Scalable Design of Cyber-Physical Transportation Systems

Dionisio de Niz
dionisio@sei.cmu.edu

While the day to day perception of a transportation system is simple for the individual, with perhaps the most common being the automobile in the US, the complexity of these systems is hidden. Perhaps most obvious in our days is the complexity of the coordination of massive transportation systems. For instance, the coordination of the use of track in the railroad system, or the air-traffic control systems. While current coordination systems solve our current problems, failures in these systems such as train collisions, airplane collisions and near collisions, as well as the problems in the development of new systems to replace the old ones signal the shortcomings in our current capacity to deal with the complexity of the new generation of these systems.

The complexity of transportations systems is not only increasing over the years but also spreading to all sectors of the industry. In particular, automobiles are becoming increasingly complex with ABS brakes, Electronic Stability Control Systems, Automatic Parking Systems, and even Radar devices to warn the driver about objects in the blind spots of the mirrors. All these innovations are still applied to the individual vehicle. However, the real leap in complexity will happen when coordination systems arrive to cars. Sample projects such as the Coordination Cruise Control by U.C. Berkeley that controls the speed of the vehicles in a platoon formation explore the benefits and complexities of these coordination systems.

Coordination systems in the transportation industry need to be safe. Specifically they need to improve the safety of all coordinated vehicles at the same time they optimize resources. It is interesting to note that, without coordination systems, safety decisions are fully distributed with each driver taking his own decisions. As soon as we start centralizing the decisions (i.e. to schedule resources), the number of points of failure needed to produce a failure starts to reduce and hence their probability of the failure to increase. As a result, we need to keep a fall-back path that can end in the individual vehicles again. This means that we will have multiple control loops at different network distances with different end-to-end timing requirements that should be properly composed.

Partitioned Design for Coordinated Decisions

The different sectors of the transportation industry all need coordination mechanisms with embedded fail-safe reaction paths composed of converging independent decisions. While some of these mechanisms already exist or are currently under development for the aviation sector, the cost of fuel and the increased traffic impose new challenges. This also applies to the automotive and rail sectors where the need of additional automation to achieve a safer and

more cost-effective operation is needed.

These trends raise the complexity of transportation systems to new levels. However, the current development process consists of design decisions that do not scale. That is, the side effects of a single design decision are numerous and complex to be evaluated in the mind of the designer. For instance, a designer may decide to use a multi-core processor to increase the performance of the system. However, this means that additional parallelism (threads) may need to be created along with protected shared data, say with mutexes. Now, to properly handle priority inversion he may decide to use the priority ceiling protocol (PCP) to also avoid deadlocks. However, the designer may forget that PCP relies on having a single highest priority thread running to ensure that no other thread would run and acquire another mutex that could lead to a deadlock. Since in a multi-core processor, more than one thread can be running at any one time, and PCP would not be able to prevent deadlocks. This example shows the set of side effects and assumptions that need to be analyzed when a decision is made.

The coordination of the airspace has been coordinated by traffic controllers. As the number of flights increases, the need of additional automation becomes evident. New systems are being studied for the next generation of air traffic control that increases the safety of the airplanes and avoids human errors. As cars follow these tracks, we would certainly observe that the number of vehicles to track and coordinate would be orders of magnitude larger. To get to these numbers it would be important to avoid centralization of control, i.e., traffic controllers, but should also observed equivalent safety. The complexity of this system gets further complicated provided that different manufacturers would create vehicles that later would need to interact among them in real-time. For instance, if a collision avoidance algorithm of a car brakes suddenly it would need to ensure that the car behind it can also brake on time. This could be done if this other car also has a similar mechanism and they can coordinate with each other. This pattern could be repeated to all the cars behind. The presence of cars without these algorithms will increase the complexity of the system provided that they would need to consider slower human reactions. In addition, given that different manufacturer develop these mechanisms; they would have the double mission of differentiate their mechanisms to provide incentives to purchase this car and to coordinate so that even though they provide different reactions, these reactions can all work together. This calls for a partitioned development processed coordinated by industry policies and standards along with certifications processes to ensure its safety.

One of the critical challenges in this arena is the transformation of the development process into a process of scalable design decisions where the safety of these decisions is verified. Such verification includes ensuring that the behavior of the independently designed mechanism that composed in an ad-hoc manner with other individual vehicles converging to a safe behavior. This involves the standardization of the critical concerns with a single interpretation that can be certified. In turn, this can lead to the standardization of the critical analysis techniques that can be certified against reference models of behavior, e.g., coordinated braking. These reference models of behavior then could be verified by a certification authority that later could analyze and certify individual products against these models.

Achieving Scalable Design Decisions

Model-Based Engineering (MBE) is a promising approach that increases the scalability of design decision by increasing the level of abstraction of the design process and automatically analyzing the side effects of the design decisions. Increasing the level of abstraction involves developing new building blocks that address the issues of interest. For instance, using real-time tasks scheduled with a fixed priority and rate-monotonic scheduling restricts the behaviors to a well-defined behavior where deadlines can be verifies. This example leads us to the second piece of MBE: analysis. This means that the new high level building blocks should be analyzable so that we can consider the side effects of a specific design and design decisions.

Enabling MBE for transportation systems involves defining the high-level system constructs and architectural patterns along with the analysis algorithms to evaluate designs using them. Additionally, the interactions between different constructs and analyses should be taken into account as well as the different assumptions of these constructs.

One of the key innovations needed for transportation systems is the design against industry-wide policies for safety behavior convergence, e.g., ad-hoc composed fail-safe behavior. The creation of new abstractions for industrial policies that can be verified against is a must. One of this potential abstractions is a reference model of behavior along with the analysis techniques and the automated development through models that is able to rule-out undesirable side effects of the a specific design. Such models would need to take into account an incremental adoption. That is, these models should account for participation of individual vehicles that do not have any automation.

Additionally, the optimization of resources in the transportation industry would take a central role in the future. However, given that the consumer of the resources (e.g. driver, pilot, airline), and the developer of the technology (e.g. car or airplane manufacturer) are both independent individuals, efficient policies and algorithms that take into account this individuality will be required. For instance, the assignment of air traffic route can be related to the number of passenger in a specific flight, the type of plane, and the cost structure of the airline. As a result, a dynamic route assignment algorithm could auction routes so that flights can optimize across legs of the flight (for multiple stop flights), and across flights that feed each other, while the global policy could be to reduce the number of routes to minimize the cost of their operation.

Dionisio de Niz is a senior member of the technical staff of the Software Engineering Institute at Carnegie Mellon University working on the evolution of the SAE AADL standard. He holds a Computer Engineering Ph.D. from Carnegie Mellon University. His research interest includes model-driven development of embedded real-time systems and real-time systems in general.