Prognostics and Secure Health Management of Electronic Systems in a Zero-Trust Environment

Varun Khemani[1], Michael H. Azarian[2], and Michael G. Pecht[3]

[1,2,3]*Center for Advanced Life Cycle Engineering (CALCE), University of Maryland, College Park, MD, 20740, USA*

vkheman@umd.edu
mazarian@umd.edu
pecht@umd.edu

ABSTRACT

Prognostics and health management (PHM) is a multifaceted discipline for the assessment of product degradation and reliability. PHM techniques have been used to detect naturally occurring faults and predict their impact on the system lifetime. An interesting question is whether these techniques could be used to detect faults that are maliciously induced. Maliciously induced faults could be due to hardware threats; e.g., electronic products that are recycled, remarked, defective, cloned, or tampered (through insertion of hardware trojans), which cause undesired system behavior such as information leakage, functional failure, and maliciously induced aging. The concern is that increased outsourcing in the fabrication of electronic products has made them susceptible to the insertion of hardware threats in untrusted manufacturing facilities. This paper overviews the need to implement PHM to ensure hardware security and how the PHM community can adapt its research to ensure safe, reliable, and secure operation of systems.

1. INTRODUCTION

The electronic systems that are critical to infrastructure, defense, and essentially every aspect of our daily life, are comprised of increasingly sophisticated circuits (Villasenor, 2011). Due to today's global economy and specialization in the semiconductor industry, a vast majority of these circuits are designed and manufactured in overseas manufacturing facilities that are often untrusted. A consequence of this is a faster time to market along with lower prices for the electronic products resulting in our prevalent consumer culture. However, the electronic supply chain globalization has come at the cost of a more complex production cycle with security vulnerabilities. The electronics ecosystem (i.e., everyone from the circuit designers to the end users), operate on the assumption that the circuits at the core of these electronic systems are secure. System trust is contingent on the absence of hardware threats, like counterfeits, which include chips that are recycled, remarked, defective, cloned, or tampered (through insertion of hardware trojans (HT)). In many cases, hardware threats are more destructive than software ones as they cannot be remedied by a software patch and are difficult to remove

Counterfeiting is an illegal practice involving passing off fraudulent copies of products as original ones for profit. A counterfeit circuit contains material, characteristics or performance inconsistencies with respect to its original circuit (Rahman et al., 2016), which might lead to degraded quality, reliability, and performance. The losses due to counterfeit circuits alone accounted for more than 25% of the counterfeit market in 2015 (Oriero & Hasan, 2019). Outsourcing to foundries that are untrusted is the main cause of counterfeiting; however, there is no standardized technique to adequately detect counterfeit circuits. Counterfeiting is carried out by both adversaries with limited manufacturing capacity (repackaging or recycling an inferior/older part as a new one) or sophisticated manufacturing capacity (tampering through HT insertion). Counterfeiting techniques that do not require sophisticated manufacturing capabilities rely on profitability through the supply of cheaper alternatives compared to the original circuit. Counterfeiting techniques that require sophisticated manufacturing capabilities for IC tampering introduce HTs into circuits that can result in altering or disabling functionality, leaking sensitive user information, or accelerated aging. For example, tampered ICs resulted in a warning failure against missile strikes for a Syrian radar system (Mitra et al., 2015) in 2007. The New York Times, in 2017, reported about the US National Security Agency (NSA) Quantum program that directly implanted HT circuitry through USB ports, and was able to acquire secret data from its adversaries all over the world. Hence, counterfeiting has started to involve both untrusted manufacturing facilities and state actors leading to worries

that more sophisticated counterfeiting will be prevalent in the future (Bhasin & Regazzoni, 2015).

The Integrity and Reliability of Integrated Circuits (IRIS) program (Bernstein, 2011) was initiated by DARPA to develop countermeasures against counterfeit electronics in U.S. cybersecurity and weapons systems. Similar programs have been initiated in Europe and in China, too (H. Li et al., 2016). The Trusted Foundry Program (Carlson, 2005) was set up to secure the manufacturing infrastructure for fabrication facilities providing microelectronics hardware to the U.S. military. It was founded in 2004 to ensure access to cutting-edge ICs from secure, domestic sources for safety-critical and mission-critical national defense systems. The program includes not only foundry capability but also all the services employed during the electronics lifecycle (design, prototyping, packaging, and assembly, etc.). The program enabled the creation of a list of trusted suppliers by providing accreditation criteria for suppliers for both cutting-edge and legacy parts. However, manufacturing at trusted foundries is expensive and financially infeasible for most commercial applications (Karabacak et al., 2018). Additionally, the U.S. military accounts for only 2% of the world's microelectronics consumption and hence has been unable to provide an adequate business case to foundries to provide secure foundry capacity (Harper, 2020). Reliance on the trusted foundry program could also be a disadvantage as secure technologies available currently (14 nm or greater) are generations behind state-of-the-art (5 nm) (Lapedus, 2018). As a result, there is a push to move away from trusted foundries and instead move towards production in zero-trust environments (Harper, 2020). Zero-Trust Architecture originally referred to a means of ensuring information and network security by eliminating the notion of trust. Instead of giving users complete access to the network, a zero-trust approach compartmentalizes data on a need-to-know basis that requires additional levels of authentication, such as onetime access codes and hardware devices, for a user to access more sensitive data (Rose et al., 2019). To address hardware security, the Zero-Trust framework needs to be extended and modified to prevent tampered circuits (infected with HT) from making it into field usage.

Hardware trojan (HT) threats can be introduced during design, fabrication, testing, and even usage of electronics; i.e., the entire semiconductor life cycle. They can be unintentional (unintended design flaws (Szefer, 2019), (Schellenberg et al., 2018)) or intentional (intended malicious design modifications (Yang et al., 2016), (Liu et al., 2017)). Through the combination of pre-silicon verification and post-silicon testing, any undesired IC modification should be possible to detect ideally. However, verification and testing require the presence of a golden model of the circuit; i.e., a circuit that is known to be free of any intentional or unintentional design modifications. Such a golden circuit might not always be available. Additionally, exhaustive verification might be a feasible option for large IC designs. During post-silicon testing, verification takes place through logic testing or reverse engineering. Logic testing involves exposing circuits to test vectors to detect manufacturing faults, but these test vectors rarely can detect HTs because HTs are designed to be stealthy and rarely triggered. Logic testing also involves comparison to a golden model. In reverse engineering, design verification occurs through destructive de-packaging. Although, it allows for more thorough HT detection, it is not scalable. Since HT detection is not always possible before circuit usage, runtime monitoring techniques have been explored; however, these techniques require extra circuitry. Hence, HT detection is a trade-off between detection effectiveness and the cost required to do so. The reader can refer to surveys (Lyu & Mishra, 2018), (Bhunia et al., 2014), for a more comprehensive review of HTs and their detection.

Prognostics and health management (PHM) is a comprehensive approach for the assessment of product reliability (Pecht & Kang, 2018). The goal of PHM is the protection of product integrity such that unanticipated problems that lead to performance degradation are avoided. Prognostics involves assessment of a system's fault progression given its operating conditions such that its lifetime; i.e., remaining useful life (RUL) can be estimated. Health management involves using the information gleaned from the prognosis stage to make decisions that minimize the system's downtime and cost of operation through scheduling of maintenance or replacement actions. PHM techniques have been used to detect naturally occurring faults and predict their impact on the system lifetime. An interesting question is whether these techniques could be used to detect faults that are maliciously induced through insertion of hardware threats.

An attempt to answer this question has been made in this paper by highlighting out the intersection of the approaches used for PHM and those used for detecting hardware threats. We also propose a framework called Prognostics and Secure Health Management (PSHM) that can be used for the simultaneous detection of naturally occurring and maliciously induced faults. Shortcomings of the PSHM framework are identified, thereby setting up further research avenues for the PHM community. The rest of the paper is organized as follows. Section 2 we elaborate on the hardware threats. Section 3 is related to the countermeasures against hardware threats and their intersection with methods used in PHM. In section 4, we bring them together to propose the PSHM approach. The conclusions follow in section 5.

2. HARDWARE THREATS

Counterfeiting is mainly achieved by attackers having limited manufacturing capacity that exploit supply chain loopholes. Aforementioned reasons lead to categorization of the counterfeiting techniques as follows (Azarian, 2018): Recycled, Relabeled and Repackaged, Illegal Manufacturing,

Low-spec components, Cloning/Reverse Engineering, Forgery and Structural Modification.

a) Recycled: As the most common form of counterfeiting, recycled ICs are reclaimed or recovered by the original component manufacturer from a used system and are then misrepresented as new. As a result, they have shorter lifespan and exhibit lower performance compared to the authentic parts. Recycling involves forced removal of components from PCBs under very high temperatures (Guin et al., 2014) followed by washing, sanding, repackaging, and remarking. This process can introduce defects and even cause complete nonfunctionally because of exposure to extreme conditions.

b) Relabeled and Repackaged: Relabeled ICs involve removal of the old marking on the package and relabeling forged information, involving sanding, painting, and other harmful processes. This is done to pass off a low-grade component as a higher grade one.

c) Illegal Manufacturing: Illegal manufacturing occurs when an external foundry builds more ICs than their contractual obligation and sells the excess for illegal profit.

d) Low-spec components: This involves replacing of part numbers from low-spec components with the part numbers of high-spec parts or mixing lower-quality pieces in with higher-quality ones.

e) Cloning/Reverse Engineering: Cloned ICs are produced through overproduction by producing illegal copies or IC reverse engineering. Reverse engineering has become a viable option because of the availability of probing and testing technologies.

f) Forgery: Fabricated ICs are shipped with documentations containing misrepresentations, for example, specification, testing, conformance certificates etc.

g) Structural Modification: IC Tampering involves structural modification for insertion of HTs. This requires advanced knowledge of circuitry and insertion capabilities. This provides the adversary with opportunities to cause system failure, leak secret information or accelerate aging. Since these structural modifications take many forms, researchers have developed various taxonomies for them.

A taxonomy for HTs was developed (Wang et al., 2008) according to their physical, activation, and action characteristics as shown in Figure 1. The physical characteristics category describes the various physical properties like, distribution, structure, size, and type. The structure category refers to instances where the adversary is forced to change the layout of some or all existing

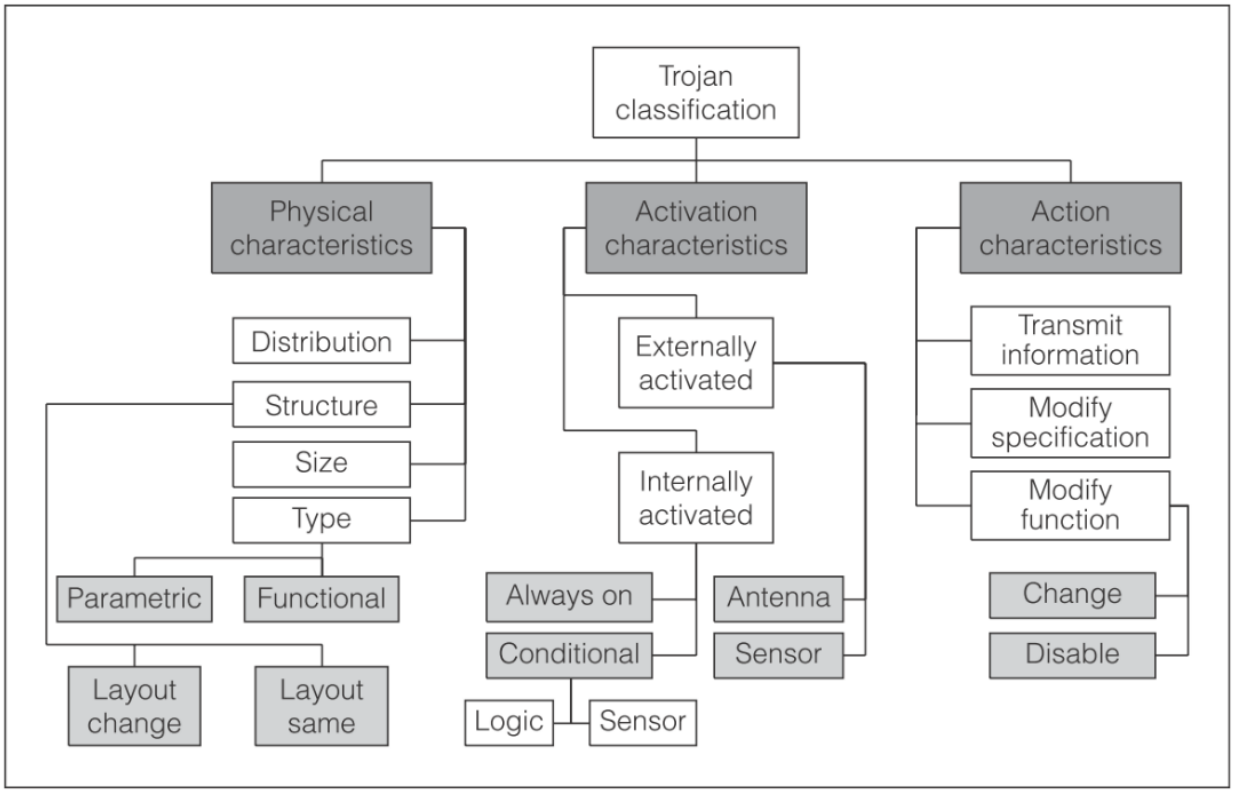

Figure 1. HT Taxonomy according to Wang et al., 2008.

components in a design to insert HTs. The size category accounts for the size and number of HTs that have been added. The type category further partitions HTs into functional (HTs involving addition or deletion of circuitry) and parametric (modification of existing logic or circuitry) classes. Activation characteristics refer to the triggers that cause activation of HTs are internal or external. External triggers can include, for example, antennae or sensors that can interact with the outside world, while internal triggers can be condition based or "always ON"; i.e., HTs that are always active and can attack the IC function anytime. Examples of "Always ON" HTs include modifications to the IC geometries or to the wiring. Condition based internal activation depends on meeting a specific threshold of voltage, temperature, logic state or counter value, etc. and being dormant otherwise. Action characteristics identify the payload; i.e., the disruption caused by the HT in terms of functionality modification, specification modification, and information leakage. Functionality modification involves changing the IC behavior through addition, removal or bypass of existing logic. Specification modification is caused by HTs that change the IC parametric properties, such as power consumption, delay, etc.

IC designers optimize their processes to ensure lifetime is guaranteed even under the effects of anticipated wearout mechanisms. The process specifications are fixed before fabrication, and it is assumed that they stay constant during fabrication. Process reliability trojans are a type of HT that can be inserted by exploiting semiconductor physics principles by modifying process fabrication parameters (Shiyanovskii et al., 2010) like gate oxide thickness, purity, and quality, and nitrogen concentration near Si/SiO2 interface, etc. This HT guarantee that a proportion of the devices produced will have an appreciably reduced lifetime due to the acceleration of aging mechanisms (Shiyanovskii et al., 2009).

3. COUNTERMEASURES AGAINST HARDWARE THREATS

Counterfeit detection is a challenging task and requires comprehensive countermeasures to ensure detection of the multitude of counterfeit types discussed earlier. These detection techniques based on the different counterfeit types are as follows,

a) Relabeled/Recycled – Aging Detection Sensors: Aging sensors are used to determine if aging occurs in ICs because of Negative Bias Temperature Instability (NBTI). NBTI results in an increased threshold voltage and reduced drain current in the transistor resulting in timing failures (Becker et al., 2014). Hence, aging sensors are used for detection of threshold voltage changes, and hence can be used for detection of counterfeits. Since different transistors age at different rates multiple aging sensors are required; thus hampering the scalability and effectiveness of the technique.

b) Illegal manufacturing/Cloned: Physical Unclonable Functions (PUF) and Hardware Metering. A PUF involves the usage of manufacturing variability to generate a fingerprint of the device (Böhm & Hofer, 2013). Since the variation is inherent to the manufacturing process and cannot be replicated externally, a PUF cannot be cloned. Hardware metering or IC metering refers to mechanisms, methods, and protocols that enable tracking of the ICs post-fabrication (Koushanfar & Qu, 2001).

c) Tampered/structural modification: Conventional HT detection approaches include Side Channel Analysis (SCA), Logic Testing (LT) and Reverse Engineering (RE). SCA methods rely on measurement of IC parameters that can be affected due to HT insertions such as transient current, transmission power, path delay, etc. SCA methods are well suited for detection of large HTs; however, in the presence of process/manufacturing variations, HT detection becomes difficult especially if the HTs are small or the circuits are large or if the measurements are noisy. SCA methods also require a golden circuit for comparison. LT methods rely on development of test vectors that can activate a HT. However, LT methods are rarely able to trigger all HTs present in an IC as HTs because HTs are designed to be stealthy and rarely triggered. In reverse engineering, ICs are destructively de-packaged and explored optically for HT insertion. Optical inspection involves comparison of the IC layout and images of the manufactured IC under test. Photos of the de-packaged IC are taken using techniques such as scanning optical microscopy (SOM) and scanning electron microscopy (SEM). Images collected are used to reverse-engineer the IC layout by reconstructing the original netlist. RE is a powerful technique for HT detection, but it is expensive, time-consuming, and impractical to apply to a large number of ICs because of its destructive nature.

All the techniques discussed so far attempt to detect a HT before the ICs are used; however, since it is impossible to detect all HTs, some HT might manifest when the IC is in operation. This is especially pertinent because adversaries try to ensure that the trojans are triggered under very rare conditions that are unlikely during testing but likely after usage. For this purpose, circuits can be designed with runtime monitoring and reconfigurable logic. Once the runtime monitoring system detects a HT in the operation phase, the reconfigurable logic acts to bypass the detected HT such that the circuit can operate safely (Bloom et al., 2009). Side-channel methods are used either before IC usage or, periodically, when the IC is idle during usage. Therefore, trojans that are controllable to be either active or dormant can easily evade side-channel detection. Hence, the authors in

(Liu et al., 2015) proposed a concurrent hardware Trojan detection (CHTD) runtime monitoring based approach that works simultaneously with normal IC operation. For safety-critical applications, one can combine logic testing, SCA, and runtime monitoring.

From the earlier discussion of counterfeit detection methods, parallels emerge between counterfeit detection and prognostics and health management. The comparison in Table 1, between the same feature (precursor) used for both counterfeit detection and prognostics and health management, helps to drive home the point about the harmonies between the two disciplines.

Table 1. Parallels between Counterfeit Detection (Security) and PHM (Health)

Feature	Security		Health	
	Author	Functionality	Author	Functionality
Quiescent supply current	(Aarestad et al., 2010)	Detection of HTs based on a chip's IDDQ	(G. Zhang et al., 2008)	Predict RUL of FETs due to failure mechanisms
Transient supply current	(Rad et al., 2010)	Detection of HTs via a sensitivity analysis of power signal	(Bhunia et al., 2002)	Fault detection and localization
Supply power	(Lamech et al., 2011)	Detection of HTs based on supply power	(Sundström et al., 2008)	Prognostic method applicable to electronic components and systems based on the analysis of the power supply.
Delay	(Xiao et al., 2013)	Detection of HTs based on clock sweeping and delay-based detection	(Ye et al., 2017)	IC fault prediction technique based on delay characteristics of the clock network.
Transmission power	(Liu et al., 2015)	Detection of HTs based on transmission power	(Q. Li & Lv, 2019)	Prognostic method applicable to electronic components and systems based on the analysis of the transmission power.
Leakage current	(Wei & Potkonjak, 2012)	Diagnosis and detection of HTs based on segmentation and gate level characterization	(H. Zhang et al., 2009)	PHM precursor parameter identification for one switch-mode power supply (SMPS)
Aging	(Lin & Ghosh, 2015)	Aging analysis for recycled IC detection	(Goodman et al., 2006)	Prognostic cell to monitor time-dependent dielectric breakdown and IC electronic aging.

Additionally, counterfeit and secure ICs are classified based on various features and/or side-channel measurements by employing machine-learning techniques. Examples include power consumption using Support Vector Machine (SVM) (Iwase et al., 2016), timing signatures such as the delay using k-Nearest Neighbors (KNN) (Lodhi et al., 2016), transmission power and one-class SVM (Liu et al., 2017). This is similar to the modus operandi of data driven PHM where failure precursors are generated for healthy and faulty circuits and machine learning algorithms are used to predict if a system is healthy or faulty.

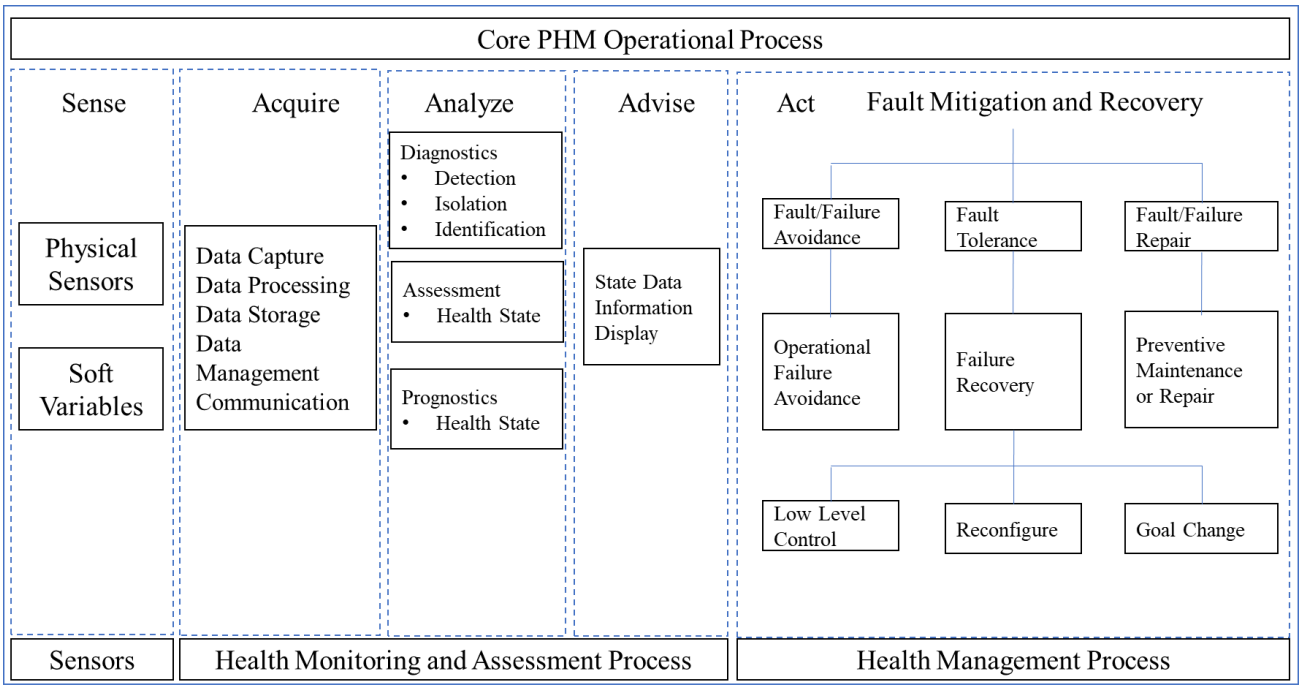

Figure 2. PHM System view according to IEEE 1856.

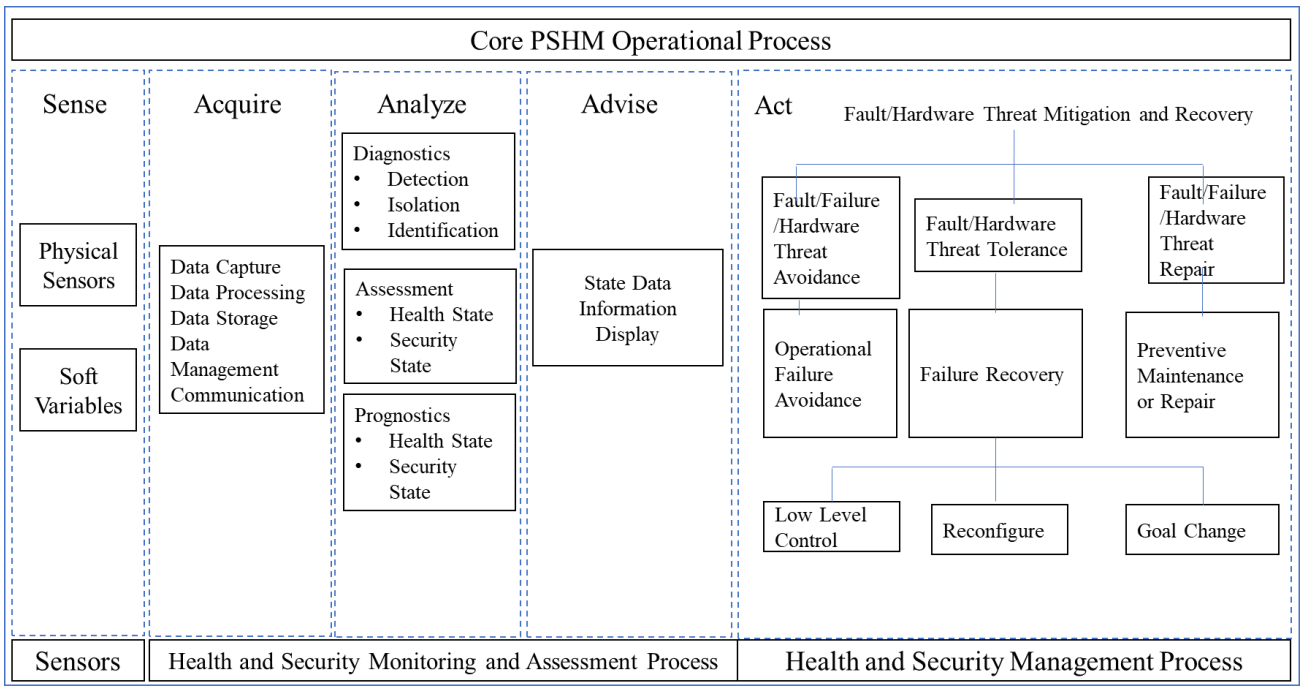

Figure 3. Developed PSHM Framework.

4. DEVELOPED PSHM FRAMEWORK

Prognostics and health management (PHM) is an approach used to increase operational availability and utilization of critical systems by reducing maintenance costs. PHM involves developing sensors and algorithms to detect anomalies from normal system operation, diagnose problems that cause the anomalies in terms of possible failure modes and mechanisms, and compute time to failure as a point estimate or ideally as a probability distribution. Once the failure distribution is computed, maintenance activities can be scheduled to optimize cost and system utilization subject to the system's operational constraints. Figure 2 provides a view of the elements within the PHM framework and how they enable the PHM capability, according to IEEE 1856 (Committee & Reliability, 2017). As shown in the diagram, the Sense process is activated using data from the system's sensors. The Acquire process is activated by the data processing which includes acquisition and manipulation built in to implement PHM. The Analyze process involves state detection, and the assessment of system health and prognostic functions. This includes fault detection, fault isolation and fault identification, estimation of the health state and RUL. The Advise process is enabled by the advisory generation (AG) function inherent in the system design or external to the system. This includes presentation of health state data, prescriptive information, or display advisories. Finally, the Health Management processes uses the information generated in the Advise section to institute actions to return the system to a healthy state. The fault mitigation and recovery processes shown in the diagram may be performed within or external to the system. The idea here is to provide both a level of autonomous failure tolerance and recovery as well as operator-initiated failure avoidance and preventive maintenance actions. Together, these system design functions and processes comprise the enterprise PHM capability.

The proliferation of hardware threats could outpace the implementation of their detection mechanisms. This might lead to a scenario where all products manufactured by untrusted manufacturing facilities are suspect until verified otherwise. This has parallels to Zero-Trust Architecture, a network security concept developed to help prevent data breaches by removing the notion of trust from an organization's network architecture. To extend the concept of Zero-Trust Architecture from the network to the hardware domain and to ensure hardware security, a paradigm shift from PHM to PSHM (Prognostics and Secure Health Management) is needed. We have seen in the previous section that there is an overlap between techniques used for PHM and those used for ensuring hardware security. Common approaches that tackle both naturally occurring and maliciously induced failures can ensure safe, reliable, and secure operation of electronic systems. These common approaches can be built on the PSHM framework proposed in Figure 3 which is a modification of the PHM framework proposed in IEEE 1856. Compared to the PHM framework, the PSHM framework has an additional security state that needs assessment and prognosis. Analogous to the health state, the security state can be defined as the summary information regarding the current ability of a system or subsystem to perform its intended function securely; i.e., independent from the impact of hardware threats. A system's security state is not directly observed and hence needs to be estimated. The estimation of the system's security state is more complex than the estimation of the system health as there are multiple types of hardware threats that can impact security. The security state could change over time as some hardware threats are triggered during IC usage. The Advise process and the Act process of the PSHM framework has to take into account both the health and security states. Reconfiguration, which is one of the possible Act scenarios, is already an active research area in dealing with hardware threats once they are discovered. Since many different types of hardware threats could be present in the system before it is even used, it is possible to extend the PSHM framework into the testing phase of systems.

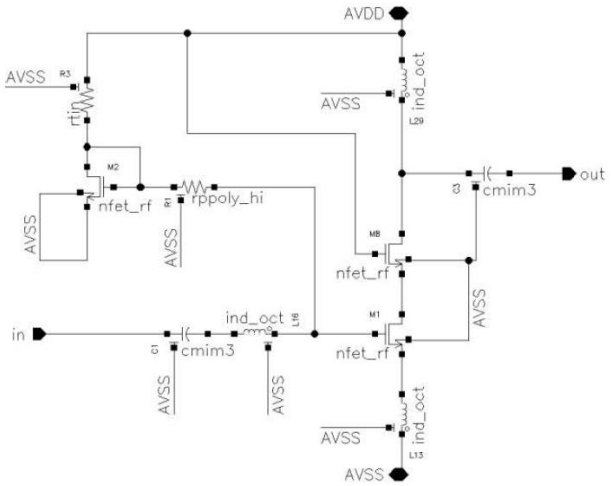

Figure 4. LNA Circuit.

For example, consider a low noise amplifier (LNA) (Figure 4), where the following hardware trojans could be inserted (Karabacak et al., 2018) - (1) electromigration based process reliability trojans, which can be simulated by adding resistances in the wires of the circuit to simulate decreased wire widths, (2) NBTI based process reliability trojans, which can be simulated by increasing the voltage threshold of the transistors in the circuit, and (3) a functional HT in the form of a dipole antenna placed with the intention of stealing information or jamming the LNA output, which can be mimicked by adding small capacitive load. Following the PHM procedure described elsewhere (Khemani et al., 2019), we can detect deviations from the nominal values for every component within a circuit. As a result, we will be able to detect the NBTI based process reliability trojans in the transistors. Detection of the functional trojans and the electromigration based trojans, requires their consideration as a fault class, such that they can be detected by the PHM process. This simple example demonstrates that it is possible

to detect both natural aging and hardware threats by extending the PHM concept to the PSHM concept.

5. CONCLUSION

The Prognostics and Health Management (PHM) of electronic systems has reached high levels of maturity, with both generic and system specific PHM techniques available. These techniques detect naturally occurring faults and predict their impact on the system lifetime. In this paper, we make the case that PHM techniques should also consider hardware threats as they result in maliciously induced faults. To this end, we propose extending the PHM approach to incorporate system security as one of the goals and develop the PSHM framework to do so. Due to the significant overlap between techniques used for PHM and those used for ensuring hardware security, the PSHM framework is not a significant departure from the PHM framework. Hence, the PSHM framework can ensure safe, reliable, and secure operation of electronic systems as it accounts for both naturally occurring and maliciously induced faults. Implementing the PSHM framework would involve defining a security state, in addition to the health state usually defined for PHM approaches. Additionally, the fault diagnosis and fault prognosis tasks become more complex because of the consideration of both naturally occurring and maliciously induced faults. The PSHM framework can bring together both PHM and hardware security researchers and practitioners under the common goal of enabling safe, reliable, and secure systems in challenging Zero-Trust environments.

ACKNOWLEDGEMENT

The authors also thank the Center for Advanced Life Cycle Engineering (CALCE) and its over 150 funding companies and the Centre for Advances in Reliability and Safety (CAiRS) at Hong Kong for enabling research into advanced topics in reliability, safety, and sustainment.
.

REFERENCES

Aarestad, J., Acharyya, D., Rad, R., & Plusquellic, J. (2010). Detecting Trojans Through Leakage Current Analysis using Multiple Supply Pad IDDQs. *IEEE Transactions on Information Forensics and Security*, *5*(4), 893–904. https://doi.org/10.1109/TIFS.2010.2061228

Azarian, M. H. (2018). An Overview of Risk-Based EEE Counterfeit Part Detection Based on SAE AS6171. *ISTFA 2018: Proceedings from the 44th International Symposium for Testing and Failure Analysis*, 51.

Becker, G. T., Regazzoni, F., Paar, C., & Burleson, W. P. (2014). Stealthy dopant-level hardware Trojans: Extended version. *Journal of Cryptographic Engineering*, *4*(1), 19–31. https://doi.org/10.1007/s13389-013-0068-0

Bernstein, K. (2011). *Integrity and Reliability of Integrated Circuits (IRIS)*. DARPA. https://www.darpa.mil/program/integrity-and-reliability-of-integrated-circuits

Bhasin, S., & Regazzoni, F. (2015). A survey on hardware trojan detection techniques. *Proceedings - IEEE International Symposium on Circuits and Systems*, *2015-July*, 2021–2024. https://doi.org/10.1109/ISCAS.2015.7169073

Bhunia, S., Hsiao, M. S., Banga, M., & Narasimhan, S. (2014). Hardware trojan attacks: Threat analysis and countermeasures. *Proceedings of the IEEE*. https://doi.org/10.1109/JPROC.2014.2334493

Bhunia, S., Roy, K., & Segura, J. (2002). *A novel wavelet transform based transient current analysis for fault detection and localization*. 361. https://doi.org/10.1145/513918.514011

Bloom, G., Narahari, B., & Simha, R. (2009). OS support for detecting trojan circuit attacks. *2009 IEEE International Workshop on Hardware-Oriented Security and Trust, HOST 2009*. https://doi.org/10.1109/HST.2009.5224959

Böhm, C., & Hofer, M. (2013). Physical unclonable functions in theory and practice. In *Physical Unclonable Functions in Theory and Practice*. https://doi.org/10.1007/978-1-4614-5040-5

Carlson, G. (2005). Trusted foundry: The path to advanced SiGe technology. *Technical Digest - IEEE Compound Semiconductor Integrated Circuit Symposium, CSIC*. https://doi.org/10.1109/CSICS.2005.1531738

IEEE 1856. (2017). *IEEE Standard Framework for Prognostics and Health Management of Electronic Systems IEEE Standard Framework for Prognostics and Health Management of Electronic Systems*. IEEE.

Goodman, D., Vermeire, B., Ralston-Good, J., & Graves, R. (2006). A board-level prognostic monitor for MQSFET TDDB. *IEEE Aerospace Conference Proceedings*, *2006*. https://doi.org/10.1109/aero.2006.1656127

Guin, U., Dimase, D., & Tehranipoor, M. (2014). Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead. *Journal of Electronic Testing: Theory and Applications (JETTA)*, *30*(1), 9–23. https://doi.org/10.1007/s10836-013-5430-8

Harper, J. (2020). *Pentagon Reshuffles R&D Priorities*. National Defense: NDIA's Business & Technology Magazine. https://www.nationaldefensemagazine.org/articles/2020/6/5/pentagon-reshuffles-rd-priorities#mainContent

Iwase, T., Nozaki, Y., Yoshikawa, M., & Kumaki, T. (2016). Detection technique for hardware Trojans using machine learning in frequency domain. *2015 IEEE 4th Global Conference on Consumer Electronics, GCCE 2015*, 185–186. https://doi.org/10.1109/GCCE.2015.7398569

Karabacak, F., Welker, R., Casto, M. J., Kitchen, J. N., &

Ozev, S. (2018). RF circuit authentication for detection of process Trojans. *Proceedings of the IEEE VLSI Test Symposium*, *2018-April*, 1–6. https://doi.org/10.1109/VTS.2018.8368666

Khemani, V., Azarian, M. H., & Pecht, M. G. (2019). Electronic circuit diagnosis with no data. *2019 IEEE International Conference on Prognostics and Health Management, ICPHM 2019*, 1–7. https://doi.org/10.1109/ICPHM.2019.8819424

Koushanfar, F., & Qu, G. (2001). *Hardware metering*. 490–493. https://doi.org/10.1145/378239.378568

Lamech, C., Rad, R. M., Tehranipoor, M., & Plusquellic, J. (2011). An experimental analysis of power and delay signal-to-noise requirements for detecting trojans and methods for achieving the required detection sensitivities. *IEEE Transactions on Information Forensics and Security*, *6*(3 PART 2), 1170–1179. https://doi.org/10.1109/TIFS.2011.2136339

Lapedus, M. (2018). *A Crisis In DoD's Trusted Foundry Program?* Semiconductor Engineering. https://semiengineering.com/a-crisis-in-dods-trusted-foundry-program/

Li, H., Liu, Q., & Zhang, J. (2016). A survey of hardware Trojan threat and defense. *Integration, the VLSI Journal*, *55*, 426–437. https://doi.org/10.1016/j.vlsi.2016.01.004

Li, Q., & Lv, Y. (2019). Radar Transmitting Power Supply Health Monitoring Based on Circuit Modeling and Simulation Technology. *2019 IEEE International Conference on Power, Intelligent Computing and Systems, ICPICS 2019*, 584–588. https://doi.org/10.1109/ICPICS47731.2019.8942530

Lin, C. W., & Ghosh, S. (2015). Novel self-calibrating recycling sensor using Schmitt-Trigger and voltage boosting for fine-grained detection. *Proceedings - International Symposium on Quality Electronic Design, ISQED*. https://doi.org/10.1109/ISQED.2015.7085470

Liu, Y., Jin, Y., Nosratinia, A., & Makris, Y. (2017). Silicon Demonstration of Hardware Trojan Design and Detection in Wireless Cryptographic ICs. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *25*(4), 1506–1519. https://doi.org/10.1109/TVLSI.2016.2633348

Liu, Y., Volanis, G., Huang, K., & Makris, Y. (2015). Concurrent hardware Trojan detection in wireless cryptographic ICs. *Proceedings - International Test Conference*, *2015-Novem*, 1–8. https://doi.org/10.1109/TEST.2015.7342386

Lodhi, F. K., Abbasi, I., Khalid, F., Hasan, O., Awwad, F., & Hasan, S. R. (2016). A self-learning framework to detect the intruded integrated circuits. *Proceedings - IEEE International Symposium on Circuits and Systems*, *2016-July*, 1702–1705. https://doi.org/10.1109/ISCAS.2016.7538895

Lyu, Y., & Mishra, P. (2018). A Survey of Side-Channel Attacks on Caches and Countermeasures. *Journal of Hardware and Systems Security*, *2*(1), 33–50. https://doi.org/10.1007/s41635-017-0025-y

Mitra, S., Wong, H. S. P., & Wong, S. (2015). The Trojan-proof chip. In *IEEE Spectrum* (Vol. 52, Issue 2, pp. 46–51). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/MSPEC.2015.7024511

Oriero, E., & Hasan, S. R. (2019). Survey on recent counterfeit IC detection techniques and future research directions. *Integration*, *66*(March), 135–152. https://doi.org/10.1016/j.vlsi.2019.02.006

Pecht, M. G., & Kang, M. (2018). *Prognostics and Health Management of Electronics* (M. G. Pecht & M. Kang (eds.)). John Wiley and Sons Ltd. https://doi.org/10.1002/9781119515326

Rad, R., Plusquellic, J., & Tehranipoor, M. (2010). A sensitivity analysis of power signal methods for detecting hardware trojans under real process and environmental conditions. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *18*(12), 1735–1744. https://doi.org/10.1109/TVLSI.2009.2029117

Rahman, F., Forte, D., & Tehranipoor, M. M. (2016). Reliability vs. security: Challenges and opportunities for developing reliable and secure integrated circuits. *IEEE International Reliability Physics Symposium Proceedings*, *2016-September*, 4C61-4C610. https://doi.org/10.1109/IRPS.2016.7574542

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2019). Zero Trust Architecture. *Nist*. https://doi.org/https://doi.org/10.6028/NIST.SP.800-207-draft

Schellenberg, F., Gnad, D. R. E., Moradi, A., & Tahoori, M. B. (2018). An inside job: Remote power analysis attacks on FPGAs. *Proceedings of the 2018 Design, Automation and Test in Europe Conference and Exhibition, DATE 2018*, *2018-January*, 1111–1116. https://doi.org/10.23919/DATE.2018.8342177

Shiyanovskii, Y., Wolff, F., Papachristou, C., Weyer, D., & Clay, W. (2009). *Exploiting Semiconductor Properties for Hardware Trojans*. http://arxiv.org/abs/0906.3834

Shiyanovskii, Y., Wolff, F., Rajendran, A., Papachristou, C., Weyer, D., & Clay, W. (2010). Process reliability based trojans through NBTI and HCI effects. *2010 NASA/ESA Conference on Adaptive Hardware and Systems, AHS 2010*, 215–222. https://doi.org/10.1109/AHS.2010.5546257

Sundström, T., Mesgarzadeh, B., Krysander, M., Klein, M., Söderquist, I., Crona, A., Fransson, T., & Alvandpour, A. (2008). *Prognostics of Electronic Systems through Power Supply Current Trends*. http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-138086

Szefer, J. (2019). Survey of Microarchitectural Side and Covert Channels, Attacks, and Defenses. *Journal of Hardware and Systems Security*, *3*(3), 219–234. https://doi.org/10.1007/s41635-018-0046-1

Villasenor, J. D. (2011). Ensuring Hardware Cybersecurity. *Electrical Engineering*, *9*. https://www.brookings.edu/research/ensuring-hardware-cybersecurity/

Wang, X., Tehranipoor, M., & Plusquellic, J. (2008). Detecting malicious inclusions in secure hardware: Challenges and solutions. *2008 IEEE International Workshop on Hardware-Oriented Security and Trust, HOST*, 15–19. https://doi.org/10.1109/HST.2008.4559039

Wei, S., & Potkonjak, M. (2012). Scalable hardware trojan diagnosis. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *20*(6), 1049–1057. https://doi.org/10.1109/TVLSI.2011.2147341

Xiao, K., Zhang, X., & Tehranipoor, M. (2013). A clock sweeping technique for detecting hardware trojans impacting circuits delay. *IEEE Design and Test*, *30*(2), 26–34. https://doi.org/10.1109/MDAT.2013.2249555

Yang, K., Hicks, M., Dong, Q., Austin, T., & Sylvester, D. (2016). A2: Analog Malicious Hardware. *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, 18–37. https://doi.org/10.1109/SP.2016.10

Ye, L., Lu, Y., Wang, X., Huang, Y., He, C., & Hou, B. (2017). Integrated circuit fault prognostics based on the delay characteristics of the clock network. *2016 International Conference on System Reliability and Science, ICSRS 2016 - Proceedings*, 22–27. https://doi.org/10.1109/ICSRS.2016.7815832

Zhang, G., Das, D., Xu, R., & Pecht, M. (2008). IDDQ trending as a precursor to semiconductor failure. *2008 International Conference on Prognostics and Health Management, PHM 2008*, 0–6. https://doi.org/10.1109/PHM.2008.4711419

Zhang, H., Kang, R., Luo, M., & Pecht, M. (2009). Precursor parameter identification for power supply prognostics and health management. *Proceedings of 2009 8th International Conference on Reliability, Maintainability and Safety, ICRMS 2009*, 883–887. https://doi.org/10.1109/ICRMS.2009.5269961

Varun Khemani received his B.E. degree in Instrumentation Engineering from the University of Mumbai, and his M.S. in Industrial Engineering from North Carolina State University. He's currently pursuing his Ph.D. in Reliability Engineering at the University of Maryland. He has work experience with Stanley, Black and Decker, Towson, MD and Aker, Mumbai, India. His research interests include reliability, functional safety and cybersecurity of electronic circuits. He's a student member of IEEE, ASME, IEEE EDS, PHM Society, and ACES. He was the recipient of the ASME Petroleum Division Scholarship in 2016.

Michael H. Azarian received the B.S.E. degree in chemical engineering from Princeton University, and the M.E. degree in metallurgical engineering and materials science and the Ph.D. degree in materials science and engineering from Carnegie Mellon University. He is a Research Scientist with the Center for Advanced Life Cycle Engineering (CALCE) at the University of Maryland in College Park, MD. Dr. Azarian's primary research interests are detection, prediction and analysis of failures in electronic components and assemblies. He has over 150 publications on electronics reliability and packaging, prognostics and health management, and tribology, and holds 6 U.S. patents. Prior to joining CALCE he spent over a dozen years in the disk drive and fiber optics industries, having worked at Bookham Technology, W.L. Gore, Censtor, and Philips Research Laboratories. Dr. Azarian is chair of the SAE G-19A Test Laboratory Standards Development Committee which is responsible for the AS6171 family of standards on detection of counterfeit electrical, electronic, and electromechanical parts. He chairs the working group responsible for the IEEE 1624 standard on organizational reliability capability of suppliers of electronic products. He was previously co-chair for the IEEE 1332 Standard on reliability programs.

Michael G. Pecht (25,000+ citations, 70+ H-Index) has a BS in Physics, an MS in Electrical Engineering and an MS and PhD in Engineering Mechanics from the University of Wisconsin. He is a Professional Engineer, an IEEE Fellow, a PHM Society Life Fellow, an ASME Fellow, an SAE Fellow and an IMAPS Fellow. He served as editor-in-chief of IEEE Access for six years, as editor-in-chief of IEEE Transactions on Reliability for nine years, editor-in-chief of Microelectronics Reliability for sixteen years, and editor of Circuit World. He has also served on three U.S. National Academy of Science studies, two US Congressional investigations in automotive safety, and as an expert to the U.S. FDA. He is the Director of CALCE (Center for Advanced Life Cycle Engineering) at the University of Maryland (UMD), which is funded by over 150 of the world's leading electronics companies at more than US$6M/year. He has written more than twenty books on product reliability, development, use and supply chain management. He has also written a series of books of the electronics.