Position Paper to the National Workshop for Research on Transportation Cyber-Physical Systems: Automotive, Aviation, and Rail

Robert Patrick Benito

The MITRE Corporation

4830 W. Kennedy Blvd. Suite 790, Tampa, FL 33609

Email: rbenito@mitre.org Voice: 732-266-6933

Cyber-physical systems are inherently dangerous. Aircraft, automobiles, trains and medical devices contain functionality that have the potential to malfunction and cause injury, death and/or environmental damage. As technology advances, these systems are taking on new characteristics. They are evolving from stove-pipe systems that require a human to be in the loop of safety critical decisions and actions, to system of systems (SoS) that operate autonomously requiring little, if any, human interaction. As these systems evolve, so must our approach of dealing with system and software safety. We must find new methods, tools and technologies to ensure the safety critical functions within these SoS are intellectually manageable and can be developed to meet certification authority requirements in addition to market demands. Further researching certain technologies and concepts can help make future SoS more intellectually manageable, easier to safety certify and provide a lower cost, more scalable alternative to current designs.

Topic: Innovations, Ideas, Abstractions and Terminology for Cyber-Physical Systems

- **What innovations and abstractions should be considered for future transportation CPS?**
    - Safety certifiable virtualization technology. Virtualization offers many benefits in the commercial IT sector. There needs to be more research into how virtualization technology (the virtualization software and supporting infrastructure) can be applied to a CPS (e.g. having multiple VMs running control programs with various safety and security levels and marshalling the interaction to prevent a hazard) to help identify the product requirements and qualities needed in a safety and security certifiable

virtualization technology. The safety and security certification feasibility of this technology will also be needed to justify the benefit.

- Cloud computing. In certain CPS, access to safety critical data must be guaranteed to make decisions and certain computer systems that control a CPS must have ultra high availability and reliability to ensure safe operation. Research into how cloud computing can be used as a cost effective solution to solve these issues (e.g. having a VM that controls an autopilot system dynamically move from a failing piece of hardware to a healthy piece of hardware) and qualities needed in safety certifiable cloud computing technology. The safety and security certification feasibility of this technology will also be needed to justify the benefit.

- Certifiable software agents and their supporting infrastructure. Software agents have the potential to aid in the decentralized management and control of CPS. Research needs to be conducted on software agents that can "learn" about the CPS environment, the CPS itself, and behaviors of people controlling CPS. These agents can be developed to process many factors that exist prior to a CPS mishap to help identify mishap causal factors and either take corrective actions or alert an operator. "Lessons learned" can be "shared" with other agents to increase their "knowledge."(e.g. A software agent in a vehicle that identifies an incoming snow storm, and automatically performs an inspection on the safety devices that will be needed to operate safely in a snow storm, and finds that the computer hardware controlling the traction control safety features is close to failure. The agent can warn the driver, notify a mechanic and order the part.) Research should also be conducted on software agents that have the ability to control a CPS and have the ability to "learn" from mistakes and "share knowledge" so that the communities of controlling agents continually improve their control capability further ensuring a safe CPS operation. There needs to be more research into how software agents can be applied in a CPS and identify the product requirements and qualities needed to make this technology safety certifiable. Determining the certification feasibility of this technology will also be needed to justify the benefit.

- Enhanced safety critical computer aided software engineering (CASE) tools and languages to support modern concepts (e.g. Safety Certifiable Java and JVM). Researching the feasibility of utilizing modern development tools and technologies that shield the modern day developer from the underlying complexities (e.g. memory management) can help avoid anomalies in software that have the potential to negatively impact system safety. Research also needs to be conducted to develop advanced safety specific modeling and analytical tools to enhance system safety activities. Ideas for these types of tools would include a tool that allows a safety

engineer to model a system in a simulated environment and have the simulation run continuous variations of external stimuli to identify any that place the system in an unsafe state. This type of a tool would be extremely helpful in a SoS environment where all variations of system interactions may not be known.

Topic: Architectures for common and specific Cyber Physical Systems

- **What are the three fundamental limitations in the design and implementation of today's automotive, aerospace and rail CPS? Possible topics include:**
  - Today's CPS lack certifiable virtualization technology.
  - Development of CPS lack of modern certifiable programming languages and development tools. The safety critical market is still utilizing C and Ada – the industry needs more modern languages and tools for implementation. The safety domain also needs advanced modeling tools to aid in testing system interactions in a SoS environment.
  - CPS development methodologies are extremely rigid and more agile methods of design, implementation and certification need to be developed.

About the Author

Patrick Benito is a Senior Information Systems Engineer for the Agile Engineering and Interoperability department with The MITRE Corporation. He is currently leading new research efforts within the U.S. Army that focus on the feasibility of using new development methodologies and technologies for safety critical systems. He began his career as a software engineer working on safety critical systems for the U.S. Army and has contributed to the U.S. Army Fuze Safety Review Board Requirements and Guidelines for Evaluation of Software for Use in Fuze and Fuze Safety and the emerging ISO Standard: Information Technology — Programming Languages — Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use.