A Holistic Approach to Cyber Physical Systems Security and Resilience

Title	A Holistic Approach to Cyber Physical Systems Security and Resilience
Publication Type	Conference Paper
Year of Publication	2020
Authors	DiMase, D., Collier, Z. A., Chandy, J., Cohen, B. S., D'Anna, G., Dunlap, H., Hallman, J., Mandelbaum, J., Ritchie, J., Vessels, L.
Conference Name	2020 IEEE Systems Security Symposium (SSS)
Date Published	Aug. 2020
Publisher	IEEE
ISBN Number	978-1-7281-4316-3
Keywords	affordable systems, composability, computer security, cyber, cyber physical system security framework, cyber weaknesses, Cyber-physical systems, cybersecurity., Embedded systems, firmware assurance, global supply chain, Hardware, Hardware Assurance, holistic approach, holistic systems engineering approach, Industries, Metrics, Mission Assurance, pubcrawl, resilience, Resiliency, Resilient Systems, risk, SAE G-32 Cyber Physical Systems Security Committee, secure systems, security, security of data, Software, software assurance, Standards, Supply chains, system integrators, system security, system security considerations, Systems Engineering, threats, Trustworthy Systems, Vulnerability

Abstract

A critical need exists for collaboration and action by government, industry, and academia to address cyber weaknesses or vulnerabilities inherent to embedded or cyber physical systems (CPS). These vulnerabilities are introduced as we leverage technologies, methods, products, and services from the global supply chain throughout a system's lifecycle. As adversaries are exploiting these weaknesses as access points for malicious purposes, solutions for system security and resilience become a priority call for action. The SAE G-32 Cyber Physical Systems Security Committee has been convened to address this complex challenge. The SAE G-32 will take a holistic systems engineering approach to integrate system security considerations to develop a Cyber Physical System Security Framework. This framework is intended to bring together multiple industries and develop a method and common language which will enable us to more effectively, efficiently, and consistently communicate a risk, cost, and performance trade space. The standard will allow System Integrators to make decisions utilizing a common framework and language to develop affordable, trustworthy, resilient, and secure systems.

URL https://ieeexplore.ieee.org/document/9197723
DOI 10.1109/SSS47320.2020.9197723
Citation Key dimase_holistic_2020

affordable systems composability computer security cyber cyber physical system security framework cyber weaknesses cyber-physical systems cybersecurity. embedded systems firmware assurance global supply chain Hardware Hardware Assurance holistic approach holistic systems engineering approach Industries Metrics Mission Assurance pubcrawl resilience Resiliency Resilient Systems Risk SAE G-32 Cyber Physical Systems Security Committee secure systems security security of data Software software assurance standards supply chains system integrators system security system security considerations systems engineering threats Trustworthy Systems Vulnerability