White paper for National Transportation CPS Workshop

Building Blocks for High Assurance Cyber-Physical Transportation Systems

Manimaran Govindarasu, Dept. of Electrical and Computer Engineering, Iowa State University (gmani@iastate.edu)

In traditional IT systems security properties, such as confidentiality, integrity, and availability are important in that order. However, control systems used in transportation systems (e.g., avionics, automotive, and train) require these properties in the reverse order of importance: availability (high priority), integrity (medium priority), and confidentiality (low priority). In addition, these systems are safety-critical real-time systems that not only require functionally correct results, but also timeliness of these results; importantly, safety is the foremost consideration in these systems. In this context, when we think about safety-critical transportation systems, all these system properties – performance, safety, and security – are important at varying degrees depending on the operating and failure modes of the system; often, there exist tradeoffs between these metrics.

Following are some key research questions in design, verification, and validation of future transport CPS systems:

1. **Performance vs. Safety vs. Security tradeoffs**

   Development of computational models, resilience metrics, and control algorithms that tradeoffs real-time performance vs. safety vs. security properties of the CPS system. Defining operational modes and developing adaptive control algorithms that balance these tradeoffs to optimize system resiliency in the face of both faults and cyber attacks is an important research problem. Resiliency metrics need to be hybrid combining multiple attributes of the system. There is a clear need for innovative techniques and computational tools that achieve a higher level of security with minimal computational overhead to the extent not to affect the real-time performance of the system.

   - Workload characterization: Traditional workload modeling focuses on real-time (and QoS) metrics and security metrics in isolation. It is important that a holistic workload characterization for CPS transport systems must capture QoS (bandwidth, delay, delay-jitter, loss, and synchronization requirements) along with security metrics (availability, integrity, confidentiality, authentication, and non-repudiation). Such workload models will aid the development of adaptive algorithms to balance the various design tradeoffs.

2. **Attack-resilient transportation systems**

   Faults are naturally occurring events due to component and/or subsystem failures; fault modeling and risk modeling of such events are fairly well understood in CPS systems. However, naturally occurring extreme events (such as hurricanes) and cyber attacks exhibit much higher level of uncertainty and hence attack-modeling and risk modeling are much more challenging and least understood. In particular, in the case of cyber attacks, the attacker has control over space (where to attack?), time (when to attack?), and their coordination (coordinated cyber attack vector) so as to maximize the system impact in terms of affecting safety, performance, and/or security properties.

   There is a clear need for developing realistic models for threats, attacks, and consequences that will result in quantitative risk models and mitigation algorithms. How to transform fault-resilient transportation of system of today to attack-resilient transportation of the future taking into safety properties and accounting the uncertainty associated with cyber attacks and naturally occurring extreme events.

3. **Modeling human-behavior in CPS systems:** Security vs. Usability tradeoff needs to be taken into account while designing secure control systems. Human-induced delays or inadvertent operations can affect real-time and safety properties (e.g., recent train accident in NYC). Therefore, human behavioral models (e.g., pilot or operators) need to be integrated with cyber-physical models in the overall modeling and control framework.