Carnegie Mellon University
Software Engineering Institute

Cyber-Physical Infrastructure Assurance

Reason for a Cyber-Physical Infrastructure Assurance

The Assistant Secretary of the Air Force for Installations, Environment, & Energy (SAF IE) is committed to increasing the energy assurance of Air Force (AF) installations.

Several Department of Defense (DoD) documents[1] provide the overarching guidance for addressing physical and cybersecurity. However, additional guidance and processes are needed to identify, assess, and reconcile the end-to-end mission threads and commensurate physical and cybersecurity threats to energy infrastructure.

The Reason AF OEA Worked with the SEI: Mission Thread Expertise

The AF Office of Energy Assurance (OEA) is tasked to develop an enterprise approach for systematically implementing physical, cyber-secure energy assurance initiatives supporting mission critical assets.

Because the cyber-physical infrastructure is a system of systems (SoS), OEA looked to SEI to lead program and portfolio mission thread development/analysis and security engineering risk assessment tasks. A mission thread is a sequence of end-to-end activities and events that takes place to accomplish the execution of an SoS capability.

SEI offers expertise in augmenting mission threads to shape SoS architecture and identify architectural risks through its Mission Thread Workshop (MTW). In this facilitated set of three phases, SoS stakeholders augment mission threads with quality attribute considerations, such as availability and security.

OEA tasked SEI to identify, assess, and reconcile the end-to-end mission thread and commensurate physical and cyber security threats.

SEI's Role: Mission Threads and Cybersecurity Risk Analysis

In this 2017 work, the Carnegie Mellon University Software Engineering Institute (SEI)

- Conducted three MTWs, one for each of three OEA priorities activities
- Provided cybersecurity engineering risk analysis to support execution of the MTWs. SEI has conducted MTWs with other customers to describe missions in context, identify attacks, illuminate attack scenarios, and highlight potential vulnerabilities that make SoS susceptible to attack.
- Developed a set of challenges (quality attribute/architecture, capability, and engineering), with assessment of impact and recommendations for mitigation, from the augmented mission threads

[1] Including Instructions & Directives on Installation Energy, the Defense Critical Infrastructure Program, Mission Assurance, Protection of Mission Critical Functions, and Risk Management Framework

OEA Use: Improve Management of Requirements

The augmented mission threads and the challenges can be used by OEA to integrate physical and cyber-security requirements and risks in energy assurance portfolio management.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-0372