# Bridging Aero and Auto CPS: Secure Software and Data Distribution*

Krishna Sampigethaya, Walter Beck, Kristy Lane, Scott Lintelman (The Boeing Company),
Radha Poovendran (University of Washington)

## Introduction

Transportation sectors are today faced with grand societal challenges of accommodating an unprecedented traffic increase, while improving travel safety, comfort and convenience, fuel efficiency, environmental benefit, and stakeholders business. Commonalities are emerging in the way aerospace and automotive sectors are responding to these grand challenges. A high-level example is the "Infotronics"[1] and the "e-Enabling"[2] visions – both broadly view a vehicle to seamlessly traverse as a CPS node in a geographically spread information network consisting of ground infrastructure, satellites and vehicles, providing network users and society with expected services as well as all the information needed to react at the very best moment. Other recent examples include the use of onboard GPS, WiFi-enabling of aircraft[3] and automobiles[4] and logical separation of in-vehicle networks. We aim to leverage such commonalities and address the following emerging problems in the automotive sector.

## Refresh and Retrieval of Vehicle's Digital Content

The future automobile will be highly dependent on software for mixed-critical functions – from the complex control of vehicular behavior to the new "infotainment" features for vehicle users. It is envisioned capable of producing and communicating data for remote diagnosis of vehicle systems (e.g., tires, engine, transmission, air bags, stability control), and vehicle environment (e.g., traffic, roads). Promising applications of such a programmable automobile warrant the need for lifecycle maintenance of embedded software and continuous retrieval of onboard data. Further, recent safety/recall events in the automotive sector indicate that vehicle hardware and software maintenance must be performed more frequently, securely and proactively than today's scheduled, vulnerable, reactive process. Furthermore, as the type and number of sensors/computers on an automobile increases the number of stakeholders and onboard equipment owners for the automobile increases, bringing in the consideration of systems-of-systems.

Additionally, software updates and onboard data are critical to guarantee safety, performance, comfort, and convenience of the future automobile. It is vital to protect integrity of software updates and onboard data during their distribution to and from network-enabled vehicles, by ensuring that they have not been tampered with and that they are from authorized, correct sources. Confidentiality of some software and vehicle information transfers mandates that data distribution over networks be protected. Therefore, a major challenge is to securely refresh and retrieve digital content of ground vehicles and support automobile product lifecycle management, while accounting for all of the above constraints.

Today, refresh and retrieval of an automobile's digital content rely on local access to the automobile at an authorized maintenance facility. Major drawbacks with this arrangement is the

---

* Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors, and should not be interpreted as the views of The Boeing Company and Ford Motor Company

[1] The 1996 Convergence Council comprising research & engineering leaders of the Detroit 3 auto manufacturers and supply base

[2] http://www.boeing.com/news/frontiers/archive/2003/august/i_ca1.html

[3] http://www.boeing.com/commercial/airports/787.html

[4] http://media.ford.com/article_display.cfm?article_id=31640

lack of timely maintenance which potentially results in performance degradation (e.g., lower fuel efficiency, higher emissions) and safety compromise (e.g., anti-lock brake stability), potential for maintenance providers to become overwhelmed with the anticipated increase in automobile software updates, and the potential loss of productive time for owners in automotive maintenance. Furthermore, although "intelligent" road transportation systems incorporate roadside sensing and some vehicle-to-infrastructure (V2I) communications for managing traffic and road conditions, as witnessed daily in many roadways these systems alone are not sufficient for resolving grand challenges such as "zero" congestion. Hence, future automobiles need a digital content refresh and retrieval capability that can leverage V2I and vehicle-to-vehicle (V2V) data communications.

Unlike IT systems, however, software and data distribution systems for mobile networked CPS such as automobiles and aircraft must be certifiable in terms of safety and security standards, as well as comply with applicable regulatory processes and procedures. Consequently, these systems are subject to more stringent requirements during design, development, verification and validation. Further, the place/time of software update and data retrieval is critical for vehicles.

Aviation is making marked leaps in the lifecycle management of software and diagnostics of future "e-enabled aircraft"[2] and the use of aircraft-to-aircraft data exchanges for the NextGen air traffic control. Complex system-of-systems applications are being developed for the end-to-end secure distribution of aircraft software and data, involving participation of onboard equipment software suppliers, airframe manufacturer, airlines, airline fleet, air traffic management, and other third party service providers. We view such advances in high confidence aviation technology to be beneficially applicable in resolving the automotive challenges described above.

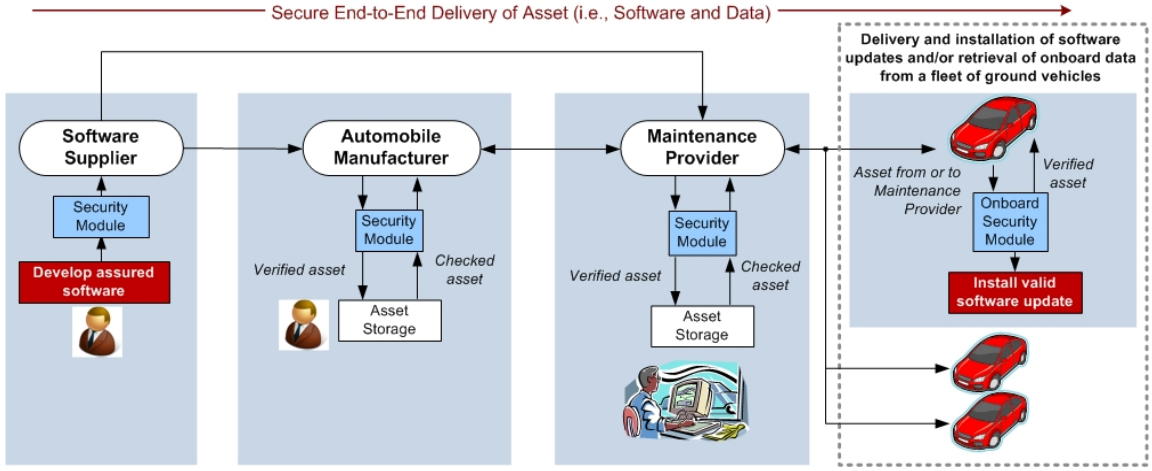


**Figure 1: Illustration of secure software and data distribution for automobiles.**

## Related Aviation Contributions for Automotive Sector

Figure 1 provides a high-level illustration of a use-case scenario of secure software and data distribution for automobiles, leveraging an abstraction of an aviation information system that performs similar functions. As shown, such a system allows participation of relevant stakeholders, including software suppliers, automobile manufacturer, and maintenance provider, to develop, verify and distribute software updates to end-user vehicles in a highly assured manner. Maintenance providers are offered the capability to perform periodic or on-demand distribution of software and retrieval of onboard diagnostics to network-enabled vehicles.

Such a technology enables the use of a high confidence automotive CPS platform in future automobiles that securely transmits and receives software/data to off-board systems-of-systems, including ground systems and other vehicles. In combination with advances in vehicular communication systems (e.g., WiFi) and in-vehicle software platforms (e.g., OnStar, OSGi) and in-vehicle network architectures, the proposed technology can streamline new network services for automobiles. Some of the envisioned unprecedented capabilities offered by the proposed technology in the short and longer timeframes include: (*i*) stakeholders can securely exchange and manage software and diagnostics of vehicles, (*ii*) manufacturers and maintenance providers can securely, automatically, remotely deliver and install software updates to one or more automobiles of the same target type or model, (*iii*) a consumer can simultaneously, securely update all of their owned vehicles, (*iv*) two or more consumers can securely exchange software updates, (*v*) neighboring vehicles on roadways can securely exchange traffic notifications to better inform alternate route choices, (*vi*) law-enforcement vehicles can securely control traffic behavior using vehicle-to-vehicle commands, and so on.

Recent developments show that advances in the future automobile will require a careful consideration of safety of automobile electronic and software systems, as well as cyber security concerns with automobile networking. Aviation presents a highly regulated environment, where air and ground technology must be ensured to have no impact on safe, expected aircraft operations. The latest efforts have been focusing on the safety related aspects of cyber security of aircraft systems and networks. Hence, ongoing regulatory efforts and emerging standards in aviation can significantly help streamline future regulatory efforts in the automotive sector.

Enabling the envisioned technology and applications as well as informing regulations and standards, will require a close collaboration between the government, the interested automotive and aviation industry partners, and interested universities, with collaboration outcomes including technology transition, joint research & development efforts, and standards development.

## Potential milestones for the next 5, 10 and 20 years

In the 5 year time frame we anticipate the development of the envisioned technology using V2I communications with non-safety-critical automobile applications. In the 10 year time frame we expect automation (without user intervention) of the V2I based technology for business-critical applications, V2V based technology for non-safety-critical traffic management applications, development/certification of V2I technology for safety-critical automobile applications. In the 20 year timeframe, we anticipate automation of V2I based technology for safety-critical applications, development/certification of V2V based technology for safety-critical applications.

## Acknowledgements

We acknowledge the discussions with Dr. K Venkatesh Prasad, Group and Technical Leader of the Ford Infotronics Research and Advanced Engineering Team, on automotive CPS themes.

## Biography of Authors

Dr. Krishna Sampigethaya, Mr. Walter Beck, Ms. Kristine Lane, and Dr. Scott Lintelman are with the Trusted Cyber Technology group in the Networked Systems Technology domain at Boeing Research & Technology, involved with high confidence cyber-physical systems research and B787 software distribution system design and development. Dr. Radha Poovendran is a Professor and the founding director of the Network Security Lab (NSL) at the University of Washington, collaborating with Boeing and Ford on aero-auto CPS.