

Systems Engineering requirements Analysis and Trade-off for Trusted Systems and Networks

*Paul Popick (Aerospace) - paul.popick.ctr@osd.mil
John Miller (MITRE Corporation) - JFMiller@mitre.org*

Copyright © 2013 by Popick, Miller. Published and used by INCOSE with permission

Abstract. This tutorial walks through a case study of a requirements analysis pattern to integrate system security for supply chain and cyber into systems engineering (SE) stakeholder requirements, requirements analysis and architectural design. This tutorial emphasizes the need to more tightly integrate security with the overall systems engineering activities and the systems engineering role. The tutorial illustrates the iterative nature of the analysis and also shows how the analysis feeds the RFP. The tutorial uses the DoD trusted systems and networks analysis pattern as the basis of the tutorial. This analysis pattern has broad applicability across industries and aligns well with the Systems Engineering technical processes in ISO 15288-2008. The analysis pattern consists of a mission / business criticality analysis, a vulnerability analysis, a threat assessment and an information assurance assessment as inputs to a risk based cost-benefit trade-off analysis. Students will gain hands on experience applying the analysis pattern to an Unmanned Aerial Vehicle (UAV) case study. The UAV case study covers the system engineering analysis of a solution in the early lifecycle phases. The interrelationship with the SE technical processes, system specification and the system technical reviews is described. Relationships to other specialty engineering disciplines will be briefly discussed. Participants are expected to have a systems engineering or program management background and experience. They will work in small teams to develop solutions and alternatives to the case study. The tutorial is presented by experienced systems engineers that have worked on major systems engineering efforts for government, communications and retail sectors solutions.

Biography

Paul Popick (Aerospace) - paul.popick.ctr@osd.mil

Paul Popick has over 40 years experience as a program director, systems engineering director, systems engineer, and software development manager. In his current assignment he is supporting the program protection policy, methodology and review of major acquisition programs for the Office of the Deputy Assistant Secretary of Defense for Systems Engineering. Mr. Popick was one of the organizers of the May 2012 NDIA Program Protection Workshop, one of the instructors of the Oct 2012 NDIA program protection tutorial and a co-chair of the INCOSE System Security Engineering Working Group. . In previous assignments, Mr Popick has led portions of major commercial and defense system integration programs for IBM Global Services and IBM Federal Systems Division. Mr. Popick has been an Adjunct Professor in project management at George Washington University, and in Systems Engineering at Johns Hopkins University. Mr. Popick is a Project Management Institute (PMI) certified Project Management Professional (PMP), and an IBM Certified Executive Project Manager. Mr. Popick is one of the originators of the IBM Global Services systems engineering method and has a patent pending for this work.

John Miller (MITRE Corporation) - JFMiller@mitre.org

Dr. John F. Miller Over 38 years of experience in systems engineering and acquisition, software engineering and development, hardware and software integration, systems development, system security engineering, software assurance, program management, quality systems definition and management, engineering and management process definition and improvement, and tactical training devices and Antisubmarine Warfare (ASW) systems. Specific experience in systems and software engineering, program management, executive level support, system security engineering, and process definition and improvement [including, experience in leading the definition and implementation of software and systems engineering/management processes according to the Capability Maturity Model – Integration (CMMI) and the ISO-9001, IEEE/ISO-12207, and IEEE/ISO-15288 Standards].