Designing agility and resilience into embedded systems

Submitted by K_Hooper on Fri, 02/02/2018 - 11:06am

Title	Designing agility and resilience into embedded systems
Publication Type	Conference Paper
Year of Publication	2017
Authors	Whelihan, D., Vai, M., Evanich, N., Kwak, K. J., Li, J., Britton, M., Frantz, B., Hadcock, D., Lynch, M., Schafer, D., DeMatteis, J., Russo, D.
Conference Name	MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)
Date Published	oct
Keywords	adversarial actors, analytic process guides system developers, ARES methodology, assessment, attack surface, attacker, autonomous aerial vehicles, best-practice security policies, computer security, CPS, cyber resilience, cyber security, Cyber-physical systems, design for cyber security, Embedded systems, Global Positioning System, high level system properties, Measurement, metric set, Metrics, Mission Assurance, mission assurance a challenging problem, mission objectives, mission success, pubcrawl, remotely located communicating devices, resilience, Resiliency, Resilient Security Architectures, RF environment, security of data, System analysis and design, systems analysis, Systems architecture, UAS, unmanned aerial systems

Abstract

Cyber-Physical Systems (CPS) such as Unmanned Aerial Systems (UAS) sense and actuate their environment in pursuit of a mission. The attack surface of these remotely located, sensing and communicating devices is both large, and exposed to adversarial actors, making mission assurance a challenging problem. While best-practice security policies should be followed, they are rarely enough to guarantee mission success as not all components in the system may be trusted and the properties of the environment (e.g., the RF environment) may be under the control of the attacker. CPS must thus be built with a high degree of resilience to mitigate threats that security cannot alleviate. In this paper, we describe the Agile and Resilient Embedded Systems (ARES) methodology and metric set. The ARES methodology pursues cyber security and resilience (CSR) as high level system properties to be developed in the context of the mission. An analytic process guides system developers in defining mission objectives, examining principal issues, applying CSR technologies, and understanding their interactions.

URL http://ieeexplore.ieee.org/document/8170806/
DOI 10.1109/MILCOM.2017.8170806
Citation Key whelihan_designing_2017

unmanned aerial systems UAS Systems architecture systems analysis system analysis and design security of data RF environment Resilient Security Architectures Resiliency resilience remotely located communicating devices pubcrawl mission success mission objectives mission assurance a challenging problem Mission Assurance Metrics metric set Measurement high level system properties Global Positioning System embedded systems design for cyber security cyber-physical systems cyber security cyber resilience CPS computer security best-practice security policies autonomous aerial vehicles attacker attack surface Assessment ARES methodology analytic process guides system developers adversarial actors