Contribution ID: **553** Type: **Paper**

Cyber Resilient Hardware Controller

General-purpose computation has launched entire industries and improved the lives of billions around the globe. But the speed of commerce has pushed application of networked computing to so-called Operational Technology (OT) such as industrial control system (ICS), programmable logic controllers (PLC) and other embedded systems including the Internet of Things (IoT) without full understanding of its security ramification. Even sensitive and safety-critical infrastructures like the nuclear industry now depend upon the ubiquitous employment of these networked computerized devices. What has become apparent is the potential for the misuse of these system, as evidenced in media reports on how cameras and digital video recorders (DVR) were used to launch the largest distributed denial of service (DDoS) attack to date. To put it more succinctly: general-purpose computers, software, and operating systems used for single purpose applications (e.g., a safety controller or video camera) have excess capabilities that are a growing target of cyber threat.

Software-based solutions are extremely flexible and offer over-the-Internet maintenance updates that greatly reduce cost, and the resulting economic incentives influenced society to digitize/automate everything possible, even our critical infrastructures. Unfortunately, the convenience of networking and the monoculture created by commodity hardware and software have made these systems the great Achilles'heel of our modern world. The commodity hardware may be far more capable than what is required for the process at hand. This extra capacity is attractive to attackers, as we learned from the Mirai botnet. Commodity software's excessive capabilities extend the attack surface of the systems without benefitting the application.

Reducing this attack surface is the primary objective of this paper. We describe the development and test of a prototype controller that can execute process logic with only hardware. The hardware-only nature of our solution prevents the controller (or any other device built on the same principle) from being repurposed via malware or other network borne cyber-attacks. We solve the cyber problem by removing the software. Our approach employs a Field Programmable Gate Array (FPGA) instead of the vulnerable Von Neumann architecture. We will discuss the novel features of our current prototype and our planned path forward to replace the FPGA with a custom 3D-printed circuit board. Ultimately, 3D printing of circuitry could significantly reduce the cost and cycle-time of the typical Application-Specific Integrated Circuit (ASIC) design process, putting this ability into the hands of each company's process engineer. A prototype controller was developed and tested in 2018 as a demonstration of how a hardware-only controller can be considered as a viable replacement for a PLC, a video camera controller or other IoT device without using software, which significantly reduces the cyber-attack surface.

The apparent inflexibility of hardware-only solutions used to be the major drawback, but their immunity to internet-borne cyber-attack is becoming a major advantage. If this type of system were widely available today, designers could deploy new systems, confident that they could not be maliciously repurposed. FPGA-based hardware-only controllers require physical access to override or replace their physically-programmed functions. They will be provably (not just theoretically) unhackable without direct physical access. The physical access requirement means that system-wide changes cannot simply be rolled out to a national enterprise from a remote location. It is true that the cost of updating hardware-based systems is higher on a per-controller basis. However, most infrastructure systems are not supposed to change function or be updated for decades at a time. Arguably, the reason most security updates or patches are needed today can be traced to the vulnerabilities of software. Thus, many security updates will no longer be needed. For critical infrastructures, the security afforded by this inflexibility will be a major strength that outweighs the incremental cost incurred by the rare need for system updates.

This paper will be presented along with a physical (or video-based) demonstration of the protype and thereby stimulate a discussion about the possible directions within this field of study that might provide more cyber resilient systems for use within the nuclear industry.

Gender

State

United States

Author: PEDERSON, Perry (Pacific Northwest National Laboratory)

Co-authors: FINK, Glenn (Pacific Northwest National Laboratory); CHRISTMAN, Nicholas (Pacific Northwest National Laboratory)

Presenter: PEDERSON, Perry (Pacific Northwest National Laboratory)

Track Classification: CC: Information and computer security considerations for nuclear security