A.8. Systems Security

Systems Security and Risk Mitigation. Management and mitigation of security risk is an essential component of modern technical and socio-technical systems. This stream will explore identification, management, and mitigation of risks in systems security themes, including security in electronic and information systems, physical systems, and cyber-physical systems.

Lead: Obaid Khan, Khairulzaman Kamarulzaman
Domains: Cybersecurity

Submissions Summary:

1. Vehicle Diagnostic Security Advancement using an MBSE Approach (Full Paper)

20734 Vehicle Diagnostic Security Advancement using an MBSE Approach

Sarah Rudder 1, Enola Technologies, ST. PETERSBURG, FL, United States

Keywords: security,MBSE,safety,reliability

Type: Full Paper
Stream submitted: A.8. Systems Security

Overview Medium and Heavy-duty (MHD) vehicles often require maintenance and diagnostics during normal operations. Vehicle Diagnostic Adapters (VDAs) are the service tools that connect the vehicle network systems to the diagnostics and maintenance software. These diagnostic tools are intermittently, but frequently connected to the vehicle by a trusted technician, but many security models ignore technicians physically connecting to the vehicle. Context VDAs are made by third parties and the specification for them lacks security controls around this operation has prompted the trucking industry to develop new security protocols for diagnostics in the International Organization of Standards (ISO) 14229. In light of the potential security concerns associated with MHD vehicle diagnostics, a Threat Analysis and Risk Assessment (TARA) is presented using Risk Assessment and Analysis Modeling Language (RAAML). Purpose This research seeks to understand how RAAML can be utilized to follow a cybersecurity approach in a modeling environment in the context of Systems Engineering (SE) activities throughout the system lifecycle. SE responsibilities that pertain to risk identification, assessment, and management include, but are not limited to, deliverables such as Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA). Approach A digital representation of the MHD vehicle diagnostic and maintenance system can be designed using Model-based Systems Engineering (MBSE). The presentation will start with a model-based description of the diagnostics system of interest, then do a deep dive into the threat analysis and risk assessment using RAAML. Insights Capturing FMEA and FTA inputs and outputs in the model enables more complete traceability and re-usability, reducing re-work and giving more transparency for risk analysis of the system design.
