Part 1 - General Implementation

Introduction

The KS-252 is a modern NSA Type 1 COMSEC device that natively supports network-based systems. Legacy COMSEC devices in many control centers use serial interfaces for the Plain-Text and Cipher-Text telemetry and command data streams. The KS-252, with its Ethernet interfaces, enables the COMSEC devices to be networked with the other control center equipment and deployed in a private cloud architecture.

COMSEC Pooling

Cloud architectures deploy suites of Applications across low-cost commercial servers, often running the various Apps on Virtual Machines. The KS-252 is well suited for cloud architectures. Architecturally, the KS-252 can be thought of as a COMSEC App on the network, creating a “pool” of COMSEC devices.

A KS-252 can be configured with a commanding algorithm or a telemetry algorithm. It supports either an encrypt channel or a decrypt channel for that algorithm. For a given telemetry or command stream, a KS-252 from the pool is dynamically configured and connected to Red Front End and Black Front End Apps.

Security considerations do impact the flexibility. The KS-252 exchanges security credentials with each connecting device, requiring each Front End Processor App that may connect with the KS-252 to have these credentials. There is also the requirement to have the proper keys loaded and many control centers choose to limit the number of keys on an individual COMSEC device. These two constraints may drive the deployed

architecture to have sub-pools of both KS-252s and the Front End Processor Apps, with a sub-pool assigned to a particular set of satellites.

Key Factors

UDP Interfaces: The KS-252’s network protocol is UDP. With UDP, delivery of packets over the network is not guaranteed. The KS-252 should be directly connected to a dedicated Ethernet network within the control center and not extended over a wide area network where packet loss can be expected.

Throughput: The KS-252 traffic interfaces operate at Ethernet’s 100 Mbps data rate. With packet overhead, the effective maximum throughput for telemetry is on the order of 90 Mbps. Front End Processor Apps that use multiple KS-252s in parallel achieve higher throughput rates.

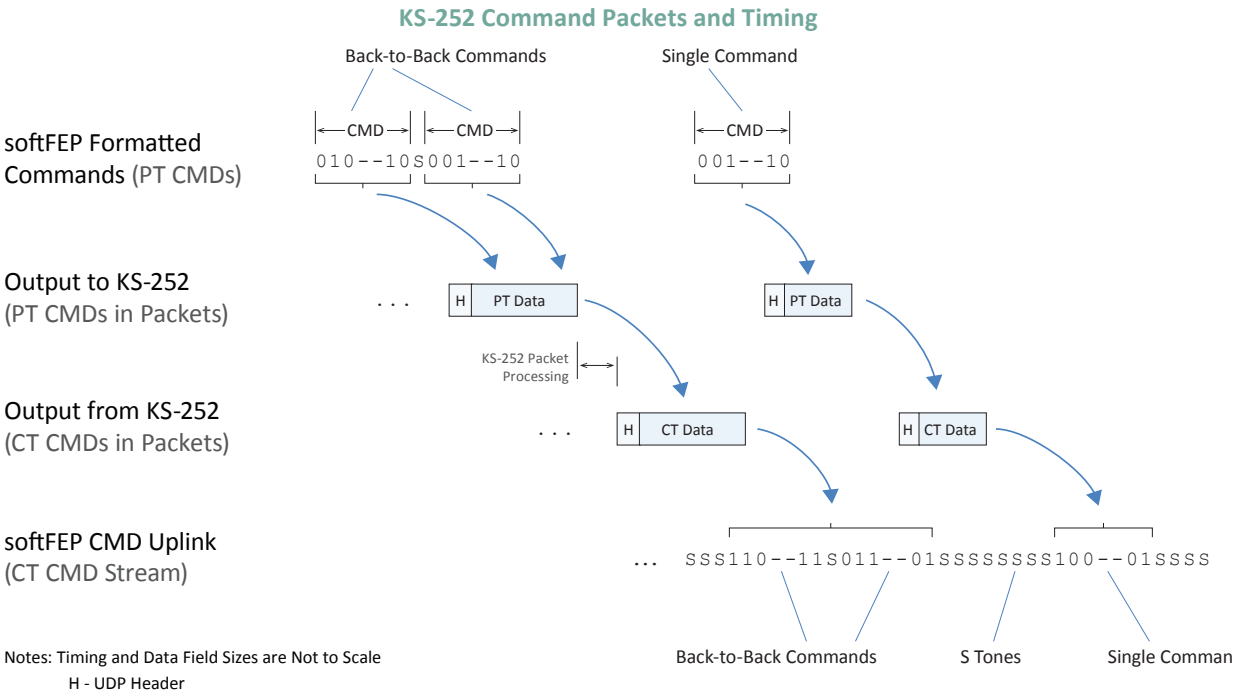
User Interface: The KS-252 provides a browser-based UI and also supports a set of GEMS messages for control and monitor of the KS-252. Most deployments use an agent on the red-side Front End Processor to interact with the KS-252 through one of these interfaces.

Part 2 - Data Flow and Timing

Timing Considerations

Legacy serial devices provide a deterministic rate at which telemetry and command data flow. The KS-252 transfers variable length packets over an Ethernet network, and this causes small amounts of "jitter" in the end-to-end data flow. Front End Processors on both the plain-text and cipher-text side of the KS-252 employ timing algorithms to give the KS-252 serial-like timing.

An example timing diagram is shown below. The KS-252 accepts multiple commands in each packet, with each command being separated by one or more S-bits. There is a one-to-one corresponding output packet. If the input packet contains two commands, the output packet contains two commands. In this example, the black side Front End Processor or modem generates a continuous serial output, filling the spacing between command packets with S-tones or other idle patterns.



Helpful Links: www.viasat.com/products/ttc-goe-ks-252

Can we help? AMERGINT's expertise is available to assist in your systems engineering and design

Randy Culver
randy@amergint.com
719-522-2802