Encrypt/Decrypt COMSEC Unit for Space-based Command and Telemetry Applications

Doug Merz, BSEET
email: dmerz@cmccinci.com

Bruce Maples, MSEE
email: bmaples@cmccinci.com

CMC Electronics Cincinnati
Mason, OH 45040

ABSTRACT

This paper describes the system-level architecture and design concept of a communications security (COMSEC) equipment intended for space-based low data rate (< 1 Mbps) command and telemetry applications. The COMSEC Unit is a stand-alone piece of equipment which provides decryption of uplink command and control information and encryption of downlink telemetry data. The system-level architecture is described followed by an overview of the digital design concepts and a discussion of applications. Finally, although specifically targeted for narrowband command and telemetry applications, this design approach is flexible enough to accommodate other algorithms of choice as well as operate in higher data rate applications.

KEY WORDS

Cryptography, Communications Security, Encryption, Decryption, Key, Authentication.

INTRODUCTION

The need for communications security (COMSEC) in command, control and telemetry functions of satellite operations is vital toward the protection of space-based assets from unauthorized access and the dissemination of sensitive information. This security model may be implemented on a space-based asset by incorporating an encryption/decryption engine into the receive and transmit data paths between the receiver/transmitter and the command and data handling (C&DH) subsystem of the spacecraft. Encrypted command and control messages from an authorized ground station would be transmitted to a satellite which would utilize the corresponding decryption algorithm. Telemetry data from the satellite would be encrypted prior to downlink transmission followed by decryption by the ground station. In addition, encryption/decryption may be utilized for higher rate data traffic where secure communications is desired.

Several cryptographic algorithms in common use today include the Data Encryption Standard (DES and TripleDES), Advanced Encryption Standard (AES), and PGP (Pretty Good Privacy) for commercial use as well as the VINSON (KY-57/58), Advanced Narrowband Digital Voice Terminal (ANDVT) and KG-84 for military applications. More recently, algorithms such as Caribou and Centurion have gained popularity in both the commercial and government sectors. Development of equipments which use these algorithms often involve a comprehensive U.S. government certification process to insure the cryptographic integrity of the design for use in processing sensitive information. The level of certification required, if any, is directly dependant upon the classification of the information the equipment is being designed to protect. This also reflects on the evaluated "strength" of the algorithm chosen for the intended application i.e. certain algorithms are certified for protecting classified information whereas other algorithms are suitable only for unclassified data.

The focus of this paper is the description of the design concept of a stand-alone encrypt/decrypt COMSEC equipment for space-based applications which is currently in development. This COMSEC Unit will interface between the on-board receiver/transmitter and the command and data handling subsystem of the spacecraft as shown in Figure 1. Encryption and decryption algorithms can be implemented with either off-the-shelf application specific integrated circuits (ASIC's) or field programmable gate array's (FPGA).

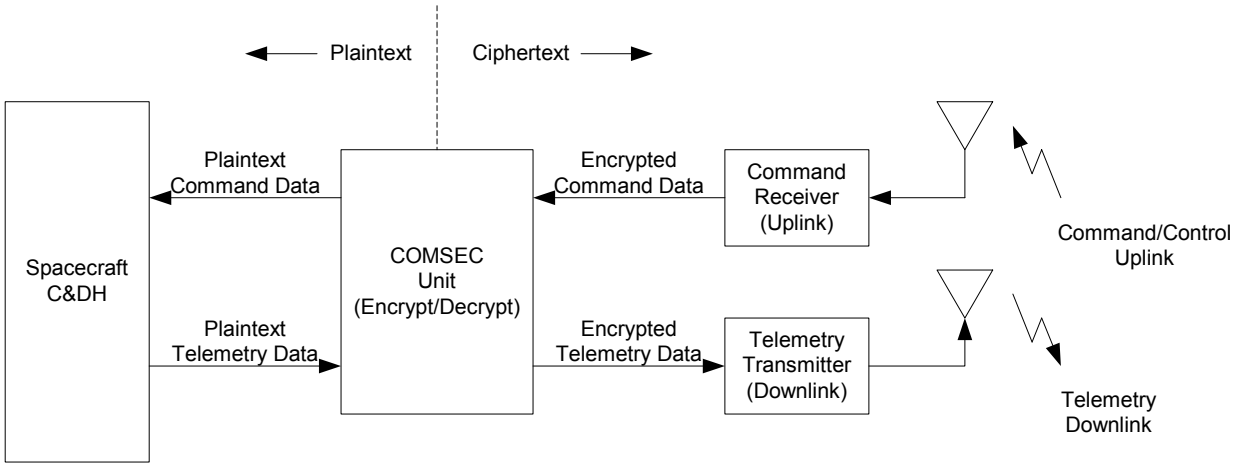

Figure 1. COMSEC Unit Top-level Spacecraft Interface Diagram

SYSTEM ARCHITECTURE

The COMSEC Unit design currently in development utilizes a flexible architecture to meet the requirement for one or more algorithms to be implemented in various applications. This flexibility translates to a cost effective product which may be easily adapted to customer needs with little or no redesign effort. The current implementation of the COMSEC Unit utilizes a dual-algorithm for both encryption and decryption. Algorithm selection is via control input from the spacecraft command and data handling subsystem. A top-level functional block diagram of the COMSEC Unit is shown in Figure 2.

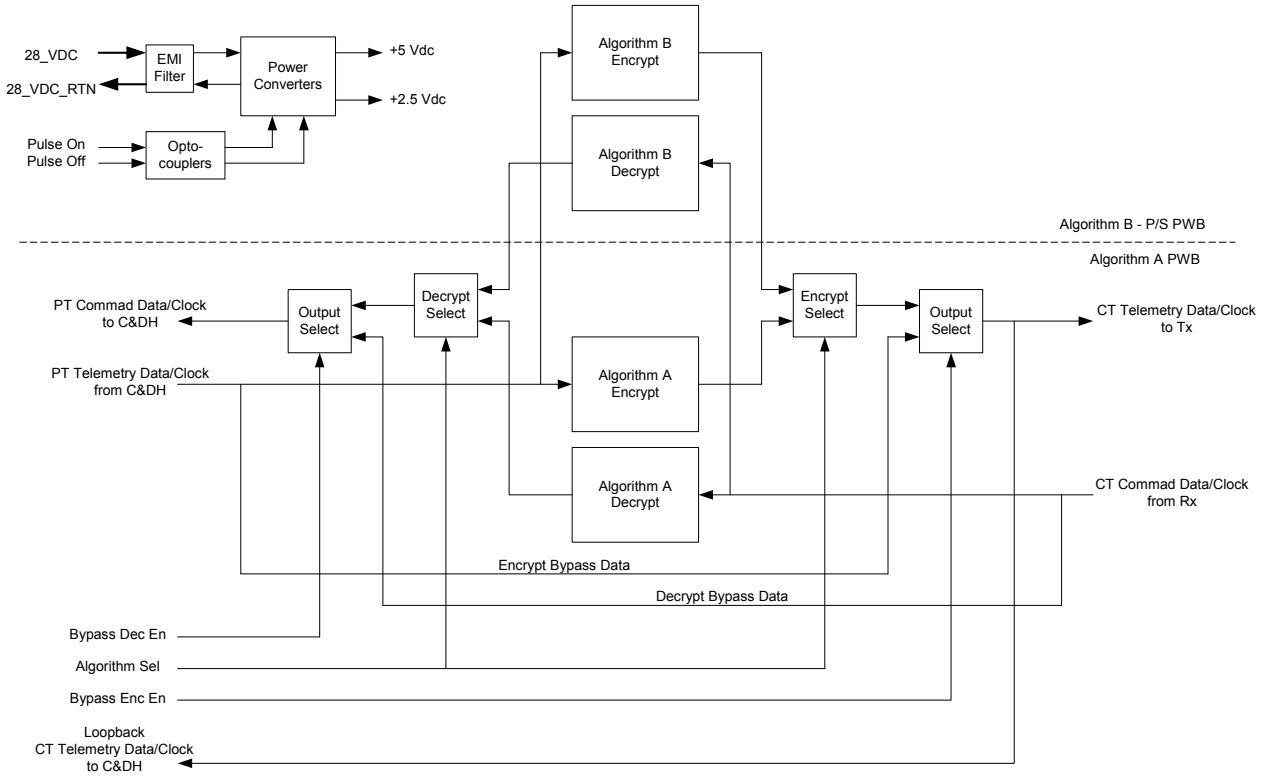

Figure 2. COMSEC Unit Functional Block Diagram (dual-algorithm)

Control inputs, which are driven by the spacecraft C&DH subsystem, provide algorithm selection and bypass control. In addition, a loopback path of the encrypted telemetry output data stream is available to the C&DH for monitoring purposes. Bypass paths for both encrypt and decrypt functions are available when it is desirable to operate in a non-secure mode (i.e. "in the clear") or to functionally remove the COMSEC device from the communication path. This may be necessary for interoperability with ground stations not having encryption and decryption capabilities or to simply relay encrypted information in the case of non-processing or "bent-pipe" transponders. Note that plaintext telemetry data is applied to both encryption engines whose outputs are multiplexed for algorithms selection. Similarly, the receive cipher text command data is applied to both decrypt engines whose outputs are multiplexed according to algorithm selection. Control and data routing/handling are provided via two FPGA's. A simplified top-level hardware block diagram of the COMSEC Unit is shown in Figure 3.

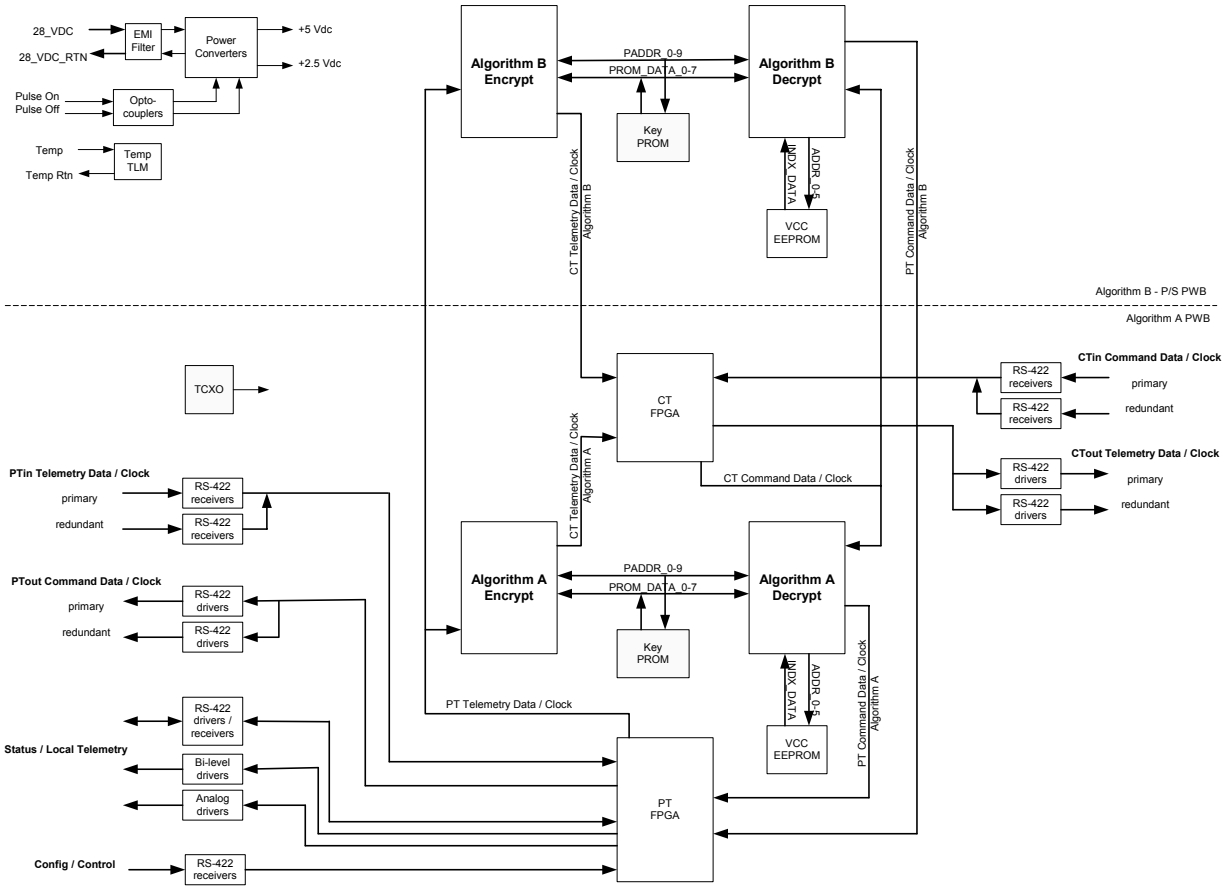

Figure 3. COMSEC Unit Hardware Block Diagram (dual-algorithm)

The COMSEC Unit design is logically and functionally partitioned to provide isolation, manufacturability and testability resulting in a robust and cost effective product. As indicated in the figure, the current design consists of two circuit card assemblies (CCA). The main or parent CCA contains one algorithm (encrypt and decrypt) and the controlling FPGA's as well as all the supporting input/output interface circuitry. The second or daughter CCA contains the second algorithm (encrypt and decrypt) and the power supply. Interface and data routing to/from the two CCA's is facilitated via board-to-board inter-connectors. For applications requiring only a single algorithm to be implemented, the daughter CCA would not be populated with the second algorithm integrated circuits. Alternatively, this board stack concept could be extended to include more than two algorithms, if desired, by including additional algorithm CCA's to the design. This concept is of course limited by the routing capabilities of the FPGA's on the parent CCA and the available size of the board-to-board inter-connectors.

Plaintext/Ciphertext Separation

The two FPGA's provide plaintext (PT) and ciphertext (CT) interfaces as well as system timing and control. Plaintext data refers to unencrypted data that must be strictly controlled to prevent unauthorized access due to its sensitive or classified nature. Ciphertext data refers to encrypted data that is suitable for transmission since the information content is protected.

Proper cryptographic design practices require both logical and physical separation between plaintext and ciphertext interfaces to prevent inadvertent crosstalk. This separation also prevents hardware or software failures from allowing plaintext information to flow unencrypted to the transmitter. The design must also provide ways to test the security and integrity of the system and report failures when detected. In this design, plaintext/ciphertext separation is provided by the encryption algorithm devices and dedicated FPGA's as well as multiple (redundant) layers of data routing and control within these devices.

DESIGN PROCESS FOR SPACE PRODUCTS

Products developed for space applications typically go through a rigorous design, development and test process. In order to develop a suitable spacecraft subsystem, requirements must first be defined by the spacecraft integrator. Subsystem requirements typically are contained in a detailed performance specification that describe the subsystem function, electrical interface, mass, power, volume and environmental specifications.

During the life of a space product, it is exposed to hostile environments that need to be addressed throughout the design process starting with the design concept. Typical launch environments include extreme temperature variation, pressure change, intense vibration and shock events. Earth orbital or deep space environments include extreme temperature variation and radiation concerns. During all lifecycle phases, the subsystem may be subjected to high levels of RF energy or reside in close proximity to RF sensitive scientific equipment. Therefore, environmental requirements for space equipment usually include electromagnetic susceptibility and emissions requirements that must also be considered during the design phase. It is important to specify and understand the impact of these environmental requirements to facilitate all aspects of the product development including circuit design, determining allowable component technologies, part selection, mechanical design, assembly and test. Quite often, heritage designs or components that have reliably flown on previous missions are used to ensure long-term reliability and reduce development cost.

System level design addresses all aspects of the system specification and provides enough detail for a design team to develop an acceptable product. Typically, the subsystem is partitioned into subassemblies, subassembly interface specifications are developed and functional descriptions of each assembly are published. System level analysis is performed utilizing various CAE tools to ensure that the system level concept is sound. A mechanical packaging concept is developed that addresses the volume required by each partitioned subassembly and provides the interface and interconnect scheme. The packaging concept also typically considers strategies to survive long term thermal cycling, permit rapid evacuation of the subsystem, remove heat from components in vacuum

and endure launch vibration and shock. The system level design phase concludes with a system level peer review.

Detailed design involves circuit design and simulation including development of programmable logic functions, component selection, electrical stress derating analysis, worst-case analysis, schematic capture and subassembly printed wire board (PWB) layout. Detailed mechanical design implements packaging and interconnection concepts developed during system design and realizes strategies for thermal management, vibration and shock. Individual chassis components are developed along with PWB outlines and component height specification drawings. Mechanical modeling and thermal analysis is performed to verify packaging implementation meets environmental requirements and to identify subassembly thermal profiles used in electrical stress derating analysis. Additionally, during the detailed design phase, test procedures and unique test equipment are developed to support integration testing, qualification testing and flight unit acceptance testing. Integration testing typically involves semi-formal verification against the specification and limited temperature cycle verification. Qualification testing typically involves full specification verification over temperature, electromagnetic compatibility, vibration and shock. Environmental qualification stress levels are typically applied at levels exceeding flight acceptance levels. Acceptance test procedures are developed to verify flight units meet specifications and to stress the subsystem beyond flight expected levels, but within design margin. Several peer reviews are typically included at logical milestones throughout the detailed design phase.

Qualification test unit subassemblies are manufactured and integrated. Integration testing is performed and specification out-of-tolerance issues, if any, are identified and corrected. Qualification testing is executed and documented. Flight units are then built and verified using the flight acceptance test procedure prior to delivery for spacecraft integration.

Component Considerations for Space Applications

Since the cost of a subsystem failure after launch can be in the hundreds of millions of dollars, high reliability components are typically selected. These components undergo extensive screening at the component level to eliminate failure due to manufacturing defects that would show up as “infant mortality” of a component after installation in the subassembly. Additionally, the parts are subject to lot testing that includes destructive physical testing (DPA), particle impact noise detection (PIND) and residual gas analysis (RGA) testing.

Radiation effects are of special concern. Many of the existing commercial technologies do not function properly or may fail completely when exposed to radiation. The most notable effects include total ionizing dose (TID) degradation, single event latch-up (SEL) and single event upset (SEU).

Total ionizing dose effects accumulate over time and may cause certain device technologies to exhibit increased current demand, increase gate leakage, modified detection thresholds or complete failure. TID effects are specified as the energy absorbed by matter or radiation absorbed dose (rad). Parts for space applications will typically be designed and/or tested to operate with little degradation in excess of 100 krad.

Single event latch-up effects are instantaneous and can be destructive to an electronic device. SEL is induced when a device is impacted by a heavy ion or proton that causes continuous high operating current. The condition is typically not self-correcting and power of the affected device must be cycled to clear the latch-up state. This high current state may load down the subsystem power bus and, if device power is not removed quickly, may destroy the component. Current monitoring circuits have previously been used to detect an SEL event and interrupt device power but typically, components specified for space applications must not be susceptible to SEL effects for the predicted environment. A component is considered SEL immune if the latch-up effect is not seen when the device is exposed at linear energy transfer (LET) thresholds greater than 100 MeV cm^2/mg.

Single event upset does not typically induce a physically damaging effect, but instead can cause electronic components to change state arbitrarily. In the case of a linear circuit, this may induce a temporary change in output voltage. When a logic gate is the victim of SEU, it may change logic state and remain in the incorrect state until reinitialized. This can cause temporary failures in systems when the logic gate is part of a state machine or critical configuration register. SEU mitigation techniques such as self-synchronizing state machines and counters or triple module redundancy (TMR) strategies are typically employed to prevent or gracefully recover from these events.

APPLICATIONS

The COMSEC Unit currently in development will be suitable for spacecraft applications requiring secure command (uplink) and telemetry (downlink) traffic utilizing multiple encryption/decryption algorithms. The capability to select from more than one algorithm via ground command is valuable for maintaining compatibility with ground stations worldwide. The flexibility of the design also permits the COMSEC Unit to be manufactured for encryption only or decryption only, if desired, to suite a given application. In addition, although this design is targeted specifically toward relatively low data rate command and telemetry applications, the design concept is extendable to higher data rate applications.

CONCLUSION

This paper has presented an approach to the design of a communications security equipment for space-based applications. Top-level functional and hardware block diagrams were presented to provide an overview of the fundamental capabilities of the device. Design awareness regarding separation of plaintext and ciphertext information in cryptographic devices was discussed. Also, the basic design process and underlying considerations associated with the development of space-qualified equipment was summarized. Finally, general applications for this type equipment was briefly discussed. This paper has provided some initial background and insight into the design of space-based cryptographic equipment by focusing on a current development effort as an example.

AKNOWLEDGEMENTS

The authors would like to acknowledge the support of CMC Electronics Cincinnati for the writing of this paper and thank the following individuals for their comments and suggestions: Mark Dapore, Rick Fry, Larry Dobbs, Bill Lampe and Carol Yelincic.

REFERENCES

[1] Sklar, Bernard, Digital Communications: Fundamentals and Applications, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1988.

[2] Spilker, James J., Digital Communications by Satellite, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1977.

[3] Skahill, Kevin, VHDL for Programmable Logic, Addison-Wesley, Menlo Park, CA, 1996

[4] Poivey, Christian, "Radiation Hardness Assurance for Space Systems", *NASA Goddard Space Flight Center report*, July 2002.