Challenges in Aviation CPS Asset Collection and Distribution

Krishna Sampigethaya, Scott Lintelman, Richard V Robinson, and Mingyan Li

Boeing Phantom Works, Bellevue, WA, USA *
{radhakrishna.sampigethaya,scott.lintelman,richard.v.robinson,mingyan.li}@boeing.com

Abstract. The future airplane will possess advanced sensing, computation and communication technologies to enable remote, automated monitoring and control of different aspects of airplane operation and maintenance. We view such an "e-enabled airplane" as a cyber-physical system to fundamentally understand its behavior and establish system requirements for ensuring reliability, safety and security with high confidence. The paper envisions an onboard sensory network that provides timely feedback to an onboard computer about the status of airplane's physical environment and parts, as well as an application that interfaces between operational airplanes and ground-based infrastructure for end-to-end delivery of critical software updates, commands and onboard health diagnostics/prognostics. Several of the presented challenges and open problems are generic, potentially accelerating research in the trustworthy design, development, verification and validation of e-enabled vehicles in the next-generation air, road and rail transportation.

1 E-enabled Airplane as a CPS

Today, aviation is faced with a formidable challenge of accommodating an unprecedented increase in air traffic, while improving passenger convenience, environmental footprint, and aerospace business. The e-enabled airplane can help to meet this challenge by employing key technological innovations, such as onboard systems integration, off-the-shelf solutions, advanced ubiquitous computing e.g., RFID and smart sensors, and timely information sharing between onboard with off-board infrastructure over open digital links. With such new features, the e-enabled airplane is envisioned to seamlessly traverse as a self-aware node in a global information network consisting of ground infrastructure and other airplanes sharing the airspace. The achievable level of situation awareness and decision making capability promise to substantially improve the capacity, safety, reliability, security, efficiency and yield of future air transportation [1, 2, 7].

However, recent developments show that the beneficial introduction of the e-enabled airplane requires a careful consideration of the networking and security aspects of the design [1, 7, 5, 6]. A cyber-physical system (CPS) framework for emerging aviation information systems can help to streamline this effort. The paper presents a step towards this direction by modeling the e-enabled airplane as a safety- and security-critical CPS on which human lives and well-being depend. As shown in Fig. 1, the airplane can be viewed as a CPS that interacts with off-board systems in the cyber world and interfaces with the physical world via onboard sensors and actuators. This view can inform the design of next-generation architectures, systems and applications for airplane operation and maintenance. The paper focuses on two critical components of this CPS: (i) the sensory network, and (ii) the electronic distribution of critical assets between ground and onboard systems, outlines the major research challenges and problems.

2 Onboard Sensory Network

As shown in Fig. 1, we consider the onboard sensory network to be a heterogeneous mix of wired and wireless sensors which are monitoring events of different criticality on the airplane. Wireless sensors bring revolutionary benefits such as reduced airplane wiring costs and flexibility to be deployed on retrofit airplanes. The RFID system senses information from tags attached to devices, such as line-replaceable units, passenger baggage, and so on. Nevertheless, the onboard sensory network poses some major design challenges and has vulnerabilities that may be exploited to deteriorate reliability, accuracy and availability of the network.

Energy harvesting. Although, onboard sensors and active tags can be expected to be maintained periodically in the order of several days to weeks, the use of battery-operated nodes adds maintenance overhead. Therefore, it is important to find ways to scavenge power from the local system on which the sensor resides, e.g., temperature, vibration, system power unit [7].

* 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. We thank Prof. Radha Poovendran from the Network Security Lab at the University of Washington for his valuable contributions to this work.

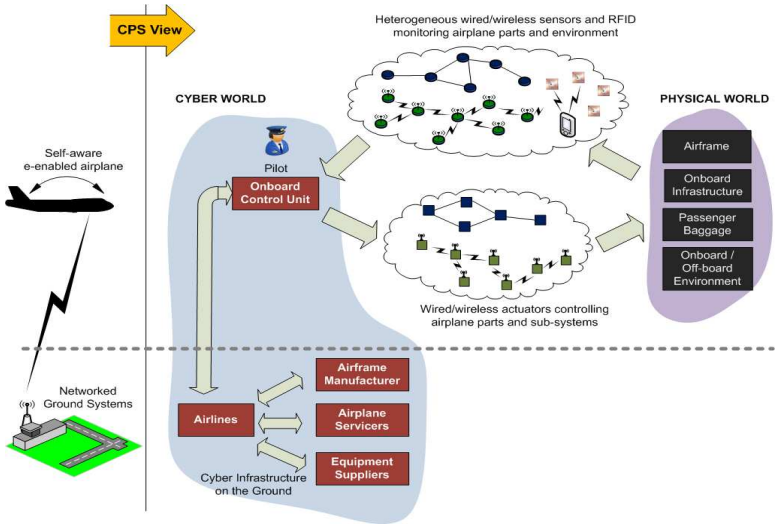

Fig. 1. An abstract view of the e-enabled airplane as a cyber-physical system and information asset flow.

Radio non-interference. As evident from recent airplane certification conditions [6], a major safety concern with onboard wireless technologies is the impact of radio interference on the operation of other onboard systems. Currently proposed solutions require isolation or prevention measures such as limitations on the technology use, e.g.,"sensing" by RFID readers is done only when airplanes are on the ground [4].

Wireless sensor network architecture. A key enabler is the the design of a wireless sensor network architecture that is efficient and non-interfering as required above, and is able to mitigate security concerns from any malicious corruption, replay or delay of data [9].

Networked control stability. Further, to use the feedback from the sensory network for real-time flight-critical operation and distributed control by onboard as well as ground controllers, it is pivotal to address the instability of networked control systems in the presence of malicious attacks.

Protection of RFID tag data. We expect the onboard RFID tags to be accessed by multiple authorized parties or data owners, each entity having different read/write rights to different sections of data stored, e.g., access by airlines for luggage logistics, manufacturer for part ordering, and third service providers for maintenance. In order to protect the data integrity and proprietary data confidentiality as well as facilitate business processes compliance, access control to the tag data must be enforced.

Security assessment tools. The sensory network is trusted to provide information that can be used in real-time, reliable, safe and useful decisions made by the onboard or off-board controllers. Accordingly, the network and security protocols must be verified and validated at an adequate level of assurance. Further, due to the dynamic nature of sensory network data, evaluation methods and visualization tools are needed to assess trust and emerging vulnerabilities in the network, i.e., (i) to assign a level of trust on data/information received from the physical world, and (ii) to understand impact of attacks on the network security and performance.

Human-computer interaction for airplane operators. The introduction of onboard networks and security technologies will require data representation and network monitoring tools to ease the cognitive load of pilots and the aircraft maintenance personnel. However, a related tool design challenge is in finding a balance between flight-operator attention and timely decision making.

3 Electronic Distribution of Airplane Assets

As shown in Fig. 1 a feature of the aviation CPS is the complexity of the design of systems handling airplane assets which are integrated across domains, e.g., airlines, suppliers, manufacturer. The end-to-end system must meet its intended usage and satisfy security requirements to meet perceived threats, while including network infrastructures, personnel, business processes etc., of each domain. For example, a system for distributing airplane loadable software and updates as well as a system for integrated vehicle health management must consistently exhibit some security properties at the suppliers, manufacturer, airlines as well as airplanes [8]. While providing significant cost and time benefits for the e-enabled airplane, such integrated systems can however offer major IA challenges due to vulnerabilities from security weaknesses and design errors.

End-to-end high assurance for system-of-systems. Formal security assessment of the entire system is necessary due to the impact of unidentified vulnerabilities on airplane operation and business, but is difficult due to the need for assuring the large number of connected components in the system. A key challenge is to design inexpensive, efficient, scalable, and user-friendly formal methods (FM) for end-to-end assurance assessment. For example, visual representations of FM with transparent analysis to facilitate the communication of FM benefits to business management, specification language that is accessible to software architects/developers without substantial training, and easy for customers to understand so they can contribute to the formal specification. Another key challenges is to design security models for multi-disciplinary global collaboration. Collaboration between various personnel is required for error-free design, documentation and assessment of the security aspects of the end-to-end system, but is made difficult due to the global multi-disciplinary nature of the personnel. Other challenges include finding interoperable domain standards and policies for networking, IT, and security.

Key and certificate management. Although the use of digital signatures for protecting airplane assets is well accepted, the need for a supporting public-key infrastructure (PKI) presents formidable challenges. One is the design of a scalable, pervasive PKI for establishing trust in large-scale, multi-stakeholder aviation applications such as airplane software distribution. This requires enabling interoperability between multiple certificate authorities and developing a standard certificate policy for multiple scenarios encountered by the airplane. Another major task is evaluating a complex PKI at an adequate assurance level [8].

Open source software security assessment. Open source software offers an cost-effective platform for e-enabled airplanes and airline ground infrastructure. However, it is important that this software be secure and reliable under real-world threats. Therefore, assessment methodologies and assurance metrics to quantify and improve the security of open source practices and products must be developed.

Impact of security on safety. Although commonality exists among the safety and security disciplines, it remains an open problem as to how the two fields can be combined. A framework must be developed to formalize the relation between safety and security which can potentially enable integration of the mainly discrete methods of security analysis into the quantitative, probabilistic approaches of safety analysis. Another key enabler is the assessment of security technologies in the context of safety certification, e.g., evaluation of avionics software/systems for encryption and authentication.

Long-term protection for information assets. Some assets of the e-enabled airplane will require protection throughout the airplane lifecycle which can span several decades. This time constraint imposes the need for careful consideration to the potential for key compromise. Increase in cryptanalytic capabilities available to the adversary over time can also increase the potential for compromise of the signing key of the source. Therefore, to extend the lifetime of asset signatures, effectiveness of mechanisms such as periodic key refresh, longer keys or provably secure/forward secure signature algorithms must be considered.

References

1. Wargo, C. and C. Dhas, Security considerations for the e-enabled aircraft, *Proceedings of Aerospace Conference*, 2003.
2. Domingo, R., Health management and monitoring systems, *Proceedings of the USA/Europe International Aviation Safety Conference*, 2006.
3. Bai, H., M. Atiquzzaman, D. Lilja, Wireless sensor network for aircraft health monitoring, *Proceedings of Broadband Networks (BROADNETS)*, 2004.
4. Porad, K., RFID in commercial aviation, *Aircraft technology engineering & maintenance*, v. 75, pp. 92-99, 2005.
5. Federal Aviation Administration, 14 CFR Part 25, Special Conditions: Boeing model 787-8 airplane, [Docket No. NM364 Special Conditions No. 250701SC], v. 72, no. 71., [Docket No. NM365 SC No. 250702SC], v. 72, no. 72., 2007.
6. FAA policy for passive-only RFID devices. FAA Regulatory and Guidance Library Online.
7. Shetty, S., System of systems design for worldwide commercial aircraft networks, *Proceedings of ICAS*, 2008.
8. Robinson, R., M. Li, K. Sampigethaya, R. Poovendran, S. Lintelman, et. al., Electronic distribution of airplane software and the impact of information security on airplane safety, *Proceedings of Safecomp*, 2007.
9. Sampigethaya, K., Poovendran, R., Bushnell, L., Li, M., Robinson, R., Security of WSN enabled health monitoring for future airplanes, *Proceedings of ICAS*, 2008.

Dr. Scott Lintelman is an Information Assurance (IA) manager in Networked Systems Technology domain at Boeing Phantom Works, responsible for Boeing's IA research strategy. Dr. Krishna Sampigethaya, Dr. Mingyan Li and Mr. Richard Robinson lead the security and high assurance effort of the Boeing Phantom Works IA group, conceptualizing, designing and developing trustworthy networked aviation information systems. The IA team has a long-standing partnership with Commercial Airplane and Integrated Defense Systems groups at Boeing, and with the Network Security Lab (NSL) at the University of Washington.