FLEXIBLE SECURE DATA COMMUNICATIONS WITH THE RANGE ENCRYPTION MODULE

Stan M. Watkins
L3 Communications Corp.
San Diego, Ca.

ABSTRACT

This paper discusses the design, application and flexibility of the Range Encryption Module (REM) developed by L3 Communications Conic Division for the Range Application Joint Program Office (RAJPO) located at Eglin Air Force Base in Florida. The REM is a burst encrypter that utilizes the National Security Agency Thornton CTIC/DS-101 Hybrid (CDH) encryption algorithm. The CDH device operates under the control of a Conic-designed digital ASIC. The CDH, ASIC, Power Management and parallel bus interface circuits reside on a single card within the REM called the Common Encryption Core (CEC). The REM and CEC card within the REM offer flexibility in many operational features, as described below.

INTRODUCTION

The REM was developed to address the need for secure communications in range data link applications. The REM operates in a TDMA network arrangement and interfaces with COTS data link components in the Metric (AN/ARQ-52) Instrumentation Pod (reference Figure 1). The instrumentation pod can be carried by any aircraft capable of launching an AIM-9 (Sidewinder) or AIM-120 (AMRAAM) missile and can be flown on several ranges. In this application, the REM interfaces with the QUALCOMM Data Link Transceiver (DLT) and the Metric Personal Computer Advanced Digital Interface Unit (PC-ADIU).

The REM has two external data interfaces (one Red and one Black) to the data link components. Each interface can be separately configured to operate using standard R³ parallel, synchronous serial (SDLC) or asynchronous serial communications. An external 1pps source must be supplied to the Red or Black interface for network synchronization; an internal 1pps is generated if either source is momentarily lost. The REM processes network messages in half duplex as required by the CDH device which dictates a single tasking mode of operation in its application.
Traffic encryption keys (TEKs) can be loaded into the REM manually, with a Data Transfer Device (DTD) through the DS-101 key load interface, or via Over the Air Transfer (OTAT) messages through the Red or Black data interface.

The key features offered by the REM are OTAT keyloads, programmable interfaces, Black to Red bypass of header and data, Red to Black bypass of header only, TDMA operation, data transfer rates up to 2 Mbits/sec with 1 msec guard bands, variable message lengths, a programmable timer for traffic key zeroization when message traffic has ceased, and immunity to power transients up to 150 ms.

**THE REM**

The REM functionality is achieved with the integration of a five-board set: Common Encryption Core (CEC), Red board, Black board, Power Supply and Mother board. The REM contains separate Red and Black cards that allow a choice of parallel, synchronous serial, or asynchronous serial communications interfaces. These cards implement a majority of the design in FPGA, allowing other interface possibilities with an FPGA.
change. At the heart of REM’s design is the CEC, which performs the REM’s cryptographic functions. The CEC offers flexibility in selection of CDH operating mode, network synchronization method, and message header bypass length. The CEC communicates with the Red and Black interface boards through a motherboard. The REM’s Red and Black power is supplied by a +28 VDC power supply board which provides MIL-STD-704/461 filtering and internal voltage generation.

The REM electronics are enclosed in a 64 cubic inch aluminum housing weighing 3 lbs. The input power requirement is +28 volts DC at 1 amp. There are four interfaces: Black data (J1), Red data (J2), Key Load (J3) and Power/Configuration (J4). The REM has been extensively tested over environments such as temperature (-55° to +85° C), humidity (100%), 60g shock and vibration at 6 g RMS. The REM has also been qualified for EMI (MIL-STD-462) and TEMPEST. The REM has been integrated and tested in the Range Application Project ground station and instrumentation pod and is in the process of certification for Top Secret applications.

![Diagram](image)

**Figure 2**

**COMMON ENCRYPTION CORE**

The CEC is primarily composed of a digital ASIC, CDH hybrid, PROM and power management circuits. The digital ASIC is a 250,000-gate device that incorporates an 8032 microcontroller and unique digital logic to achieve cryptographic control and data management of the CDH device. The ASIC is fabricated with a 0.8 micron CMOS process. The ASIC is supplied a 60 MHz clock that is divided in half to provide a 30 MHz clock to all internal components. The ASIC’s primary interfaces are with the CDH, the key
load interface, and the external interfaces through the Parallel Command and Status Port (PCSP).

The interface to the CDH controls its operating mode, key selection, cryptographic operation (encrypts, decrypts, and bypass), and error handling. In the REM, the CDH operates in Mode C with unique unscrambled ID number initialization, and key selection is driven by a field in the message header. The Key Load interface to the CDH supports the loading and zeroization of Master Key Encryption Keys (MKEKs) and Black Traffic Encryption Keys (BTEKs) from a DTD and the loading and zeroization of traffic keys via messages. The PCSP interface (PCSPI) is similar in operation to many processor interfaces and is the conduit to the Red and Black boards for the processing of system and REM message headers to and from the host system.

Plain and cipher text data is transferred into and out of the ASIC through four 1024 deep FIFOs. The Red data interface consists of Plain Text Interface (PTI) input and output FIFOs, and the Black data interface consists of Cipher Text Interface (CTI) input and output FIFOs.

**PROCESSOR FUNCTIONS**

The CEC hardware operation is complemented with an 8032 microcontroller that provides message processing, hardware control, error handling, status reporting, and built-in test (BIT) functions. The message processing capability handles all incoming message traffic, and includes the processing of programmable configuration parameters. The microcontroller software monitors and controls hardware functions such as key selection, encrypt and decrypt process activation and time out, power loss, and resetting of hardware elements. Error handling is performed on messages, hardware tasks and software functions. The detected errors are dispositioned, and reported in the REM status message. BIT is performed on power up and when commanded. The BIT includes comprehensive tests of REM hardware and software functions, such as memory (FIFOs, RAM and PROM), CEC to REM interfaces, and timers.

**CEC MESSAGE PROCESSING**

The REM message format contains a header, data and checksum, as shown in Figure 3. The Message Indicator (MI) in the REM header is part of the unique message number used in the encryption and decryption process. The REM sets the MI when the message is encrypted, then uses the MI for decryption on the other end of the data link. The control word contains the key elements for processing message traffic: the sender ID, key group indicator and message type.
The data field is the only part of the message that is encrypted on an encrypt message. The checksum is a two’s complement sum of words 1 through the end of the data field.

Black to Red bypass messages do not conform to the REM message structure shown above. In a mobile configuration, the REM relays unencrypted uplink messages from the DLT to the PC-ADIU, bypassing the decryption process. The bypass message type is distinguished by bit 2 in the System Header. If bit 2 is not set, the entire message is passed from Black to Red host without decryption. If bit 2 is set, the message contains REM header words, data, and checksum.

The CEC processes REM-formatted messages through three interfaces: the PTI handles plain text data for the Red host interface, the CTI handles ciphertext data for the Black host interface, and the PCSPI handles REM header information, which is passed between the CEC and REM Interface (REMI) hardware. Message data received at the PTI and CTI is buffered in the respective input FIFO and held until the header is read and acted on and the message checksum is validated. The CEC processes two basic categories of messages: “To” and “Through” the REM. The “To” category includes initialization, OTAT, key zeroization, status and BIT request messages. These messages are read by the microcontroller and processed internally. The “Through” category includes encrypt, decrypt and bypass messages. For encrypt and decrypt “Through” messages, the data is routed through the CDH (encrypted or decrypted) and then transferred to the output FIFO where it is held until the outgoing header information is ready for transmission out to the network.

CEC USE IN OTHER SYSTEMS

The CEC is modular in design, which provides for embedment into other systems. Only requiring power and an interface adapter, the CEC can communicate with an external processor or to other standard hardware communications devices. The CEC is a 3” x 3.5” double-sided board with a 3/8” height and the board current requirement is less than 500 ma. The CEC, as with the other boards, uses two wedge locks at either side of the board to physically secure the CEC in place and provide a path for CEC heat transfer to a housing or chassis.
RED BOARD

The Red board is primarily composed of three Actel 1280 (8,000 gate) FPGAs. The Red board FPGAs contain the Plain Text Host Interface (PTHI), Plain Text Network Engine (PTNE) and REMI controller (RC) functions. The PTHI provides the functionality of the three interface types, R^3, synchronous serial and asynchronous serial. One of these functions is enabled by selecting the interface type on the J4 configuration pins. The PTNE is primarily a state machine that performs the message parsing of header and data. The header is transferred to the RC while the message data is sent to the CEC PTI. The PTNE also provides an interrupt to the CEC for message start and performs message checksum validation for received messages and generation for transmitted messages. The RC manages the incoming and outgoing header data and the PCSP interface with the CEC. The RC selects the Red or Black 1pps source for network synchronization (based on configuration pin settings) and generates the 1pps if either source is not present. The PCSP interface is provided through a 50-pin male motherboard connector (P2) and the Red host connection is achieved through the 51 pin external male connector (J2).

BLACK BOARD

The Black board uses two Actel 1280 FPGAs and the TEMPEST interface circuits. The Black board FPGAs contain the Cipher Text Host Interface (CTHI) and Cipher Text Network Engine (CTNE) functions. These designs provide the same functionality as those in the Red board with the only difference being the TEMPEST interface between the two FPGAs. The CTNE interface to the RC is provided through a 30-pin male motherboard connector (P1) and the Black host connection is achieved through the 51 pin external female connector (J1).

POWER SUPPLY AND MOTHERBOARD

The power supply will filter and regulate MIL-STD-704E +28 volt dc and provide an isolated Red and Black +5 volts for the REM electronics. This power along with configuration signals is bussed through the motherboard to the required circuit boards. The power supply also provides backup power to maintain configuration and traffic keys during power interruptions up to 150 ms. The design provides reverse voltage protection and a switching DC/DC converter which operates from +16 to +50 VDC with a 70% efficiency rating. The motherboard provides interconnection between the four other boards in the REM and contains no active circuitry.
THROUGHPUT AND LATENCY

Tables 1 and 2 show throughput and latency times for messages passing through the REM using the highest data rate interface, Synchronous Serial 2 Mbps, on both Red and Black interfaces. Timing for the other interfaces is slower. Table 1 shows throughput time, measured from the first bit/byte into the REM until the last bit/byte out of the REM. Table 2 shows latency time, measured from the last bit/byte into the REM until the first bit/byte out of the REM. Times are shown for messages of different lengths and with a provision made for a traffic key change. The entire message is 8 bytes longer than the number of data bytes shown to account for the 2 byte system header, 2 byte MI field, 2 byte REM control word field, and 2 byte checksum.

The latency time recorded for the short message with a key change is longer than the time recorded for the long message with a key change because the key change begins when the message header has been received, so the key change is occurring while the rest of the long message is being received. Once the last bit/byte of the long message is received, the microprocessor is finished with the key change and ready to send data through the CDH immediately. When the last bit/byte of the short message is received, the microprocessor must wait to finish the key change before it can begin to send data through the CDH. This results in a longer time for the shorter message.

<table>
<thead>
<tr>
<th>Table 1: Throughput Times for Sync Serial 2 Mbps Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Without Key Change</strong></td>
</tr>
<tr>
<td><strong>2 Bytes</strong></td>
</tr>
<tr>
<td>Data</td>
</tr>
<tr>
<td>Encrypt</td>
</tr>
<tr>
<td>Decrypt</td>
</tr>
<tr>
<td>Bypass</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2: Latency Times for SS 2 MHz Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Without Key Change</strong></td>
</tr>
<tr>
<td><strong>2 Bytes</strong></td>
</tr>
<tr>
<td>Data</td>
</tr>
<tr>
<td>Encrypt</td>
</tr>
<tr>
<td>Decrypt</td>
</tr>
<tr>
<td>Bypass</td>
</tr>
</tbody>
</table>

CONCLUSION

The Range Encryption Module provides burst mode secure communications for range instrumentation applications. The flexible architecture allows easy adaptation to a variety of ground and airborne applications.