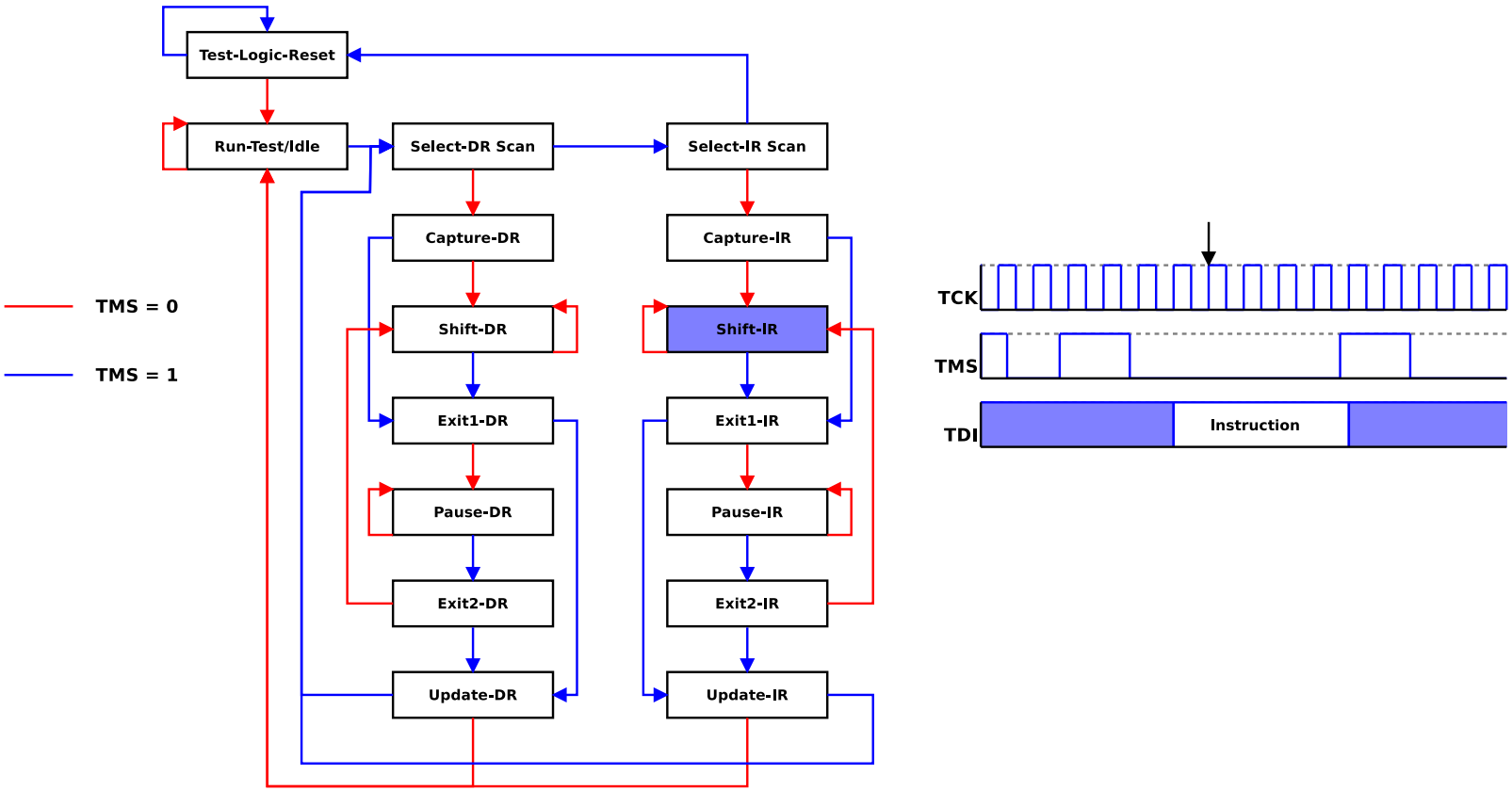


Figure: TAP Controller Example (7/13)

TAP Controller State Machine

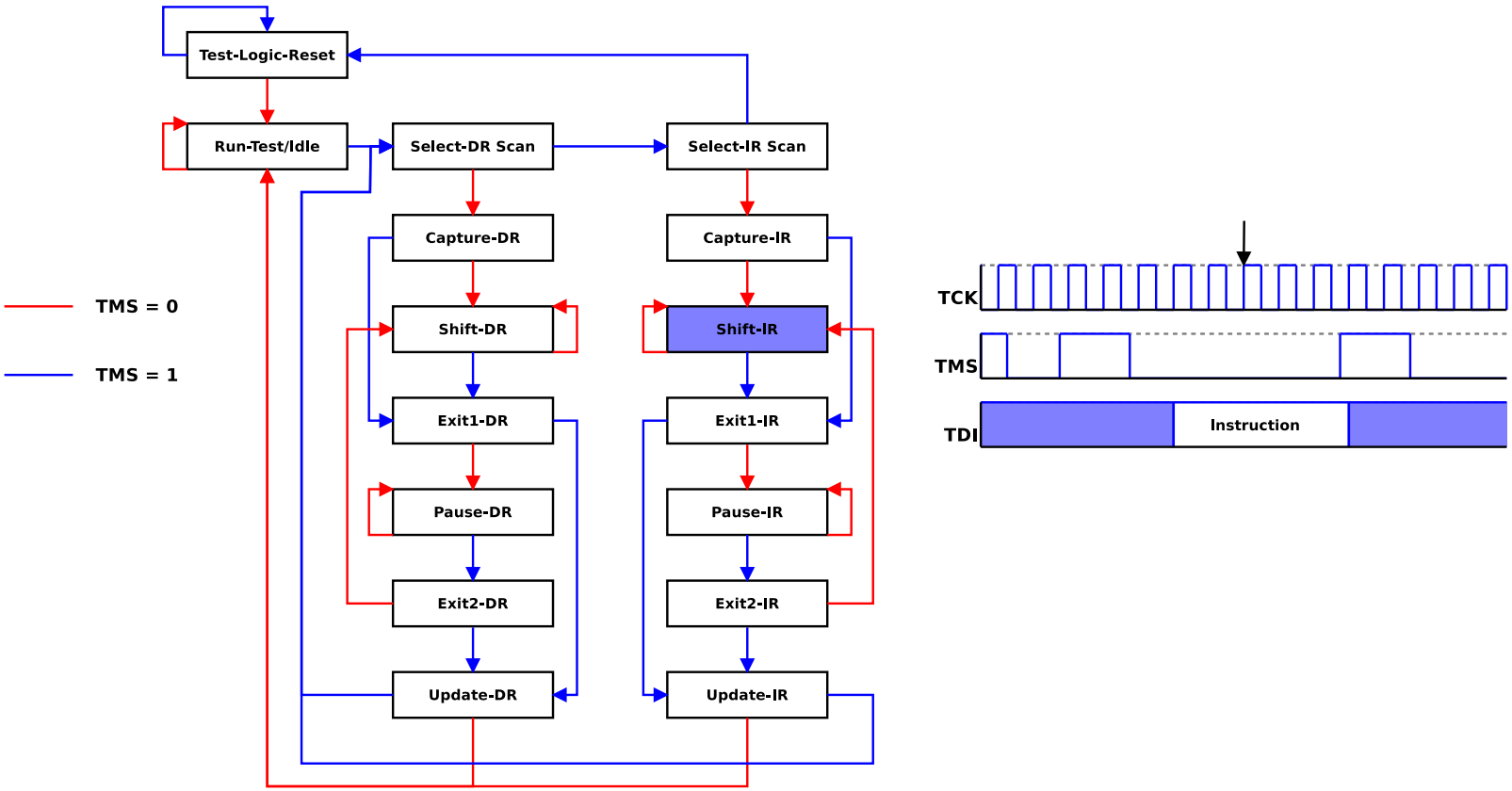


Figure: TAP Controller Example (8/13)

TAP Controller State Machine

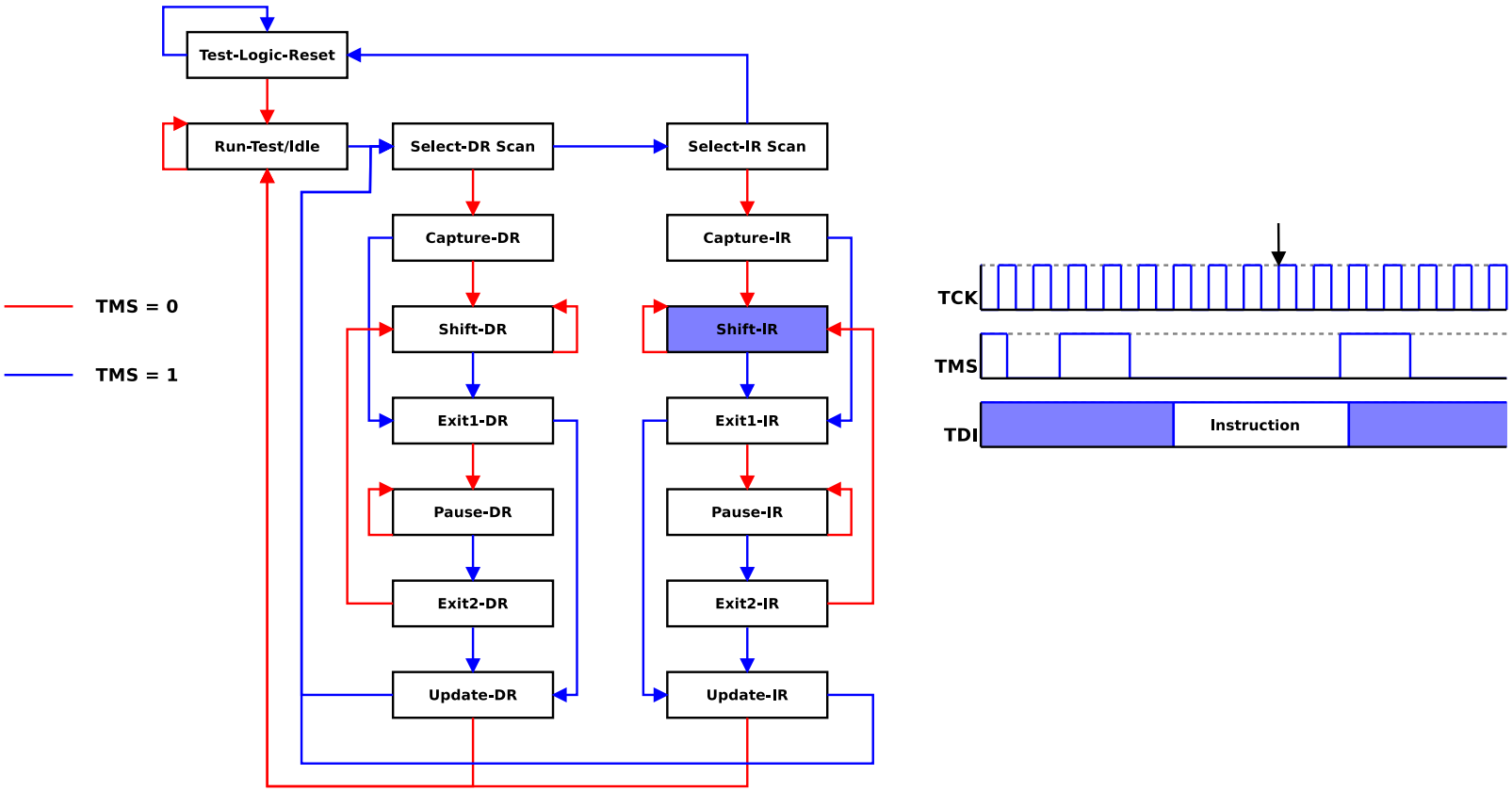
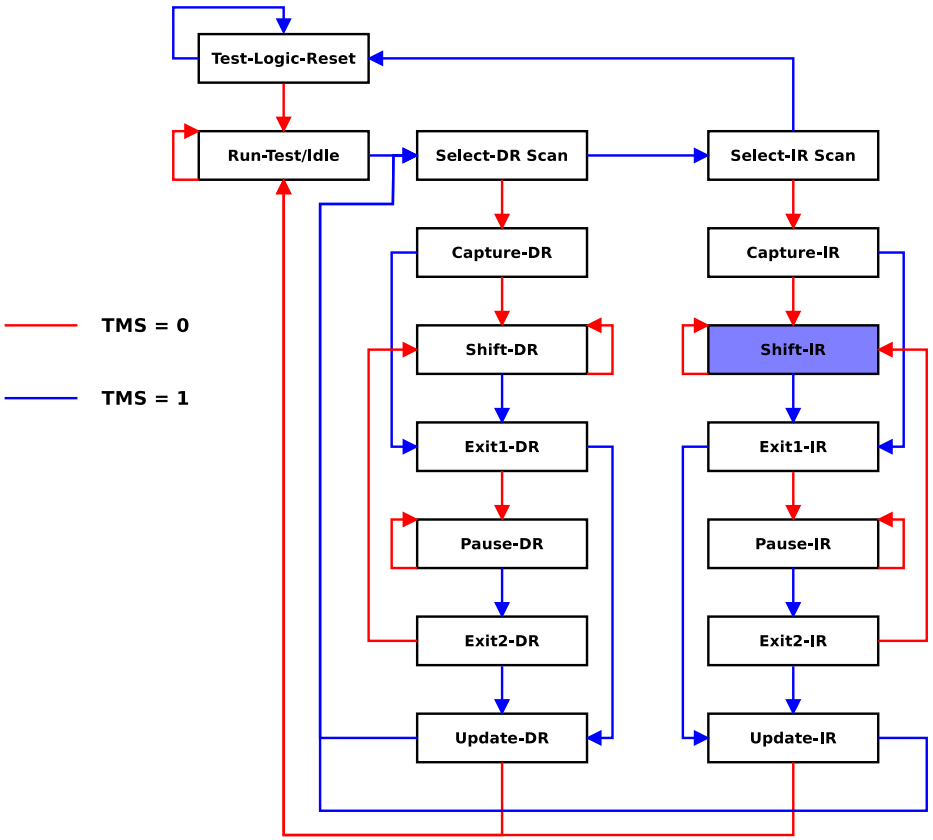


Figure: TAP Controller Example (9/13)

TAP Controller State Machine



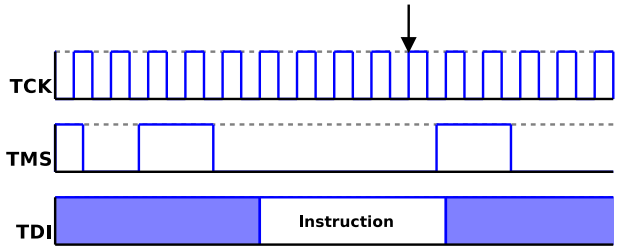


Figure: TAP Controller Example (10/13)

TAP Controller State Machine

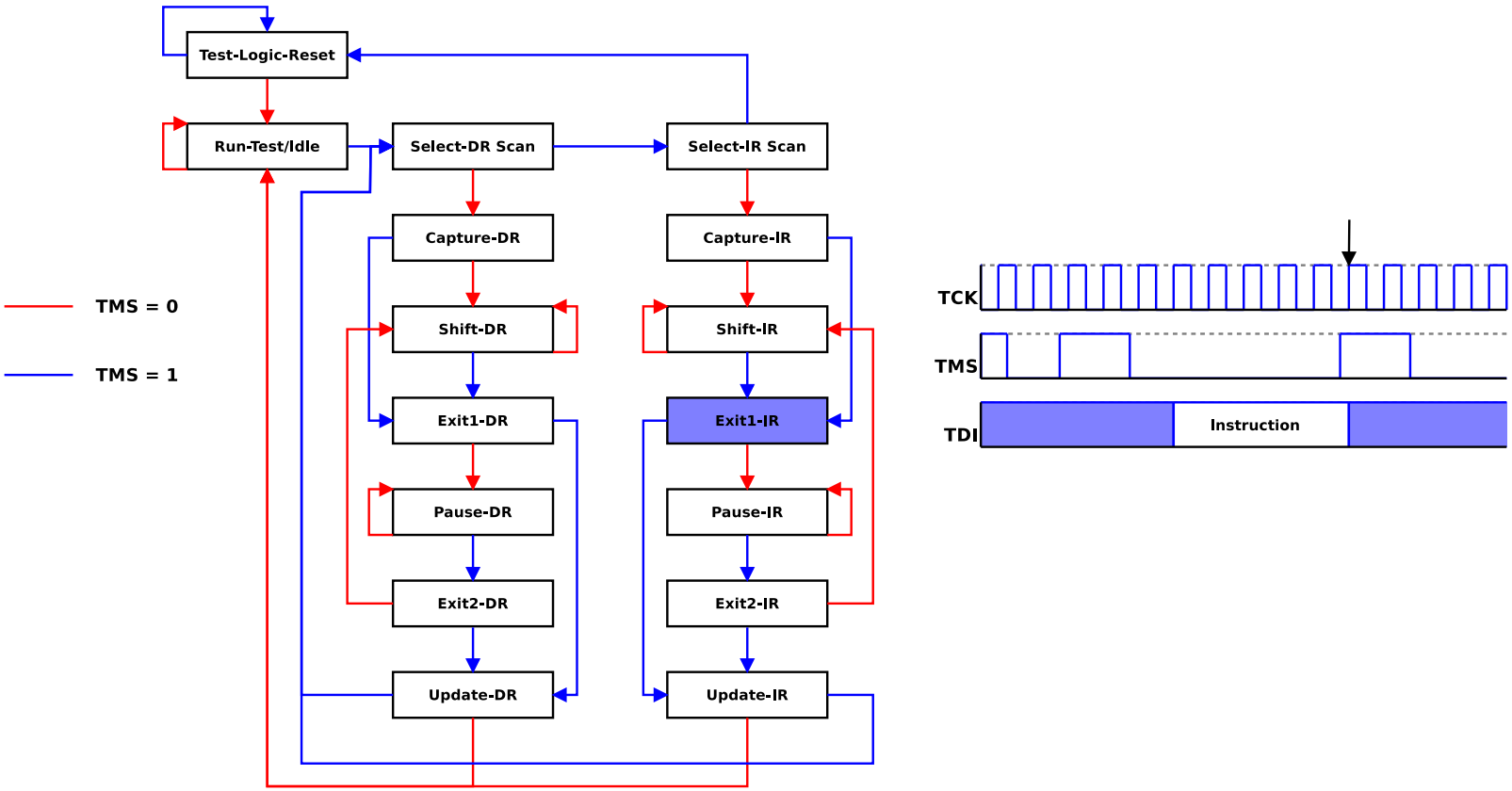


Figure: TAP Controller Example (11/13)

TAP Controller State Machine

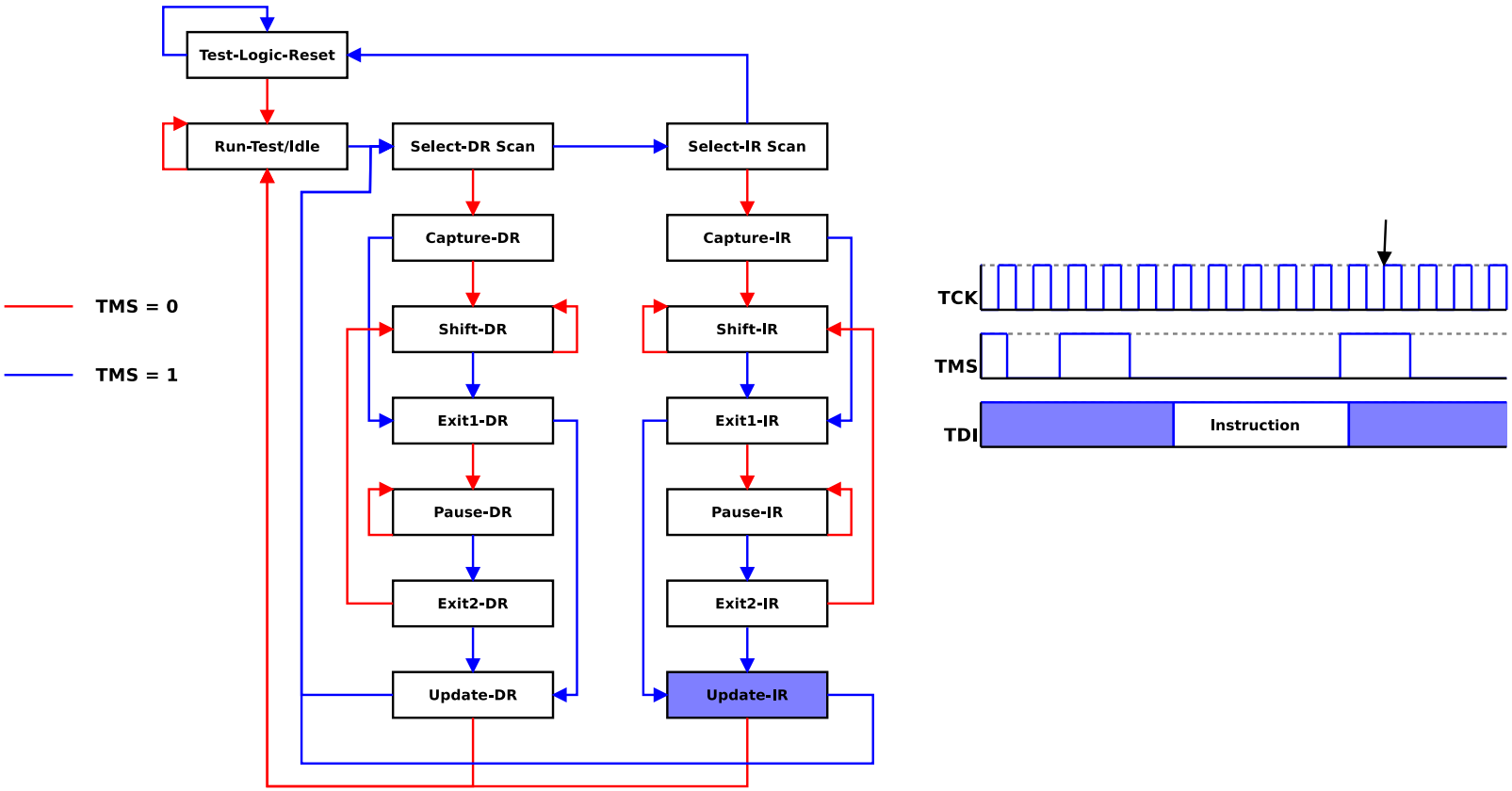
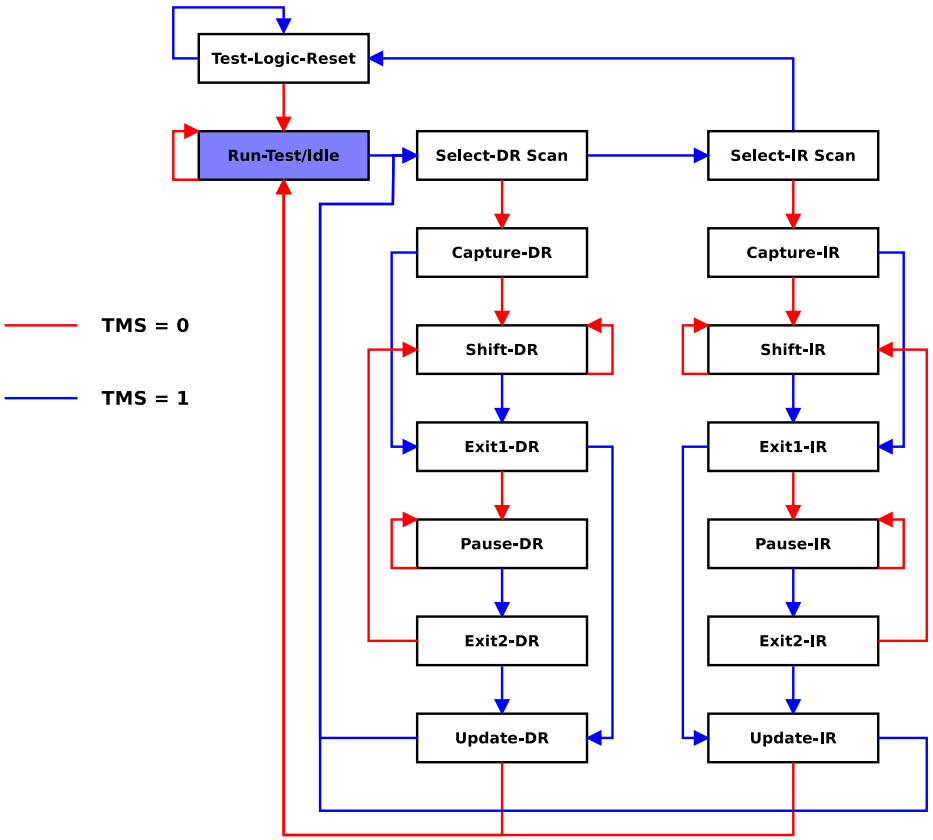


Figure: TAP Controller Example (12/13)

TAP Controller State Machine



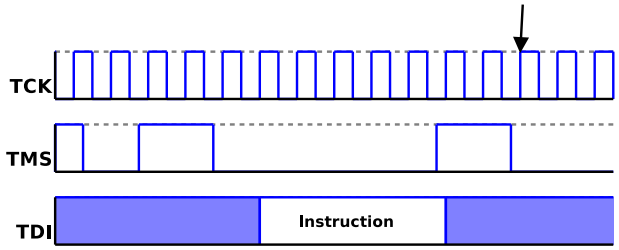


Figure: TAP Controller Example (13/13)

Daisy Chain

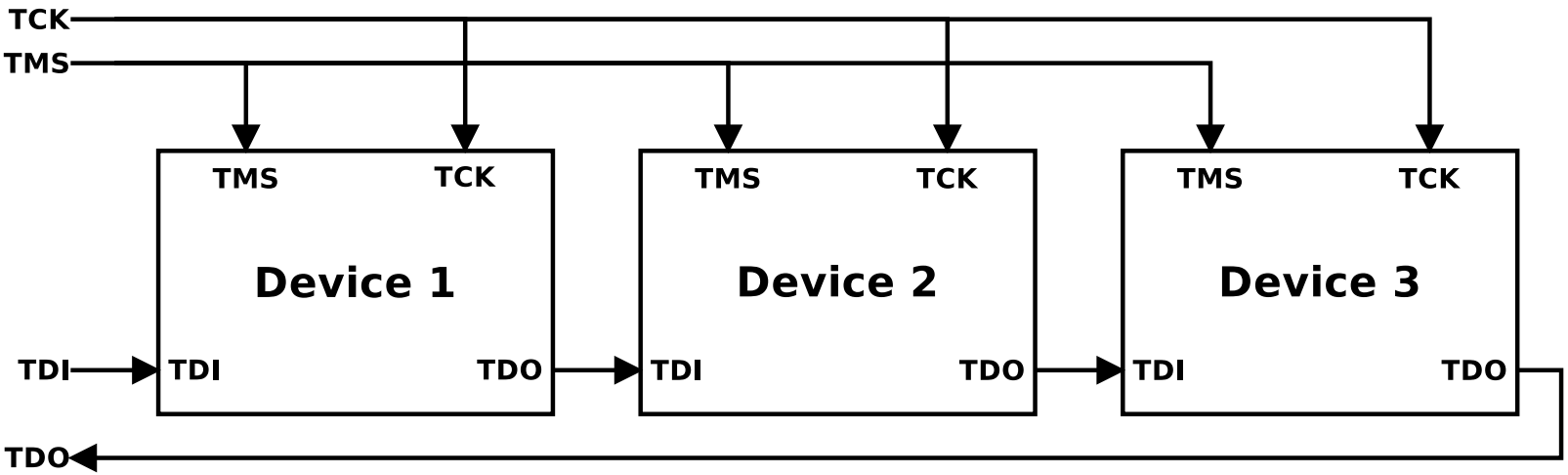


Figure: Daisy Chain

BYPASS

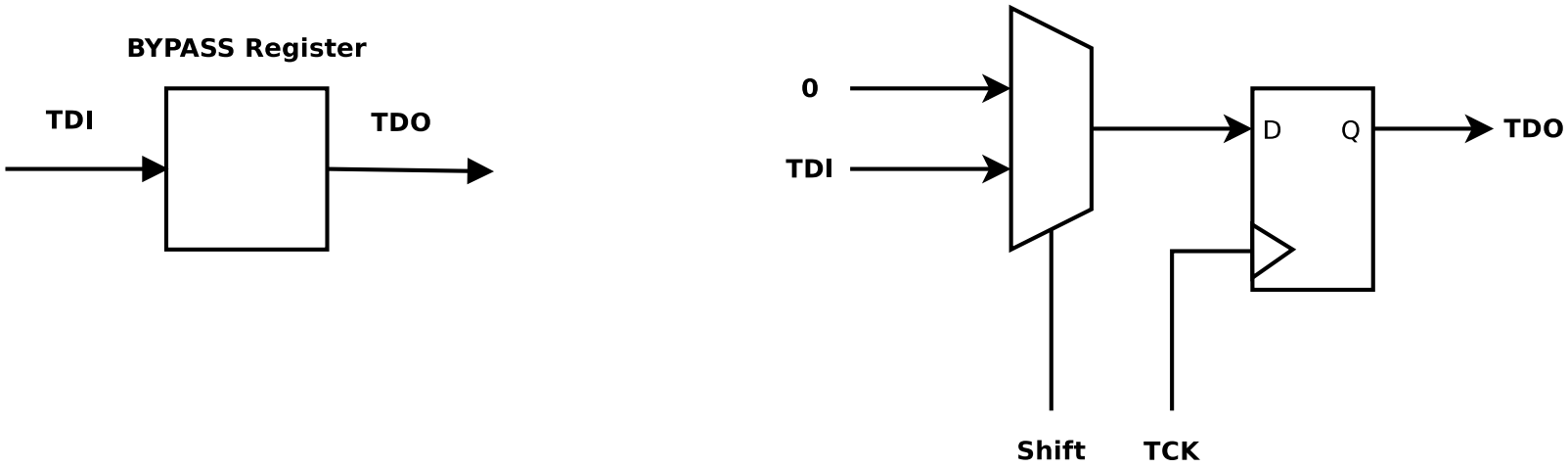


Figure: BYPASS Register

BYPASS

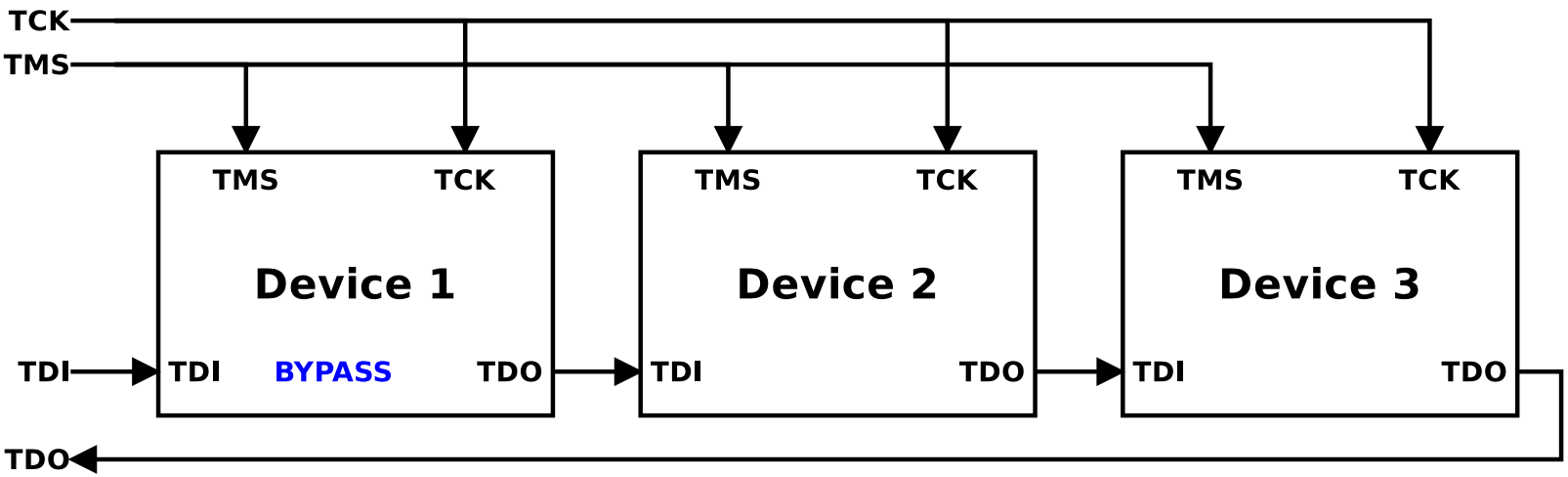


Figure: BYPASS and Daisy Chain (1/3)

BYPASS

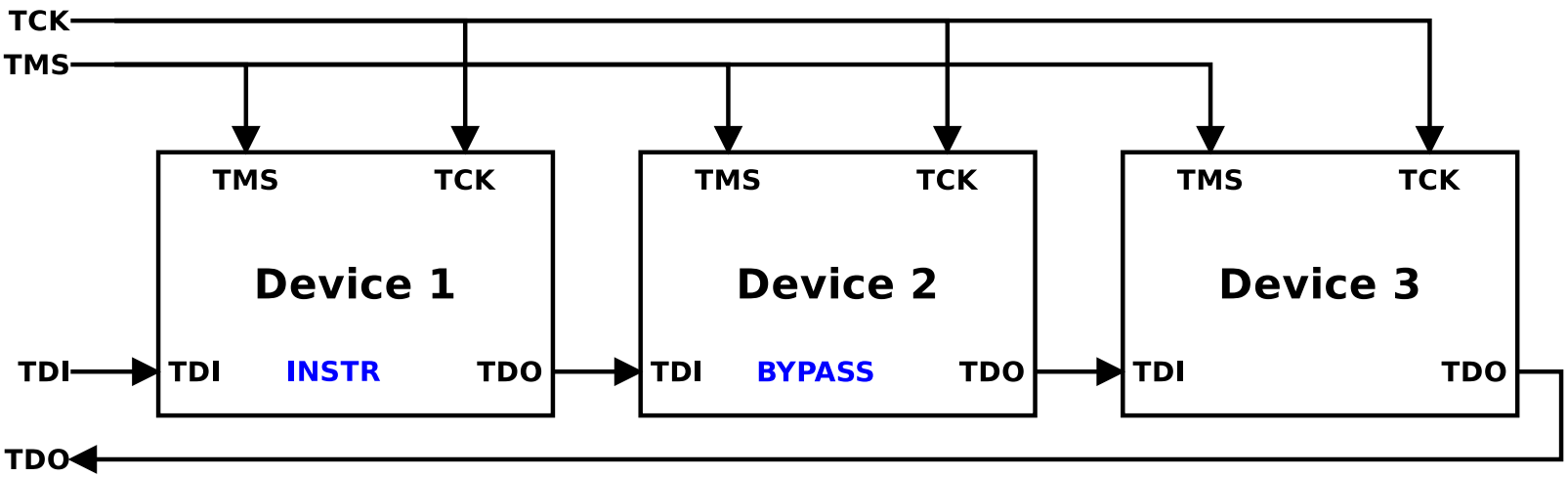


Figure: BYPASS and Daisy Chain (2/3)

BYPASS

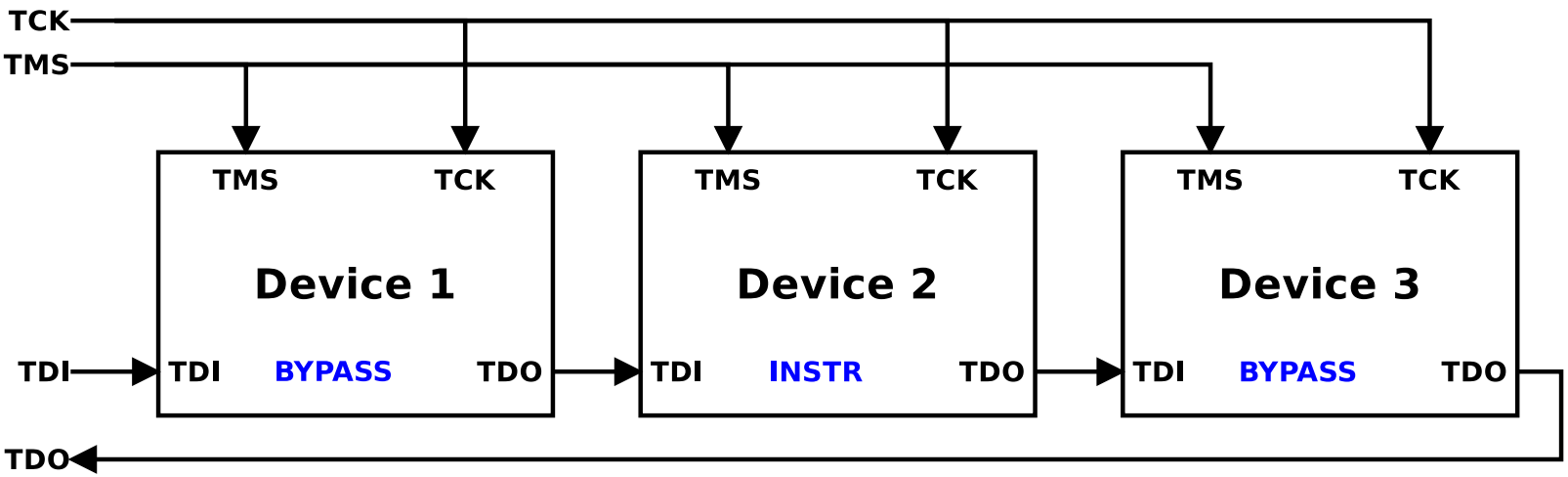


Figure: BYPASS and Daisy Chain (3/3)

Boundary Scan

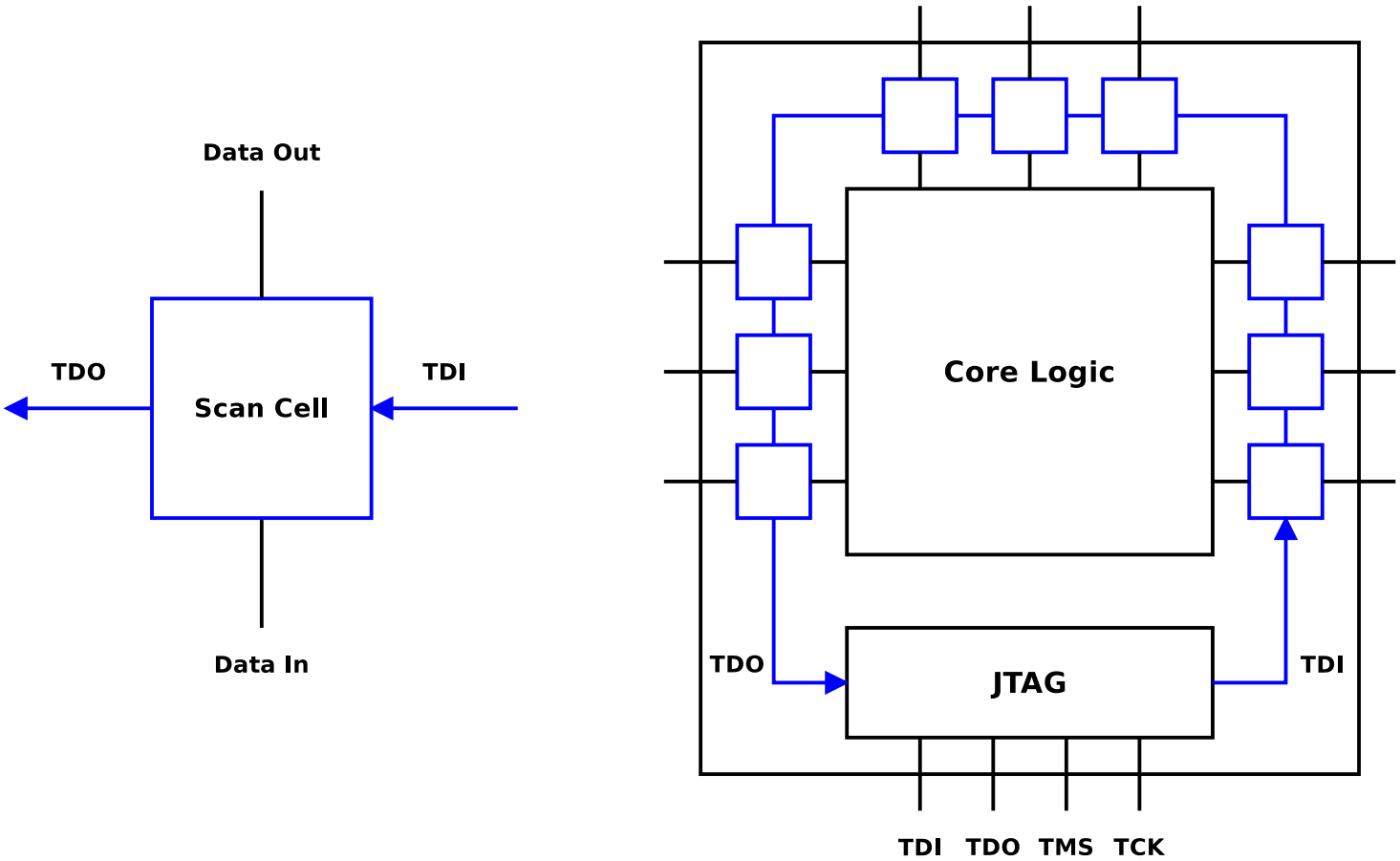


Figure: Boundary Scan

Boundary Scan Instructions

- EXTEST
- SAMPLE/PRELOAD
- INTEST

Boundary Scan

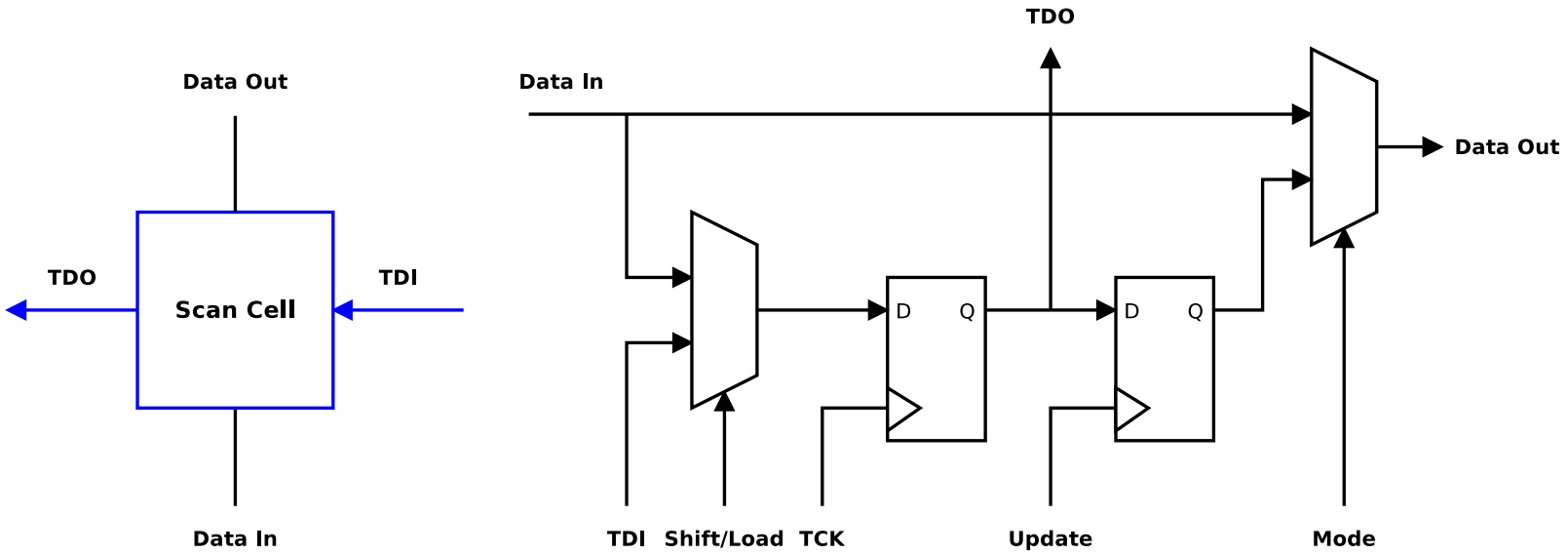


Figure: Scan Cell

Boundary Scan Description Language

- Describes boundary scan layout for a specific integrated circuit
- VHDL subset
- Provided by manufacturer

UC3 JTAG Overview

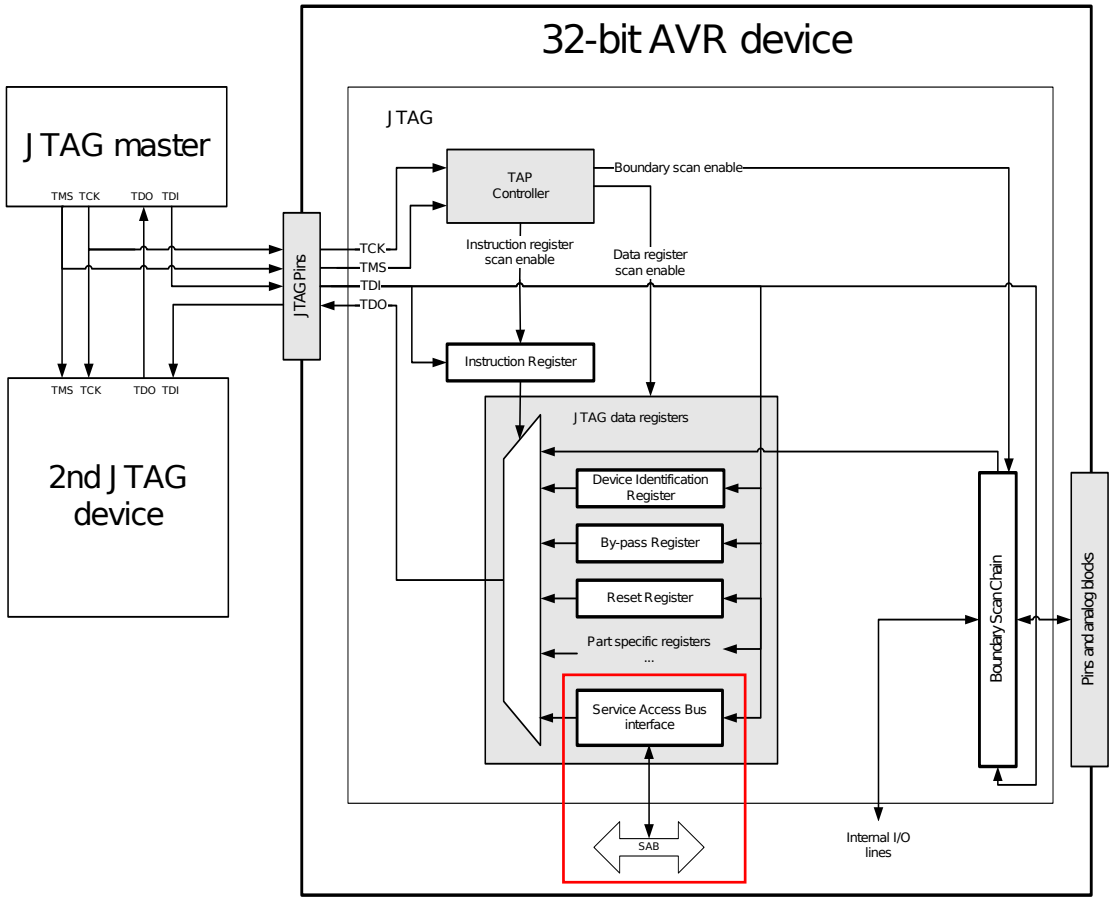


Figure: UC3 JTAG Overview

UC3 On-Chip Debug Overview

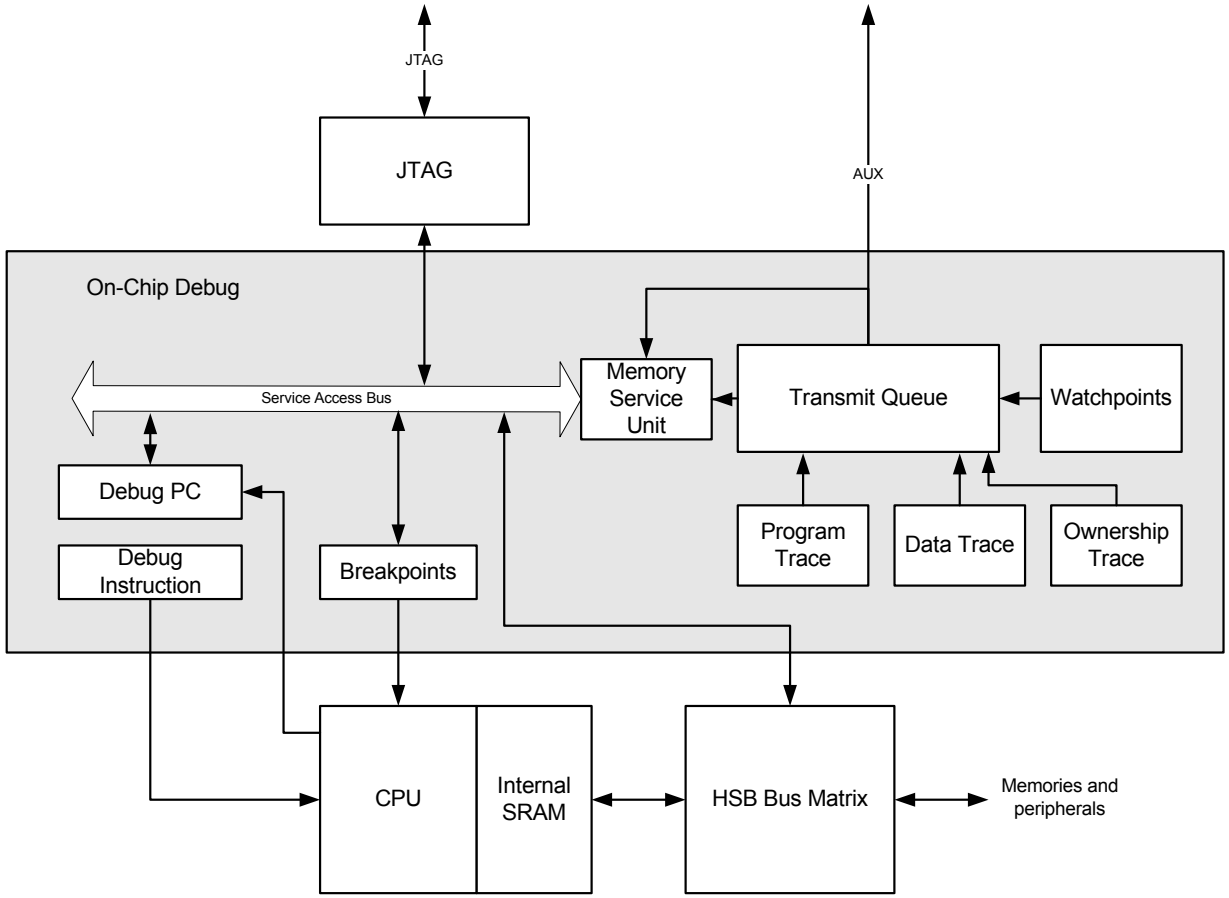


Figure: UC3 On-Chip Debug Overview

SAB Slaves

Slave	Address [35:32]	Description
Unallocated	0x0	Intentionally unallocated
OCD	0x1	OCD registers
HSB	0x4	HSB memory space, as seen by the CPU
HSB	0x5	Alternative mapping for HSB space, for compatibility with other 32-bit AVR devices.
Memory Service Unit	0x6	Memory Service Unit registers
Reserved	Other	Unused

Figure: SAB Slaves

- **HSB**: High Speed Bus

Finding Pinout

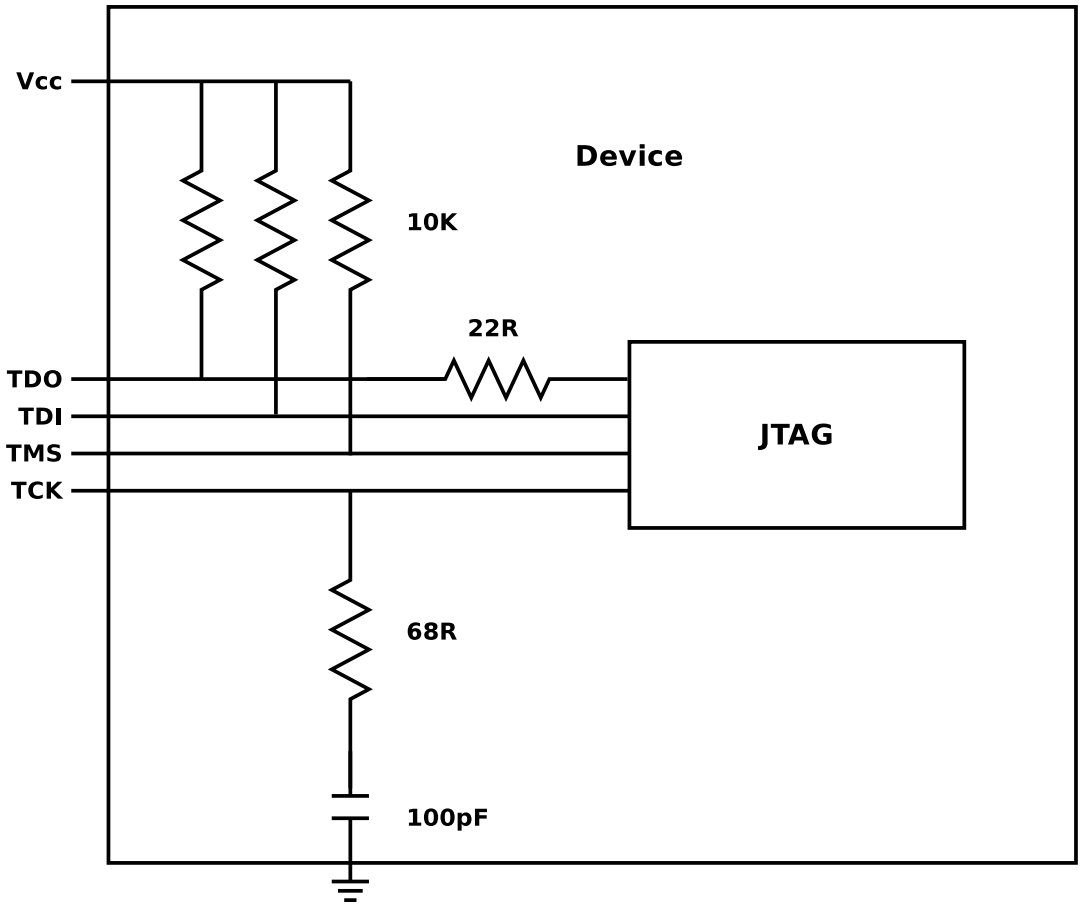
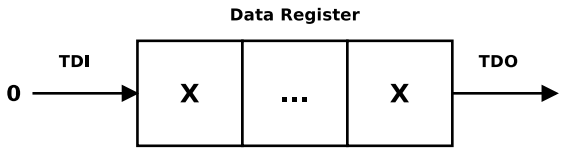


Figure: Pullup Resistors

Data register length scanning



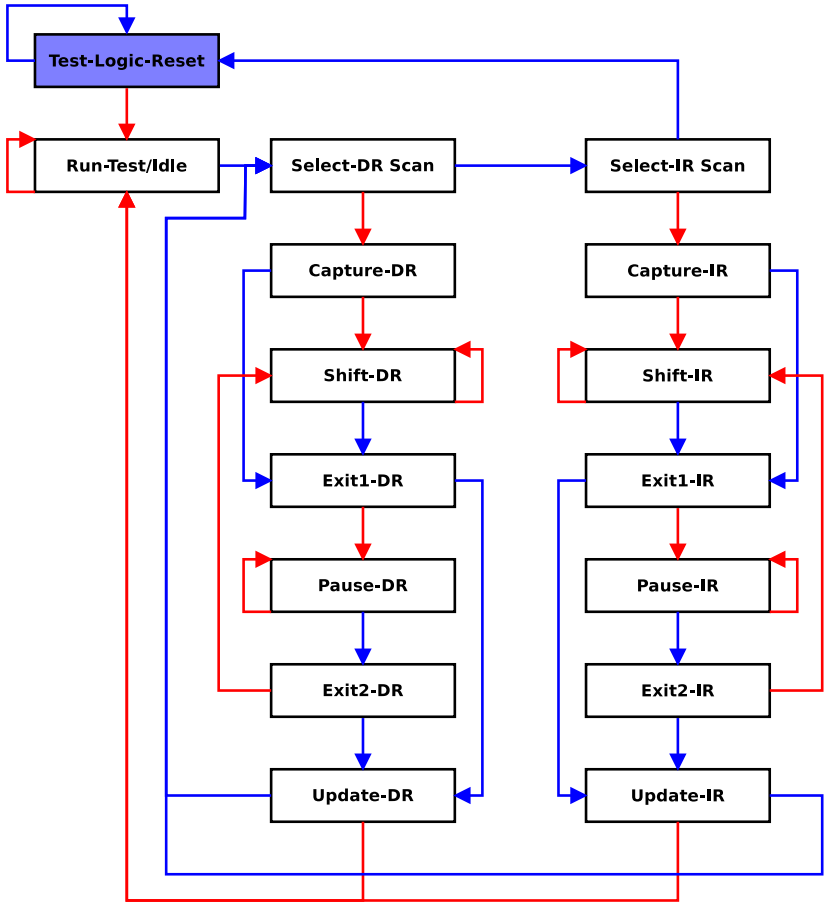
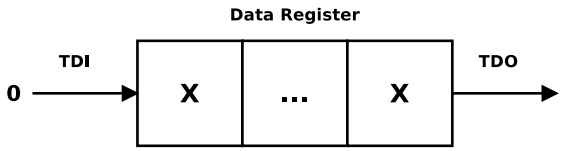


Figure: Data register length scanning (1/25)

Data register length scanning



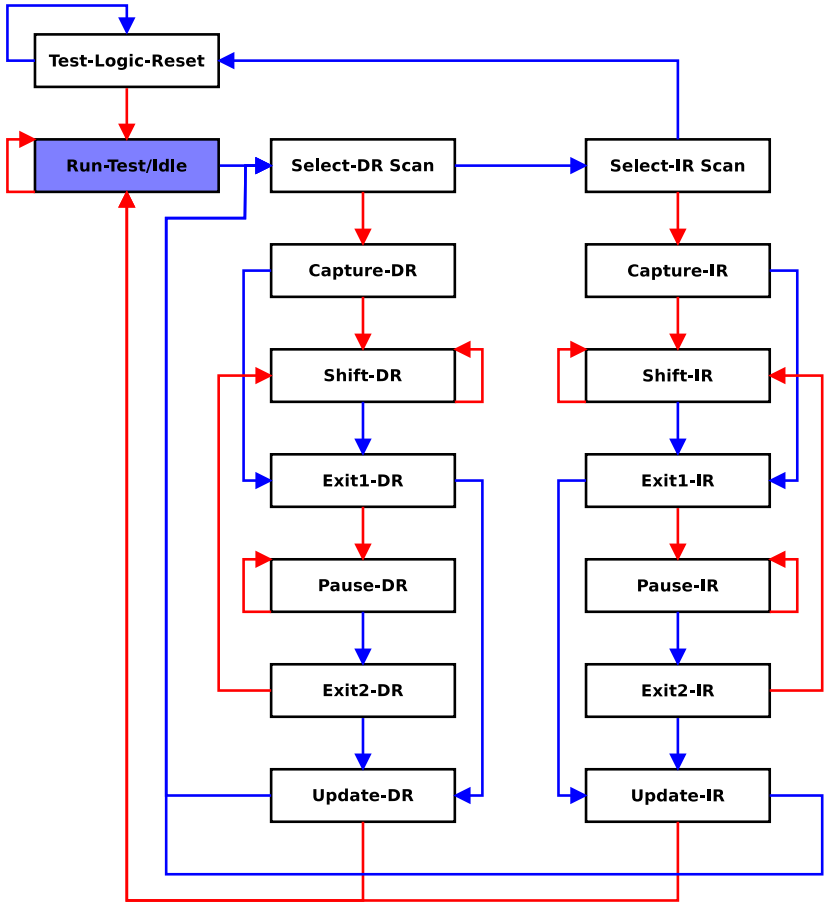
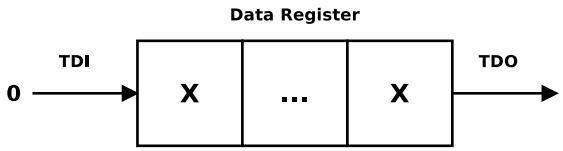


Figure: Data register length scanning (2/25)

Data register length scanning



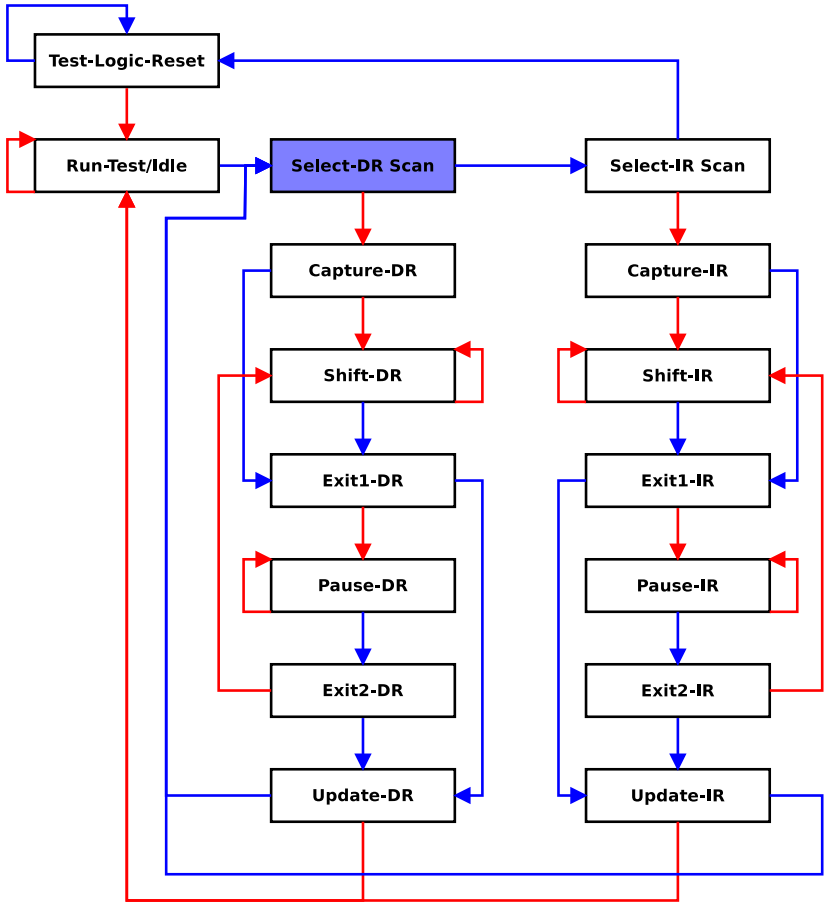
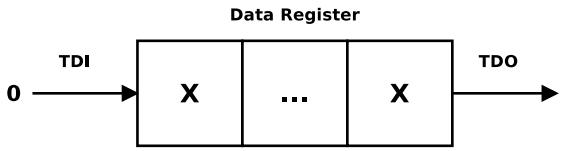


Figure: Data register length scanning (3/25)

Data register length scanning



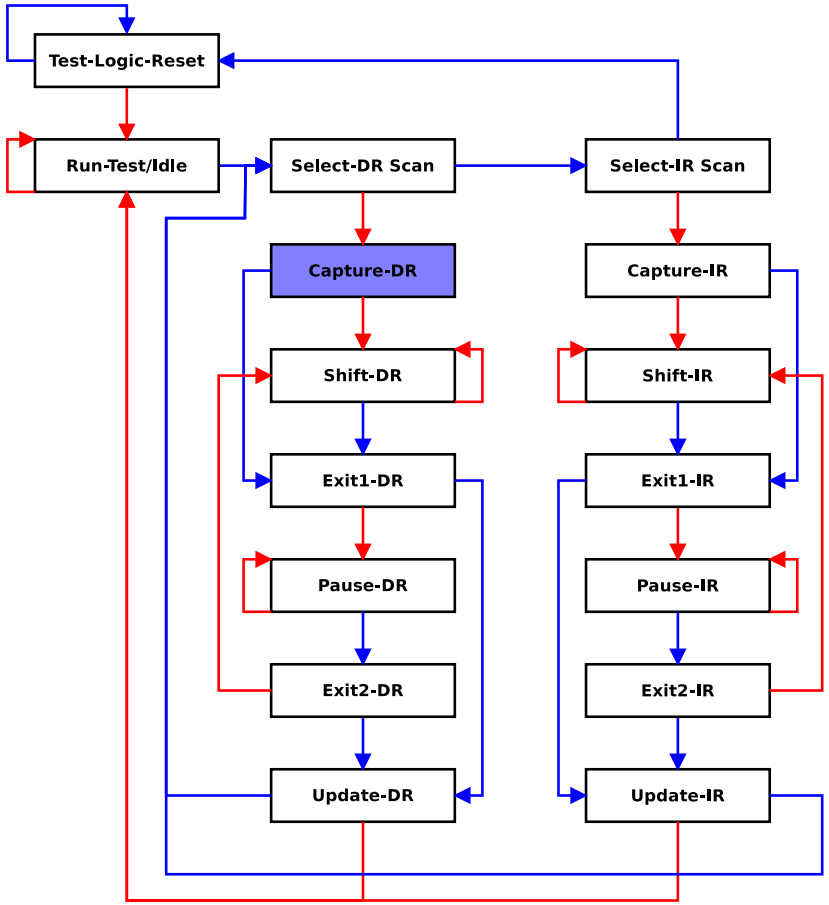
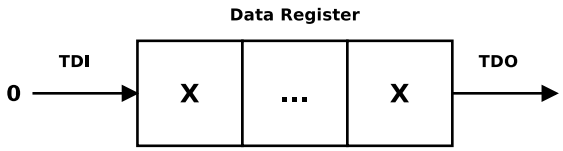


Figure: Data register length scanning (4/25)

Data register length scanning



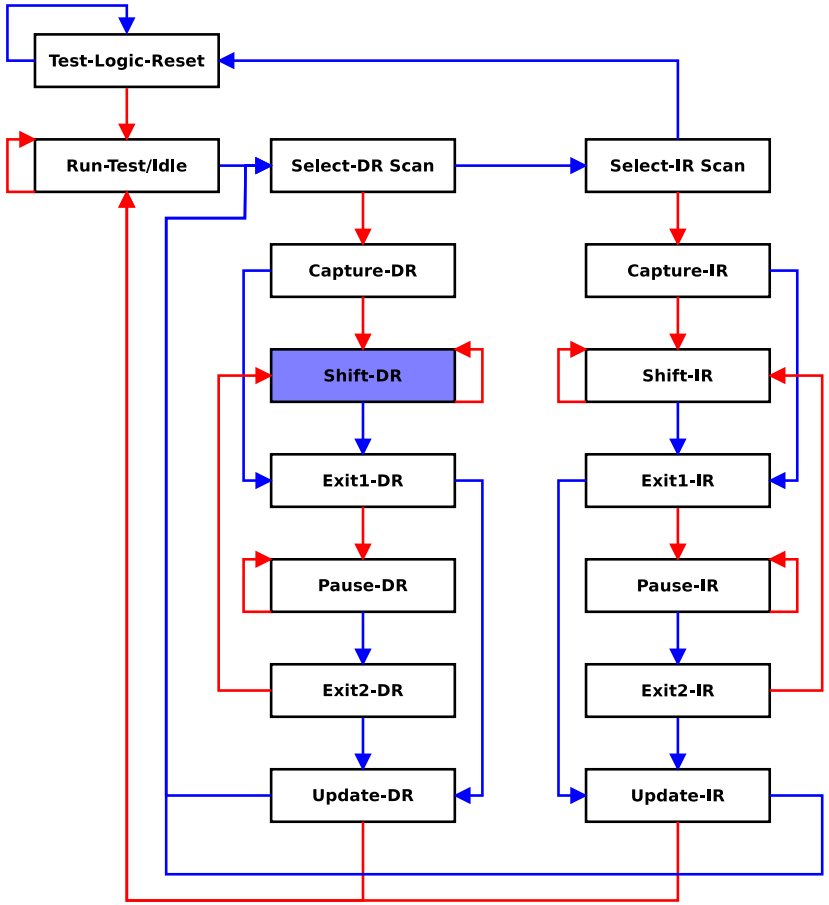
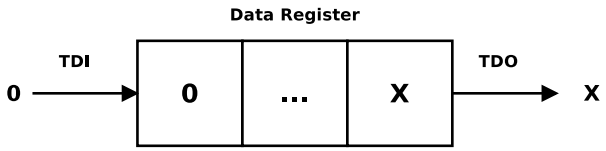


Figure: Data register length scanning (5/25)

Data register length scanning



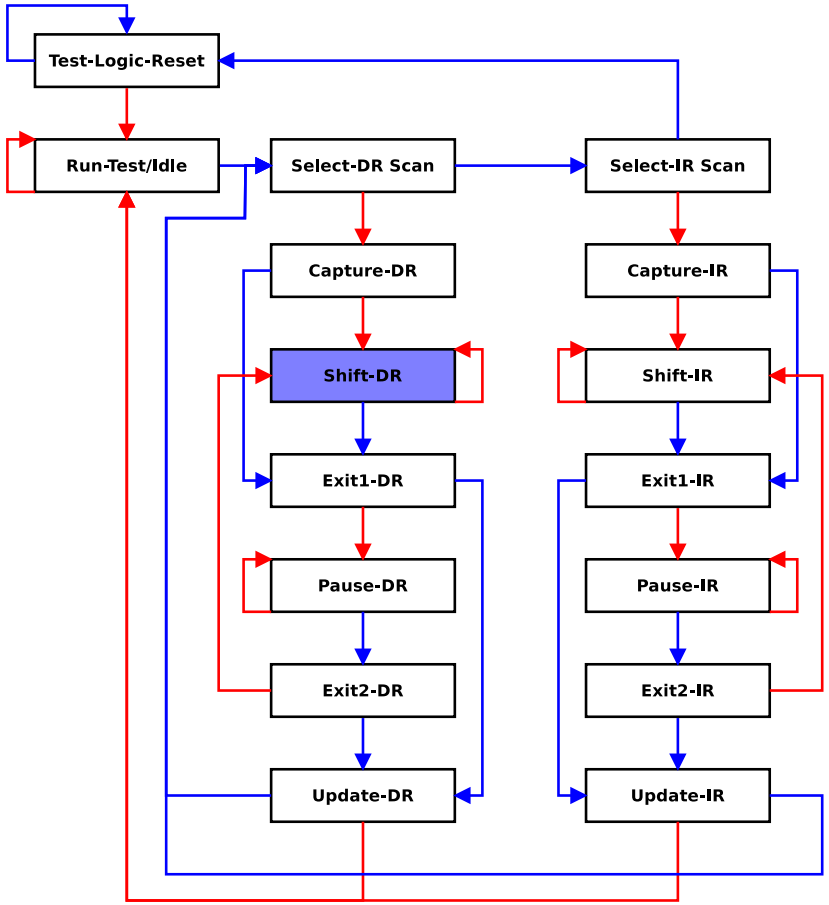
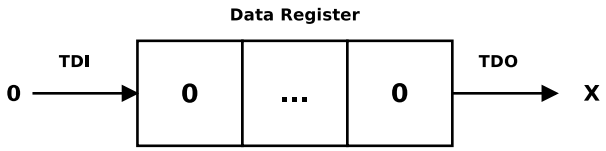


Figure: Data register length scanning (6/25)

Data register length scanning



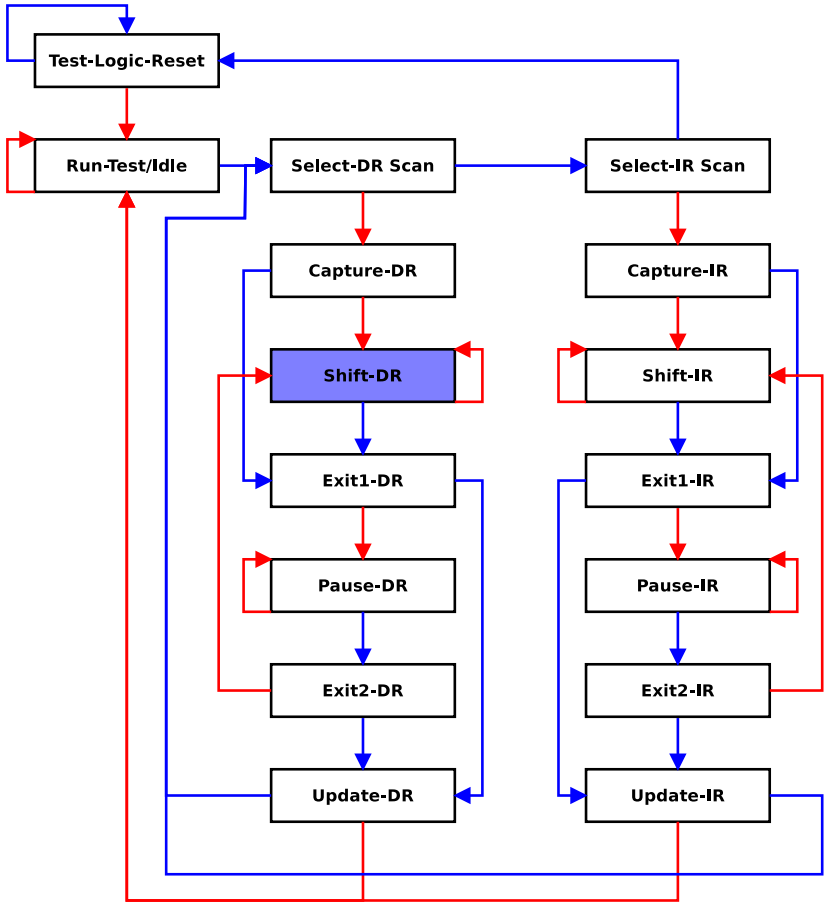
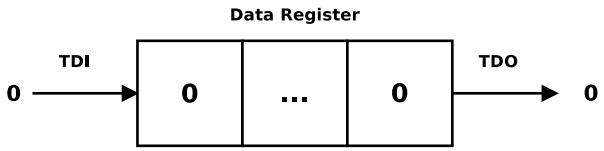


Figure: Data register length scanning (7/25)

Data register length scanning



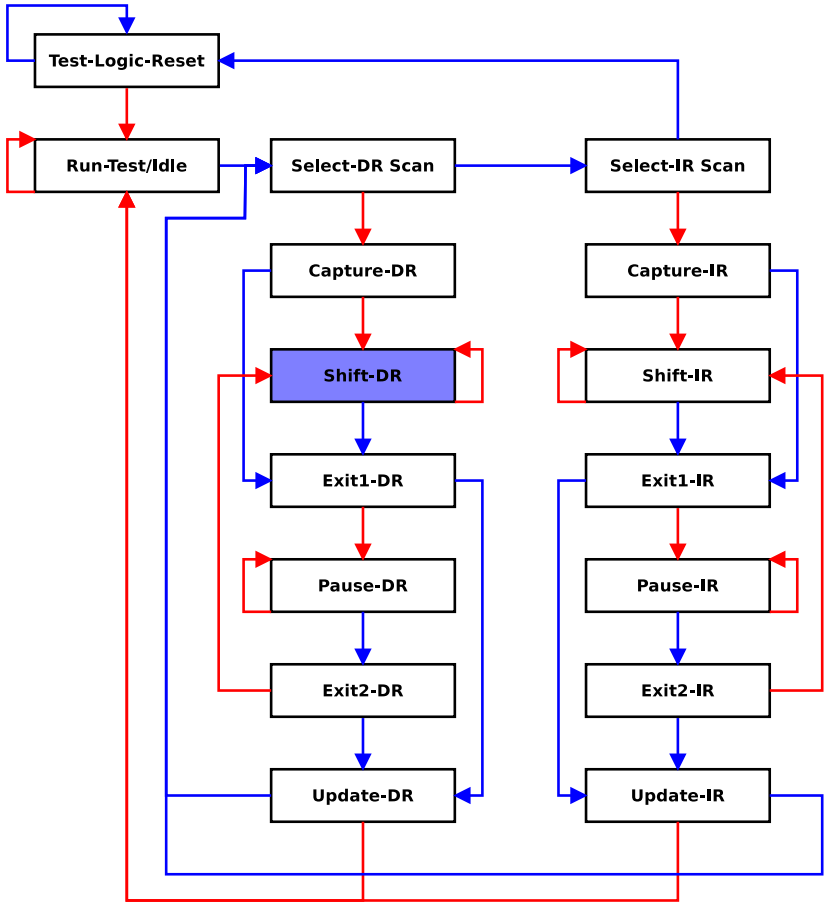
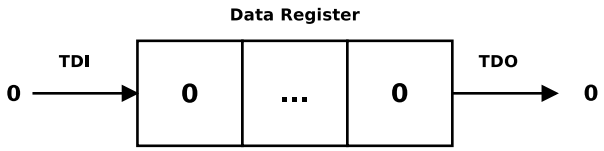


Figure: Data register length scanning (8/25)

Data register length scanning



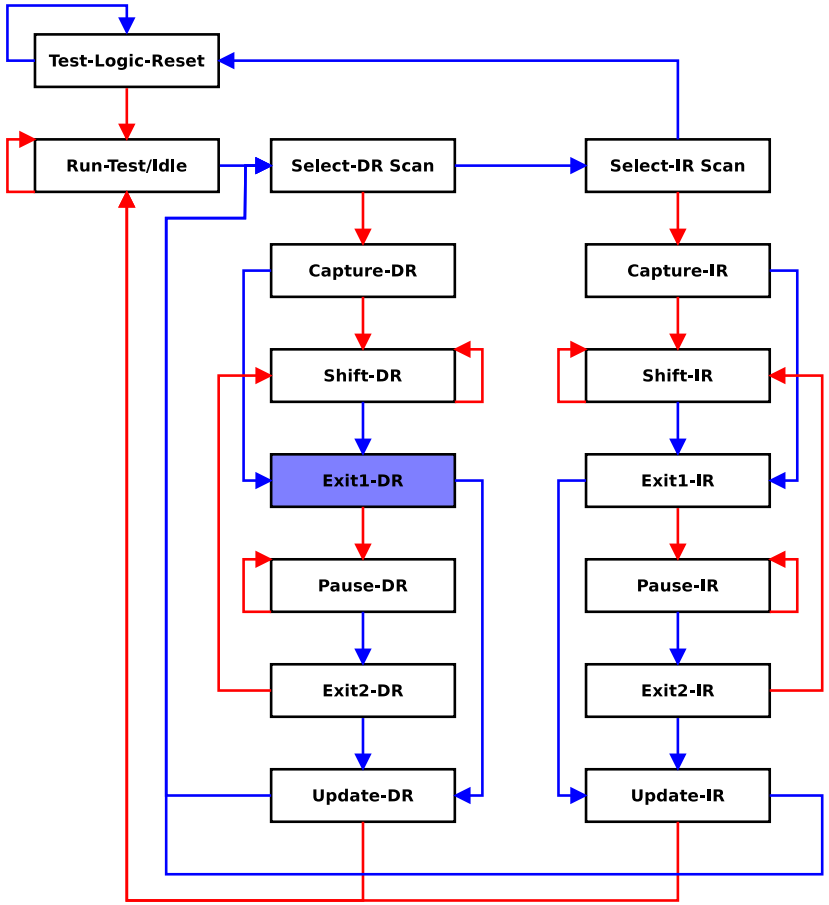
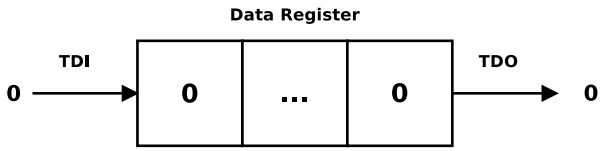


Figure: Data register length scanning (9/25)

Data register length scanning



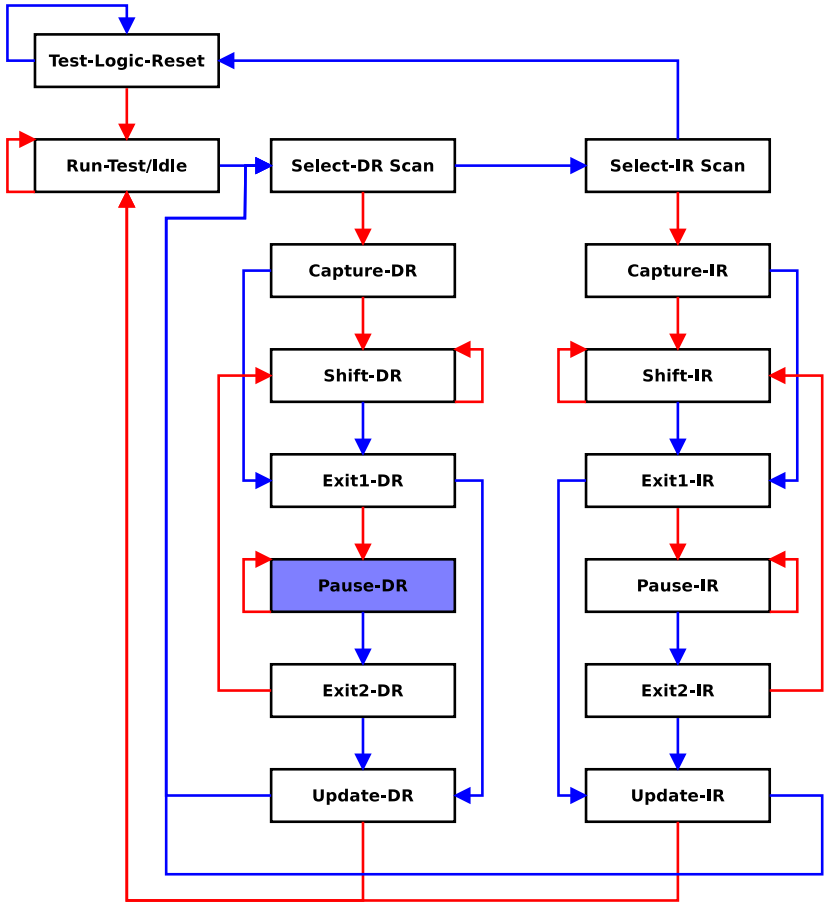
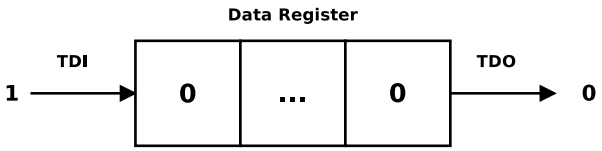


Figure: Data register length scanning (10/25)

Data register length scanning



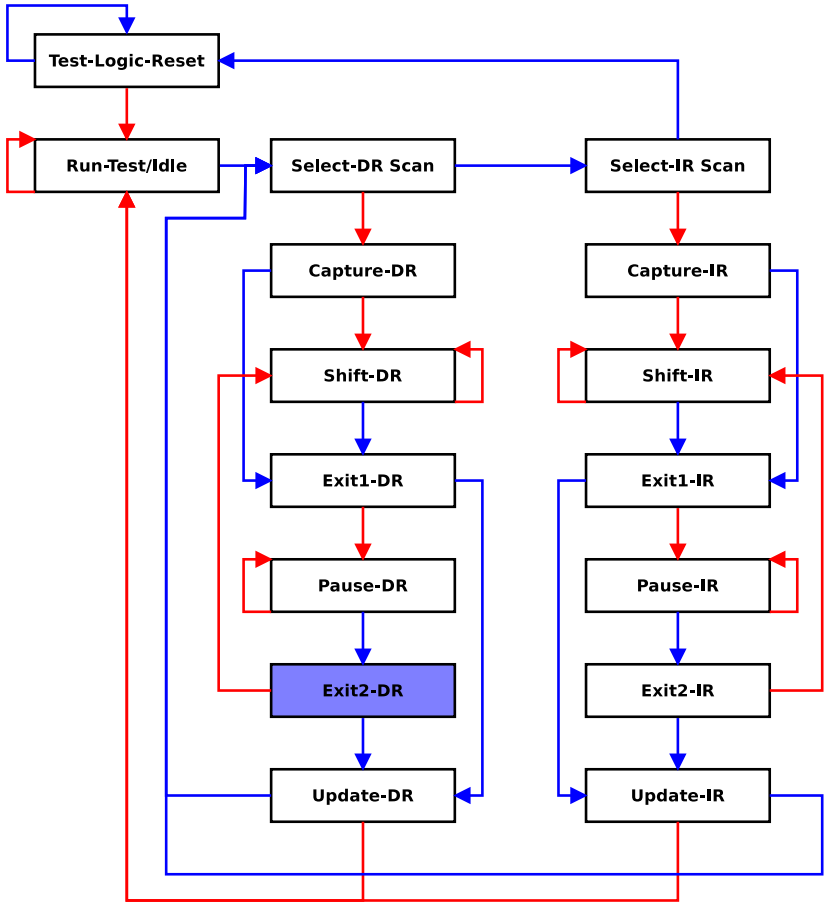
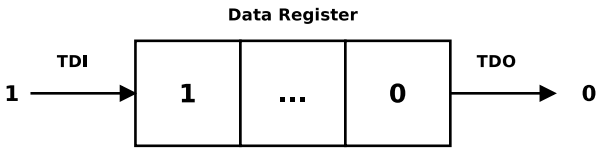


Figure: Data register length scanning (11/25)

Data register length scanning



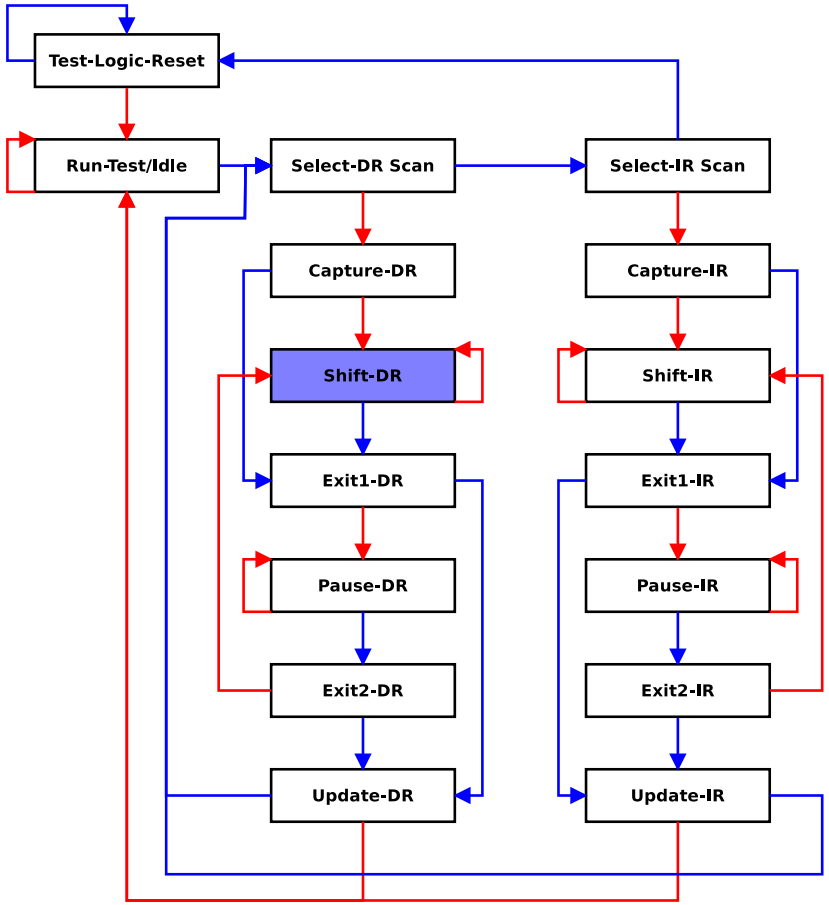
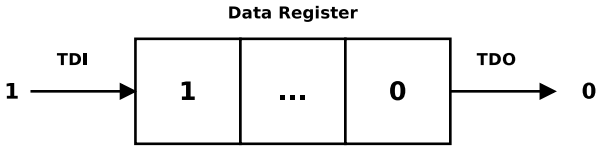


Figure: Data register length scanning (12/25)

Data register length scanning



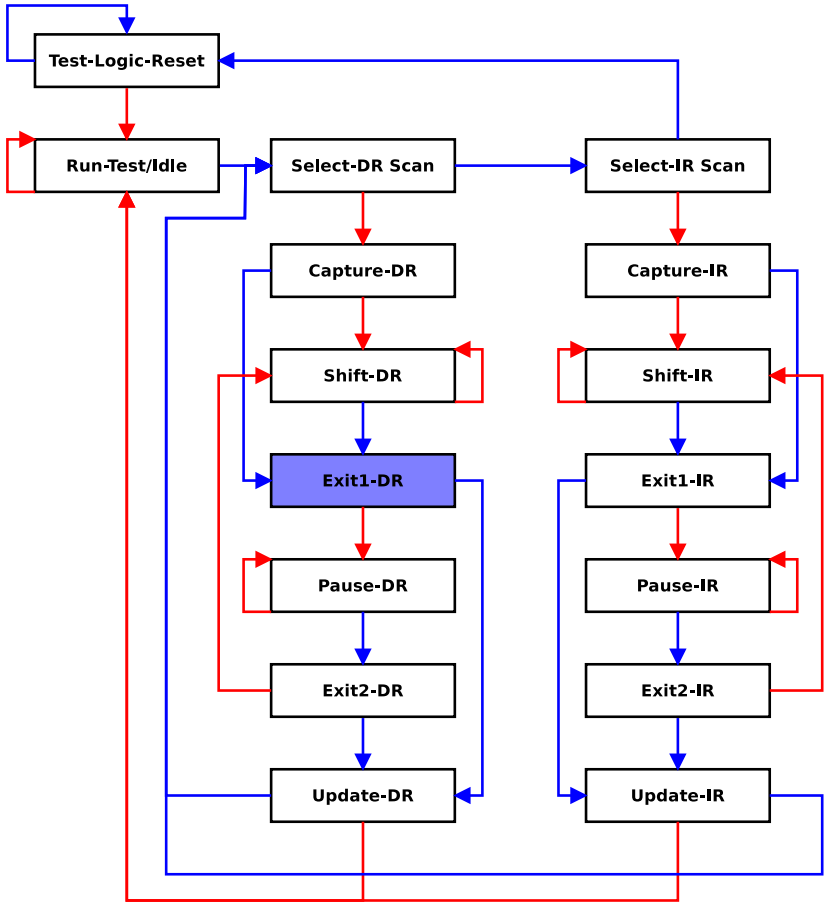
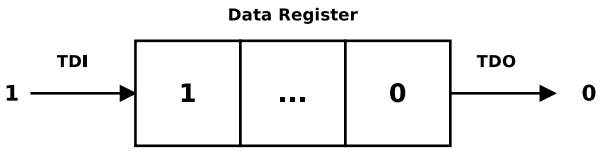


Figure: Data register length scanning (13/25)

Data register length scanning



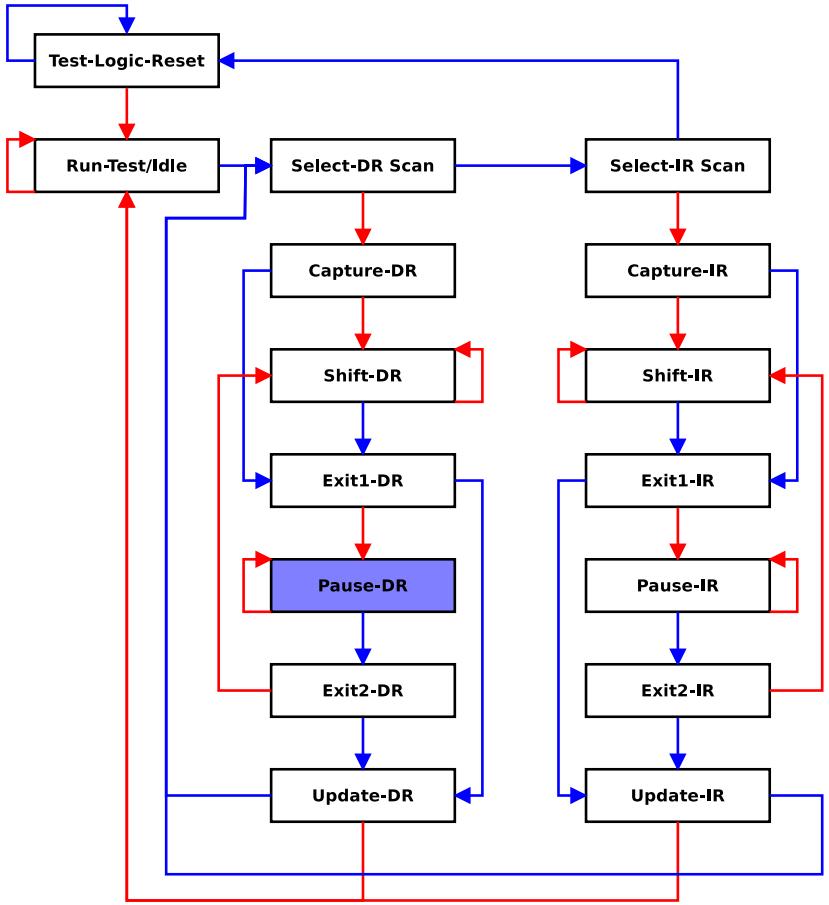
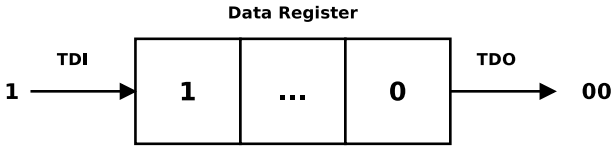


Figure: Data register length scanning (14/25)

Data register length scanning



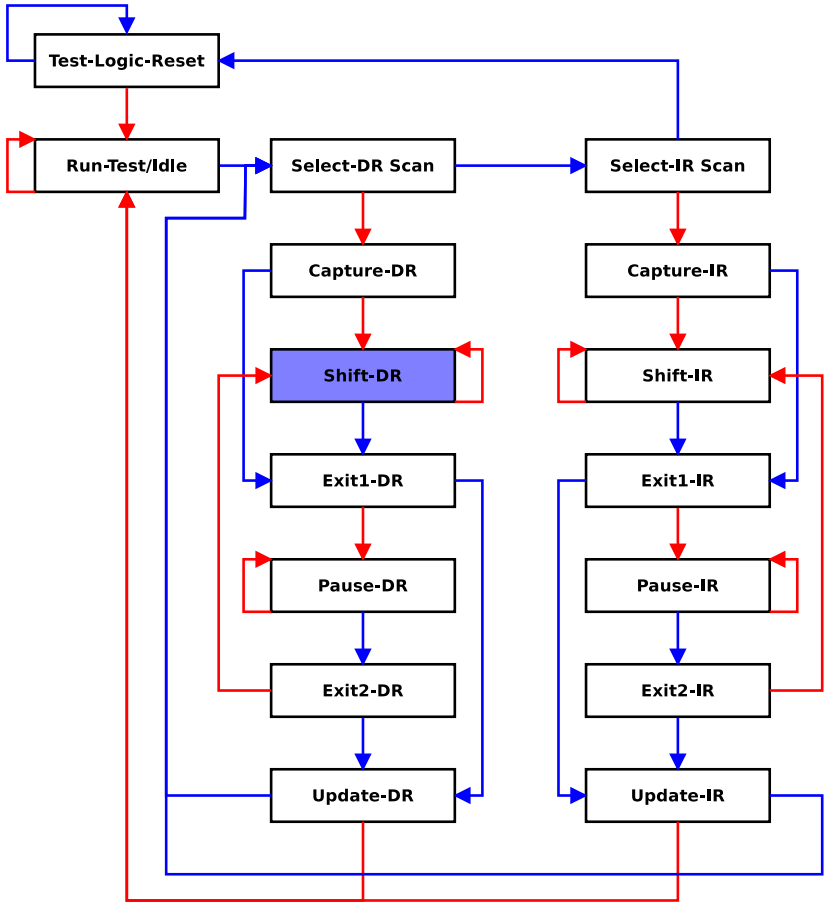
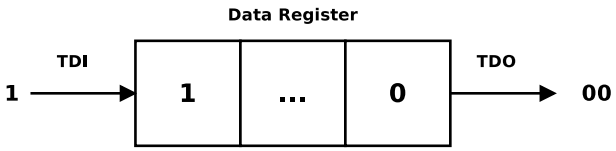


Figure: Data register length scanning (15/25)

Data register length scanning



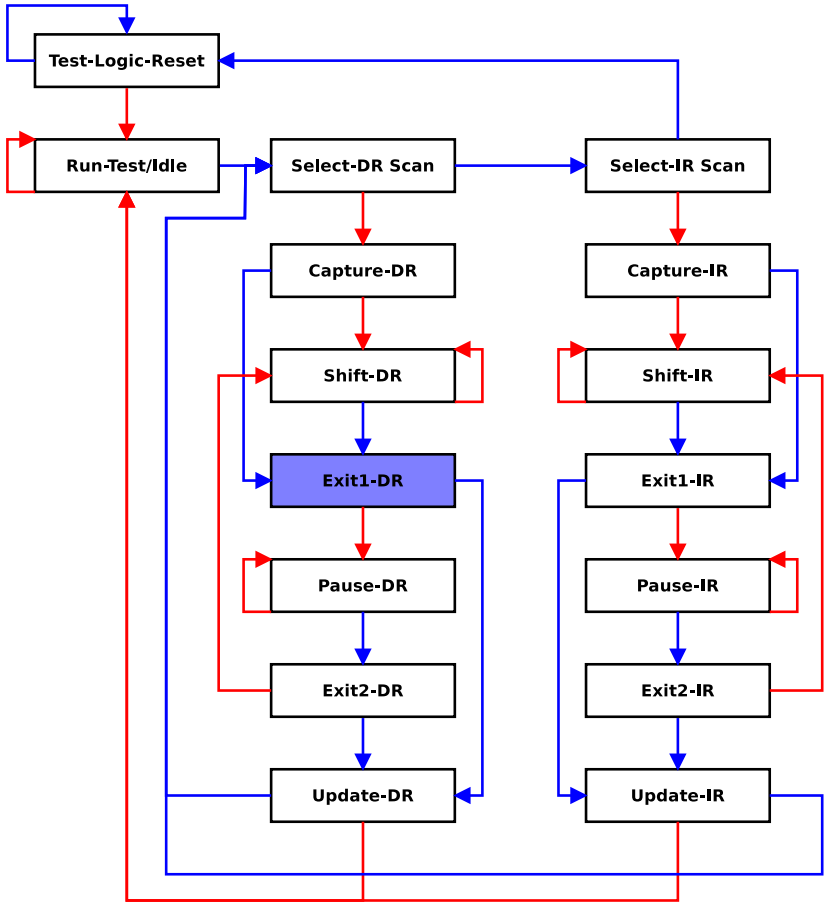
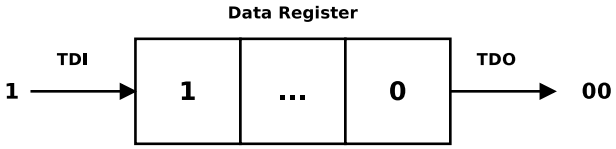


Figure: Data register length scanning (16/25)

Data register length scanning



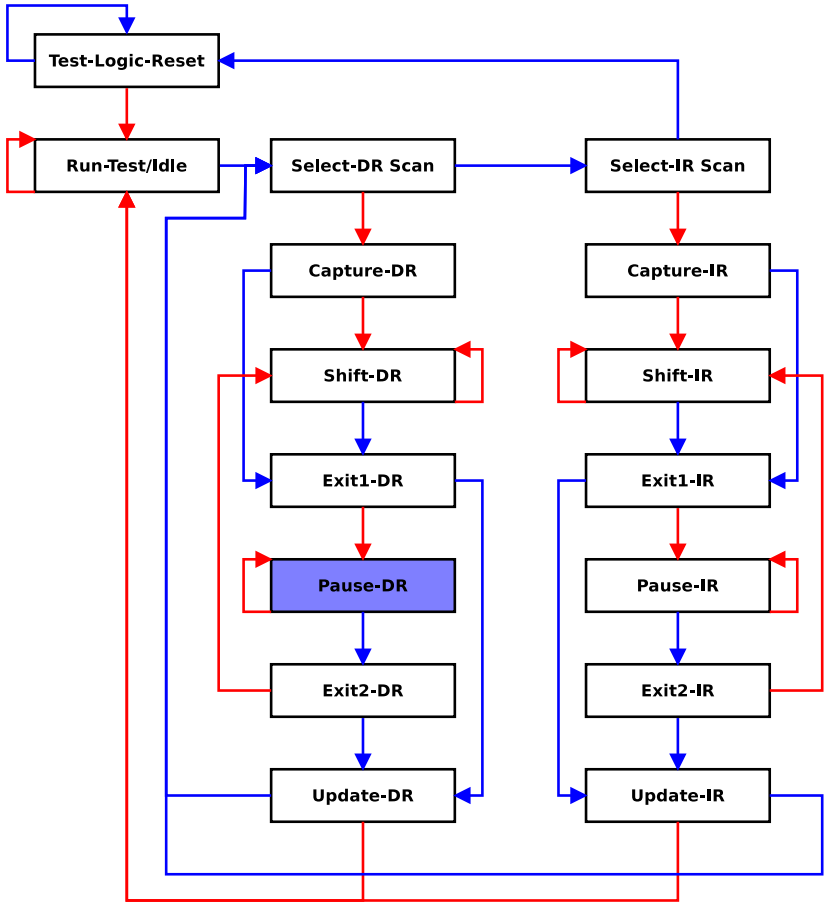
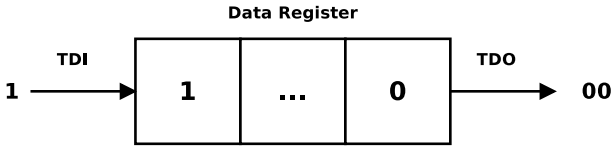


Figure: Data register length scanning (17/25)

Data register length scanning



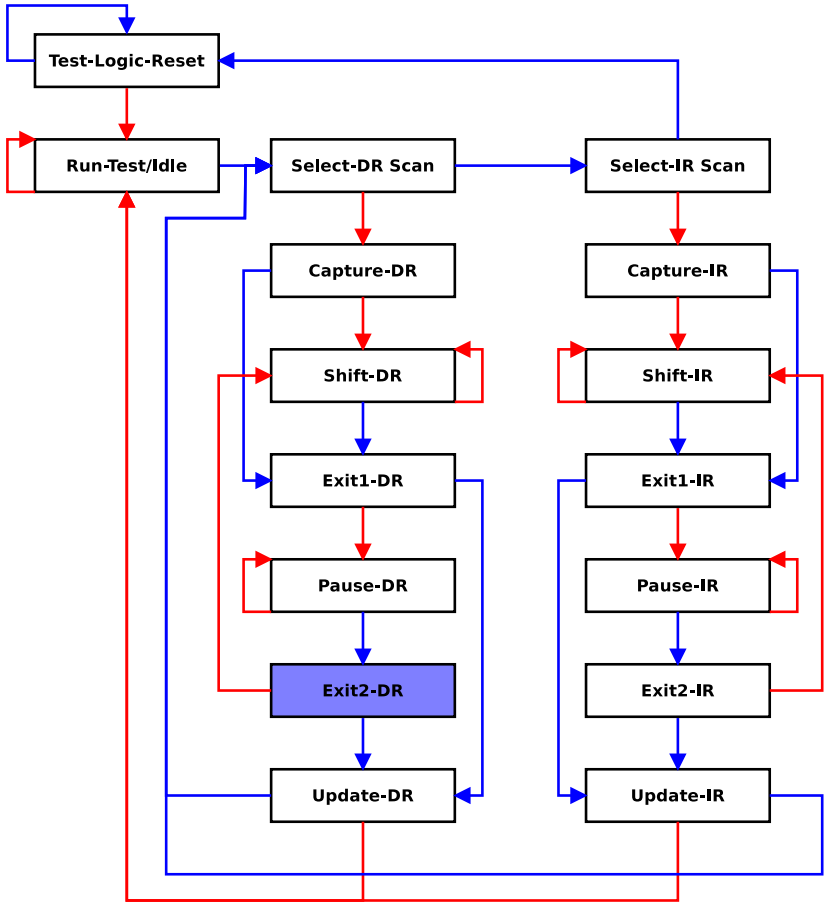
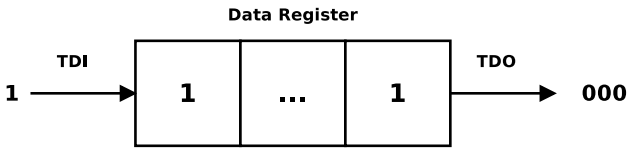


Figure: Data register length scanning (18/25)

Data register length scanning



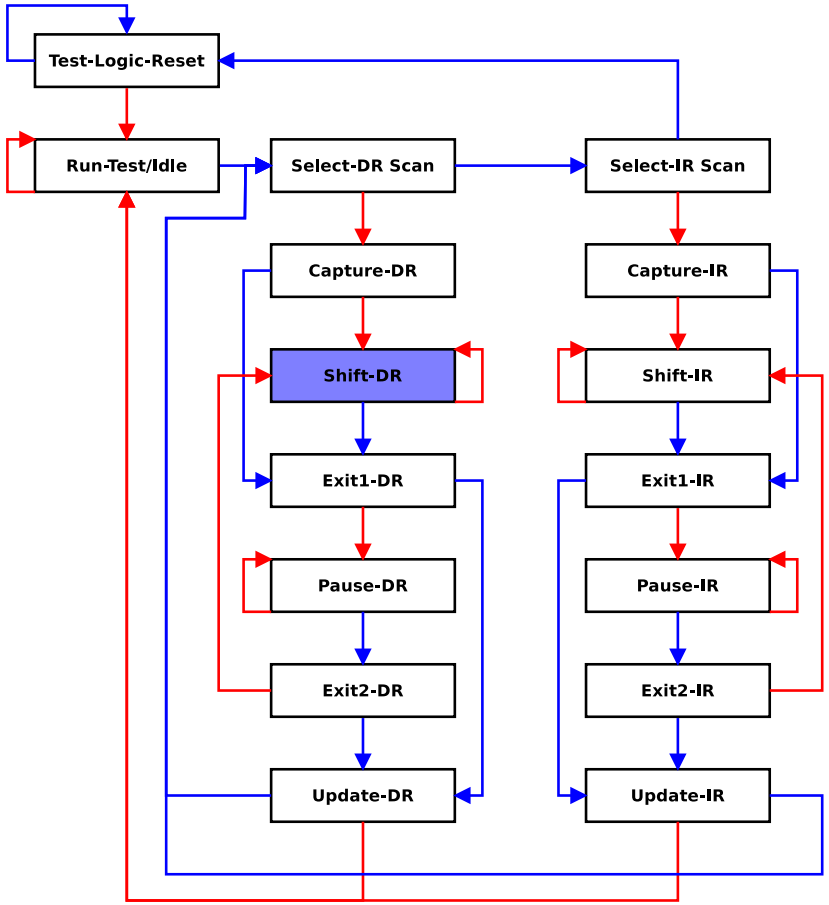
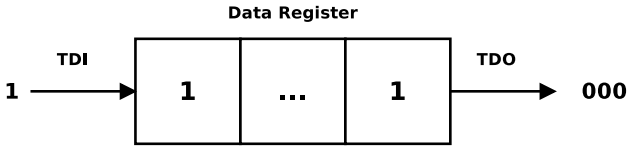


Figure: Data register length scanning (19/25)

Data register length scanning



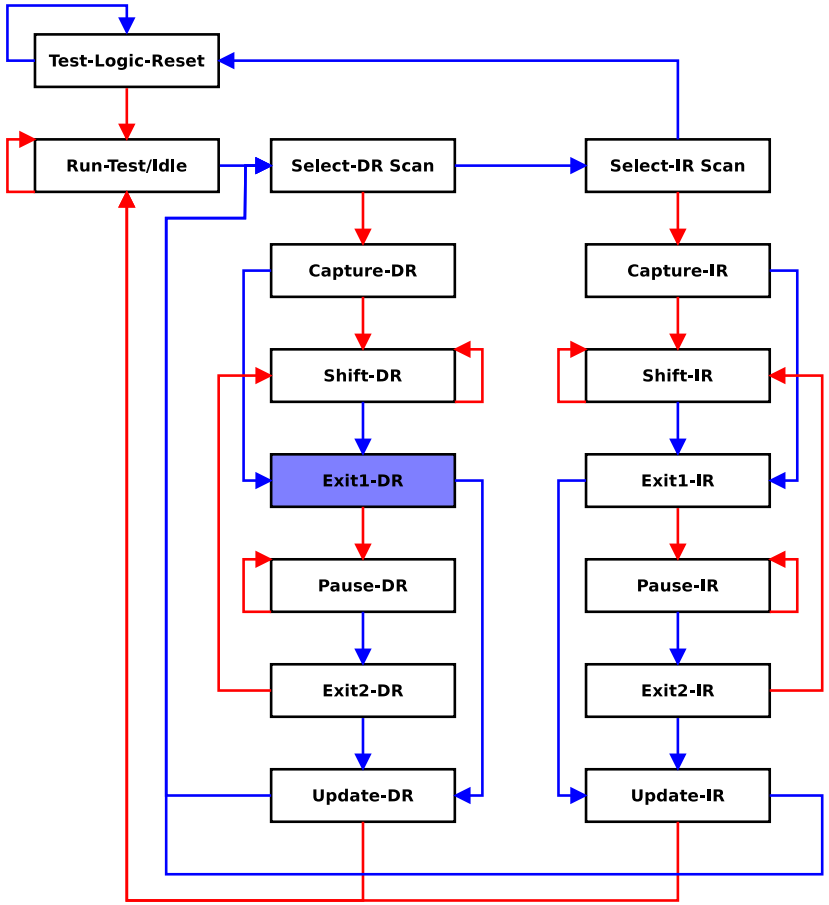
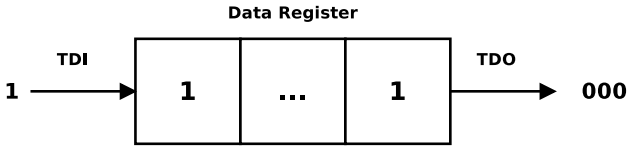


Figure: Data register length scanning (20/25)

Data register length scanning



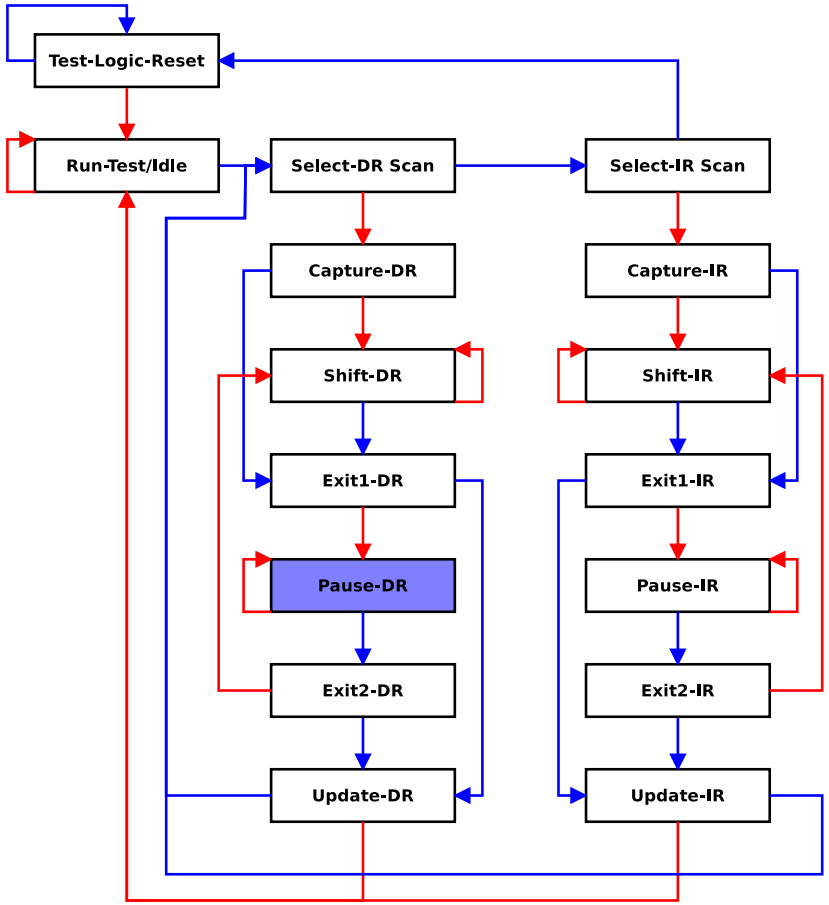
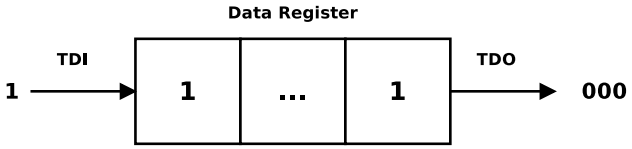


Figure: Data register length scanning (21/25)

Data register length scanning



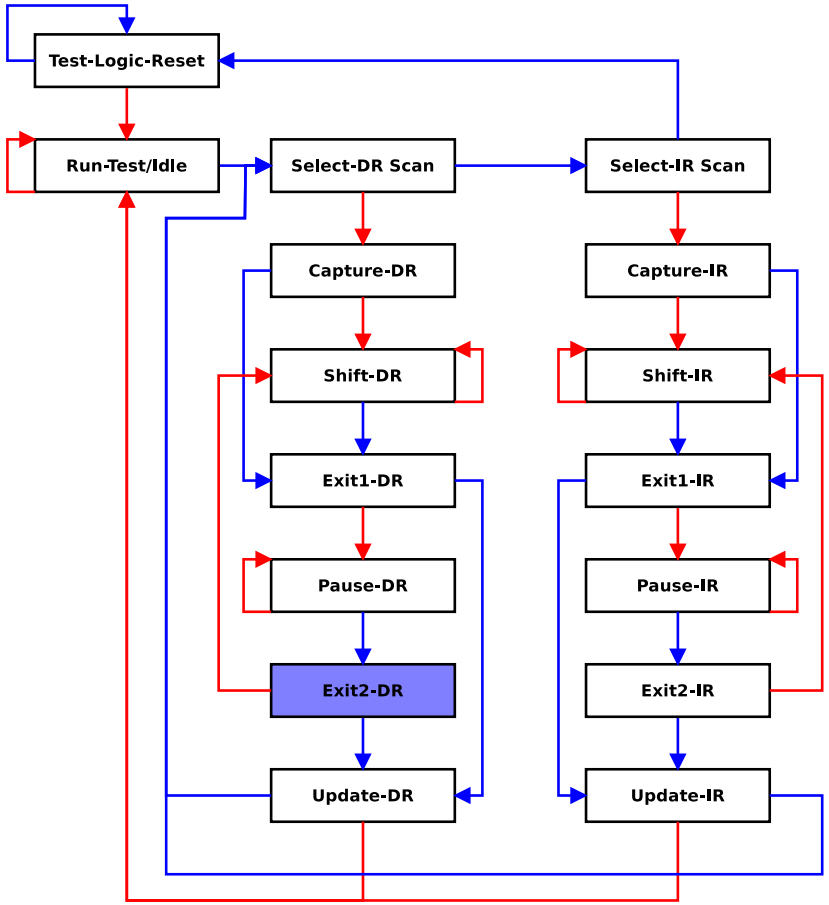
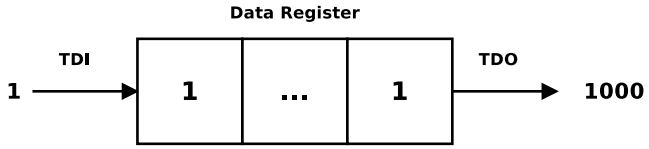


Figure: Data register length scanning (22/25)

Data register length scanning



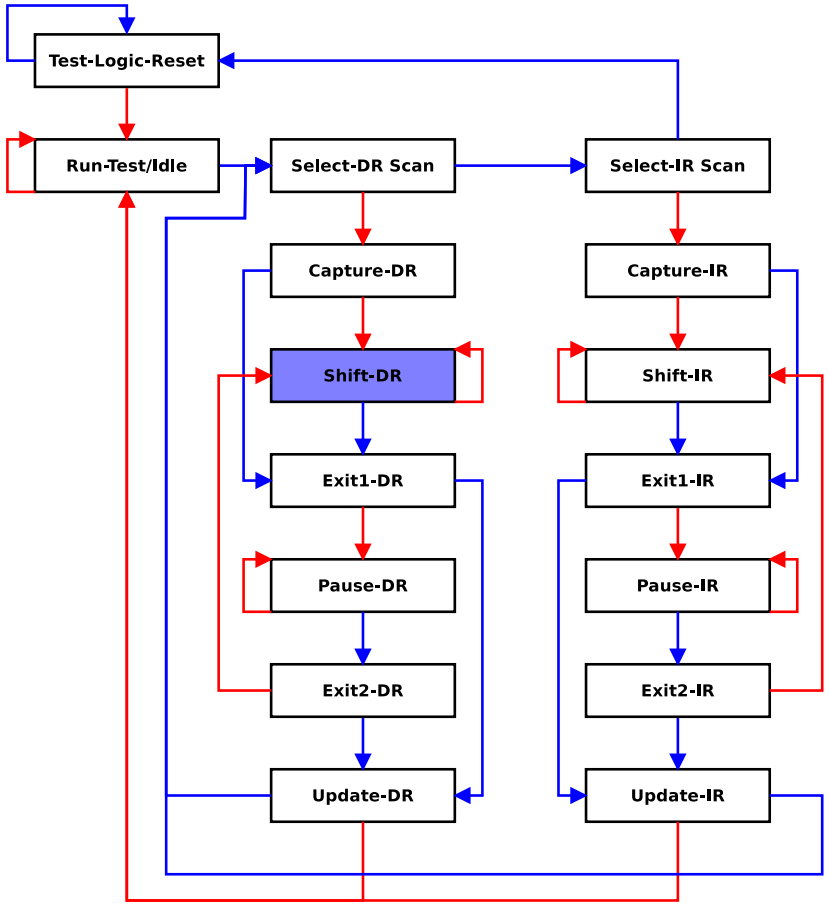


Figure: Data register length scanning (23/25)

Data register length scanning

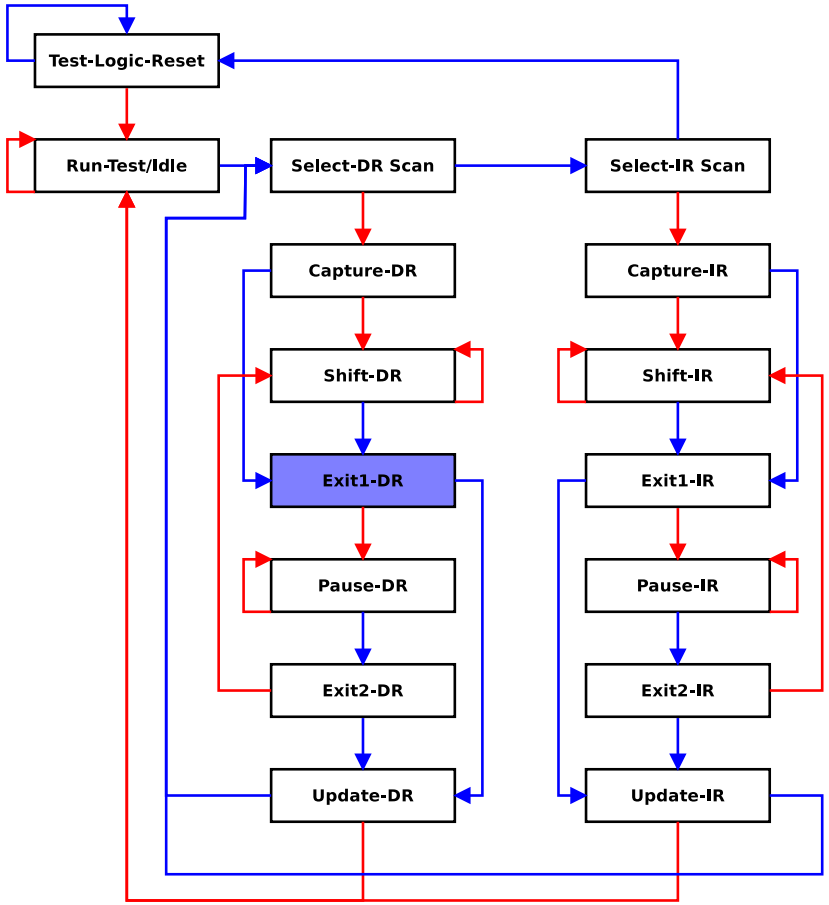


Figure: Data register length scanning (24/25)

Data register length scanning

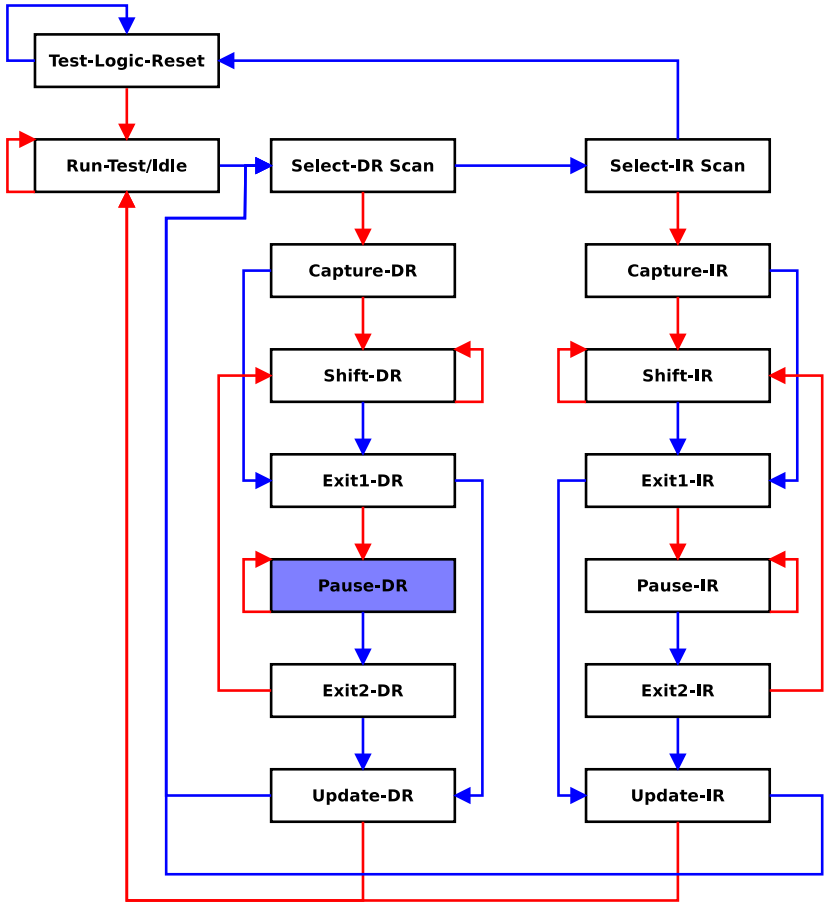


Figure: Data register length scanning (25/25)

Daisy Chain length scanning

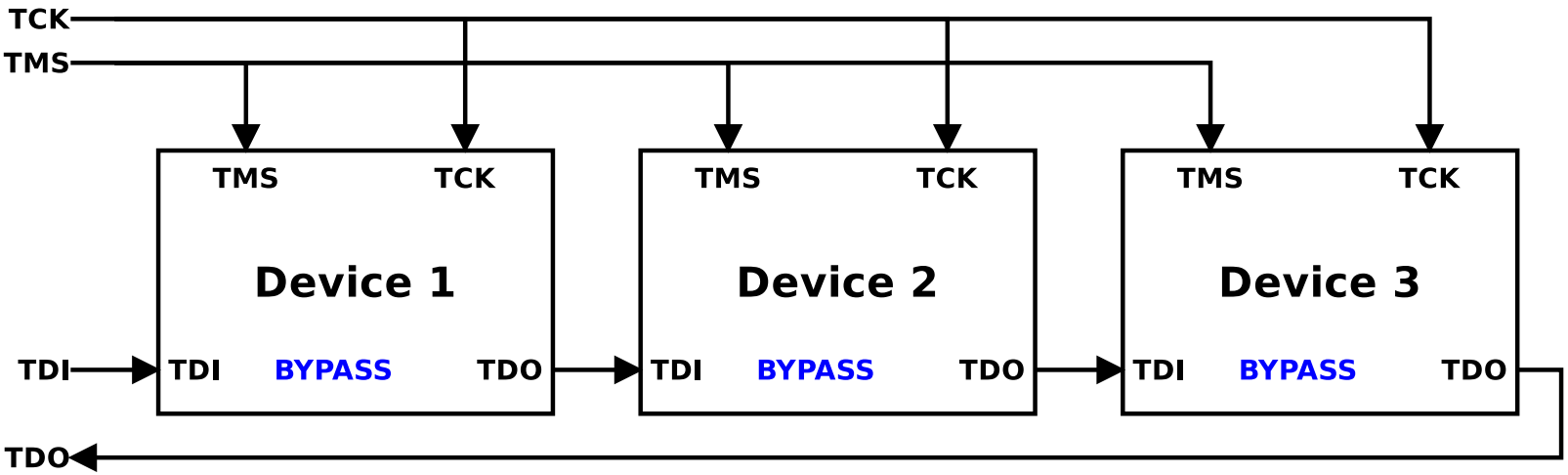


Figure: Daisy Chain length scanning

OpenOCD Low Level JTAG Commands


```
irscan auto0.tap 0x1
drscan auto0.tap 512 0 -endstate DRPAUSE

drscan auto0.tap 1 0 -enstate DRPAUSE
```

UC3 JTAG Analysis

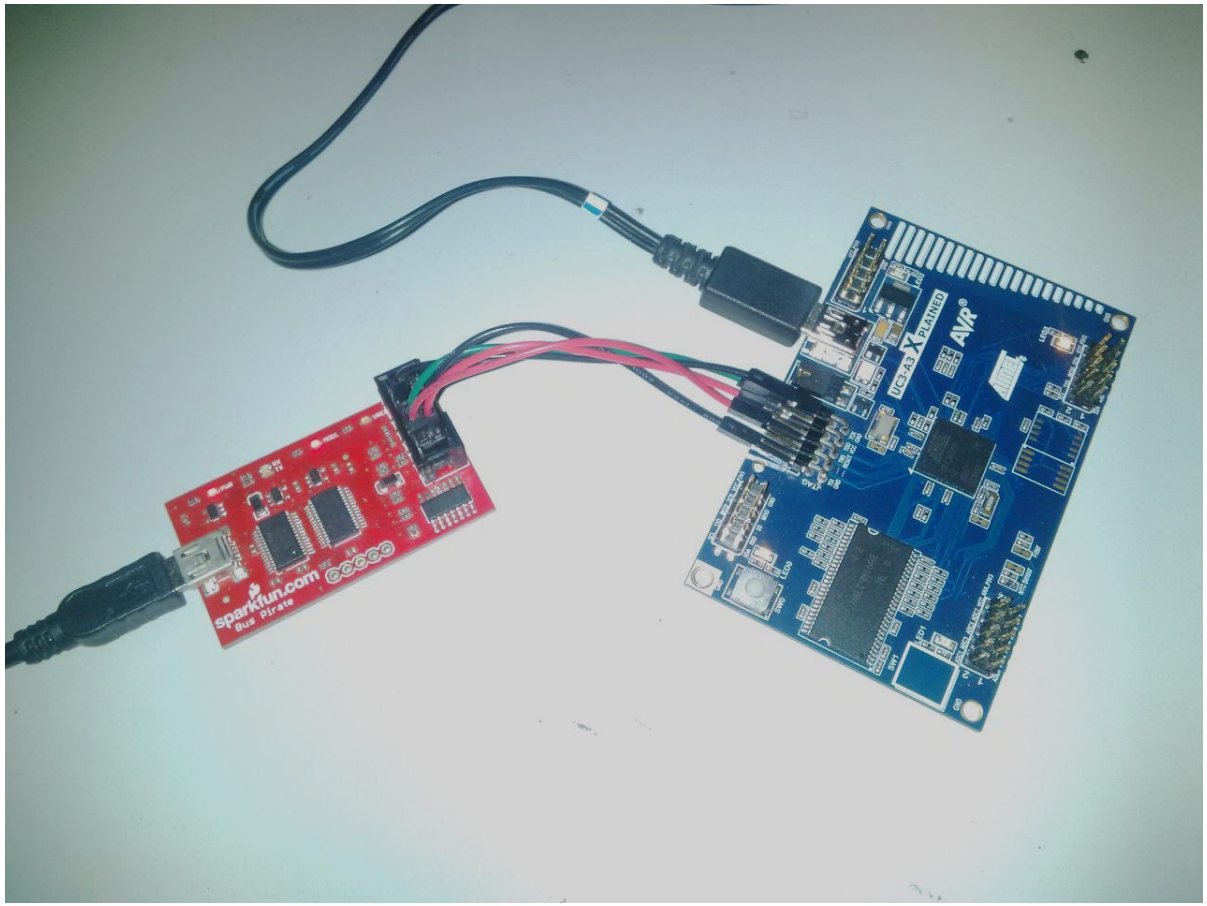


Figure: Bus Pirate as JTAG probe

UC3 JTAG Data Register Length

Opcode: Length

0x0: 1	0x8: 1	0x10: 34	0x18: 4
0x1: 32	0x9: 1	0x11: 35	0x19: 1
0x2: 224	0xa: 1	0x12: 34	0x1a: 1
0x3: 224	0xb: 1	0x13: 1	0x1b: 1
0x4: 224	0xc: 5	0x14: 34	0x1c: 1
0x5: 1	0xd: 1	0x15: 39	0x1d: 0
0x6: 1	0xe: 1	0x16: 1	0x1e: 1
0x7: 1	0xf: 1	0x17: 16	0x1f: 1

UC3 JTAG Data Register Length

Opcode: Length

0x0: 1	0x8: 1	0x10: 34	0x18: 4
0x1: 32	0x9: 1	0x11: 35	0x19: 1
0x2: 224	0xa: 1	0x12: 34	0x1a: 1
0x3: 224	0xb: 1	0x13: 1	0x1b: 1
0x4: 224	0xc: 5	0x14: 34	0x1c: 1
0x5: 1	0xd: 1	0x15: 39	0x1d: 0
0x6: 1	0xe: 1	0x16: 1	0x1e: 1
0x7: 1	0xf: 1	0x17: 16	0x1f: 1

- BYPASS, CLAMP, CHIP_ERASE
- IDCODE
- Boundary Scan
- AVR_RESET, SYNC
- Service Access Bus
- ???

Instruction 0x18

- Present in BSDL file but not in datasheet

```
attribute INSTRUCTION_OPCODE    of UC3A3256-BGA : entity is
"   PRIVATE0                    ( 10011 ), " &
"   PRIVATE1                    ( 01100 ), " &
"   BYPASS                      ( 11111 ), " &
"   CLAMP                       ( 00110 ), " &
"   EXTEST                      ( 00011 ), " &
"   IDCODE                      ( 00001 ), " &
"   INTEST                      ( 00100 ), " &
"   PRIVATE2                    ( 11001 ), " &
"   PRIVATE3                    ( 11010 ), " &
"   PRIVATE4                    ( 11011 ), " &
"   PRIVATE5                    ( 10001 ), " &
"   PRIVATE6                    ( 10010 ), " &
"   PRIVATE7                    ( 10000 ), " &
"   PRELOAD                     ( 00010 ), " &
"   SAMPLE                      ( 00010 ), " &
"   PRIVATE8                    ( 10111 ), " &
"   PRIVATE9                    ( 11000 )  " ;
```

- Strange behaviour when Data Register is set to 1 or 2

Nexus (IEEE-ISTO 5001-2003)

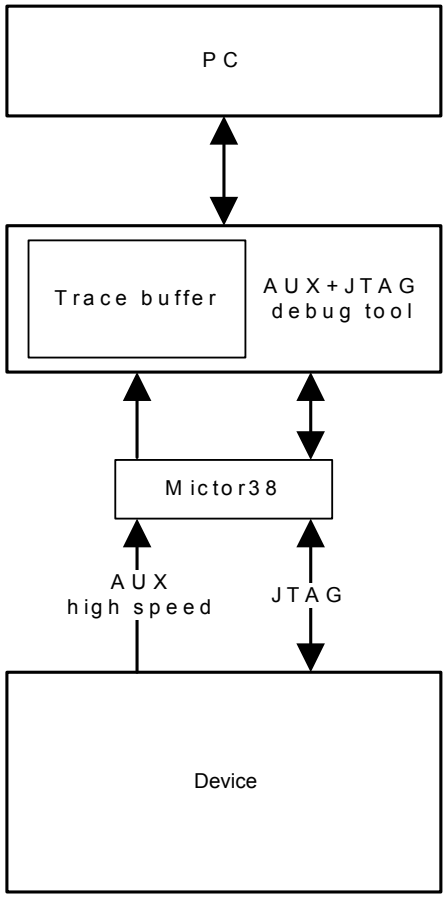


Figure: AUX+JTAG based debugger

References

- http://www.fpga4fun.com/JTAG.html
- http://www.elinux.org/JTAG_Finder
- http://events.ccc.de/congress/2009/Fahrplan/events/3670.en.html

Contact

- Git: `git.psurply.com/uc3jtag`
- IRC: `Ptishell@irc.rezosup.org`
- Mail: `surply@lse.epita.fr`
- Twitter: `@Ptishell`