Accessing On-chip Instruments Through the Life-time of Systems

Erik Larsson
Lund University, Lund, Sweden
Email: erik.larsson@eit.lth.se

Farrokh Ghani Zadegan
Lund University, Lund, Sweden
Email: ghanizadegan@ieee.org

***Abstract*—The electronic systems we find in almost every product today are implemented using integrated circuits (ICs) mounted on printed circuit boards (PCBs). Developing electronic systems is a challenging task due to complexity and miniaturization. A single IC can contain billions of transistors, which are smaller than ever. As a result more Design-for-Test (DfT) features, so called instruments, are embedded on-chip in modern ICs to handle and monitor various activities. Many defects are handled at IC manufacturing; however, there are many problems occurring after ICs are being mounted on PCBs. In many cases, it is unfortunately not possible to reproduce the problem when the electronic system is taken to a repair shop. These problems are known as No Trouble Found (NTF). One obstacle is the limited access to the on-chip DfT instruments that exist in most ICs. We will discuss access to on-chip DfT instruments through the life-time of electronic systems. We will focus on electronic systems using the IEEE 1687 standard.**

***Index Terms*—IEEE Std. 1687, DfT instrument, access time, security**

I. Introduction

The increasing transistor count of integrated circuits (ICs) enables the implementation of more functionality in each IC. However, high transistor count increases design complexity making it an difficult task to get everything as intended. Typically, a significant amount of effort is spent on post-silicon validation, debugging, wafer sort, package test, burn-in, printed circuit board bring-up, and printed circuit board assembly. Even if great effort is spent on these activities during manufacturing, there is a growing need of power-on self-test and in-field test. To ease all these activities, Design-for-Test (DfT) features, so called instruments are embedded in ICs. These instruments are accessed at manufacturing test and in-field testing; hence, the embedded instruments are accessed through the life-time of the IC.

The process for instrument design, integration and usage can be described as follows. An *instrument designer* develops an instrument, for example a temperature sensor. An *instrument integrator* selects and integrates a number of instruments, for example temperature sensors onto the IC, and ensures the instruments can be accessed from the chip boundary (pins). An *instrument user* can access the instruments. Note that there are a number of different instrument users. Some instrument users access instruments at the manufacturing phase when performing post-silicon validation, debugging, wafer sort, package test, burn-in, later other instrument users access instruments to perform printed circuit board bring-up, printed circuit board assembly manufacturing test, and finally there are instrument users that access instruments at power-on self-test and in-field test. In cases, when a system malfunction during operation, there is a need to take the system, or parts of it, to a repair-shop to identify the problem. In these situation, it is desirable to be able to access embedded features.

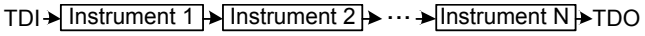


Fig. 1. Chaining instrument shift-registers into a regular scan-chain

In this paper we introduce IEEE 1687 and detail works using IEEE 1687.

II. Introduction to IEEE 1687

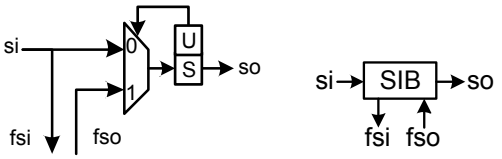
A straight-forward scheme to enable access to instruments is to make use of scan-chains, see Fig. 1. The instrument integrator simply connects all instruments into a long shift-register (scan-chain). For instrument access, the instrument users simply shifts data through the scan-chain to access desirable instruments. The drawback is that all instruments are *always* accessed even when a single instrument is to be accessed. For a large IC with many instruments the access time becomes very high.

IEEE 1687 (IJTAG) [1] enables flexible access, mainly through the JTAG test access port (TAP) [2], to the on-chip instruments. IEEE 1687 makes it possible to include only those instruments on the scan-path that are desired at the moment. IEEE 1687 introduces two new languages, Instrument Connectivity Language (ICL) and Procedural Description Language (PDL), to standardize the access and control of on-chip instruments.

ICL describes the instruments port functions and logical connection to other instruments and to the JTAG TAP, and PDL describes how an instrument should be operated. The idea in introducing ICL and PDL is to provide an adequate and standardized description of the IEEE 1687 network, instruments, and instrument access procedures, and to enable ICL and PDL interpreter tools to automate the retargeting of access procedures.

To enable variable-length (flexible) scan-path, IEEE 1687 introduces two components:

1) a Segment Insertion Bit (SIB), which is used to include in, or exclude a scan-chain from the active scan-path. Fig. 2 shows a simplified schematic of a possible implementation of a SIB, as well as a symbol which we will use through the rest of this paper. Fig. 2(a) shows



(a) Simplified schematic (b) Symbol

Fig. 2. Segment Insertion Bit (SIB)

only as few components and terminals as are needed to explain the operation of a SIB: a one-bit shift-update register, and a mux. However, a realistic schematic would contain more components (such as logic gates for gating control signals, keeper muxes for the registers, and delay elements to avoid race condition) and terminals (such as selection and control signals used to enable shift and update operations).

2) a *ScanMux* control bit, which is a shift-update register that can be placed anywhere on the scan-path to configure one or more scan multiplexers (ScanMux components). Fig. 3 shows a two-bit ScanMux control register used to configure a network of two instruments. In this work, we consider one-bit ScanMux control bits, to control two-input muxes which bypass instrument shift registers in, e.g., daisy-chained architectures.

Both SIBs and ScanMux control bits must be configured to have the correct value every time the scan-path they are on is accessed.

The flexibility in an 1149.1-2013 [3] TDR is achieved by defining segments of that TDR as *selectable*. A selectable segment mux with a one-bit wide control, is similar to the SIB component specified by 1687. Moreover, 1149.1-2013 also allows for controlling a selectable segment mux from another part of the scan-path or from other TDRs. The selectable segments can be nested to create a hierarchical network for accessing instruments, similar to what is achievable by a hierarchical IEEE 1687 network.

Although there are differences between 1149.1-2013 and 1687 in implementation details, the corresponding reconfigurable networks described under each of the two standards show the same behavior regarding instrument access time.

1149.1-2013 and 1687 use a similar Procedural Description Language (PDL) for describing the operation of embedded instruments. For example, assuming that the DFT feature in Fig. 4 is a BIST instrument, to operate on this BIST instrument there is a need of PDL commands (read/write) to configure the SIBs such that the BIST instrument is placed on the scan-path. While the BIST instrument is running, there is no need to access the network for this particular instrument. Hence, the PDL commands can be divided as commands that configure and access the network, such as read/write, and as commands that utilize a given network configuration without requiring any accesses, such as a command used for waiting for a number of clock cycles. The idea is that the retargeting tool generates network configuration vectors/commands. The user needs only to specify what should be written to the registers of the BIST engine (for example algorithm selection and start command).

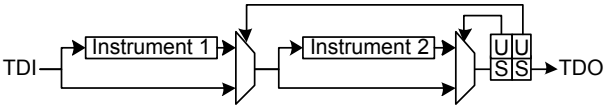


Fig. 3. A network configured by a two-bit ScanMux control register

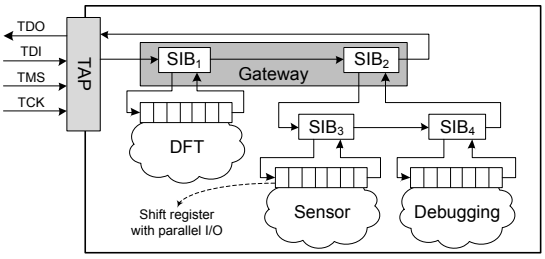


Fig. 4. A 1687 network with three instruments inside a chip

III. Previous works

In this section, we present previous works on IEEE 1687 in respect to standards, access optimization, in-field usage, security aspects, and case studies.

The boundary scan (IEEE 1149.1) [2] and the standard for embedded core test (SECT) [4] suffers from drawbacks when used for accessing on-chip instruments. The boundary scan (IEEE 1149.1) does not allow flexible access to any instrument [2] and the standard for embedded core test (SECT) [4] has no test controller and there is no description of the test infrastructure. IEEE 1687 [1] and the updated IEEE 1149.1 [3] both allows flexible access to any instrument at any time. IEEE 1687 makes use of ICL and PDL, discussed above, to meet these goals.

In the progress to IEEE 1687, several works outlined ideas and requirements [5], [6], [7], [8], [9], [10]. Designing the IEEE 1687 network and optimizing the access has gained much interest [11], [12], [13], [14], [15], [16], [17] [18] [19], [18], [19], [20], [21], [22]. For in-field use there are works [23], [24], [25], [26]. An important aspect in allowing access to embedded instruments is the ability to be able to only allow the instrument user to access the instruments the instrument integrator wants to disclose [27], [28], [29], [30], [31]. There are reports on cases studies using IEEE 1687 [32], [33].

References

[1] "IEEE Standard for Access and Control of Instrumentation Embedded within a Semiconductor Device," *IEEE Std 1687-2014*, pp. 1–283, Dec 2014.

[2] IEEE Association, "IEEE Std 1149.1-2001, IEEE Standard Test Access Port and Boundary-Scan Architecture," 2001.

[3] "IEEE Standard for Test Access Port and Boundary-Scan Architecture," *IEEE Std 1149.1-2013 (Revision of IEEE Std 1149.1-2001)*, 2013.

[4] IEEE Association, "IEEE Std 1500-2005, IEEE Standard Testability Method for Embedded Core-Based Integrated Circuits," 2005.

[5] A. L. Crouch, "IJTAG: The Path to Organized Instrument Connectivity," in *Proc. IEEE Int'l Test Conf. (ITC)*, Oct. 2007, pp. 1–10.

[6] J. Rearick and A. Volz, "A Case Study of Using IEEE P1687 (IJTAG) for High-Speed Serial I/O Characterization and Testing," in *Proc. IEEE Int'l Test Conf. (ITC)*, Oct. 2006, pp. 1–8.

[7] J. Rearick et al., "IJTAG (Internal JTAG): A Step Toward a DFT Standard," in *Proc. IEEE Int'l Test Conf. (ITC)*, 2005.

[8] K. Posse et al., "IEEE P1687: Toward Standardized Access of Embedded Instrumentation," in *Proc. IEEE Int'l Test Conf. (ITC)*, 2006, pp. 1 –8.

[9] M. Portolan, B. Van Treuren, and S. Goyal, "Executing IJTAG: Are Vectors Enough?" *Design Test, IEEE*, vol. 30, no. 5, pp. 15–25, Oct 2013.

[10] M. Keim et al., "Industrial Application of IEEE P1687 for an Automotive Product," in *Euromicro Conference on Digital System Design (DSD)*, Sept 2013, pp. 453–461.

[11] F. G. Zadegan et al., "Test Time Analysis for IEEE P1687," in *Proc. ATS*, 2010, pp. 455–460.

[12] ——, "Design automation for IEEE P1687," in *Proc. Design, Automation Test in Europe Conference (DATE)*, March 2011.

[13] F. G. Zadegan et al., "Test Scheduling in an IEEE P1687 Environment with Resource and Power Constraints," in *Proc. Asian Test Symposium (ATS)*, 2011, pp. 525 –531.

[14] F. G. Zadegan et al., "Access Time Analysis for IEEE P1687," *IEEE Transactions on Computers*, vol. 61, no. 10, pp. 1459–1472, Oct. 2012.

[15] ——, "Reusing and Retargeting On-Chip Instrument Access Procedures in IEEE P1687," *Design & Test of Computers, IEEE*, vol. 29, no. 2, pp. 79 –88, april 2012.

[16] F. Ghani Zadegan, G. Carlsson, and E. Larsson, "Robustness of TAP-Based Scan Networks," in *Proc. IEEE Int'l Test Conf. (ITC)*, 2014.

[17] R. Baranowski, M. Kochte, and H.-J. Wunderlich, "Fine-grained access management in reconfigurable scan networks," *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, vol. 34, no. 6, pp. 937–946, June 2015.

[18] ——, "Modeling, Verification and Pattern Generation for Reconfigurable Scan Networks," in *Proc. IEEE Int'l Test Conf. (ITC)*, 2012, pp. 1–9.

[19] R. Baranowski, M. A. Kochte, and H.-J. Wunderlich, "Scan Pattern Retargeting and Merging with Reduced Access Time," in *Proceedings of IEEE European Test Symposium (ETS'13)*. IEEE Computer Society, 2013, pp. 39–45.

[20] R. Cantoro, M. Montazeri, M. S. Reorda, F. G. Zadegan, and E. Larsson, "On the Testability of IEEE 1687 Networks," 2015. [Online]. Available: http://lup.lub.lu.se/record/8301410/file/8301425.pdf

[21] R. Baranowski, M. A. Kochte, and H.-J. Wunderlich, "Reconfigurable scan networks: Modeling, verification, and optimal pattern generation," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 20, no. 2, pp. 30:1–30:27, Mar. 2015. [Online]. Available: http://doi.acm.org/10.1145/2699863

[22] R. Krenz-Baath, F. Zadegan, and E. Larsson, "Access time minimization in ieee 1687 networks," in *Test Conference (ITC), 2015 IEEE International*, Oct 2015, pp. 1–10.

[23] K. Petersen, D. Nikolov, U. Ingelsson, G. Carlsson, F. Zadegan, and E. Larsson, "Fault injection and fault handling: An mpsoc demonstrator using ieee p1687," in *On-Line Testing Symposium (IOLTS), 2014 IEEE 20th International*, July 2014, pp. 170–175.

[24] A. Jutman, S. Devadze, and K. Shibin, "Effective Scalable IEEE 1687 Instrumentation Network for Fault Management," *IEEE Design & Test*, vol. 30, no. 5, pp. 26–35, Oct 2013.

[25] K. Shibin, S. Devadze, and A. Jutman, "Asynchronous Fault Detection in IEEE P1687 Instrument Network," in *IEEE 23rd North Atlantic Test Workshop (NATW)*, May 2014, pp. 73–78.

[26] F. Ghani Zadegan, D. Nikolov, and E. Larsson, "A self-reconfiguring ieee 1687 network for fault monitoring," in *Test Symposiutm (ETS), 2016 IEEE European*, May 2016, pp. 1–6.

[27] A. Zygmontowicz, J. Dworak, A. Crouch, and J. Potter, "Making it harder to unlock an lsib: Honeytraps and misdirection in a p1687 network," in *Proceedings of the Conference on Design, Automation & Test in Europe*, ser. DATE '14. 3001 Leuven, Belgium, Belgium: European Design and Automation Association, 2014, pp. 195:1–195:6.

[28] J. Dworak, A. Crouch, J. Potter, A. Zygmontowicz, and M. Thornton, "Don't forget to lock your sib: hiding instruments using p1687," in *Test Conference (ITC), 2013 IEEE International*, Sept 2013, pp. 1–10.

[29] J. Dworak, Z. Conroy, A. Crouch, and J. Potter, "Board security enhancement using new locking sib-based architectures," in *Test Conference (ITC), 2014 IEEE International*, Oct 2014, pp. 1–10.

[30] J. Dworak and A. Crouch, "A call to action: Securing ieee 1687 and the need for an ieee test security standard," in *VLSI Test Symposium (VTS), 2015 IEEE 33rd*, April 2015, pp. 1–4.

[31] R. Baranowski, M. Kochte, and H.-J. Wunderlich, "Securing access to reconfigurable scan networks," in *Test Symposium (ATS), Asian*, Nov 2013, pp. 295–300.

[32] H. von Staudt and A. Spyronasios, "Using ijtag digital islands in analogue circuits to perform trim and test functions," in *Mixed-Signal Testing Workshop (IMSTW), 2015 20th International*, June 2015, pp. 1–5.

[33] T. Payakapan, S. Kan, K. Pham, K. Yang, J.-F. Cote, M. Keim, and J. Dworak, "A case study: Leverage ieee 1687 based method to automate modeling, verification, and test access for embedded instruments in a server processor," in *Test Conference (ITC), 2015 IEEE International*, Oct 2015, pp. 1–10.