Trains, Planes, and Automobiles

Panagiotis Tsiotras, Eric Feron, and Marilyn Wolf

Georgia Tech

Car and airplane designers each have lessons that they can teach the other. This paper concentrates on what we think automotive designers can learn from aircraft designers, with a short note on the converse. We will also consider some key issues that both disciplines need to work on.

Cars and airplanes have some common constraints:

- Safety-critical subsystems.
- Non-safety critical subsystems that may interact with the safety-critical subsystems.
- Functionality assigned by role: pilot/driver vs. passenger, etc.
- Similar trends in avionics/automotive electronics platform architecture development.

Recognizing these similarities, traditionally, the automotive industry has followed the steps of aircraft industry when it comes to on-board control systems. Figure 1 summarizes this connection over the years.

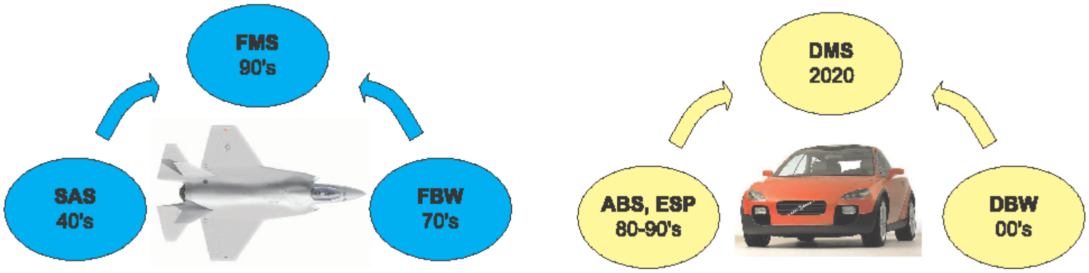

Figure 1: The automotive industry can use the experience from aerospace industry for developing the next generation of active control systems for passenger vehicles. Initially using only stability augmentation systems (SAS), the aerospace industry has moved to fly-by-wire (FBW) and complete flight management systems (FMS), whose purpose is to alleviate the pilot's workload and make sure that the airplane does not violate its design limits ("envelope protection"). A similar technology roadmap will lead to the development of "drive-by-wire" (DBW) and "drive-management systems" (DMS) for the next generation of passenger vehicles.

The first control systems introduced in airplanes were relatively simple stability augmentation systems (SAS), whose main objective was to increase the stability of certain modes of the airplane (e.g., modify the damping and natural frequency of the short-period mode, increase the damping of the dutch-roll mode, etc). With the advent of fast and reliable computers, and the development of more sophisticated control algorithms, the airplane manufacturers moved quickly to more comprehensive flight managements systems (FMS) which use actively controlled modules, known as "fly-by-wire" (FBW) systems. FBW systems, originally developed for high-performance military fighter aircraft are truly feedback systems: the on-board computer(s) intercepts the pilot's commands, interprets them accordingly, and decides the actual actuator input to apply at each instant of time. With a FBW system there is no direct mechanical connection between the pilot and the actuators. It is the job of the FBW/FMS system to alleviate the pilot from excessive workload and make sure that the airplane flies within its designed flight envelope ("envelope protection"). The success of

FBW systems has made them a standard component in all current military aircraft as well as in the new generation of civilian aircraft. Incidentally, the Airbus A320 was the first civilian aircraft to use FBW (late 80's). The benefits in noise reduction, passenger comfort and fuel economy as a result of the use of the FBW persuaded other aircraft manufacturers to incorporate FBW in their airplanes. Boeing's B777 FBW/FCS can fly the airplane even with a single engine failure, and it can even land the airplane completely autonomously, without the pilot's intervention.

Current active safety systems on-board passenger vehicles (e.g., ESP, TCS, ESP) can be best classified as the equivalent of “SAS automotive technology.” Their purpose is to maintain/increase stability. The next logical step is the development of “drive-by-wire” (DBW) and drive management systems (DMS) similar to the FBW and FMS the aircraft industry has embraced long time ago. Such systems will not only help avoid dangerous, abnormal driving conditions, but they will also ensure safe escape from these conditions initiated by the driver because of his improper (re)action.

Despite the apparent similarities, there are also distinctive differences between aircraft and automobiles.

- Airplanes are much more sensitive to weight costs.
- Airplanes must be certified in both design and manufacture, while cars do not.
- Airplanes have much longer lifespans.
- Cars are driven by operators with relatively little experience while airplanes are flown by highly trained pilots (and often crews).
- Airplanes receive much more careful maintenance from licensed mechanics.
- Cars evolve in much more complex environments than airplanes do.

The fact that the human operator on an airplane is an “expert” has certain ramifications in the way the control system is designed and is (supposed to be) operated. The pilot licensing process ensures, for instance, that certain standards are maintained. This implies some “uniformity” in terms of expected pilot performance. Airline pilots receive recurrent training that enforces even more uniformity. This is not the same for vehicles, where the driver abilities, health, age and condition vary widely (not to mention the plethora of vehicle types).

The previous observation raises the issue of customization (or adaptation/robustification) of the car control system to the individual driver and/or vehicle. Do we currently have verification and validation (V&V) methods for such customized systems that are platform, operator and environment independent?

We also believe that aircraft avionics systems are not designed to be sufficiently robust to attack. We believe that automotive electronics systems must be even more robust than avionics systems because both their passengers and mechanics are less firmly vetted.

Embedded computing systems are prone to a variety of traditional attacks, such as denial-of-service. However, because they operate in real time, they are also vulnerable to new classes of attacks. For example, quality-of-service attacks do not need to disable the server, only delay its response to deadline-driven computations. Even if a node in the network does not pass on messages, it may be distracted by QoS attacks. This is most important for the envisioned new “infrastructure to vehicle” (I2V) and “vehicle to infrastructure” (V2I) or “vehicle to vehicle” (V2V) architectures (see Figure 2).

Automobiles are also more vulnerable to mechanics’ attacks than are airplanes because car mechanics are not licensed. Engine controller hacking has been a popular hobby for over 20 years. Consider a malicious bug introduced into a number of engine controllers that cause these engines to stop at a preset time. The resulting accident would only be worse if not all cars were infected with the bug.

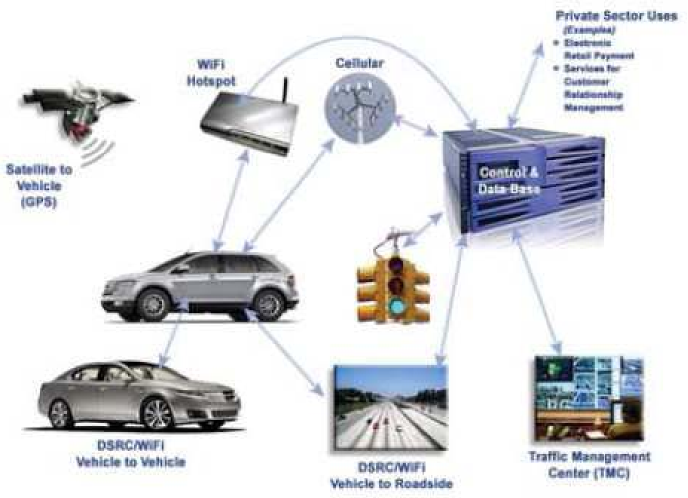
Private Sector Uses
(Examples)
• Electronic Retail Payment
• Services for Customer Relationship Management
WiFi Hotspot
Cellular
Satellite to Vehicle (GPS)
Control & Data Base
DSRC/WiFi Vehicle to Vehicle
DSRC/WiFi Vehicle to Roadside
Traffic Management Center (TMC)

Figure 2: In the future, drivers, vehicles, roads and traffic management systems will be joined together in an interconnected network making use of V2I, I2V and V2V technologies. It is imperative to ensure the integrity of the envisioned network infrastructures from attacks, such as denial-of-service. (Figure from, B. Gharavi, K. V. Prasad, and Ioannou P. "Scanning advanced automobile technology" in Proceedings of IEEE, Special issue on advanced automobile technologies, pp. 328–333, February 2007).

One would think that aircraft would be considerably advanced at this point in the development of secure avionics platforms. However, in our view, current computing platform architectures are not sufficiently robust to withstand failures and attacks to appropriate levels of reliability. Modern aircraft contain multiple networks: safety-critical, operationally important, passenger comfort. These networks are often separated by firewalls. First, we believe that safety critical networks should be physically and logically separate. Second, we need to develop firewalls that are designed to handle both traditional and embedded attacks. Airplanes often combine safety-critical and non-safety-critical data on the same network to save weight; cars often do the same to reduce cost. We believe that more work needs to be done to ensure that the hardware and software of such communication networks are safe and reliable.

Attacks do not necessarily have to be deliberate. Modern computer systems rely on software upgrades. Upgrades can cause many types of problems: software incompatibility, timing problems, etc. (We point out that HP printers use software from a wide range of programming languages and designed over decades; these printers use digital signatures to verify compatibility between modules at run time, a truly scary prospect.) Users can also cause problems by connecting their computers to the vehicle network, as much by compatibility as by malicious intent. Some combination of proper design and usage methodology may be required to ensure safe operation.

Panagiotis Tsiotras is professor of aerospace engineering at Georgia Tech. His interests include the guidance and control of aircraft, ground vehicles and spacecraft. His contact information is tsiotras AT gatech.edu / 404-894-9526.

Eric Feron is Dutton/Ducoffe professor of aerospace software engineering at Georgia Tech. His interests include safety-critical systems such as aircraft and automobiles. His contact information is feron AT gatech.edu / 404 894 3062.

Marilyn Wolf is Rhesa "Ray" S. Farmer, Jr., Distinguished Chair in Embedded Computing Systems at Georgia Tech. Her interests include embedded computing architectures and system design, VLSI systems and biochips. Her contact information is marilyn.wolf AT ece.gatech.edu / 404-894-5933.