Sequentially Triggering "Time-Bomb" Trojan into Hardware Wired Microsequencer

GRIGORE MIHAI TIMIS, ALEXANDRU VALACHI
Technical University "Gh.Asachi"Iasi,
Faculty of Automatic Control and Computer Engineering
ROMANIA

Abstract: - This paper presents an analysis of a sequential Triggered "Time Bomb" hardware Trojan (HT). Major security concerns have been rising up since malicious modification of hardware or fabrication IC can lead to an altered functional behavior, potentially with disastrous consequences in safety-critical applications. Due to the stealthy nature of the hardware Trojans the conventional design and time verification and post manufacturing testing cannot be readily extended. There are a large number of possible instances and operating modes for the hardware Trojans in a digital system. Since the hardware Trojan insertion can modify the functionality of the digital integrated circuit (IC), alter its behavior, generate denial of service (DoS), the HT threats should be analyzed with maximum importance through the entire lifecycle of the IC.

Key-Words: - Hardware Trojan (HT), Sequential Triggered "Time Bomb" Trojan, Hardware Trojan attacks, Hardware Microsequencer.

Received: March 14, 2023. Revised: November 25, 2023. Accepted: January 6, 2024. Published: March 19, 2024.

1 Introduction

The hardware security to ensure Trust in ICs has been developed as an important topic of research during recent periods. This tendency has resulted in new security threats such as hardware (HT) insertion. A hardware Trojan can perform such destructive actions such as DoS, damage to functions or performance etc. [1]. If the chip contained with the HT is deployed in the secure-sensitive fields such as education, military, economy and medical treatment, it may have severe consequences. Due to the stealthy nature of the hardware Trojan the post-manufacturing logic testing is not suitable for detecting it. In order to evade detection the Trojan will trigger a malfunction due to rare circuit conditions. If the Trojan acts as a sequential state machine or "time bomb" the rare conditions for activation of the Trojan might not be realized during the testing period. Hardware Trojan (HT) insertions can be classified into three categories: internal trigger, external trigger, storage, driver, [1-6].

In [2,12-16] the authors propose a simple classification for the hardware Trojans:

• combinational – the activation depends on the occurrence of a particular condition

• sequential – the activation depends on the occurrence of a specific sequence of rare logic values

The Trojan's Trigger refers to the activation mechanism while the Trojan Payload represents the affected circuit functionality, [17].

In Fig 1 is presented the Trojan taxonomy based on trigger and payload mechanisms,[2].

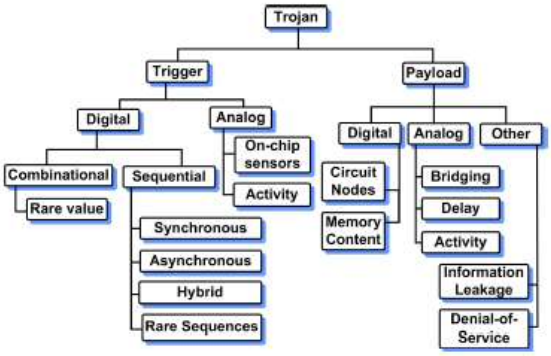

Fig.1. Hardware Trojan Taxonomy

Based on [7] the Trojans are classified regarding their trigger and payload mechanisms.

The trigger mechanism is split in two types: analog and digital [18]. Digital triggered Trojans are classified into sequential and combinational types, [20].

The sequentially triggered Trojans which also called also "time bombs" are activated by the occurrence of

a specific sequence. One of the common sequential Trojans is the synchronous counter which will trigger the malfunction due to a particular count value, [21].

Fig. 2 shows the Trojan's triggering "time-bomb" using a synchronous counter.

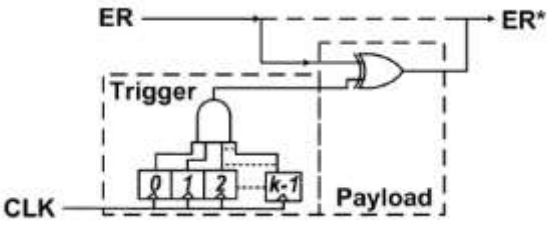

Fig.2. Trojan's triggering method using "time-bomb" synchronous counter type.

According [9-11], based on the Payload mechanism, Trojans can be classified into two main classes:
• Digital Trojans can affect the logical values at internal payload nodes
• Analog Trojans affect the circuit parameters like power, performances etc.

2. Sequentially Triggering "Time-Bomb" Hardware Trojan – a case study example

For a case study we propose to design a two color led digital semaphore system which is usually used on the train railway sections.
There is the following functionality:
• Red – Danger/Stop
• Green – Clear.
The train may proceed subject to any speed restrictions applying to the section of line or to the train itself.
The system has three buttons (B_1,B_2,B_{res}) and two leds (Green, Red) as in Fig. 3:

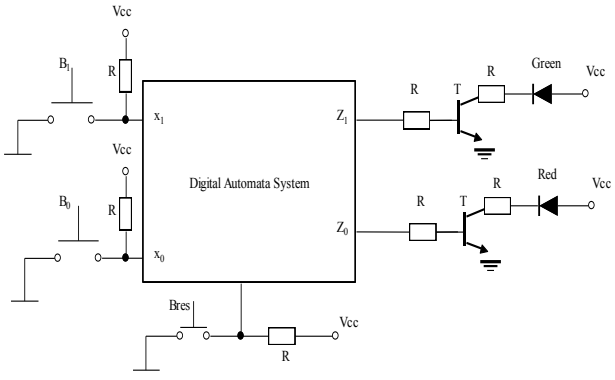

Fig.3. Digital Automata System
These three buttons will provide three inputs into the Digital Automata System:

• Push button B_0 will provide x_0 input with the following functionality: when the button is pushed (ON) the input x_0=1, when button is released (OFF) the input x_0=0.
• Push button B_1 will provide x_1 input with the following functionality: when the button is pushed (ON) the input x_1=1, when button is released (OFF) the input x_1=0.
• If the output signal z_1=1 it means that the green led will be on, if the output signal z_0=1 means that the red led will be on.
• B_{res} will provide a system hard reset so both leads will be off and the digital automata system will provide outputs z_1=0, z_0=0.

These two led will be on after the completion of the following sequence, (1):

$$B_1B_0 : OFF\_OFF \rightarrow OFF\_ON \rightarrow ON\_ON \rightarrow ON\_OFF \rightarrow$$
$$\rightarrow OFF\_OFF \Rightarrow GreenLed = ON, \mathrm{Re}dLed = OFF$$
$$B_1B_0 : OFF\_OFF \rightarrow ON\_OFF \rightarrow ON\_ON \rightarrow OFF\_ON \rightarrow$$
$$\rightarrow OFF\_OFF \Rightarrow GreenLed = OFF, \mathrm{Re}dLed = ON \quad (1)$$

As it's described in [3], the optimized fluence graph is shown in Fig. 4:

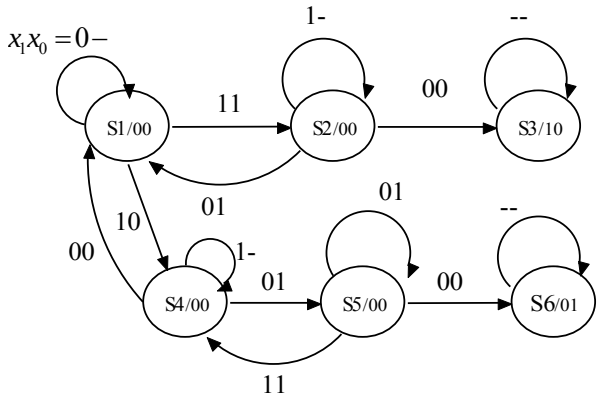

Fig.4. Optimized Fluence Graph

Based on the optimized fluence graph from Fig. 4, it represents the digital semaphore system's algorithm, the functional organization chart can be deducted like in Fig. 5. It can be observed that the green led will be

ON during state S_3 when $z_1 = 1$. Similarly, the red led will be ON during state S_6 when $z_0 = 1$.

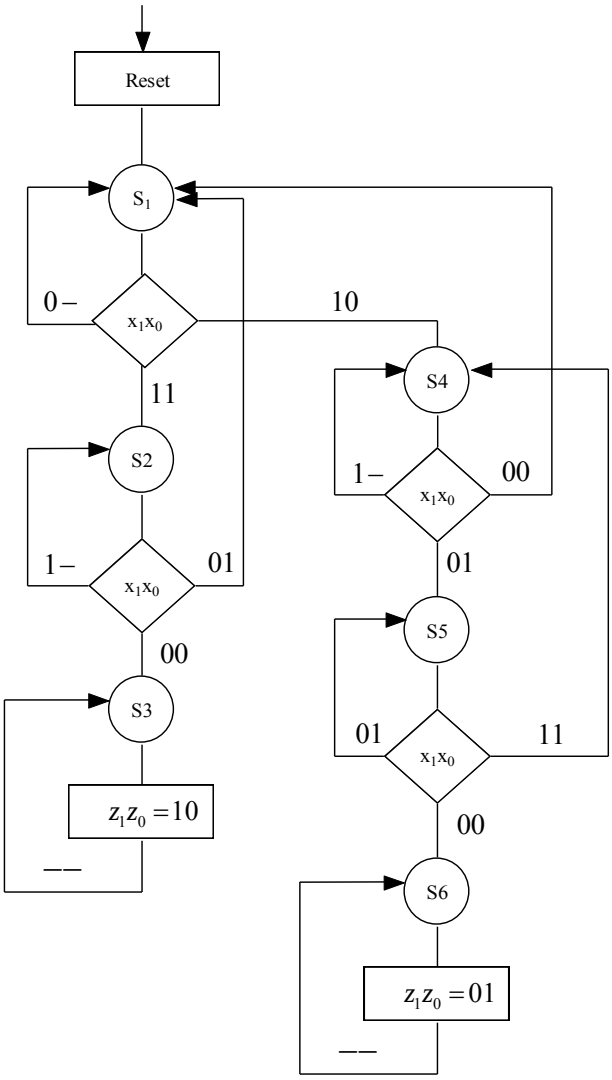

Fig.5. Functional Organization Chart

From the functional organization chart it was deducted the transition table, like in Fig. 6.

The equations which result from the transition table are, (2).

$$y_{2,n+1} = S_1 + S_5$$

$$y_{1,n+1} = 0$$

$$y_{1,n+1} = S_2$$

$$INC = S_1 \cdot x_1 \cdot x_0 + S_2 \cdot \overline{x_1} + S_4 \cdot \overline{x_1} \cdot x_0 + S_5 \cdot \overline{x_1} \cdot \overline{x_0}$$

$$\overline{PL} = \overline{S_1 \cdot x_1 \cdot \overline{x_0} + S_2 \cdot \overline{x_1} \cdot x_0 + S_5 \cdot x_1 \cdot x_0}$$

$$\overline{RES} = \overline{S_1 \cdot \overline{x_1} + S_4 \cdot \overline{x_1} \cdot \overline{x_0}}$$

$$Z_1 = S_3$$

$$Z_0 = S_6 \qquad (2)$$

Present State	$X_1 X_0$	Next State	$Y_2Y_1Y_0$	Z_1Z_0	Operation	INC PL $\overline{RES}$
S_1	0- 10 11	S_1 S_4 S_2	--- 100 ---	00 00 00	Reset Load Increment	0 1 0 0 0 1 1 1 1
S_2	00 01 1-	S_3 S_1 S_2	--- 001 ---	00 00 00	Increment Load Reset	1 1 1 1 0 1 0 1 1
S_3	--	S_3	---	10	Hold	0 1 1
S_4	00 01 1-	S_1 S_5 S_4	--- --- ---	00 00 00	Reset Increment Hold	0 1 0 1 1 1 0 1 1
S_5	00 01 11	S_6 S_5 S_4	--- --- 100	01 00 00	Increment Hold Load	1 1 1 0 1 1 0 0 1
S_6	--	S_6	---	01	Hold	0 1 1

Fig.6. Transition table

The "golden model" implementation for the wired microsequencer is shown in Figure 6.

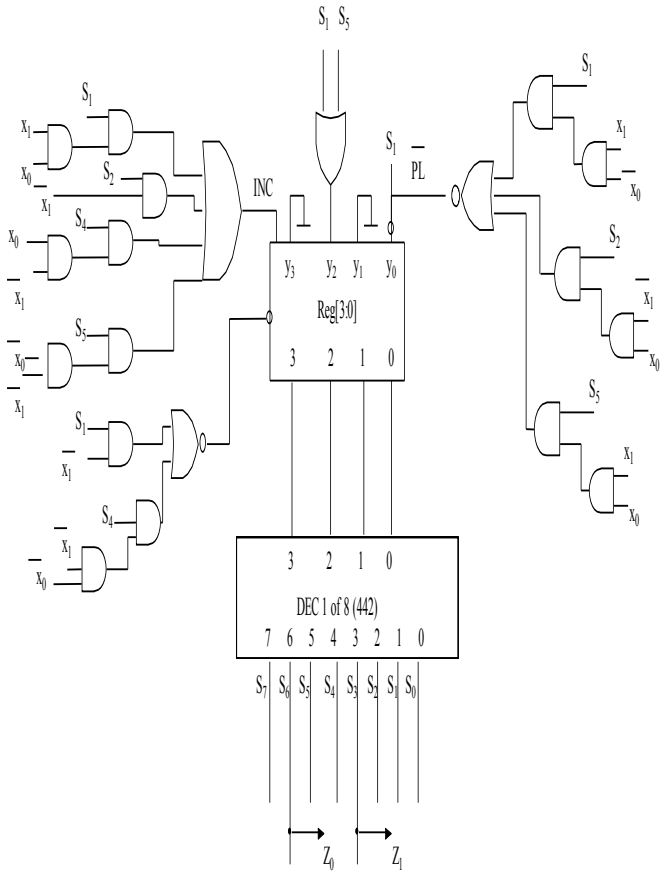

Fig.8. "Golden model" implementation for the wired microsequencer

In case of the Hardware Trojan is stealthy attached to the "Golden Model", Fig.9 shows the Trojan "Time-Bomb" triggering method: when the 8-bit upper counter reaches the full range value 0xFF(255) the output of the logic AND becomes 1 logic. It is logic XOR'ed with the original X_1 value and the payload "hijacked" output became X_{1p}. This moment represents the time when the "Time-Bomb" Trojan is activated. Since this signal is "corrupted", hence it will lead to malfunction of the hardware microsequencer logic system thus the Trojan is activated and can "harm" the entire digital system.

Based on the experimental model (this will be a future research article), it was observed that as much as the 8-bit counter clock signal is faster, that's how quickly the Hardware Trojan acts.

For example, 74HC590 is a 8bit counter which has a clock frequency of 21MHz for temperatures between -40 °C to +85 °C.

Considering the f=21MHz, the 8bit counter will reach the maximum count value at $7.56 \times 10^{10}\ 1/h$.

As can be observed, since the clock frequency is increased, the Hardware Trojan can be faster activated and if the clock frequency is decreased, the Hardware Trojan can be slower activated.

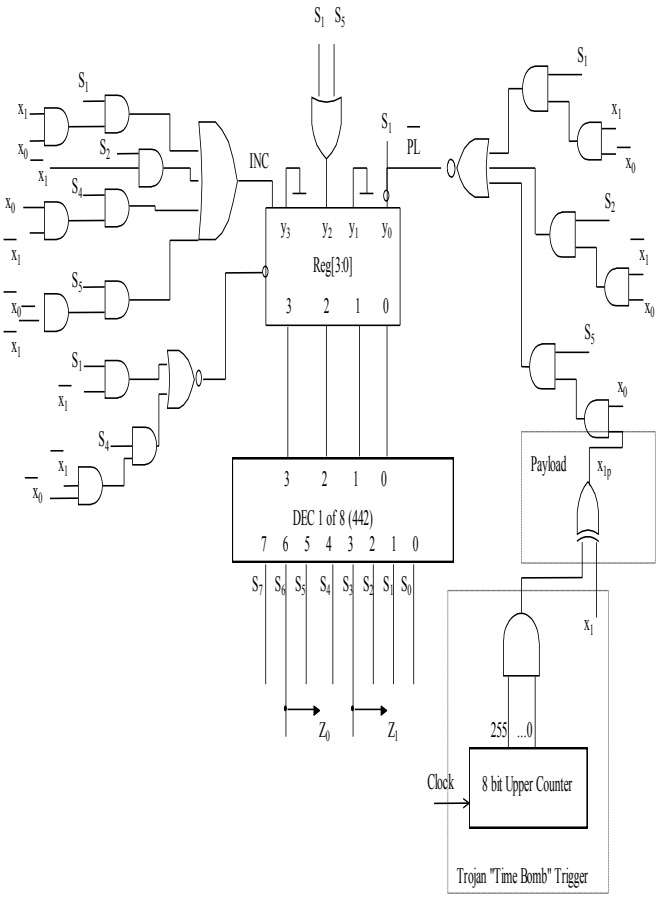

Fig.9. Trojan "Time Bomb Trigger" implementation in the wired hardware microsequencer

The described "Time-Bomb" Trojan triggering logic method can be replicated also on all the remaining input signals X_1, INC, PL, RES, hence the digital system can be fully "hijacked".

It can be observed that since the X_1, X_0, INC, PL, RES were hijacked by the "Time-Bomb" Trojan, the logic decoder (DEC) will decode wrong states rather than the "Golde Model" design. Thus, the digital system outputs Z_1,Z_0 are "Hijacked" so the values will not be the same as in the "Golden Model".

Since the proposed architecture is part of a digital semaphore system, the malfunction of it could lead to improper functional behavior hence the accidents rate is highly increased.

As an observation, the presented triggering method of the "Time-Bomb" Trojan can be applied on any digital system.

On the other hand, the Hardware Trojans detection method represents the subject of a future research paper.

3. Conclusion

In this paper there was presented a "Time-Bomb" Trojan triggering method for Hardware Trojans.
The assertion techniques of the Hardware Trojan have become a sensitive security concern for digital systems. Thus, the detection methods became a very challenging problem. By the nature of the "Hardware Trojan" it is designed to avoid detection since they usually run in "hidden" mode and are activated when certain conditions are fulfilled.
Regarding the detection of the triggering "Time-Bomb" Trojan there can be used a shadow-latch based on delay characterization techniques. This will be the subject for a future research paper.

Because of the varied nature of the Hardware Trojans, the detection of them became very challenging and it required a combination of techniques both during design and test in order to provide an acceptable level of security.
Another method to trigger "Time-Bomb" Trojans is by using an asynchronous counter or hybrid counter. These methods will be the subject for a future research paper.
A 100% detection of the Hardware Trojans seems to be impossible because of the diversity of the Hardware Trojans types. Major future challenges would include developing detection mechanisms for the digital and analog Trojans. which can implement various types of activation conditions. There are widen methods regarding the triggering modes which avoid the IC's testing procedures (eg. different combinations of the primary inputs).
This study can be combined with Artificial or Computational Intelligence and this will represent the subject for a future research paper.

References:

[1] Mohammad Tehranipoor and Farinaz Koushanfar, "A survey of hardware trojan taxonomy and detection", IEEE Design & Test of Computer, 27:10-25,2010.
[2] Rajat Subhra Chakraborty, Seetharam Narasimhan, Swarup Bhunia, "Hardware Trojan: Threats and Emerging Solutions", 978-1-4244-4823-4, 2009, IEEE.
[3] Zie Zhang; Feng Yuan; Lingxiao Wei; Zelong Sun; Qiang Xu "VeriTrust: Verification for hardware trust" 50th ACM/EDAC/IEEE Design Automation Conference (DAC), 29 May-7 June 2013, IEEE
[4]] Syed Kamran Haider, Chenglu Jin, Masab Ahmad, Devu Shila, Omer Khan, Marten van Dijk, "Advancing the State-of-the-Art in Hardware Trojans Detection", IEEE Transactions on Dependable and Secure Computing (Volume: 16, Issue: 1, Jan.-Feb. 1 2019).
[5] Matthew Hicks, Cynthia Sturton, David Wagner, "Defeating UCI: Building Stealthy and Malicious Hardware", Proceedings of the 2011 IEEE Symposium on Security & Privacy
[6] A. Waksman, Matthew Suozzo, S. Sethumadhavan, "FANCI: identification of stealthy malicious logic using boolean functional analysis", Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, Published 2013, IEEE
[7] Jie Zhang, Feng Yuan, Qiang Xu, "DeTrust: Defeating Hardware Trust Verification with Stealthy Implicitly-Triggered Hardware Trojans", CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications SecurityNovember 2014 Pages 153–166.
[8] Song Yao; Xiaoming Chen; Jie Zhang; Qiaoyi Liu; Jia Wang; Qiang Xu; Yu Wang; Huazhong Yang, "FASTrust: Feature analysis for third-party IP trust verification", Published in 2015 IEEE International Test Conference (ITC), 06-08 October 2015, DOI: 10.1109/TEST.2015.7342417
[9] Chee Hoo Kok; Chia Yee Ooi; Michiko Inoue, "Net Classification Based on Testability and Netlist Structural Features for Hardware Trojan Detection", Published in 2019 IEEE 28th Asian Test Symposium (ATS), 10-13 December 2019, DOI: 10.1109/ATS47505.2019.00020.
[10] ML Flottes, S Dupuis, PS Ba and abd B Rouzeyre, "On the limitations of logic testing for detecting Hardware Trojans Horses", International Conference on Design & Technology of Integrated Systems in Nanoscale Era IEEE,pp.1-5,2015.
[11] Yu Su; Haihua Shen; Renjie Lu; Yunying Ye, "A Stealthy Hardware Trojan Design and Corresponding Detection Method", Published in 2021 IEEE International Symposium on Circuits and Systems (ISCAS), 22-28 May 2021, DOI: 10.1109/ISCAS51556.2021.9401770
[12] W. Hu, L. Zhang, A. Ardeshiricham, J. Blackstone, B. Hou, Y. Tai, et al., "Why you should care about don't cares: Exploiting

internal don't care conditions for hardware Trojans", pp. 707-713, 2017.
[13] I. Exurville, L. Zussa, J.B. Rigaud and B. Robisson, "Resilient Hardware Trojans Detection based on Path Delay Measurement", In International Symposium on Hardware-Oriented Security and Trust (HOST'15), pp. 151–156, 2015.
[14] Ayush Jain; Ziqi Zhou; Ujjwal Guin, "Survey of Recent Developments for Hardware Trojan Detection", 2021 IEEE International Symposium on Circuits and Systems (ISCAS), 22-28 May 2021, DOI: 10.1109/ISCAS51556.2021.9401143, IEEE.
[15] I. Exurville, L. Zussa, J.B. Rigaud and B. Robisson, "Resilient Hardware Trojans Detection based on Path Delay Measurement", In International Symposium on Hardware-Oriented Security and Trust (HOST'15), pp. 151–156, 2015.
[16] Ovidiu Ursaru, Cristian Aghion, Mihai Lucanu, Liviu Tigaeru, "Pulse width Modulation Command Systems Used for the Optimization of Three Phase Inverters", Advances in Electrical and Computer Engineering Journal. Suceava, Romania, 2009, pag.22-27.
[17] M Tehranipoor, H. Salmani, X. Zhang, X. Wang, R. Karri, J. Rajendran and K. Rosenfeld, "Trustworthy Hardware: Trojan Detection and Design-for-Trust Challenges", In IEEE Computer, pp. 66–74, 2011.
[18] N. Jacob, D. Merli, J. Heiszl and G. Sigl, "Hardware Trojans: current challenges and approaches", in IET Computers & Digital Techniques, 8(6):264– 273, 2014.
[19] Farimah Farahmandi; Prabhat Mishra, "FSM Anomaly Detection Using Formal Analysis", Published in 2017 IEEE International Conference on Computer Design (ICCD), DOI: 10.1109/ICCD.2017.55
[20] Dejian Li, Qizhi Zhang, "Hardware Trojan Detection Using Effective Property-Checking Method", Electronics 2022, https://doi.org/10.3390/electronics11172649
[21]] Sophie Dupuis, Marie-Lise Flottes, Giorgio Di Natale and Bruno Rouzeyre, "Protection against Hardware Trojans with Logic Testing: Proposed Solutions and Challenges Ahead", DOI 10.1109/MDAT.2017.2766170, IEEE Design

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.