Understanding Cyber Technologies in a Physical Way

MILICA D. ĐEKIĆ, Subotica, Serbia
GYULA MESTER, Óbuda University, Budapest, Hungary

Professional Paper
UDC: 004.738:343.7
004.3:62-7
DOI: 10.5937/tehnika2105690D

In this paper, we would discuss a bit more how cyber technologies operate in a physical way and why it's important to understand the limitations of a physical reality. So commonly – mathematical terms would get assumed as abstract – so they could be considered as somehow perfect. On the other hand, the reality would offer many boundaries and obstacles that should be avoided or better explained. As it's known, cyber technologies belong to digital systems containing so many electronic components that would have their physical performances. Those performances as well as the entire cyber defense of such digital technologies would be analyzed deeper through this effort.

Key words: *cyber defense, intelligence, electronics, design, project, etc.*

1. THE CORRELATION BETWEEN CYBER DEFENSE AND DIGITAL TECHNOLOGIES

Cyber technologies would include computers, web and mobile systems commonly being correlated with the digital circuitries. As everyone would know – the computer and many networks would deal with the 0s and 1s making such electronics binary. In general, digital technologies would use the system of switching indicating that the state is 0 when a switch is normally opened or state is 1 when the switch is regularly closed. Those are how it works in a theory, but let's try to deal with the practice. The practice would invoke much nonlinearity which would make things a bit complicated. For instance, the voltage being linked with the 0 would have many disturbances and it would usually take the values between 0 and 2 V. On the other hands, the logical 1 would also get a noisy signal and oscillate within a range including 3 and 5 V [1-6].

So, that's how we would introduce digital systems being made from electronic components such as resistors, transistors, diodes, capacitors and much more. All these components are somehow reliable within the certain spectrum of physical variables. For instance, much military digital equipment could handle a very cold weather and also work properly at a quite hot climate condition. The main challenge with the digital systems is they could get infected with some malware which could put them into cycle or cause a thermal heat raising the voltage on. Practically, this would indicate that all systems dealing with 0s and 1s could potentially get vulnerable in cyber defense sense.

Many hackers would know this and they would try to exploit such vulnerabilities developing and using the sophisticated cyber weapons that would cause harm to digital system in hardware manner. The fact is that some skillfully prepared malicious codes could do a damage of hardware components simply putting the system into a repeating condition or increasing the voltage to those circuits [7-14], [19-23].

The quite good recommendation here could be that the circuitry should be better designed attempting to connect the entire system with the ground in case of electrical shock. Also, we would suggest that material science could make more researches trying to discover the materials which could take more extreme conditions. Also, the good correlation between cyber defense and digital systems could be that all digital systems are potentially hackable, so that's why it's so significant to protect them from cyber harm.

Finally, we would be aware that digital circuits would – in a practice – getcorrelated with the printed boards or some micro-chips and mainly created using silicon and applying the special techniques of packaging offering an opportunity to put more electronic components in a very small size of area. Luckily, silicon is still with the suitable price for a reason it could get easily available from sand in the deserts worldwide [1-18].

Author's address: Milica Đekić, Subotica, Vase Pelagića 39a
e-mail: milicadjekic82@gmail.com
Paper received: 27.09.2021.
Paper accepted: 05.10.2021.

2. HOW DIGITAL SYSTEMS CORRESPOND TO PHYSICAL REALITY

Digital systems are so abstract mainly corre-sponding to mathematics, rather than a physical world. They are so simple to get made for a reason of using lots of resistors, capacitors, diodes, transistors and many other similar electronic elements. In a mathematical script – it so common to deal with many 0s and 1s trying to describe a digital signal, but in a reality there would be a certain spectrum of voltages and currents which should get satisfied. As we said before, some electronic elements are more or less sensitive to a voltage rise. For instance, resistors and diodes are especially vulnerable if voltage goes high for the reason of their current – voltage characteristic curves suggesting that quite small voltages could cause a breakdown which means the current would go exponentially up like in the case of short circuit phenomenon [19-25]. Through this effort we intend to illustrate some digital circuit's examples in order to discuss better what their weaknesses could be. Such an example would be given in a Figure 1.

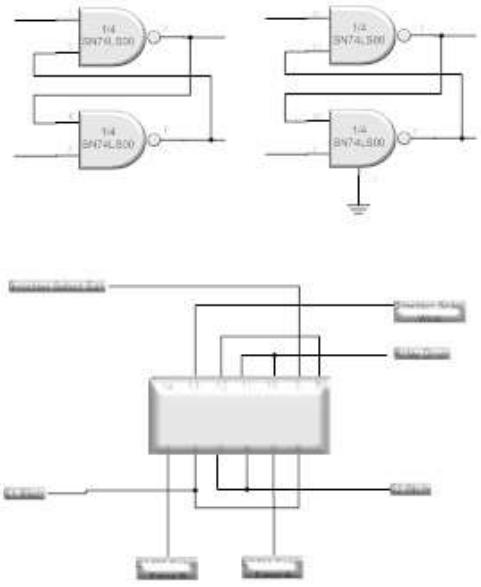

Figure 1 - The example of digital circuitry

As it's given in the Figure above – in digital electronics, we can deal with the logic gates being AND, OR, NOT, XOR and so on or with the integrated circuits (ICs) which could offer many connectors. The logic gates could be made out of diodes, resistors and transistors, while the ICs are something like chips using the special techniques of packaging on a small piece of area. In a practice, it's so important to do a good design of these circuits paying so much attention on security and safety of your work. Sometimes it's sufficient to connect your effort with the ground to make it safe and so commonly you would need to use the micro-relays to provide a certain level of security to the entire system. At the beginning, we would suggest that in case of the voltage increase – some sensitive elements such as resistors and especially diodes could suffer the thermal heat and simply deal as a short circuit to the entire printed board. The short circuit means that the current would get extremely high and – by Jules law – produce the big heat that would burn the entire element and cause hardware harm to that digital technology. Next, we would represent the SR flip-flop and explain some weaknesses of that memory's device [26-29]. The illustration is given in a Figure 2.

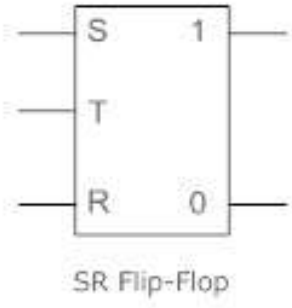

Figure 2 - The SR flip-flop

As it's known, the flip-flops are quite reliable memory elements that would operate in a stable manner in many cases. For instance, the SR latch would remember the state being brought to its entry and so successfully deal with the nearly all inputs. The case when this memory device may get confused is when a 1 is brought to the both inputs – set (S) and reset (R). In such a case, the output state would get undefined and the entire flip-flop would begin oscillating or, in other words – working in a quite unstable way. If such a memory element would get put in the repeating conditions making its inputs cause the instability at the output – the entire memory section would start oscillating and potentially some valuable data could be lost. The best way to protect such memory elements from harm could be to apply more secure methods of a board's design. Many experts would agree that hardware as well as software could be concerning from a perspective of the user's experience. Here, we have mentioned some hardware damages usually being so non-repairable and – in addition, we would mention that those sorts of concerns could easily be the consequence of skillfully prepared hacker's attacks which would cause a damage of the entire hardware simply putting a malware into a computer.

3. WHAT ARE THE LIMITATIONS OF CYBER TECHNOLOGIES?

Digital technologies on the paper and digital technologies in a reality could be somehow different.

Those on the paper would strongly rely on mathematics which would bring a certain level of perfection, while those in a reality would cope with a physical imperfection dealing with nonlinearities and many other limitations of the nature. The fact is our nature being so balanced and symmetric on a one side and so beautiful on another side is still quite limited and with lots of boundaries. Cyber technologies would like many technical systems get their warranties promising how long they can work, what they can take and how they can be fixed in case of damage. Also, cyber systems relying on digital technologies would easily get hacked, so it's significant to take care about their security from the both aspects – software and hardware. Many would describe mathematics as a God's science and our physical reality would be somehow similar to the projection of that science into a real world which would still have flaws putting aside all perfections that such an abstract creation of mind gave us [30-31].

Through this effort, we would mention that material science and engineering could play a big role into creating more superior digital systems. Simply, try to imagine a material with much better performances being used for a production of electronics pieces. As it's known, digital technologies would assume lots of electronics and use power supplies to their work. So interestingly, these systems would consume electricity to their operation and as everything working on electricity – they would deal with some sort of electromagnetic field being typical to electronics systems. For instance, for such a reason – it's not recommended to let electrical and electronic devices work during the thunderstorm because they could so easily attract the flesh and suffer their complete damage as well as put at risk people being close to them. Finally, cyber technologies are still so new with the history of the human kind and could illustrate some sort of the great technological revolution bringing us the both – good and bad things – to deal with.

4. DISCUSSIONS

The point of this paper would be to suggest how cyber defense could be correlated with the digital systems. As we would see through the previous sections, digital systems would so commonly use some sort of electricity source and deal with the current and voltage. That's how the binary digits being 0s and 1s would be represented – using the certain level of the voltage. If anyone amplifies such a voltage – many electronic elements could suffer the breakdown and the entire system could deal with the non-repairable damage. Also, there would be the risk of repeating condition that could put many memory devices into the undefined state. In total, it's all about the smart design and intelligent selection of materials which would be used to make a circuit. Finally, we would recommend that the ongoing science and technologies could go deeper and bring us many new advancements as well as progressive ideas and solutions.

5. CONCLUSIONS

The aim of this effort has been to provide a better perspective to cyber technologies as something having the strong basis in a reality. Hope we would motivate more researchers' community which would give its effort in finding answers to many questions. Above all, this effort could bring a good insight how cyber defense would be understanded in a practice – at a micro-level.

REFERENCES

[1] Cheng H, Ding Q, Overview of the Block Cipher, in Proc. Second International Conference on Instrumentation, Measurement, Computer, Communication and Control, Harbin, China, pp. 1628-1631, 2012.

[2] Geler J. *Designing and Developing 802.1 1n Wireless Networks*, Cisco Systems Inc., 2010.

[3] C.-W. Phan R, Umar Siddiqi M. A Framework for Describing Block Cipher Cryptanalysis, *IEEE Transactions on Computers*, 55(11):1402-1409, 2006.

[4] Stallings W. *Cryptography and Network Security: Principles and Practice*, Prentice-Hall, Inc., New Jersey, 1999.

[5] Ronald J. T, Widmer NS. *Digital Systems – Principles and Applications*, Prentice-Hall International, Inc., 1998.

[6] Zhang Y, Luo J, Hu H. *Wireless Mesh Networking: Architectures, Protocols and Standards*, Taylor & Francis Group, New York, 2007.

[7] Rodic A, Katic D, Mester Gy. Ambient Intelligent Robot-Sensor Networksfor Environmental-Surveillance and Remote Sensing, in Proc. of *the IEEE SISY*, pp. 39-44, 2009,

[8] Mester Gy. Obstacle avoidance and velocity control of mobile robots, in *Proc. 2008 6th International Symposium on Intelligent Systems and Informatics*, pp. 1-5, 2008.

[9] Mester Gy. Sensor-Based Control of Autonomous Wheeled Mobile Robots, *The IpsiBgD Transactions on Internet Research*, TIR, Vol. 6, No. 2, pp. 29-34, 2010.

[10] Mester Gy. Modeling of the Control Strategies of Wheeled Mobile Robots, in Proc. of *the Kandó Conference 2006*, pp. 1-3, Budapest, Hungary, January 12-13, 2006.

[11]Mester Gy. Obstacle - Slope Avoidance and Velocity Control of Wheeled Mobile Robots Using Fuzzy Reasoning, in Proc. of *the IEEE 13th International Conference on Intelligent Engineering Systems*, INES 2009, Barbados, pp. 245-249, 16-18.04.2009,

[12]Mester Gy. Novi trendovi naučne metrike, in Proc. of *the XXI Skup Trendovi Razvoja: "Univerzitet u Promenama..."*, TREND 2015, paper No. UP 1-3, pp. 23-30, Zlatibor, Serbia, 23-26.02.2015,

[13]Mester Gy. Backstepping Control for Hexa-Rotor Microcopter, *Acta Technica Corviniensis-Bulletin of Engineering*, Faculty Engineering Hunedoara, Vol. 8, No. 3, pp. 121-125, ISSN 1584-2665, July–September 2015.

[14]Mester Gy. *Modeling of Autonomous Hexa-Rotor Microcopter*, in Proc. of *(MechEdu 2015)*, pp. 88-91, ISBN 978-86-918815-0-4, Subotica, Serbia, May 14-16, 2015.

[15]Mester Gy, Rodic A. Navigation of an Autonomous Outdoor Quadrotor Helicopter, in Proc. of *the 2nd International Conference on Internet Society Technologies and Management ICIST*, ISBN 978-86-85525-10-0, pp. 259-262, Kopaonik, Serbia, 1-3.03.2012.

[16]Mester Gy. New Trends in Scientometrics, in Proc. of *the SIP 2015, 33nd International Conference Science in Practice*, pp. 22-27, Schweinfurt, Germany, 07-08.05.2015.

[17]Rodic A, Mester Gy. Control of a Quadrotor Flight, in *Proc. of the ICIST Conference*, pp. 61-66Kopaonik, Serbia, 03-06.03.2013.

[18]Mester Gy. Metode naučne metrike i rangiranja naučnih rezultata, in Proc. of *57th ETRAN Conference*, pp. RO3.5.1-3, Zlatibor, Serbia, 3-6.06.2013.

[19]Đekić M. D. Kako sačuvati kontinuitet u poslovanju uprkos cyber incidentima, *Tehnika*, Vol. 70, No. 2, pp. 346-349, 2015.

[20]Đekić M. D. Cyber procedure za poslovno okruženjeu Srbiji, *Tehnika*, Vol. 71, pp. 471-474, 2016.

[21]Đekić M. D. The Cloud's Computing Security, *Tehnika*, Vol. 73, No. 2, pp. 300-304, 2018.

[22]Đekić M. D. The Internet of Things Security, *Tehnika*, Vol. 72, No. 2, pp. 309-312, 2017.

[23]Đekić M. D. The Commerce Crime and Ways of Conducting a Financial Security, *Tehnika*, Vol. 71, No. 5, pp. 782-786, 2016.

[24]Đekić M. D. Cyber Procedures for a Business Environment in Serbia, *Tehnika*, Vol. 71, No. 3, pp. 471-474, 2016.

[25]Đekić M. D. The Internet of Things Cybersecurity Standardization, *Tehnika*, Vol. 74, No. 4, pp. 603-607, 2019.

[26]Đekić M. D. The Application of Marketing for Small and Medium-sized Enterprises Competiveness Risein the Republic of Serbia, *Tehnika*, Vol. 72, No. 4, pp. 587-590, 2017.

[27]Đekić M. D. A Smart Configuration of Computer asa Prevention from Hacking and Cyber Espionage, *Tehnika*, Vol. 71, No. 5, pp. 761-764, 2016.

[28]Đekić M. D. How to Create Training for the IT Industry's Staffs?, *Tehnika*, Vol. 71, No. 4, pp. 644-647, 2016.

[29]Đekić M. D. *How to Maintain a Business ContinuityDespite Cyber Incidents*? Tehnika, Vol. 70, No. 2, pp. 346-349, 2015.

[30]Đekić MD. The Use of Video Detection as aFunction of Traffic Safety, *Tehnika*, Vol. 66, No. 3, pp. 471-475, 2011.

[31]Đekić M. D. How a modern business could respondto the Phishing Attack Challenges, *Tehnika*, Vol. 72, No. 3, pp. 455-459, 2017

REZIME

RAZUMEVANJE NOVIH TEHNOLOGIJA U FIZIČKOM SMISLU

U ovom radu bismo prodiskutovali kako nove tehnologije rade u fizičkom smislu i zbog čega je važno razumeti njihova ograničenja u fizičkoj stvarnosti. Vrlo često matematički pojmovi se uzimaju kao apstraktni, te stoga njih razmatramo kao savršene. S druge strane, stvarnost nudi mnogo granica i prepreka koje je potrebno zaobići ili bolje objasniti. Kao što je poznato, nove tehnologije podpadaju pod digitalne sisteme koji sadrže elektronske komponente sa sopstvenim fizičkim performansama. Te performanse kao i celokupna visokotehnološka bezbednost će biti dublje analizirani u ovom doprinosu.

Ključne reči: *visokotehnološka bezbednost, saznanje, elektronika, projektovanje, projekat*