Secure, Mission Critical Communications Require a New, Easy to Implement Approach

Barry Dowdy, Security Systems Manager for Aerospace and Defense Solutions

Securing Critical Communications

Critical communications systems are prevalent in the aerospace and defense industry. Many are mission critical tactical voice and command and control links that save lives by providing situational awareness to warfighters in the field and by accurately commanding and controlling the destination of various airborne and ground-based platforms. Ease of use and integration; reduced size, weight, and power (SWaP); and reduced time-to-market (TTM) are essential design considerations to systems integrators and original equipment manufacturers (OEMs) that require embedded security solutions for critical communications systems. Ease of use and integration is essential for nonsecurity experts to efficiently implement security features. Reduced SWaP is essential in operational environments to reduce the load carried by foot-mobile warfighters and to optimize the efficiency of military communications systems. Reduced TTM is essential for systems integrators and OEMs striving to meet urgent operational needs, generate revenue, and capture their share of the market. Some secure critical communications applications include military radio communications and unmanned system data and command links. An efficient approach to embedded security solutions can help systems integrators and OEMs meet secure critical communications challenges in these applications.

Military Radio Communications

The demand for SWaP-efficient tactical radios delivered expeditiously to the warfighter drives the need for encryption modules that are easy to use and integrate. New designs for tactical radio equipment manufacturers include easy to use and integrate, SWaP-efficient embedded security solutions that reduce an equipment manufacturer’s TTM.

Historically, radio frequency (RF) signal chain designs have been consumed with board layout and signal processing efforts that require significant engineering expertise and time to achieve a working design. Reduced SWaP was achieved by selecting the most efficient discrete components and chassis materials. An alternative approach to reducing SWaP includes integrating RF system-in-packages (SiPs) or modules directly into a signal chain design. For example, advancements include a new direct-conversion RF transceiver and field programmable gate array (FPGA) preconfigured as part of a modern signal chain on a SWaP-efficient circuit card assembly.

New RF transceiver devices combined with an FPGA and proven security features can reduce engineering expertise and time required to achieve a secure RF signal chain design. FPGAs in this signal chain configuration can be partitioned with a signal processing block, a trusted execution environment (TEE), and customer IP. The FPGA can also include a security application programming interface (API) between the TEE and signal processing partitions that provides access to security features for encrypted traffic, key management, secure boot, secure update, and secure storage. Overall, this design approach makes it easier for a systems integrator or OEM to integrate RF signal chain components and security features in a secure communications system while reusing proven RF signal chain and security functionality.

TTM can be reduced by starting with a predesigned security solution that frees up engineering resources to do what they do best instead of spending valuable time designing and implementing security features. In addition to reduced TTM, this approach also reduces upfront development/nonrecurring engineering (NRE) costs. The savings include the NRE efforts of several engineers over an 18- to 24-month period of performance, which equates to about $3M to $5M.

In addition to development time, encryption certifications through the National Security Agency (NSA) or National Institute of Standards and Technology (NIST) can take 18 to 24 months. This can increase a company’s TTM if the certification efforts are started late in the design process or after the fact. If so, the certifying authority will have to spend more time evaluating and understanding the existing design. Alternatively, TTM is reduced by engaging NSA or NIST early in the encryption design process with NSA or NIST compliant encryption algorithms and supporting documentation and by providing security modules that are easy to use and integrate. Modern embedded security solutions protect the entire signal chain—from antenna to bits—securing military communications through robust system hardware and software-based cryptographic technologies. In addition, these solutions include well documented and defined security packages for existing hardware or embeddable FPGA-based encryption modules based on a scalable/flexible high assurance cryptographic processing platform capable of running on various families of FPGAs.
An example development effort includes a next-generation software-defined radio (SDR) that requires an RF transceiver, FPGA, and an embedded encryption solution. In this case, the embedded encryption solution can be developed and certified in parallel with the SDR design. Starting this process with FIPS or NSA Suite B compliant cryptographic cores also reduces development time and certification risk as the algorithms have already been approved for use. Moreover, the use of previously certified encryption modules can further reduce certification time and risk.

Unmanned Systems

Unmanned systems consist of unmanned aircraft systems (UAS), robots, and autonomous tactical vehicles. These unmanned systems often include sensors, video sources, and communications systems for receiving and transmitting information to and from the platform. The information is transmitted via data link systems from the platform to a ground control station, command center, or remote control device. As such, unsecure, unmanned systems are vulnerable to cyber security attacks. An adversary or malicious actor can hijack a remote platform by masquerading as a legitimate remote control device. An adversary or malicious actor can also capture and/or manipulate sensor data and video. Accordingly, critical communications and command and control links should be secured to prevent cyber security attacks.

Security solutions for communications and command and control links include software and firmware for existing hardware, embeddable encryption modules, secure RF signal chain modules, and in-line security modules. These security solutions are generally provided through partnerships with unmanned systems integrators and security solution providers.

Sypher Ultra

These new easy to use designs that reduce SWaP and TTM were developed by teams at Analog Devices, Inc. (ADI). For example, an ADI product available to secure critical communications systems and reduce SWaP and TTM is Sypher™ Ultra, which reduces the complexity of implementing security features on the family of Xilinx® Zynq® UltraScale+™ MPSoC (ZUS+) FPGAs. Sypher Ultra security features include secure boot, secure update, secure key storage, secure data in motion (traffic encryption), and secure data at rest. These features isolate sensitive cryptographic operations, protect IP, secure communications, manage device identity, and enable the distribution of software updates with confidence. Sypher Ultra security features can be implemented by nonsecurity experts using reference design software/firmware, an API, a graphical user interface (GUI), and user guides.

Military communications systems and the data and command and control links on unmanned systems are examples of critical communications that must be secured for protected and safe operations. An FPGA-based security solution integrated in a SiP can help a systems integrator or OEM reduce SWaP and their TTM by starting certification efforts early in the signal chain design process. For more information related to ADI’s security solutions, visit analog.com/securitysolutions.

About the Author

Barry Dowdy possesses an extensive background in secure communications. As part of ADI’s Trusted Security Solutions Group, Barry has taken on the role of security systems manager for aerospace and defense solutions. Leveraging his experience as a Marine Corps communications officer, U.S. defense acquisition specialist, and business development professional in the defense industry, Barry is focused on developing security solutions for critical communications in aerospace and defense. He can be reached at barry.dowdy@analog.com.

Online Support Community

Engage with the Analog Devices technology experts in our online support community. Ask your tough design questions, browse FAQs, or join a conversation.

Visit ez.analog.com