# IEEE Std. P1687.1 for Access Control of Reconfigurable Scan Networks

Larsson, Erik; Xiang, Zehang ; Murali, Prathamesh

*Published in:*
2020 IEEE European Test Symposium (ETS)

*DOI:*
10.1109/ETS48528.2020.9131555

2020

*Document Version:*
Publisher's PDF, also known as Version of record

Link to publication

*Citation for published version (APA):*
Larsson, E., Xiang, Z., & Murali, P. (2020). IEEE Std. P1687.1 for Access Control of Reconfigurable Scan Networks. In *2020 IEEE European Test Symposium (ETS)* IEEE - Institute of Electrical and Electronics Engineers Inc.. https://doi.org/10.1109/ETS48528.2020.9131555

*Total number of authors:*
3

LUND UNIVERSITY

PO Box 117
221 00 Lund
+46 46-222 00 00

# IEEE Std. P1687.1 for Access Control of Reconfigurable Scan Networks

Erik Larsson, Zehang Xiang and Prathamesh Murali
Lund University, Lund, Sweden
Email: erik.larsson@eit.lth.se

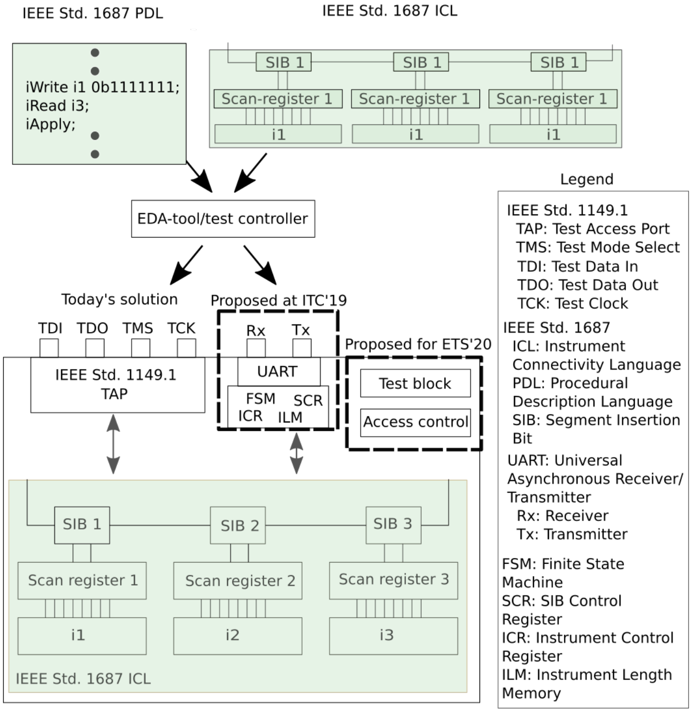
***Abstract*—We address access control of reconfigurable scan networks, like IEEE Std. 1687 networks. We propose an on-chip test block to perform: (1) test for faulty scan-chains, (2) localization of faulty scan-chains and (3) repair by excluding faulty scan-chains, and an access control block to (1) control so scan-chains (instruments) are only accessed in allowed combinations, (2) detection of access attempts to instrument in not allowed combinations, and (3) monitoring how theses attempts are made. The key features are two-fold. First, in respect to operation and maintenance. If the physical implementation of an IEEE Std. 1687 network changes due to faults, the instrument connectivity language (ICL) and procedural description language (PDL) need to be updated. To avoid keeping track and updating ICL and PDL for each individual integrated circuit (IC), proposed test block, placed at each IC, makes adjustments of PDL according to the faults of the particular IC. Second, a centralized access control block with key information about the network to detect and handle un-authorized access.**

## I. Introduction

Reconfigurable scan networks (RSNs), like IEEE Std. 1687 networks, offer an infrastructure to connect on-chip instruments in a flexible and scalable manner, see Figure 1. Dynamic reconfiguration of the active scan-path to include or exclude instruments can be achieved by the use of segment insertion bits (SIBs). IEEE Std. 1687 includes two description languages, instrument connectivity language (ICL) and procedural description language (PDL) [1]. ICL describes how instruments are interconnected. Figure 1 shows the schematic equivalent of the network's ICL. PDL describes how to operate on instruments. Figure 1 shows PDL with one iApply group to concurrently write data to instrument *i1* and read data from instrument *i3*. While the main interface today to IEEE Std. 1687 is the IEEE Std. 1149.1 test access port (TAP), the IEEE Std. P1687.1 [2] working group is exploring how to use functional ports, like serial peripheral interface (SPI), inter-integrated circuit (I2C), universal serial bus (USB), and advanced microcontroller bus architecture (AMBA), see Figure 1.

To operate on instruments, PDL and ICL are given as inputs to an Electronic Design Automation (EDA) tool or an embedded controller and the output is access (test) patterns. For the PDL in Figure 1, smart access patterns include instruments *i1* and *i3*, while instrument *i2*, is excluded from the active scan-path as the PDL specifies operations on instruments *i1* and *i3*, but not on instrument *i2*. While there are works on analysis [3], design [4] [5], [6], [7], and fault management [8] [9] of IEEE Std. 1687, these works assume the network to be without faults. Work tested for faulty RSN networks [10], but do not include reapir, and work addressed protection of RSN networks [11], but not detection and handling of un-authorized access.

With flexible and scalable access to on-chip instruments, there is a need to ensure access control, which is the topic of this paper. The paper has two contributions: *test and repair* including (1) test to detect faulty scan-chains, (2) localization of faulty scan-chains, and (3) repair of faulty reconfigurable scan networks, and *access control* addressing (1) control to ensure that instruments are only accessed in allowed combinations, (2) possibility to detect attempts to access instruments in not allowed combinations, and (3) information about the way attempts are performed, which helps in finding potential Trojans.



```
iWrite i1 0b1111111;
iRead i3;
iApply;
```

Fig. 1. Illustration of today's and proposed solution to access an IEEE Std. 1687 network

The key features of our scheme is two-fold. First, in respect to operation and maintenance. The PDL and ICL needed to operate instruments can be stored in a central database that is shared among several ICs or stored embedded (compressed) locally near each individual IC. In both cases, PDL and ICL need to be updated according to the unique status of individual ICs. For example, assume a central database with PDL and ICL serving many ICs. As long as all ICs are free from faults, the same PDL and ICL can be used for all ICs. However, as soon as an IC has faults, for example a faulty scan-chain, the PDL for this IC must be modified. For example, assume that scan-chain *3* (Figure 1) is faulty, then the iApply group, for this particular IC, must be updated such that iRead *i3* is removed, which makes instrument *i3* to be excluded from the active scan-path. In the worst case, there is a need to keep track of PDL for each individual IC, which is unfeasible in practise. To avoid keeping track and updating ICL and PDL for each individual integrated circuit (IC), proposed test block, placed at each IC, makes adjustments of the PDL according to the fault status of the particular IC. Second, central access control with key information from the IEEE Std. 1687 network to control access to instrument, detect when un-authorized access occurs, and report how the attempt was performed. We believe these two important aspect have not been addressed prior to this work.

## II. Test, Localization, and Repair

The principle to test for faults in scan-chains is built on traditional scan-chain test where a test sequence is shifted through the scan-chain but no capture and update is used [12] [10]. The test scheme includes a test block and a command to perform test of scan-chains. The test command consists of 2 bytes, in a similar way as the data and control commands, see [13]. The output (return value) is a single bit indicating if there was any faults or not (1-bit). When the test block receives a test command, the test block automatically sets the active scan-path to include all instruments, generates and shifts in a test sequence, and compares the output sequence with the expected test sequence.

The objective of localization is to pin-point faulty scan-chains. The principle is that the RSN is configured so that only one scan-chain is active at a time. For each individual scan-chain a test sequence is shifted through the scan-chain and the output is compared against the input sequence.

At repair, the original PDL will be applied and instruments accessed through faulty scan-registers will automatically be excluded from the active scan-path by the hardware component. For example, if the scan-chain related to instrument *i3* in Figure 1 is faulty, the test and localization process has set the value 110 in the repair register. This indicates that instrument *i3* will not be included in the scan-path due to the 0, while the other instruments are not faulty, indicated by 1, see Figure 2. When the original PDL in Figure 1 is applied, the SCR will contain 101 as the PDL specifies that instruments *i1* and *i3* should be active, see Figure 2. Given the combination of the repair register and SCR, the FSM performs a bitwise AND between the two registers to receive the SCR to be used $\boxed{1}\boxed{0}\boxed{0}$. We observe that the "used SCR" does not include instrument *i3*, which is faulty, hence, the FSM in our component automatically excludes instrument *i3* while instrument *i1* is included.

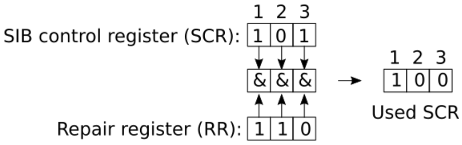

1 2 3
SIB control register (SCR): 1 0 1
& & &
1 2 3
1 0 0
Used SCR
Repair register (RR): 1 1 0

Fig. 2. Repairing RSN

## III. Controlling access to instruments

The assumed threat model is that someone tries to access instruments in a not allowed combination. Our objective is to prevent such access, report when it occurs, and report which instruments are involved, to help pin-point Trojans.

For illustration, take the system in Figure 1 and assume that instrument *i3* should only be accessed when it is the only instrument in the active scan-path. To enable this, we complement SCR with a logic function and an access control register (ACR), see Figure 3. In this example, the PDL in Figure 1 will try to access *i1* and *i3* by setting SCR so that instruments *i1* and *i3* are active at the same time. However, as ACR is specified to 001 the logic function will indicate that when instrument *i3* is on the active scan-path it must be the only instrument. In this case, the content of SCR is not accepted by the ACR and the logic function. The result is that access to instruments in this combination can be blocked, a signal can be sent to indicate that an attempt to access instruments in a not allowed combination has been made, and that the involved instruments, the content of SCR, are reported, as the information that instrument *i1* was included in the PDL may help in determining if instrument *i1* is a Trojan.

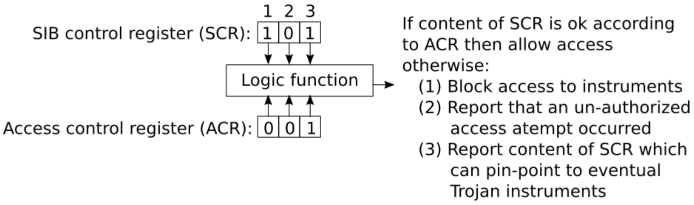

1 2 3
SIB control register (SCR): 1 0 1
Logic function
Access control register (ACR): 0 0 1
If content of SCR is ok according to ACR then allow access otherwise:
(1) Block access to instruments
(2) Report that an un-authorized access atempt occurred
(3) Report content of SCR which can pin-point to eventual Trojan instruments

Fig. 3. Controlling access to instruments

## IV. Conclusions

In light of the on-going development of IEEE Std. P1687.1, we showed the benefit of including key information about the IEEE Std. 1687 network in the hardware component interfacing the IEEE Std. 1687 network. In particular, we showed that key information gives the possibility to perform test and repair as well as the possibility to control and prevent the inclusion of instruments in the active scan-path in not allowed combinations.

## References

[1] "IEEE standard for access and control of instrumentation embedded within a semiconductor device," *IEEE Std 1687-2014*, 2014.

[2] IEEE P1687.1, "Standard for the Application of Interfaces and Controllers to Access 1687 IJTAG Networks Embedded Within Semiconductor Devices," Dec. 2016.

[3] F. G. Zadegan and others, "Test Time Analysis for IEEE P1687," in *Proc. ATS*, 2010, pp. 455–460.

[4] F. Ghani Zadegan *et al.*, "Design automation for IEEE P1687," in *Design, Automation & Test in Europe Conference (DATE)*, 2011.

[5] Krenz-Baath *et al.*, "Access time minimization in IEEE 1687 networks," in *International Test Conference (ITC)*, 2015.

[6] Z. Zhong, G. Li, Q. Yang, and K. Chakrabarty, "Access-time minimization in the ieee 1687 network using broadcast and hardware parallelism," in *2018 IEEE International Test Conference (ITC)*, 2018, pp. 1–10.

[7] F. G. Zadegan *et al.*, "Upper-bound computation for optimal retargeting in ieee1687 networks," in *2016 IEEE International Test Conference (ITC)*, Nov 2016, pp. 1–10.

[8] F. Ghani Zadegan *et al.*, "A self-reconfiguring IEEE 1687 network for fault monitoring," in *European Test Symposium (ETS)*, 2016.

[9] A. Jutman *et al.*, "Reliable health monitoring and fault management infrastructure based on embedded instrumentation and IEEE 1687," in *AUTOTESTCON*, 2016.

[10] R. Cantoro *et al.*, "Test of reconfigurable modules in scan networks," *IEEE Trans. on Computers*, vol. 67, no. 12, pp. 1806–1817, Dec 2018.

[11] J. Dworak *et al.*, "Don't forget to lock your sib: hiding instruments using p1687," in *IEEE Inter. Test Conference (ITC)*, Sep. 2013, pp. 1–10.

[12] D. Adolfsson *et al.*, "On scan chain diagnosis for intermittent faults," in *2009 Asian Test Symposium*, Nov 2009, pp. 47–54.

[13] E. Larsson, P. Murali, and G. Kumisbek, "IEEE Std. P1687.1: Translator and Protocol," in *International Test Conference*, 2019, pp. 1–10.