Thin Wing EMA - System on Chip with Synchronized TRust and Assurance (SaSTRA)

Parag Kshirsagar
United Technologies Research Center
E Hartford, CT USA
kshirsp@utrc.utc.com

Vivek Venugopalan
USC Information Sciences Institute
Arlington, VA USA
vivekv@isi.edu

***Abstract*—Thin Wing Electromechanical Actuator (EMA) offers significant benefits with respect to power density and performance for flight control systems in the next-generation of aircrafts. The cyber physical system (CPS) security design for such EMAs is of immediate need because of the safety critical nature of the application which has not being addressed so far. This research proposes to develop a novel system on chip (SoC) approach using COTS FPGA - SoC with Synchronized TRust and Assurance (SaSTRA) to demonstrate resiliency of the Thin Wing EMA in presence of CPS vulnerabilities. The research takes a holistic approach of embedding and synchronizing Root of Trust (RoT) and security monitors within multiple layers of the CPS to provide a mechanism for FPGA assurance at the application level.**

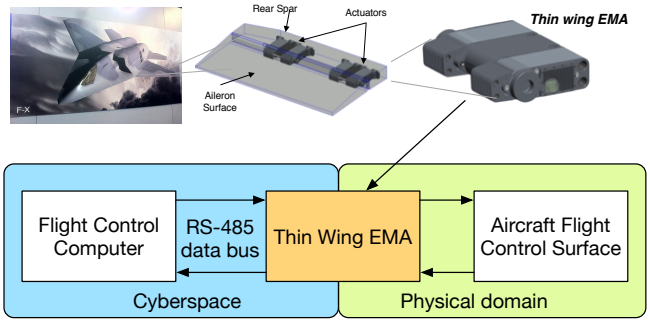

Fig. 1. CPS composition of the Thin Wing EMA system.

I. Introduction

In the embedded systems community, a cyber-physical system (CPS) is modeled by stacking firmware, software, and hardware abstraction layers over the underlying computation platform. Security, trust, and assurance are seldom applied to a complete system and solutions are devised to target only certain layers of the CPS. Software security countermeasures are built on the principle of isolation, so that an attack cannot extend into other components. Each layer within a CPS is designed with its own Root-of-Trust (RoT) that provides assurance regarding the trustworthy operation of the specific CPS layer. It is truly difficult to design a CPS with RoT designed to address all types of threat vectors and embed assurance; the RoT can ensure trustworthy operation if it is fine-tuned to the specific application targeted by the system hardware and software layers. Therefore an opportunity exists on improving hardware assurance given the various layers of the CPS.

II. Background

Resiliency against cyber attacks on Computing-Enabled Networked Physical Systems (CNPS) has gained high priority in recent times (http://www.nitrd.gov). The Cyber Security and Privacy (CSP) component focuses on the detection, prevention, and recovery of a CPS from cyber attacks along with the privacy of the information embedded in a CPS.

The Thin Wing Electro-Mechanical Actuator (EMA) system shown in Figure 1 is essentially a CPS where the flight control computer (FCC) generates a flight command to the EMA system which in turn actuates the wing control surfaces and also reports sensor feedback to the FCC.

Most of the research efforts in this area focus on the FCC shown in Figure 1. Anomaly detection and prevention using backup controllers have been studied [1], and control systems resilient to DoS attacks have also been investigated [2]. The DoS attack interrupts the communication between the sensors and the control system, and may also affect system integrity by modifying sensor data. Since the sensors may be the most vulnerable components, watermarking of the sensor signal may be used to establish an acceptable threshold for noise embedded in the system [3] to detect the presence of an attack. However, the threshold for the noise can be learned by a clever attacker using multiple simulations to help mask the attack. Cryptographic algorithms do not secure a system as certificates can be stolen or keys can be extracted using side-channel techniques. The classic example of the Stuxnet attack highlights malware being injected surreptitiously even when the CPS is physically isolated [4].

Trust is typically not considered as a metric to evaluate the security of a CPS. Efforts focusing on detection of malware and protection of controller does not ensure trust in sensor and actuator communication which is critical in bridging the cyber and physical domains in a CPS. Accordingly, trust needs to be embedded inside the CPS and maintained through analysis of the communication within the CPS. At the hardware ar-

chitecture level, safeguards need to be built to monitor the communication between third party IP cores and alert the system in the case of anomalies. Therefore, the cyber costs for evaluating safeguards implemented in the hardware platform may consist of data packet inspection, supervisory monitoring schemes, and behavioral policies may be acceptable compared to the economic and human costs of the physical system's degradation or destruction.

To address the aforementioned aspects, the research in this paper is will highlight the SASTRA architecture and elaborate on the interface between security monitors and anomaly detection within each layer. Then an example of anomaly detection is also provided followed with future work.

III. SASTRA Architecture

The main components of SaSTRA are: (i) distributed security monitors embedded in software and hardware in different layers; (ii) security enforced in software through verified microkernel; (iii) secure enclaves to protect confidentiality of critical system parameters; (iv) hardware binding to a synchronized RoT for accountability; and, (v) anomaly detection using application knowledge and machine learning techniques by monitoring system behavior and I/O access policies.

A. Synchronized Root of Trust

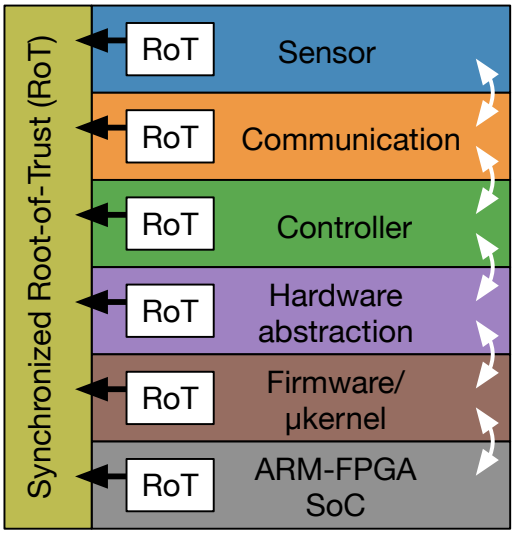

Fig. 2. Proposed SOC embedded system layers of the Thin Wing EMA cyber physical system.

Figure 2 shows the concept of RoT implemented in multiple the layers of the CPS wherein a synchronized state will result in identifying which layer of the CPS has been compromised and thereby determines overall assurance of the CPS. The RoT embedded in each layer captures the computational and I/O operations executed by the specific layer using a combination of registers. The value recorded by the RoT registers implemented in hardware corresponds to the vulnerability state of the layer due to the specific computational or I/O operations being executed at that time, and also the output of security monitor in each CPS layer.

B. Security Monitors

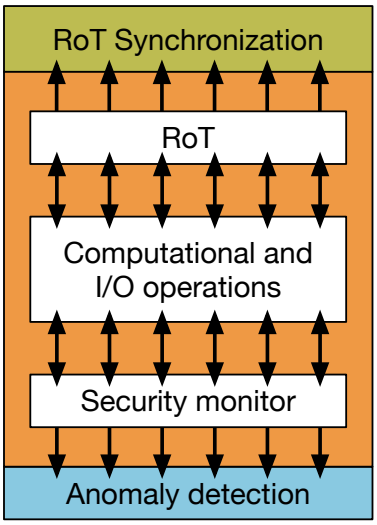

Fig. 3. Proposed structure within each layer of the SoC

Figure 3 shows the internal layout of a single CPS layer where the security monitor detects violations in the policies and actions associated within a layer to update the anomaly detection module. The uniqueness of SaSTRA results from a synchronized state of all the RoTs and monitors inside a CPS; where an attack to a specific layer of the CPS can be detected and the overall system assurance can be measured for trustworthy operation. Although security monitors have lower area implementation overhead, frequent sampling of these monitors across all the layers can result in significant latency overhead. Hence, statistical methods can result in optimized and intelligent sampling of security monitors based on operations associated with the specific CPS layer reducing the impact of latency overhead.

C. Hardware & Software Bindings

Security is enforced in the software layers using verified microkernel such as *sel4* [5]. Secure enclaves derived from Intel's Intel's Software Guard Extensions (SGX) [6] platform can be used to store sensitive information required for the successful operation of the device. Hardware bindings are implemented using custom wrappers that connect the individual RoT modules on all the layers to a centralized RoT. This centralized RoT captures the individual RoT states of all the layers and provides indication if a certain layer is being attacked.

D. Anomaly Detection

This module requires fast inferencing of the vulnerability based on the event based operation. It is designed based on application knowledge, logic state of synchronized RoT and

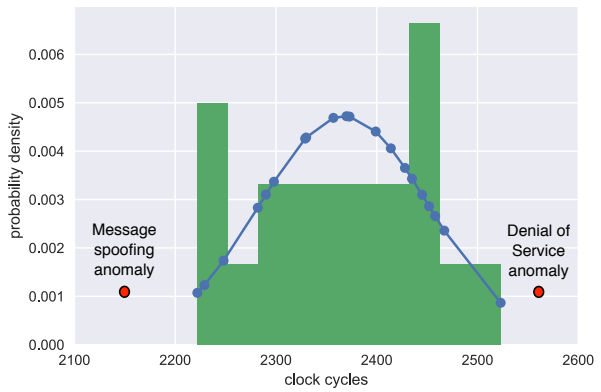

Fig. 4. Probability of anomaly in a CPS layer detected by the security monitor

optimally sampled output of security monitors. Figure 4 shows a normal operation of an IP core based on the number of clock cycles required to perform the task (green bars) and its weighted distribution (blue line) [7]. As an illustration, in case of an anomaly such as message spoofing or denial or service (DoS) attack, the number of clock cycles required will vary and is shown in red. Hence the combined probability distribution function resulting from the anomaly will deviate significantly from the normal operation enabling detection of vulnerability to the specific layer. For reduced latency, methods related to pattern recognition using machine learning will be leveraged for anomaly detection through security monitors and synchronized RoT.

E. Metrics

The required probability loss of function of the Thin Wing EMA system is $< 10^{-7}$. Then the CPS design metrics can be benchmarked for reliability, cost, and performance. Detailed metric definition is currently under progress and will be reported in future publication. Given the proposed approach, the FPGA assurance will be quantified using risk probability analysis of the CPS design.

IV. Summary and Future Work

The proposed SaSTRA testbed consists of distributed security monitors that capture snapshots of the operations in each layer and assesses the trustworthiness of that layer depending on the type of operations/instructions being executed. These key aspects of the methodology are being developed and implemented on a Xilinx Ultrascale plus FPGA platform. This proposed design method will be broadly applicable for other COTS FPGA based control systems for legacy, existing, and on the next generation of aircraft platforms.

Acknowledgement

This material is based on research sponsored by the Air Force Research Labs (AFRL) under contract number FA8650-15-C-2500. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views, and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Air Force Research Labs (AFRL) or the U.S. Government.

References

[1] A. A. Cárdenas, S. Amin, and S. Sastry, "Research Challenges for the Security of Control Systems," in *Proceedings of the 3rd Conference on Hot Topics in Security*, ser. HOTSEC'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 6:1–6:6.

[2] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and Secure Networked Control Systems under Denial-of-Service Attacks," *Hybrid Systems: Computation and Control: 12th International Conference, HSCC 2009, San Francisco, CA, USA, April 13-15, 2009. Proceedings*, pp. 31–45, 2009.

[3] Y. Mo and B. Sinopoli, "Secure Control against Replay Attacks," in *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept 2009, pp. 911–918.

[4] A. Matrosov, E. Rodionov, D. Harley, and J. Malcho, "Stuxnet under the Microscope," *ESET LLC (September 2010)*, 2010. [Online]. Available: https://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

[5] G. Klein, J. Andronick, K. Elphinstone, T. Murray, T. Sewell, R. Kolanski, and G. Heiser, "Comprehensive formal verification of an OS microkernel," *ACM Transactions on Computer Systems (TOCS)*, vol. 32, no. 1, pp. 2:1–2:70, Feb. 2014.

[6] "Intel Software Guard Extensions Programming Reference," October 2014. [Online]. Available: https://software.intel.com/sites/default/files/managed/48/88/329298-002.pdf

[7] V. Venugopalan and C. D. Patterson, "Architectural Refinements for Enhancing Trust and Securing Cyber-Physical Systems," in *IEEE International Conference on Advanced and Trusted Computing (ATC)*, San Francisco, CA, August 2017, pp. 1509–1516.