Pinout analysis and recovery of monolithic/embedded devices.

(preview version)

Duration: 3 days

1. Introduction to embedded/monolithic device analysis. Packages. Internal structure. PCB layouts. NAND die/crystal layouts. Controllers. Chip-off data recovery from embedded devices

Practise 1: Review of different embedded devices.

2. Device preparation for analysis. Coating removal techniques and safety procedures during device preparation. Required tools and accessories. Special adapters for embedded/monolithic device analysis for logic analyzer

Practise 2: Coating/Solder mask removal and fixing device on adapter

3. PCB layout analysis. Track, pads, via and other connections. Internal connections. Route of track from controller to NAND. Minimal and satisfactory conditions for pinout analysis. Optimization of the connection scheme. Test points search.

Practise 3: Test points search and minimization of connections

4. Additional techniques of preparation and preliminary analysis of device. Test points analysis. NAND crystal and controller location. Analysis of the connections and their typical patterns. Power and ground connection patterns.

Practise 4: Test points analysis

5. Microsoldering technology with practice on real devices. Required tools and workspace arrangement. The proper techniques of wire attachment. Map of test connection

Practise 5: Microsoldering of monolithic/embedded device

6. Logic analyzer. Connection of device. Software concept. Channels. Signals. Triggers. Decoders. Buffer and frequency. Thresholds. Features. Standard layout of signals in logic analyzer

Practise 6: Device connection, signal triggering, study of logic analyzer features

7. NAND protocol and signals. Default states of signals. Control signals. Different pinouts of data bus. Power and ground. Relation between multiple CE and R/B signals on the NAND chips.

8. Detailed signal analysis with logic analyzer. Behavior of NAND protocol. NAND activation and status signals. Data bus, order of bits and its decoding. Data bus synchronization. Control signals. Command bus and its synchronization. Address bus and its synchronization. Multi-die (multi-crystal) NAND chips and their signal behavior

Practise 7,8: NAND protocol analysis and signal determination

9. Time and dynamics of signals in NAND protocol. Typical order of signals and its pattern analysis on the time scale. Length and density of different groups of signals.

Practise 9: Search of NAND signal sequences and patterns

10. Command cycles and commands. General format of commands. Description of most frequent commands and review.

Practise 10: Analysis of NAND commands and their meaning

11. Flash storage device initialization process at the start up. Sequence of commands. Reference for command pattern recognition

Practise 11: Discovering sequence of command during initialization process

12. Determination of signals and pinout of unknown embedded/monolithic device.

Practise 12: Determination of signal and pinout of unknown test device

Practical part – full day

1. Pinout analysis of device from practice #2 with logic analyzer with further resoldering and testing in VNR.

2. Monolithic memory card microsoldering, pinout analysis and testing in VNR.

3. Practise on logic analyzer. Signal analysis and pinout reverse engineering.

4. For choice: pinout analysis of device or logic analyzer practice with signal analysis

What you learn

- internal structure of monolithic devices
- preparation of embedded device for further analysis
- microsoldering
- visual analysis of monolithic device and workflow optimization
- usage of adapters
- work with logic analyzer
- typical signals of NAND protocol and their recognition
- pinout analysis of unknown monolithic device