Turkish Journal of Computer and Mathematics Education
DOI: https://doi.org/10.17762/turcomat.v9i3.13912 *Vol.09 No.03 (2018), 1205-1211*

Research Article

Methods of Functional Safety Analysis for Cyber Physical Systems Integrated Circuits

Umang Garg

Asst. Professor, Department of CSE (Computer sc)

GEHU-Dehradun Campus

Abstract: Integrated circuits (ICs) are used in a wide variety of real-world systems. Interacting ICs (also known as cyber-physical systems or hybrid systems) with physical systems is a common component of many real-world systems used for safety-critical applications. Potentially catastrophic results from even a minor breakdown in any component of the system need cautious deliberation before any action is performed. Safety analysis of integrated circuits is becoming more important as a growing number of systems depend on ICs to meet the functional requirements of safety-critical applications. There has been a shift away from the old method of creating cyber-physical systems, whereby both the digital and physical elements were created separately. In this work, we compile a variety of approaches for efficiently and affordably satisfying functional safety standards at the level of the application.

Keywords: Integrated Circuits (ICs), cyber physical systems, hybrid systems,

Introduction

Improvements in semiconductor technology have resulted in smaller transistors that utilise less power. This has paved the way for further integration of functions inside a single IC. As we go to more advanced technological nodes, the factors that help reduce transistor size and power expenditure also have an adverse influence on dependability. Age increases the likelihood of negative biases temperatures instability (NBTI), hot carrier injection (HCI), and particle-induced single event upsets (SEU) [1, 2]. The biggest risk to the reliable operation of ICs is posed by random failures produced by atmospheric particle impacts, which are only one of several failure sources. While low-cost techniques for random failures are still under development, risk from lifetime failures may be minimised via the application of systematic design approaches [3]. The increased failure rate of ICs is complicated by the difficulty of assessing their potential failure processes [4]. Because their failure processes are predictable and readily investigated, electronic components of today are gradually replacing their mechanical predecessors. The intricacy of current IC design, fabrication, and operation, however, necessitates a far more strict approach. When comparing a mechanical steering system to a steer-by-wire system [5], failure situations in the mechanical system may include complete loss of steering control or insufficient steering. While mechanical steering doesn't have this risk, a bit flip in the IC might cause the opposite direction to be taken by a steer-by-wire system. Due to the complexity of evaluating failure situations and the ever-decreasing size of technological nodes, it is essential to keep the effectiveness, space, and operational overheads enforced for safety functions to a minimum. Therefore, we must reconsider IC safety evaluations along various axes, such as cheaper protective circuit components [6], improved design techniques [7], and improved architectural approaches [8].

Evolution of Functional Safety System

Technology advancements have led to smaller, quicker, and more power-efficient transistors, allowing for higher levels of integration. Driven by Moore's law [9] and Dennard's scaling rule [10], the number of transistors in ICs has expanded dramatically. The development of System-on-Chip (SoC) designs [11,12] represents a significant change in the IC design paradigm. As a result, designers were able to save time and money by incorporating many formerly separate components into a single IC. Improvements in these systems have led to a larger firmware / software footprint [13]. Since these ICs have been used in the development of

machine learning and AI, the field has grown in complexity [14,15,16,17]. Initially, transportation, industrial plants, space, and medical systems were thought to be at the most risk for IC failures owing to faults. The failure rate and the use of integrated circuits (ICs) to replace mechanical components have made it necessary for even consumers to understand functional safety criteria for electronic products.

Functional Safety Concerns of Integrated Circuits

Traditional approaches to meeting functional safety standards have relied on redundancy mechanisms. As indicated in Figure 1, redundancy-based control designs [18,19,20] were developed to allay worries in such systems. Examples include 1oo2 (1-out-of-2), 2oo3 (2-out-of-3), etc. Architectures based on redundancy provide considerable extra work during implementation. The higher price tag for functional safety was less of a problem in the past since the scope of system deployment was less than it is now. In recent years, there has been a greater need to impart functional safety with decreased design overheads due to the increased expense paid in building such redundant systems due to their widespread deployment across a variety of applications. Functional safety analysis methodologies are growing more intricate since they rely on the architecture and application in lieu of redundancy. For this, you'll need to do a thorough study of the circuit, learn how the system would react to the loss of each flip-flop and logic gate, and then implement measures to make it more resilient.

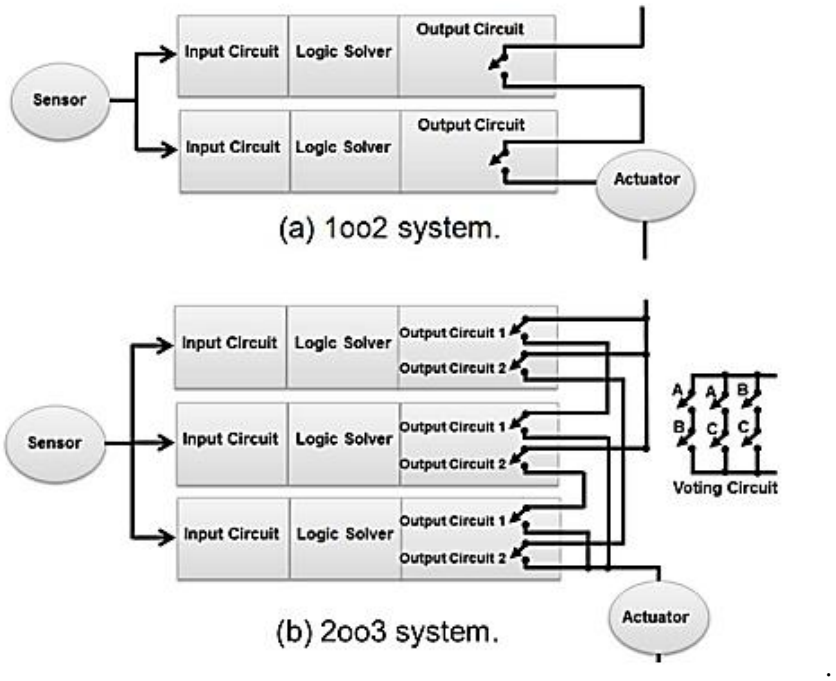

Figure 1. Representative fault tolerant systems.

It became increasingly challenging to conduct a full study of failure modes using traditional methods like Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA) as ICs grew in size and complexity. This problem is shown by a number of functional safety issues, such as the ones involving Toyota's unexpected acceleration recalls and Ford's inadvertent gear change related recalls, both of which involved automobiles. As more and more systems become autonomous and can make choices for themselves based on a given set of parameters, the need of a thorough safety analysis has become paramount. The functional safety analysis approaches now in use have shortcomings, as shown by recent mishaps involving Uber and Tesla. Different functional safety standards developed to mitigate risks by providing appropriate criteria and methods as functional safety became relevant to various end applications. Safety requirements of electrical, electronic, and programmable electronic safety related systems are addressed, for instance, in IEC 61508. All other functional

safety criteria are built upon this one. ISO 26262 is a modification of IEC 61508 intended for use in automobile E&E systems. The concerns of avionics' functional safety are addressed in DO178. Since the need for security is not uniform across applications, different functional safety criteria must be applied to various final systems..

Literature Review

Sylvain Frey et.al(2016) The security of cyber-physical systems (CPS) is becoming more important as CPS become more integrated into daily life. In this research, we report findings from an exploratory analysis of past security events in order to assess such aspects for one subset of CPS: industrial control systems (ICS). Our research questions the common practise of assigning responsibility to human error or offering oversimplified explanations for the many factors that might contribute to a security breach. We point out that (i) perception mistakes are critical in these kinds of occurrences and (ii) latent design factors, such as incorrect specifications of a system's boundaries and capabilities, play a crucial role in moulding perceptions and causing security problems. For ICS, whose lifespan is often measured in decades, such design-time concerns are especially crucial. We use this research to talk about the potential difficulties in fixing hidden design problems in future smart CPS used in such industrial contexts.

László Horváth et.al(2016) Through the information content (IC) driving of product representation and cyber CPS unit entities, this study presents a unique idea and technique for active knowledge support for the aforementioned goals of product model. Former definitions of IC referred to it as "deliberately organised and personalised knowledge" used in the context of making product-related decisions. Active information content (AIC) structure for enabling CPS in IC and multilayer transfer structure for linking AIC to different structured IP environments are the main contributions of the described study.

Yong Peng et.al (2015) Industrial control systems (ICS) are Cyber-actual Systems (CPS) that have direct impacts on the actual environment, which is the main distinction between IT and ICS. Cyber-Physical assaults are the term used in this study to refer to cyber assaults that have the potential to cause physical harm.

Jui-Hung Chien et.al (2015) In this research, we investigate the testing procedure used throughout the stacked-die manufacturing process. We go through the issues with the conventional testing method. In this study, we propose a cyber physical system (CPS) for evaluating pre-bond interposers without physical interaction in order to increase manufacturing yield. An infrared camera and a heated laser are the centrepieces of the testing setup we suggest.

Formal Verification Based Approach for Accurate Safety Analysis

The analysis may be done independently on each module after the application tolerance has been distributed across them. The reliability of a circuit module for usage in mission-critical systems may be measured with the use of fault injection. Since application-specific tolerance is not systematically accounted for in the current fault injection techniques utilised in the IC sector, negative assessments are made. The workloads utilised for fault injection often cover just a small sample of the functional situations (conditions and states), hence the assessment is not comprehensive. There is currently no solution to the open challenge of ensuring the workloads utilised in fault injection based safety assessment are sufficient. Recent publications have also drawn attention to other limitations of fault injection-based approaches in practise. An alternative to fault-injection simulation approaches is formal verification, which has been offered in the literature. However, they also come with additional difficulties, such as the time-consuming need of modelling the whole range of system attributes, and the lack of application-related input limitations, both of which lead to the designation of almost all parts as crucial. Because of the complexity of real-world systems, it may be difficult to determine whether individual parts are benign or harmful. This is due to the fact that the analytical accuracy relies on the performance variations which may be allowed under varied usage / application settings, and the physical components (which are fundamentally analogue in nature) must be included in these systems. In this chapter, we suggest innovative techniques for assessing the security of such systems. Key innovations include (i) modelling input restrictions

(values and sequences) as a function of the variety of applications. (ii) Simulating an output variation over time, depending on certain application-specific limits. (iii) This analytical framework is more precise and less pessimistic than is attainable with current approaches due to the use of formal techniques. Two industrial circuits and the ITC benchmark circuits were used for this investigation.

Improved Safety Analysis Framework

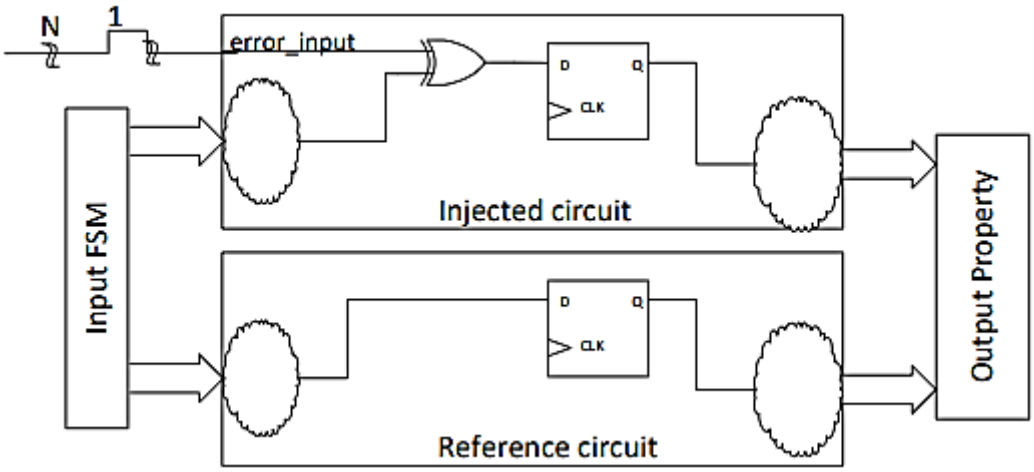

Figure 2. Illustration of FV based safety analysis.

The proposed safety evaluation method is shown in Figure 2. To ensure there is always a working circuit, it has been duplicated. A defect may be induced into the system by reversing the input of each flip-flop. To do this, we use Ex-Or logic on the flip-flops' inputs, designating one as the "main" input and the other as the "error" input. As many flip-flops as there are error input ports.

Safety Analysis of Benchmark Circuits

Circuit	#flip-flops	Tolerance = ±2			Tolerance = ±4		
		#safe FF	% Savings	Time (S)	#safe FF	% Savings	Time (S)
b03	30	7	23.33	53	12	40.00	56
b04	66	4	6.06	192	6	9.09	182
b08	21	4	19.05	33	6	28.57	32
b10	17	2	11.76	36	3	17.65	31
b11	31	3	9.68	64	4	12.90	69
Average			13.98			21.64	

Table 1. Safety analysis of benchmark circuits.

When putting the proposed design through its initial round of testing, a variety of ITC benchmark circuits [99] are employed. When calculating the output values, acceptability intervals of 2 and 4 are taken into consideration. The tolerance values for the reference circuits are shown here in spite of the fact that these values have no influence on the actual performance of the circuits; this is done to highlight the usefulness of the approach that has been described. We can determine how many flip-flops are dependable in spite of the fact that these mistakes may occur thanks to this method. The number of flip-flops that can be saved may be calculated

by contrasting the quantity of secure flip-flops obtained in this manner with the whole quantity of flip-flops that are now in operation. (This demonstrates that these flip-flops do not compromise comfort in order to achieve a higher level of safety). The results of five different ITC benchmark circuits are shown in Table 1. The proportion of flip-flops that were deemed safe and the amount of time it took to evaluate the whole circuit are both shown for each of the two criteria of output value tolerance provided here: 2 and 4 over the right output.

Fault Injection Workload Analysis

Analysing the circuit's behaviour in the presence of faults and checking whether the built-in protection mechanisms can identify them are both part of the fault injection based functional safety study procedure. The completeness of the study is heavily dependent on the selection of workloads used for safety assessment. Workloads are chosen without it based on toggle coverage [22]. An upper limit (e.g. 70%, 90%, 99%) on this coverage must be specified depending on circuit size and simulation duration for practical reasons.

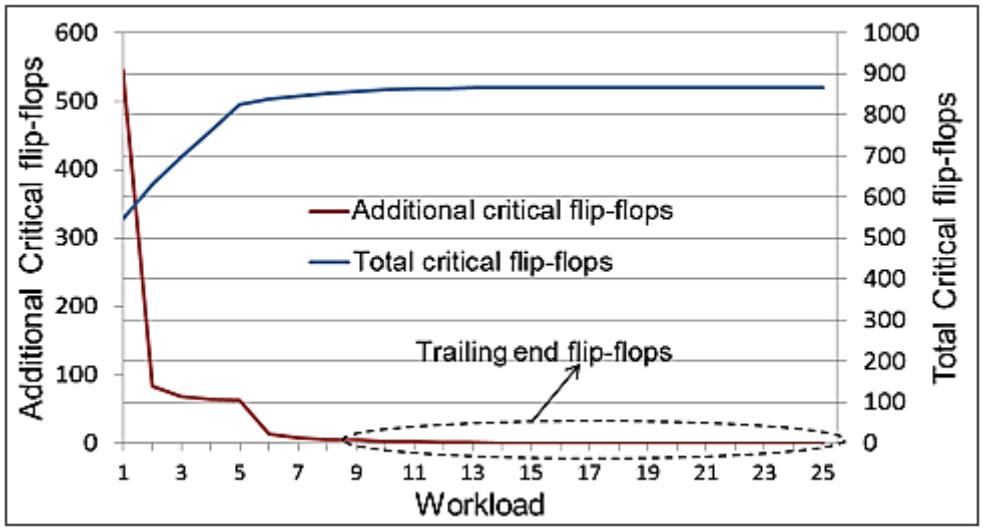

Figure 3The total number of significant flip-flops that are determined as being unique for each task.

We have evaluated the safety of a sample module under 25 distinct workloads that meet the toggle coverage criterion in order to have a better grasp of the situation. The results are shown in Figure 3 below. The Y-axis shows the total number of distinct flip-flops that were deemed essential across all workloads, while the X-axis represents the total number of workloads. The number of significant flip-flops found reaches a maximum somewhere around the tenth workload and then steadily decreases with each successive task. These flip-flops are known as "trailing end" flip-flops. We cannot be certain that all crucial flip-flops at the tail end are found in a typical analysis. In this paper, we provide a cheap method of detecting these lagging-end flip-flops.

Conclusion

In this research, we argue that a functional safety assessment is best conducted using a workload augmentation technique that relies on perturbations. Several experiments on safety-essential control functions and an inverter application were performed to prove that the proposed strategy is successful in identifying extra crucial flip-flops. The required number of flip-flops has been found to be between 12 and 26% higher. Our results show that, with certain adjustments to safety assessment methods and application-level tolerance, it is possible to meet the overall hardware overhead and reliability standards, despite the additional load. In this way, we may meet the criteria without lowering the bar on quality. These findings contribute to the growing body of data

supporting the suggested perturbation approach for discovering additional flip-flops of vital consequence with manageable analytical complexity and little overhead expenditures.

References

1. S. Frey, A. Rashid, A. Zanutto, J. Busby and K. Follis, "On the Role of Latent Design Conditions in Cyber-Physical Systems Security," *2016 IEEE/ACM 2nd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, Austin, TX, USA, 2016, pp. 43-46, doi: 10.1145/2897035.2897036.
2. L. Horváth, "Intelligent property support for cyber-physical product system modeling," *IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, Beijing, China, 2017, pp. 3474-3479, doi: 10.1109/IECON.2017.8216588.
3. Y. Peng *et al*., "Cyber-Physical Attack-Oriented Industrial Control Systems (ICS) Modeling, Analysis and Experiment Environment," *2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, Adelaide, SA, Australia, 2015, pp. 322-326, doi: 10.1109/IIH-MSP.2015.110.
4. Jui-Hung Chien, Nien-Tzu Chang, Chia-Hung Huang, Shih-Chieh Chang and Wei Han Wang, "Cyber physical system (CPS) for contactless IC testing," *2015 10th International Microsystems, Packaging, Assembly and Circuits Technology Conference (IMPACT)*, Taipei, 2015, pp. 340-343, doi: 10.1109/IMPACT.2015.7365222.
5. D. Lorenz, G. Georgakos, and U. Schlichtmann, "Aging analysis of circuit timing considering NBTI and HCI," in International On-Line Testing Symposium, 2009.
6. R. C. Baumann, "Radiation induced soft errors in advanced semiconductor technologies," IEEE Transactions on Device and Materials Reliability, 2005. [3] M. Alam, "Reliability and process variation aware design of integrated circuits," Journal for Microelectronics Reliability, Elsevier, 2008.
7. R. Mariani and G. Boschi, "A systematic approach for failure modes and effects analysis of system-on-chips," in International On-Line Testing Symposium, 2007.
8. R. Isermann, R. Schwarz, and S. Stolzl, "Fault-tolerant drive-by-wire systems," IEEE Control Systems, 2002.
9. T. Calin, M. Nicolaidis, and R. Velazco, "Upset hardened memory design for submicron cmos technology," IEEE Transactions on Nuclear Science, 1996.
10. V. Prasanth, V. Singh, and R. Parekhji, "Derating based hardware optimisations in soft error tolerant designs," in VLSI Test Symposium, 2012.
11. P. Subramanyan, V. Singh, K. K. Saluja, and E. Larsson, "Multiplexed redundant execution: A technique for efficient fault tolerance in chip multiprocessors," in Design, Automation & Test in Europe, 2010.
12. R. R. Schaller, "Moore's law: past, present and future," IEEE spectrum, 1997.
13. R. H. Dennard, F. H. Gaensslen, V. L. Rideout, E. Bassous, and A. R. LeBlanc, "Design of ion-implanted MOSFET's with very small physical dimensions," IEEE Journal of Solid-State Circuits, 1974.
14. R. Saleh, S. Wilton, S. Mirabbasi, A. Hu, M. Greenstreet, G. Lemieux, P. P. Pande, C. Grecu, and A. Ivanov, "System-on-chip: Reuse and integration," Proceedings of the IEEE, 2006.
15. W. Wolf, A. A. Jerraya, and G. Martin, "Multiprocessor system-on-chip technology," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2008
16. D. Edenfeld, A. B. Kahng, M. Rodgers, and Y. Zorian, "2003 technology roadmap for semiconductors," Computer, 2004.
17. K. Ovtcharov, O. Ruwase, J.-Y. Kim, J. Fowers, K. Strauss, and E. S. Chung, "Accelerating deep convolutional neural networks using specialized hardware," Microsoft Research Whitepaper, 2015.

18. Y. Shen, N. C. Harris, S. Skirlo, M. Prabhu, T. Baehr-Jones, M. Hochberg, X. Sun, S. Zhao, H. Larochelle, D. Englund et al., "Deep learning with coherent nanophotonic circuits," Nature Photonics, 2017.
19. S.-C. Lin, Y. Zhang, C.-H. Hsu, M. Skach, M. E. Haque, L. Tang, and J. Mars, "The architectural implications of autonomous driving: Constraints and acceleration," in ACM SIGPLAN, 2018.
20. S. Liu, J. Tang, Z. Zhang, and J.-L. Gaudiot, "Computer architectures for autonomous driving," Computer, 2017.
21. A. Hayek and J. Börcsök, "Safety chips in light of the standard IEC 61508: survey and analysis," in International Symposium on Fundamentals of Electrical Engineering, 2014.
22. E. Ugljesa and J. Börcsök, "Evaluation of sophisticated hardware architectures for safety applications," in International Symposium on Information, Communication and Automation Technologies, 2009.
23. W. M. Goble and H. Cheddie, Safety Instrumented Systems verification: practical probabilistic calculations. ISA, 2004.
24. D. H. Stamatis, Failure mode and effect analysis: FMEA from theory to execution. ASQ Quality Press, 2003
25. R. Mariani, G. Boschi, and F. Colucci, "Using an innovative SoC-level FMEA methodology to design in compliance with IEC61508," 2007
26. K. Kalaignanam, T. Kushwaha, and M. Eilert, "The impact of product recalls on future product reliability and future accidents: Evidence from the automobile industry," Journal of Marketing, 2013.
27. M. Ebrahimi, A. Evans, M. B. Tahoori, R. Seyyedi, E. Costenaro, and D. Alexandrescu, "Comprehensive analysis of alpha and neutron particle-induced soft errors in an embedded processor at nanoscales," in Design, Automation & Test in Europe, 2014