ECSEL Joint Undertaking
Electronic Components and Systems for European Leadership

Cyber Physical System based Proactive Collaborative Maintenance

D1.2 Consolidated State-of-the-Art of Sensor-based Proactive Maintenance Appendix 6:

Security approach to prevent unauthorized access to sensors via test bus

Work Package	WP1 - Service platform architecture requirement definition. Scenarios and use cases descriptions
Version	1.0
Contractual Date of Delivery	30/04/2016
Actual Date of Delivery	03/06/2016
Dissemination Level	Public
Responsible	Erkki Jantunen
Contributors	Franc Novak (JSI), Anton Biasizzo (JSI), Gregor Papa (JSI)

The MANTIS consortium consists of:

Num.	Short Name	Legal Name	Role	Country
1	MGEP	Mondragon Goi Eskola Politeknikoa J.M.A. S.Coop.	CO	ES
2	MONDRAGON	Mondragon Corporacion Cooperativa S.Coop.	BEN	ES
3	IKERLAN	Ikerlan S.Coop.	BEN	ES
4	TEKNIKER	Fundacion Tekniker	BEN	ES
5	FARR	Fagor Arrasate S.Coop.	BEN	ES
5.1	KONIKER	Koniker S.Coop.	TP	ES
6	GOIZPER	Goizper S.Coop.	BEN	ES
7	ACCIONA	Acciona Infraestructuras S.A.	BEN	ES
8	MSI	Mondragon Sistemas De Informacion S.Coop.	BEN	ES
9	VTT	Teknologian Tutkimuskeskus VTT Oy	BEN	FI
10	LUAS	Lapin Ammattikorkeakoulu Oy	BEN	FI
11	NOME	Nome Oy	BEN	FI
12	FORTUM	Fortum Power And Heat Oy	BEN	FI
13	SQ	Solteq Oyj	BEN	FI
14	WAPICE	Wapice Oy	BEN	FI
15	AAU	Aalborg Universitet	BEN	DK
16	DANFOSS	Danfoss A/S	BEN	DK
17	UNIV	Universal Foundation A/S	BEN	DK
18	HGE	Hg Electric A/S	BEN	DK
19	VESTAS	Vestas Wind Systems A/S	BEN	DK
20	SIRRIS	Sirris Het Collectief Centrum Van De Technologische Industrie	BEN	BE
21	ILIAS	Ilias Solutions Nv	BEN	BE
22	ATLAS	Atlas Copco Airpower Nv	BEN	BE
23	3E	3e Nv	BEN	BE
24	PCL	Philips Consumer Lifestyle B.V.	BEN	NL
25	PHC	Philips Medical Systems Nederland B.V.	BEN	NL
26	PHILIPS	Philips Electronics Nederland B.V.	BEN	NL
27	S&T	Science and Technology B.V.	BEN	NL
28	TU/E	Technische Universiteit Eindhoven	BEN	NL
29	RUG	Rijksuniversiteit Groningen	BEN	NL
30	UNINOVA	UNINOVA - Instituto de Desenvolvimento de Novas Tecnologias	BEN	PT
31	ISEP	Instituto Superior de Engenharia do Porto	BEN	PT
32	INESC	Instituto de Engenharia de Sistemas e Computadores do Porto	BEN	PT
33	ADIRA	ADIRA - Metal Forming Solutions S.A.	BEN	PT
34	ASTS	Ansaldo STS S.p.A.	BEN	IT
35	CINI	Consorzio Interuniversitario Nazionale per l'Informatica	BEN	IT
36	AIT	Austrial Institute of Technology GmbH	BEN	AT
37	HBM	Hottinger Baldwni Messtechnik GmbH	BEN	AT
38	INNOTEC	Innovative Technology and Science Limited	BEN	UK
39	AITIA	AITIA International Inc.	BEN	HU
40	BME	Budaperst University of Technology and Economics	BEN	HU
41	JSI	Josef Stefan Institute	BEN	SI
42	XLAB	XLAB d.o.o.	BEN	SI
43	FHG	Fraunhofer Institute for Experimental Software Engineering IESE	BEN	DE
44	M2X	M2Xpert GmbH & Co KG	BEN	DE
45	STILL	STILL GMBH	BEN	DE
46	BOSCH	Robert Bosch GMbH	BEN	DE
47	LIEBHERR	Liebherr-Hydraulikbagger GmbH	BEN	DE

Document Revisions & Quality Assurance

Revisions:

Version	Date	By	Overview

0.1	18/04/2016	Franc Novak (JSI), Anton Biasizzo (JSI), Gregor Papa (JSI)	First Draft
1.0	02/06/2016	Mikel Muxika (MGEP)	Format correction Deliverable info update

Abstract

Testing of complex electronic systems is a difficult problem. One of the popular solutions in practice is the application of JTAG test bus also defined as IEEE Std 1149.1. JTAG infrastructure consists of scan chains, which enable easy test access to system internal logic. Industrial applications of boundary scan technology are today supported by a variety of sophisticated electronic design automation (EDA) tools, which simplify boundary scan infrastructure insertion as well as test generation and application. Most automated test equipment manufacturers have included IEEE 1149.1 support into test systems, which are commonly used during production testing as well as system maintenance. In many cases, maintenance of systems with JTAG infrastructure is performed remotely via internet. In this way, the maintenance costs can be reduced but on the other hand, the access to system□s internal logic represents potential security vulnerability. In the following, we briefly describe the security threats and proposed countermeasures. Next, we propose a low cost solution based on the JTAG bus locking mechanism. The original solution, proposed in 2006, will be customized to different requirements as regards employed technology, level of security and hardware overhead. Developed solutions will be scalable to meet the needs of different partners. Deliverables will include VHDL description of the locking mechanism, test bench and working prototype on a FPGA device.

Table of Contents

1 Introduction 2
2 JTAG vulnerability and countermeasures 3
3 Proposed solution 5
4 Related standards 6
References 7

1 Introduction

JTAG or boundary-scan test bus [1], [2] based on the scan-design principle is widely used for test and maintenance of electronic systems. JTAG infrastructure (defined under standard IEEE 1149.1) [3] allows on-line access to system internal states, which offers efficient means for test and maintenance. The basic configuration of a test or maintenance of a JTAG-based system is shown in Figure 1. The JTAG test bus is driven by a particular serial protocol, which controls the access mechanism of the boundary scan infrastructure on the system under test from a remote test system. The test bus controller performs adequate transformation of the test data supplied by the remote test system and generates necessary control signals, which allow data to be shifted along the boundary scan path in the system under test and control the execution of standard or custom boundary scan test instructions.

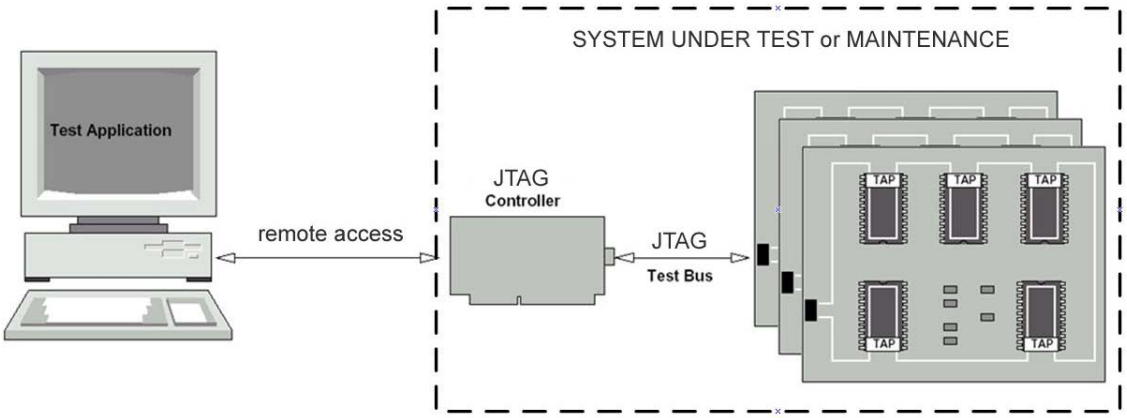

Figure 1: Basic configuration of a test or maintenance of a JTAG-based system

While its benefits are well proven in practice, its applications also have some drawbacks since the access to system□s internal logic represents potential security vulnerability. Critical infrastructure systems such as power plants, chemical plants, etc. with process control systems incorporating JTAG connected to internet in order to upload firmware upgrades or perform remote system maintenance are vulnerable: an attacker familiar with the IEEE Standard 1149.1 can break into a system and disturb its normal operation by executing an invasive test sequence which may lead to a catastrophic event. Another threat, not catastrophic but still with serious consequences refers to the systems programmed via JTAG bus (i.e., FPGA based systems, embedded systems with ARM controllers, etc.). In such cases, JTAG can be used to reveal system□s internal structure, so hackers or other interested third parties can steal intellectual property. Consequently, the risk of system brake-in should be seriously considered and appropriate countermeasures taken. In the following we give some more details on system security threat and show how the problem could be resolved in the frame of MANTIS project.

2 JTAG vulnerability and countermeasures

Any chip that uses scan design and any system built around it (either in some ad hoc design-for-test solution or with test or application infrastructure defined by the above standards) provides access to the system's internal logic and may be vulnerable to hackers.

As an illustrative example of vulnerability case study of scan design consider the implementation of DES algorithm with inserted scan chain using Synopsys Test Compiler [4]. Assuming that the attacker knows the DES algorithm (it is public), and assuming that the attacker has access to the high level timing diagrams (provided by the ASIC vendor), the authors show that the attacker needs less than 42000 clock cycles to determine the scan chain structure, recover round key and discover the user key.

So far, the countermeasures have been directed mainly at preventing unauthorized access to the system internal logic and stealing intellectual property. At the International Test Conference, Charlotte, 2004, a panel discussion "Security vs. Test Quality: Can We Really Only Have One at a Time?" R. Kapur [5] proposed to employ encryption techniques to encrypt sensitive data that is made available to the user in order to perform scan test. In this case, the scan chain logic of the tested unit includes decoding logic at scan-in and encoding logic at scan-out.

The application of cryptographic algorithms in scan design chain is, however, not trivial. The logic implementing a cryptographic algorithm is itself a complex sequential circuit which requires some design for test solution and built-in self-test seems to be the only possible choice in order to avoid the transfer of the internal data sensitive information to an attacker.

Typical cryptographic algorithms are block based. For example, DES is a symmetrical block cipher an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher-text bit-string of the same length. In the case of DES, the block size is 64 bits. Scan chain data decoding/encoding by a DES algorithm implemented in hardware requires a number of 64-bit blocks for the subsequent stages of processing. The resulting logic may represent a non-negligible overhead especially when accompanied by a BIST. In the implementation of DES algorithm reported in [4], 198 flip-flops were used for encoding logic: 64 for the input register, 64 for the output register, 64 for data manipulation and 4 for the controller. The same amount of hardware is needed for decoding. Another drawback is incompatibility of the length of a scan chain with the size of the block of a cryptographic algorithm, which additionally complicates control logic. Besides, special software must be provided by the ASIC vendor for proper interpretation of the scan test results (i.e., for fault diagnosis more precise than merely pass/fail test result).

Theft of intellectual property is, however, not the only vulnerability threat of scan design. Test infrastructure of IEEE Std. 1149.1 is often employed for field reconfiguration, troubleshooting and system maintenance [6]. For example, making a field upgrade to the firmware stored in programmable logic devices can be performed remotely by providing access to the boundary-scan via internet. Likewise, in some implementations of system maintenance, system's boundary-scan is permanently connected to a low-cost test equipment (i.e., a dedicated PC) for remote diagnostics. All such solutions represent a potential weakness in system's security. An attacker may crack the system and get access to the test port. Executing some pin-permission instruction (i.e., an instruction which disconnects the component I/O pins from the system logic) during normal system operation may lead to a serious damage. Although intimate knowledge of the boundary-scan infrastructure and the boundary-scan instruction codes of the system is required to break into the system, worst case scenarios cannot be ruled out in safety critical applications. A recent study of analyzed cyber-attacks incident reports from various infrastructure control systems shows a fivefold increase from 1994 to 2004. The type of the incidents is changing from accidental and internal to external. From 2002 to 2004, 66 percent were classified as external, 22 percent were accidental and only 3 percent were internal [7], [8]. The threat of sophisticated web attack on boundary-scan based systems calls for appropriate countermeasures.

Different attack scenarios and defences for JTAG are studied in [7]. This approach uses a keyed hash, a stream cipher, a message authentication code, and defines challenge/response protocol to prevent the attacks on JTAG. The drawback is the fuse usage for keyed hashes since once the hashes are compromised the device remains exposed. The stream ciphers are also weaker then block ciphers but they are suitable if messages are short and if continuous data stream is required.

The JTAG test access port design that enables the digital rights management is described in [8]. This solution uses hashes and challenge/response protocol to enable the access of the JTAG infrastructures. It can have different hashes for groups of JTAG instructions thus providing a hierarchy of the JTAG access. Like in the previous solution, the hashes are hardwired, which means that a successfully attacked device remains compromised. However, on the JTAG data stream it does not apply encryption, thus it is vulnerable to eavesdropping and man-in-the-middle attacks.

Another approach is to use public/private key pairs in the authentication process. Special care has to be taken for key management and exchange. Furthermore, additional hardware performing asymmetric encryption cores has to be provided. As far as we know, an intensive work in this direction is underway by other groups and their solutions are likely to be reported in the forthcoming publications.

3 Proposed solution

One of the possible solutions is a security extension of the JTAG standard that we proposed in 2006 [9]. The security extension conforms to the IEEE 1149.1 standard and disables all except basic JTAG instructions, unless the proper locking key is loaded. This solution is very simple and uses little hardware resources however the keys are stored and exchanged in plaintext. This opens the possibility of the eavesdropping on the JTAG bus as well as retrieving the keys from the storage within the device. In the frame of MANTIS project we plan to improve the above locking mechanism and develop solutions that are customized to different requirements as regards employed technology, level of security and hardware overhead. Developed solutions can be adapted to meet the needs of different partners. Their application will increase the security of system maintenance infrastructure and thus improve overall system reliability.

While IEEE Std 1149.1 is defined for assembled boards, similar approach at the System-on-Chip (SoC) level has been defined by the IEEE Std 1500. Consequently, the developed solutions in the frame of Mantis are applicable also for systems including testing infrastructure complying to IEEE Std 1500 [10].

4 Related standards

Standard Organization	Number	Title	Publishing Year	Work Package	Task
IEEE	1149.1	IEEE Standard Test Access Port and Boundary-Scan Architecture	2001	WP3	T3.1 □ T3.6
IEEE	1500	IEEE Standard Testability Method for Embedded Core-based Integrated Circuits	2005	WP3	T3.1 □ T3.6

References

[1] Parker, K.P. The boundary-scan handbook, Third edition, Kluwer Acad. Publ. 2003.

[2] Bleeker, H., Van Den Eijuden, P., De Jong, F.: Boundary-scan test, A practical approach. Kluwer Acad. Publ. 1993.

[3] IEEE Standard Test Access Port and Boundary-Scan Architecture. IEEE Std1149.1-2001, Institute of Electrical and Electronics Engineers, 14-Jun-2001.

[4] Miller, A. Trends in process control system security. IEEE Security & Privacy, 2005, Vol. 3, No. 5, pp. 57-60.

[5] Kapur, R. Security vs. Test Quality: Are they mutually exclusive? Proc. of the ITC, Charlotte, 2004, pp1414.

[6] US Computer Emergency Readiness Team, Control Systems Cyber Security Awareness, http://www.us-cert.gov/reading˙room/Control˙System˙Security.pdf

[7] Rosenfeld, K., Karri, R. Attacks and Defenses for JTAG, IEEE Design and Test of Computers, 2010, Vol. 27, No. 1, pp. 36-47.

[8] Clark, C.J. Anti-tamper JTAG TAP design enables DRM to JTAG registers and P1687 on-chip instruments, Proc. HOST 2010, Jun. 2010, Anaheim, CA, USA, pp. 19-24.

[9] Novak, F., Biasizzo, A. Security extension for IEEE Std 1149.1. Journal of Electronic Testing, Theory and Practice, Vol. 22, No. 3, June 2006, pp. 301□303.

[10] IEEE Standard Testability Method for Embedded Core-based Integrated Circuits, IEEE Std 1500, Institute of Electrical and Electronics Engineers, 29 August 2005