

SECURE SYSTEMS Embedded Silicon Data Vault



Secure Systems Limited

Hardware Based Data Security for Embedded Systems

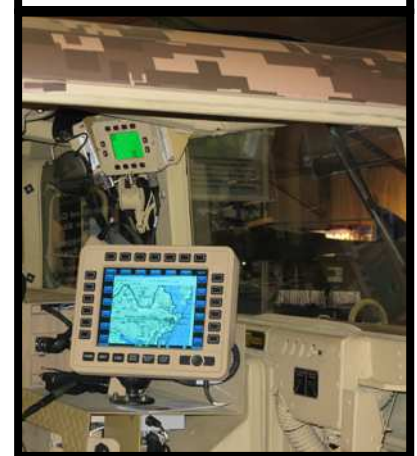
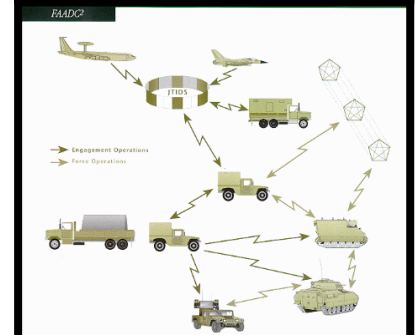
Network centric warfare has resulted in greater volumes of data being generated and processed in combat zones. When a net-centric system has to be abandoned in a combat zone lives do not need to be put at risk removing sensitive data.

The **Embedded Systems Silicon Data Vault (ESDV)** provides Common Criteria and FIPS approved, encrypted protection of data on all types of tactical systems: **ruggedised PCs, vehicle and weapon mounted computerised systems** and **portable data storage devices**.



The ESDV is a secure hard disk drive using **hardware based full disk encryption** to protect data-at-rest. Touch screen, keyboard and/or USB token-based authentication is available to ensure that only authorised personnel will ever gain access to classified data.

The 2.5" (or 3.5") SATA hard disk drive form factor ensures the TS-SDV retrofits into any standard mounting bay in your ruggedised laptop, portable weapon system or vehicle mounted weapon system. Adaptors are available for fitting to 3.5" bays.



The West Australian - 17 March 2010

"Australian troops have been forced to call in an airstrike to destroy one of their own vehicles after it was crippled in an insurgent ambush. Assessing the situation, senior officers decided it was best to destroy the Bushmaster rather than risk lives and equipment trying to retrieve it.

It was stripped of all sensitive equipment and the troops pulled back to a safe distance to call in an airstrike on the vehicle. A coalition fighter plane dropped two bombs on the Bushmaster, blowing it to pieces."



Current net-centric systems often require Commanders to order the removal of hard disk drives when under duress and needing to abandon the system. With the ESDV's full disk encryption and the Enhanced Secure Erase functionality one click will ensure the data on the drive is secured and cannot be accessed by hostile forces. Commanders can be assured that the data stored on the ESDV will not be compromised.

Technical Specification



Common Criteria



FIPS 140-2 Validation



Encryption	Security	Testing & Certification
AES 128 or 256 bit Dedicated hardware encryption chip Distributed key management	Pre-Boot authentication Touchscreen or USB token authentication Tamper evident chassis	Australian Government High Grade Assurance FIPS 140-2 Common Criteria

Secure Systems

UNITRONIX Pty Ltd

PO Box 486, Morisset NSW 2264
NSW: Tel: 61 2 4977 3511 Fax: 61 2 4977 3522
WA: Tel: 61 8 9455 2424 Fax: 61 8 9455 2458
unitsyd@unitronix.com.au www.unitronix.com.au

8/152 Balcatta Road, Balcatta WA 6021

Tel: +61 (0)8 9240 8708

Fax: +61 (0)8 9240 8709

www.securesystems.com.au