

Safety-Security Co-Engineering of Control Systems

Authors : Elena A. Troubitsyna

Abstract : Designers of modern safety-critical control systems are increasingly relying on networking to provide the systems with advanced functionality and satisfy customer's needs. However, networking nature of modern control systems also brings new technological challenges associated with ensuring system safety in the presence of openness and hence, potential security threats. In this paper, we propose a methodology that relies on systems-theoretic analysis to enable an integrated analysis of safety and security requirements of controlling software. We demonstrate how to create a safety case - a structured argument about system safety - with explicit representation of both safety and security goals. Our approach provides the designers with a systematic approach to analysing safety and security interdependencies while designing safety-critical control systems.

Keywords : controlling software, integrated analysis, security, safety-security co-engineering

Conference Title : ICECECE 2017 : International Conference on Electrical, Computer, Electronics and Communication Engineering

Conference Location : Paris, France

Conference Dates : October 19-20, 2017