Cyber Physical Systems Security – A Call to Action & Request for Your Participation

There is a critical need for government, industry, and academic collaboration and action in addressing vulnerabilities unique to hardware assurance of electronic parts, assemblies and security of cyber physical systems (CPS). Stakeholders across the supply chain need to look at the problem holistically and address all areas of concern with a perspective towards resilience to cover vulnerabilities unique to the CPS architecture that includes software, firmware, and hardware. There are interdependencies in cyber physical systems security that impact multi-purpose and dual-use (commercial/government) systems that need to be considered with the approach. It is a pervasive threat environment.

What are Cyber Physical Systems?

Cyber physical systems are defined as technologies that combine the cyber and physical worlds that can respond in real time to their environments.¹ Cyber physical systems include electronic parts, assemblies, systems, and system elements that operate as a single, self-contained device or within an interconnected network providing shared operations. An added distinction of this CPS definition is a requirement affecting a tangible output through command and control electronics embedded in the device or distributed across network nodes.² The command and control system could be manipulated through a physical process and/or physical input of the data flow.

Examples of cyber physical systems include wearable medical devices, smart grid, autonomous vehicles, Supervisory Control and Data Acquisition (SCADA) systems, industrial control systems (ICS), Internet of Things (IoT) systems, Satellite Communication Systems for commercial and government integration, and embedded systems that includes software, firmware, and electronics hardware.

How are Cyber Physical Systems Vulnerable?

Attack vectors are introduced through vulnerabilities in electronic parts, systems, and system elements that could be used to compromise cyber physical system function or gain access to critical and sensitive system information. Reported attacks to date were the result of exposed weaknesses due to vulnerabilities in electronic parts, assemblies, and system elements of cyber physical systems which include firmware, software and electronic hardware. The intent of the attacks ranges from economic espionage to denial of service and even more nefarious objectives.

Cyber attackers exploit vulnerabilities in the systems engineering design of the platform that have not been designed for security and resiliency to survive attacks. For example, agents have recorded raids by operatives in some countries, all apparently looking for security weaknesses in electronic parts, assemblies, systems, and system elements in cyber physical systems that could be employed to disrupt the delivery of water and electricity and impede other functions critical to the economy, welfare of our society, and security of our critical infrastructure.³ Satellite hacking

---

¹ The National Institute of Standards and Technology (NIST)


³ Bloomberg. Ugly Gorilla
attacks against Landsat-7 and Terra AM-1 achieved command and control of the cyber physical system (four incidents were publically reported in the years 2007 – 2008). The Stuxnet attack was a game changer on the ability to target attacks on specific cyber physical systems that continues to evolve and be exploited. A recent example includes a state sponsored vulnerability utilizing a tiny chip that could be exploited to infiltrate systems. A recent GAO report noted that DoD is just beginning to grapple with vulnerabilities in U.S. weapons systems that have ‘critical’ cybersecurity problems. Attacks are not only state sponsored on the critical infrastructure, but include attacks on commercial systems, such as commercial vehicles. A Washington Post article notes that “As more physical objects are controlled and operated through the Internet, the possibility that hackers could hurt people or sabotage equipment — as opposed to simply stealing information — may be poised to increase.” Further attacks are being reported on a daily basis.

Hackers exploit vulnerabilities in electronic parts, assemblies, systems, and system elements in cyber physical systems that comprise of a broad range of attack strategies impacting multiple areas of concern (Figure 1). Systems level hackers study the system to determine the vulnerabilities that enable a pervasive attack. Cyber physical systems are susceptible to successful attacks due to unintended vulnerabilities introduced with the integration of complex hardware, software, and firmware supporting the cyber physical system without a holistic and integrated approach to close the gaps in the multiple areas of concern with a perspective of designing resilient systems.

**Call to Action**

The call for action emphasizes solutions using a holistic approach to cyber physical systems security from a systems engineering perspective. A systems engineering approach that includes analysis of the system operating environment defined by the operational, functional, and architectural systems engineering elements can help close the gaps. The solution should include developing a common lexicon of terms and metrics for assessing vulnerabilities associated with design of the system with the goal of a more robust and resilient CPS. This call to action introduces important elements characterizing different risks and vulnerabilities to physical hardware that could impact system level attributes with risks of loss of integrity, disruption of functionality, and loss of availability of the CPS, impacting capability being delivered to customers through the platform.

Solutions should address gaps in the resiliency of hardware assurance and security from persistent threats to cyber physical systems. Standardization is needed to codify the cyber physical systems security framework and to provide requirements and guidance for implementation. The path for designing standardized metrics for effectiveness will include a risk-based design for security to complement prioritized, risk-based, efficient, and coordinated actions

---

4 DefenceTech.Org, October 28, 2011


7 [https://www.gao.gov/assets/700/694913.pdf](https://www.gao.gov/assets/700/694913.pdf)

8 SAE International: Chapter 5, “Engineering for Vehicle Cyber Security. Available at: [https://www.sae.org/publications/books/content/r-464/](https://www.sae.org/publications/books/content/r-464/)

9 [https://www.washingtonpost.com/business/2018/10/10/nearly-all-new-us-weapons-systems-have-critical-cyber-security-problems-auditors-say/?tid=ss_mail&utm_term=.5d9f74ca9d64](https://www.washingtonpost.com/business/2018/10/10/nearly-all-new-us-weapons-systems-have-critical-cyber-security-problems-auditors-say/?tid=ss_mail&utm_term=.5d9f74ca9d64)
utilizing existing best practices and standards as they are available. The advancement of the solution will enable designs of connected systems with built-in self-management of system security embedded within the design.

Therefore, collaboration is proposed that includes government, industry, and academia recognizing a need for action in developing a systems engineering approach to standardization of cyber physical systems security, including the following:

- Characterize the risk of the CPS, assess vulnerabilities, and recommend mitigating actions.
- Advance the knowledge of how vulnerabilities are introduced and exploited in cyber physical systems.
- Identify best practices for addressing different areas of concern utilizing existing processes, procedures, and standards when possible.
- Close gaps in Hardware and Software Assurance (HwA/SwA) and integrate holistic approach through CPSS Systems Engineering Effort.
- Develop a detailed taxonomy for cyber physical system security.
- Establish and standardize methods for identifying vulnerabilities in cyber physical systems that could be introduced at any point in the CPS life cycle.
- Standardize a systems engineering approach to address cyber physical systems security with a goal of designing resilient systems that can survive an attack.
- Develop cost-effective design and evaluation methods for mitigation of risk in cyber physical systems security design that includes assessing effectiveness of solutions.

The call to action emphasizes the sense of urgency to address gaps with a goal of completing standard work by FY 2022 or sooner if possible. The effort will include a roadmap for completion with an emphasis on addressing areas of concern currently uncovered.

Some of the information in this subject area will need to continue to be controlled by government classification programs, ITAR and EAR. The call for action should lead to industry, government, and academic collaboration for addressing the current gaps in the state-of-the-art for cyber physical systems security. The action will enable industry compliance in addressing gaps through industry standard work.

**SAE G-32 Cyber Physical Systems Security Committee**

SAE has approved and chartered the G-32 Cyber Physical Systems Security Committee to address the call to action to codify the cyber physical systems security (CPSS) framework and to provide requirements and guidance for implementation to address the different areas of concern. The G-32 is a cross-sector (e.g., Aerospace, Automotive, Industrial Control Systems, Internet of Things, Medical, etc.) international committee consisting of subject matter experts and policy makers from industry, government and academia.

The G-32 consists of a main cyber physical systems security (CPSS) committee, a software assurance (SwA) subgroup, and a hardware assurance (HwA) subgroup. Members of the subgroups will become members of the main committee for purposes of voting during balloting. All three groups (CPSS, SwA, HwA) plan to meet virtually approximately every other week for an hour to discuss open issues and review contributed work from committee members.
**Request for Your Participation**

We are providing this document as a formal request for your participation in the committee effort. Individuals actively participating in the committee should anticipate approximately four hours per week of time for each effort (CPSS, SwA, HwA) you have been asked as a subject matter expert to contribute. The expected duration of the committee is four years. The time will consist of attending virtual WebEx meetings and working on individual contributions to complete standard work. WebEx meetings for each group (CPSS, SwA, HwA) will be held approximately every other week for an hour. Individuals participating in the effort should also anticipate travel with approximately two face-to-face meetings in regions based on synergistic events (e.g., DMSMS/DMC) or proximity to policy makers (e.g., Washington, D.C. or London). Most face-to-face meetings will have WebEx options for those who are unable to attend in person.

Organizations who have individuals actively participating in the committee will have a voice at the table, and will have an advantage of taking early action to address concerns ahead of standard work that could be invoked in contracts or through regulations. In addition, individuals participating in the committee will have an opportunity to network with peers working on the problem, which provides both excellent benchmarking and business opportunities for organizations addressing the problem, and developing product and service solutions in this space.

---

**Figure 1: Areas of Concern for Cyber Physical Systems Security**