DTS3

3-Slot Network Attached File Server

CURTISSWRIGHTDS.COM

Key Features

- File serving (NFS, CIFS, FTP, HTTP)
- Block storage (iSCSI)
- Ethernet recording and packet capture (PCAP)
- Remote boot of network clients (PXE, DHCP)
- Full disk encryption - hardware and software
- Disk partitioning

Applications

- Deployed network-centric systems
- Mobile data loader
- Remote embedded client boot
- Flight test instrumentation

Overview

The Data Transport System 3-slot (DTS3) is a rugged, network attached storage (NAS) system for use in helicopters, fixed-wing aircraft, mobile ground vehicles, and ground stations. With three removable memory cartridges (RMC), the mission, map, and maintenance data can be stored and retrieved separately. Two layers of AES-256 bit encryption can protect your critical data-at-rest.

Secure Data-at-Rest

Every DTS3 includes software full disk encryption (SWFDE). The user controls the use of SWFDE via the Command Line Interface (CLI) where data is encrypted with an AES-256 bit algorithm. Whether you add the optional hardware full disk encryption (HWFDE) module or not, the DTS3 always supports SWFDE. Within the optional DTS3 HWFDE module, sensitive data is encrypted with AES-256 prior to storage on the RMCs. The encryption ASIC has been FIPS 140-2 validated. Also the AES-256 algorithm itself has been FIPS validated.

The encryption keys can be passed to the DTS3 in plain text or encrypted. The keys can be cleared by command, push button, or discrete input.

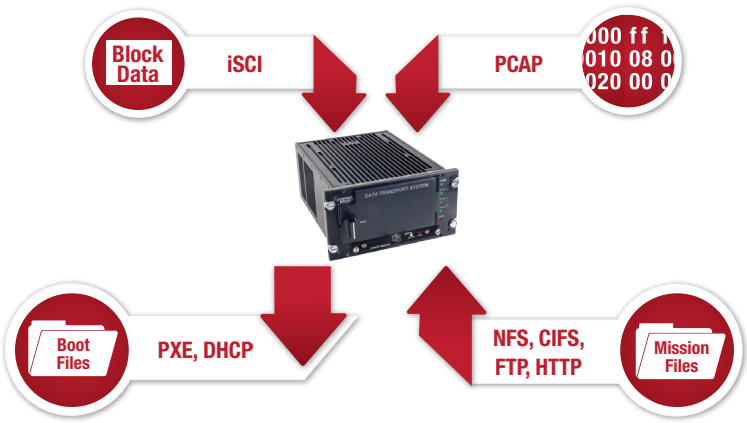

Figure 1: DTS3 in network-centric system with different clients

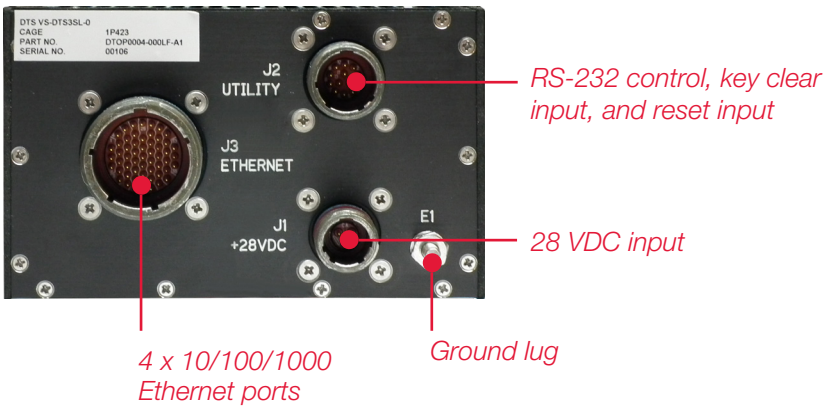

Figure 2: DTS3 detailed rear view

Net-Centric Architecture

Modern unmanned vehicles, ISR aircraft, and mobile ground vehicles are built around a network-centric architecture. The backbone of such systems is Gigabit Ethernet (GbE) operating at 1.25 gigabits per second. With a network switch (or redundant switches) in the middle of the system, any network-enabled device can communicate with any other similar device. NAS devices like the DTS3 allow any client to retrieve stored files or save new captured files. A NAS device provides size, weight, and power (SWaP) advantages by negating the need for local storage in each computer, display, or management device. These network clients can use the DTS3 to store sensor or maintenance data and to retrieve the latest mission and digital map data. Supporting industry standard NAS protocols like NFS,CIFS, FTP, or HTTP, enables the clients to use different operating systems (Linux®, VxWorks®, Windows®, etc) or CPUs (PPC, Intel®, Arm®, etc), permitting system design flexibility.

Figure 3: DTS3 with AES-256 crypto module

iSCSI Block Storage

The DTS3 also supports iSCSI protocol, enabling network clients to use the DTS3 as a block storage device. With the DTS3 acting as an iSCSI target, a network client can be the iSCSI initiator, having full control over how and where the blocks are stored.

All iSCSI data is encrypted in the DTS3 prior to storage. A separate partition must be set up for use by the iSCSI initiator. That partition can be equipped with its own unique software encryption pass phrase if needed.

Network Client Boot with PXE

The DTS3 provides the additional protocol called Pre-boot Execution Environment (PXE). Upon power up, PXE allows client devices to obtain boot files from the DTS3. These boot files will be up-to-date when the RMC is loaded by the commander or pilot prior to deployment. With this approach, there is no need to add the extra weight of local storage in each client. Eliminating all the local client drives can result in considerable platform SWaP savings.

In addition to SWaP savings, remote boot also provides the benefit of faster maintenance of the client software. Instead of requiring each client to be physically removed from the platform and transported back to the depot for software updates, the RMC can be loaded with the latest software for each client. This approach can provide a huge cost savings over a long program life.

All PXE boot files would be encrypted in the DTS3 prior to storage. A separate partition can be set up for storage of the PXE files. That partition can be equipped with it own unique software encryption passphrase if needed, restricting access to these important boot files.

White Paper: *Using NetBoot to Reduce Maintenance and SWaP-C in Embedded Systems*

Ethernet Packet Capture

In addition to standard NAS operation, the DTS3 has a special mode that allows the capture of Ethernet packets. This is essentially a *sniffer* mode where every character is captured and stored into a *.PCAP file. Packet capture is a handy feature for flight test instrumentation (FTI) systems like Curtiss-Wright's Acra KAM-500 to support trouble shooting of Ethernet problems.

The user can specify which of the four DTS3 Ethernet ports is dedicated to packet capture. The user can also specify the RMC onto which the data is stored.

If the SWFDE feature or HWFDE option are used, then all the stored packets will be encrypted like normal NAS files. Upon reading the *.PCAP files, the data is decrypted for analysis.

The *.PCAP files are stored on a specific RMC in the DTS3 as directed by the user command. These files can be read with shareware like Wireshark®.

A separate partition can be set up for storage of PCAP files. That partition can be equipped with it own unique software encryption passphrase providing access control if required.

DTS3 packet capture is ideal for troubleshooting Ethernet problems and in FTI applications. Either case is an example where post mission analysis of not only the data, but also the actual packets is important.

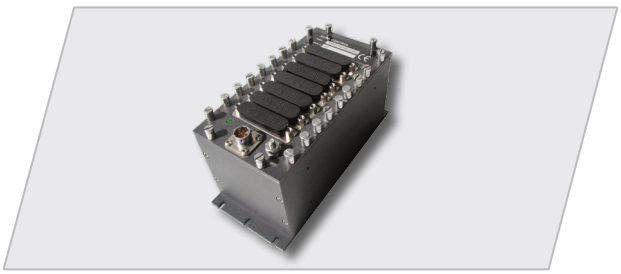

Figure 4: KAM500

Scalable, Rugged Storage

The DTS3 supports three RMCs. SSDs range from 256 GB to 2 TB. Each disk consumes about 2.5 W of power, weighs only 0.7 lbs (318 g), and is small enough to fit in a shirt or flight-suit pocket. MLC flash memory can be selected to balance cost and endurance. Each disk is individually addressable by clients to specifically save or retrieve functional data like mission, map, or maintenance information.

A convenient RMC download station is available. This small device converts SATA from the RMC to USB. The USB port can be connected to virtually any computer to off-load data from the RMC or to put data onto the RMC.

Figure 5: USB download station

Removable Memory Cartridge

The Removable Memory Cartridge (RMC) is uniquely designed to avoid obsolescence issues commonly seen with memory cartridges. The RMC is based on industry standard 2.5" SATA SSDs, enabling the RMC to take advantage of the industrial base and incorporate any of the widely available 2.5" SSDs. As a result the 2.5" SSD RMC design allows DTS3 to leverage the dynamic and fast paced technical developments of the SSD industry.

Figure 6: RMC connector and front view

The RMC has also been designed to reliably support programs for many years with a 100,000 insertion cycle connector that includes a SATA interface. The RMC is well suited for deployed applications requiring the storage of data and then the removal and transport to another location. Such applications include ISR applications, any mobile application (ground radar, ground mobile, or airborne ISR pods), any heavy industrial application (steel, refinery), cockpit data, or video/audio data collection.

Optionally, an empty RMC can be purchased and the SSD of your choice can be added. This could include SSDs certified to encryption standards needed for your program, or SSDs providing a specific MIL secure erase function (NSA 9-12 for instance).

Figure 7: 3 RMCs labeled for 3 functions

When transporting the RMC from platform to the ground station, the data is consider unclassified. Due to the complexity of the two DTS3 layers are not certified. Must have been copied from DTS1. encryption layers, it is recommended that a DTS3 be used for the ground station.

Disk Partitioning

The DTS3 can be setup to support data files, block or packet capture data but data types must be stored separately. Data can be directed to a particular RMC, or an RMC can be partitioned, providing more options for the user. The partitioned RMC can appear like several virtual disks where separate partitions can be configured for each data type.

White Paper: *Using Software Full Disk Encryption and Disk Partitioning to Protect and Isolate Network Attached Storage Functions*

If the SWFDE feature is used, different software encryption can be set up for each partition in order to compartmentalize access.

DTS3 Specifications

Physical

- Dimensions (H x W x D)
  - 3.0 x 5.0 x 6.5” (76.2 x 127 x 166.7 mm)
- Weight
  - DTS3 (with 3 RMCs): 5.5 lb (2.5 kg)
  - RMC: 0.7 lb (0.32 kg)
- Mounting options
  - DZUS panel

NFS Power

- Input power: +28 VDC (MIL-STD 704E)
- Power dissipation: 35 watts peak with 3 RMCs (approximately 2 watts per RMC)
- Peak inrush current: 5 amps, 2 millisecond duration
- Performance (128 KB transfers)
  - All 4 Ethernet ports
    - Writing: 60 MBps each = aggregate of 240 MBps
    - Reading: 60 MBps each = aggregate of 240 MBps
  - Single Ethernet port
    - Writing: 112 MBps
    - Reading: 112 MBps

Removable Storage Cartridge (RMC)

- Data reliability: <1 non-recoverable error in 10^{14} bits read
- SSD endurance
  - <5,000 writes (MLC)
- User capacities (Note 1)
  - Unformatted: 256 GB, 1 TB, 2 TB
  - Formatted: 235 GB, 940 GB, 1.88 TB

Notes

1. 1 GB = 1,073,741,824 bytes.

Security and Encryption

- Hardware full disk encryption (HWFDE)
  - Available on the following version: VS-DTS3SL-F
  - AES256 bit (ASIC)
  - FIPS 140-2 certified ASIC (#1472)
- Software full disk encryption (SWFDE)
  - Standard feature on both versions, customer controlled
  - AES256 bit (dm-crypt)
  - Linux Unified Keying System (LUKS)
- Encryption Key(s) Clearance
  - Command
  - Front panel push button
  - Rear panel connector discreet input

Environmental Compliance

- Temperature
  - Operating: -40 to 55°C (71°C for 30 minutes)
  - Non-operating: -40 to 85°C
- Humidity
  - Operating: 0% to 100% (condensing)
  - Non-operating: 0% to 100% (condensing)
- Shock (operating): 20 g's peak, 11 ms wide, 2kHz frequency range
  - MIL-STD 810 Method 516.4, Procedure 1
  - MIL-STD 810 - half sine
  - MIL-STD 810 - terminal peak sawtooth
  - MIL-STD 810 - initial peak sawtooth
  - MIL-STD 810-20 impacts per axis, total of 60 impacts
- Vibration
  - Sine: 4 G peak, 74-2k Hz sine wave (RTCA/ D0-160D, Curve T modified as indicated)
  - Random: 0.02 g^2/Hz from 5Hz to 2kHz (60 minutes per axis, in each of three mutually perpendicular axes)

EMI Compliance

Evaluated with respect to MIL-STD-461F

- CE101: conducted emissions, power leads, 30 Hz to 10 kHz
- CE102: conducted emissions, power leads, 10 kHz to 10 MHz
- RE101: radiated emissions, magnetic field, 30 Hz to 100 kHz
- RE102: radiated emissions, electric fields, 2 MHz to 18 GHz
- CS101: conducted susceptibility, power leads, 30 Hz to 150 kHz
- CS114: conducted susceptibility, bulk cable injection, 10 kHz to 200 MHz, Curve 5
- CS115: conducted susceptibility, bulk cable injection, impulse excitation
- CS116: conducted susceptibility, damped sinusoid transients, cables and power leads, 10 kHz to 100 MHz
- RS101: radiated susceptibility, magnetic fields, 30 Hz to 100 kHz
- RS103: radiated susceptibility, electric fields, 2 MHz to 18 GHz, 200 volts/meter

TABLE 1 DTS3 Ordering Information

PRODUCT NUMBER	DESCRIPTION
VS-DTS3SL-0	DTS3 without HWFDE
VS-DTS3SL-F	DTS3 with HWFDE
VS-RMC2USB-00	RMC SATA to USB conversion fixture w/o encryption
VS-RMC2USB-F	RMC SATA to USB conversion fixture w/encryption

See RMC product sheet for information