**Type of proposal:** workshop

**Length of workshop:** half day (3 hours)

**Title:** Internet of Things in Education: the current state and the future

**Description:** The purpose of this workshop is to discuss the up-to-date scenarios where IoT technologies are being applied in Education, and how IoTs may affect positively or negatively the overall learning experiences. Additionally, to the educational application of IoT, discussions on the trust concerns of IoT as well as how to educate engineers to build IoT systems will be presented. A panel discussion will ensue covering software assurance especially addressing the risk of third-party custom software component integration, open source software and/or general-purpose off-the-shelf software.

**Part I: 9:00 am – 9:45 am- Keynote speaker (45 mins)**

Jeffrey Voas, National Institute of Standards and Technology

“The Main Trust Concerns of IoT”

Description: The Internet of Things (IoT) refers to systems that involve computation, sensing, communication, and actuation (as presented in NIST Special Publication (SP) 800-183). IoT involves the connection between humans, non-human physical objects, and cyber objects, enabling monitoring, automation, and decision making. The connection is complex and inherits a core set of trust concerns, most of which have no current resolution. This publication identifies 17 technical trust-related concerns for individuals and organizations before and after IoT adoption. The set of concerns discussed here is necessarily incomplete given this rapidly changing industry, however this publication should still leave readers with a broader understanding of the topic. This set was derived from the six trustworthiness elements in NIST SP 800-183. And when possible, this publication outlines recommendations for how to mitigate or reduce the effects of these IoT concerns. It also recommends new areas of IoT research and study. This publication is intended for a general information technology audience including managers, supervisors, technical staff, and those involved in IoT policy decisions, governance, and procurement.

**Part II: 9:45 am – 10:30 am Speakers (45 hour)**

Mohamand Kassab (30 min)

“How Could Internet of Things Change the Way we Think and Learn?”

Description: Internet of Things is a rapidly growing network of a variety of different connected objects. Now, because of their ubiquitous nature, educational institutions are looking to incorporate IoT technologies in the teaching and learning activities. This paper contributes to
the ongoing discussion on the benefits and challenges of incorporating IoTs in education. More precisely, it provides 1) a summary that reports on results of a systematic literature review we conducted on IoT in education, 2) a framework for describing and classifying scenarios that involve IoTs for education, 3) a demonstration of a tool we developed to provide an adaptive learning experience in response to a remote learner’s emotions, and 4) a discussion on two domain-related quality requirements in IoTs for education; namely, security and humanization.

Joanna DeFranco (15 min)

Description: Educating the next generation of engineers to be able to design and develop the rapidly increasing need for Internet of Things (IoT) and Cyber Physical System (CPS) devices is imperative. The goal of this study is to determine the state of this educational need. This paper presents a: (1) mapping study to learn about existing research and proposed courses educating students to build IoT and CPS systems; and a (2) Programs Review for CPS/IoT-related courses currently being offered at the top 50 universities ranked by Collegechoice.net. The resulting courses from the mapping study and programs review are extensively analyzed and mapped to the NIST Network of Things primitives and the ACM/IEEE Computer Science Knowledge Areas. In addition to highlighting specific projects, the goal of this paper is to assist in the effort to build or adapt programs that academic institutions currently offer to meet the current and future IoT/CPS training and employment needs.

Coffee Break (10:30 am – 10:45 am) (15 minutes)

Part III: 10:45 am – Noon - Panel (1 hour 15 min)

Dr. Thierry Wandji, Dr. Stacy Prowell, Dr. Robin A. Gandhi, Ms. Keesha M. Crosby

“Software Assurance and Software Certification for High Assurance Mission Critical Systems”

Description: According to DoD, Software Assurance relates to the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software. Nowadays, many DoD developed weapon systems are software-intensive systems; which mean that software controls a significant portion of weapon systems functionalities or capabilities. This software is often an integration of components including third-party custom software, open source software and/or general-purpose off-the-shelf software, limiting our understanding of risk. DoD needs a robust software security certification process that provides the evidence necessary to manage such risk in high assurance environments. Software development processes for high assurance environments can benefit from an integrated certification framework that helps assess, measure, and manage security risk originating from software artifacts. This panel will discuss how NAVAIR is attempting to tackle this problem.
Workshop Leaders:

Mohamad Kassab (muk36@psu.edu) is an associate research professor in Software Engineering at Penn State Great Valley. He received his Ph.D. degree in computer science from Concordia University in Montreal, Canada. With more than 18 years of industrial experiences, he worked in different roles before establishing his career in academia, among which: senior quality engineer at SAP, senior associate at Morgan Stanley, senior quality assurance specialist at NOKIA, senior software developer at Positron Safety Systems. Dr. Kassab’s research interests include developing a formal, integrated and quantitative approaches, architectural frameworks and tools to modeling and assessing software quality requirements.

Joanna F. DeFranco (jfd104@psu.edu) earned her Ph.D. in computer and information science from New Jersey Institute of Technology, M.S. in computer engineering from Villanova University, and a B.S. in Electrical Engineering and Math from Penn State University. She is an Assistant Professor of Software Engineering with the Pennsylvania State University. She worked in industry for 12 years as an Electronics Engineer for the Navy as well as a Software Engineer at Motorola. Her research interests include software engineering teams, Internet of Things, and effective communication and collaboration in technical teams.

Workshop Speakers:

Dr. Jeffrey Voas is a computer scientist at the National Institute of Standards and Technology (NIST) in Gaithersburg, MD. Before joining NIST, Voas was an entrepreneur and co-founded Cigital (1992). After 13 years at Cigital, Voas accepted a director position at Science Applications International Corporation (SAIC) and was named an SAIC Technical Fellow (2005-2009). He has served as the IEEE Reliability Society President (2003-2005, 2009-2010), and serves as the IEEE Computer Society's Second VP (2010). Voas is IEEE Division VI's Director-Elect (2010)

Dr. Stacy Prowell serves as the Chief Cyber Security Research Scientist and is the Program Manager for the lab's Cybersecurity for Energy Delivery Systems program. Dr. Prowell's research focuses on exploiting physical sensors and properties to detect and prevent intrusion, and on deep semantic analysis of compiled software. Dr. Prowell's work on a system for deep analysis of compiled software led to the Hyperion system, which received a 2015 R&D 100 award and two awards for technology transfer. Previously, Dr. Prowell worked in the CERT Program of the Software Engineering Institute on automated analysis of malware. Dr. Prowell is an IEEE Distinguished Lecturer for the Transportation Electrification Community. In his spare time Dr. Prowell is an Associate Professor of Electrical Engineering and Computer Science at the University of Tennessee, an Associate Professor of Computer Science at Tennessee Technological University, and is a member of Sigma Xi and a senior member of the IEEE.
Dr. Robin A. Gandhi is Charles and Margre Durham Associate Professor of Information Assurance at the University of Nebraska, Omaha. He has conducted several case-studies to explore the problems with requirements, secure coding activities and risk assessments in practice. He received his Ph.D. from The University of North Carolina at Charlotte. AFOSR, NIST, NASA, NSF, DHS S&T and AFRL have supported his research. He is a member of IEEE and ACM professional communities and the DHS Software Assurance Workforce Education and Training Group. His recent activities have brought software assurance requirements to the forefront of the US federal assessment and authorization process for IT systems.

Dr. Thierry Wandji is the software security technical lead for Navair and Cybersecurity Professor at the University of Maryland University college and Morgan State University where he is involved in many research projects on software security risk assessment. He has over 15 years of software reliability and security research experience and has coordinated and led multiple advanced research projects to develop tools to quantitatively assess the cybersecurity risks and software maturity in naval aviation. Throughout his career, Dr. Thierry Wandji has worked for IBM and Rockwell Collins before joining NAVAIR. He received his Ph.D from George Washington University.

Keesha M. Crosby is the Founder of Tri-Guard Risk Solutions. Ms. Crosby has more than 20 years hands-on experience in security engineering. Ms. Crosby earned her Bachelor of Science Mathematics from Tuskegee University and Masters in Systems Engineering from George Washington University. Her research was published by NIST in SP 800-160 Appendix J and serves as the first ever software assurance controls. She has published software security articles in peer reviewed journals like such as IEEE and Crosstalk (Defense Software Engineering Journal). She was recently awarded a patent for upcoming product - Software Assurance Compliance-verification and Risk Evaluation (SACRE).