SecComm Vehicle (SCV)
Datasheet

The Ultra Electronics AEP SecComm Vehicle (SCV) "In-Vehicle" solution is a secure, feature rich, multi-bearer mobile data communications solution, specifically designed for Public Sector organisations that have a need to provide an encrypted two-way information flow between remote vehicles and command and control centres, providing the highest level of continuous, secure communications within a "mission critical" environment.

The solution provides the remote In-Vehicle work force with access to the same secure data applications and services, as colleagues working in command and control centres. CESG approved for use to restricted, confidential and short term secret, the solution automatically detects the available networks and selects the appropriate network connection, based on user prioritisation criteria, data size and type.

The SCV allows the efficient use of mobile data technologies, ensuring users can maximise the benefit from the available information regardless of location, specifically enabling users to send and received details of incidents, check databases while on a way to an incident and communicate electronically with their Command and Control Centres. The SCV eliminates the tedious and time-consuming task of manually re-inputting information into electronic media applications, by delivering information that is more detailed to the user at the point of need, in comparison with the amount, type and level of detail of information that is typically conveyed via existing processes.

Features

- Approved to CESG's Enhanced Grade

- Supports multitude of network topologies

- Multi-bearer network optimised for high data throughput via commercial carriers where available.

- Bulk data synchronisation/ transfer via secure on-site Wi-Fi

- Sophisticated tamper protection and compromise control for encryption devices

- Continuous random number generation checks

- High Reliability

- Feature rich management platform

- Automatic network selection

- Automatic network configuration

- Optional satellite for global coverage e.g. BGAN, VSAT, Vipersat

- Effective data compression over very slow circuits

In-vehicle element

Boot mouted anti-vibration rubbedised case, containing the following

- Application acceleration device
- VX Series Multi bearer router & processor, integrating

mobile data software and commercial network access airtime

- AEP Net Remote encryption device
- Application acceleration device

AEP

Ultra ELECTRONICS

The SCV multi-bearer router, routes the traffic to and from multiple communication networks, supporting WAN connections with multiple technologies, including, GPRS, 3G, Wi-Fi, Internet, Tetra and IP VPN. Optionally, the unit is customisable for connection to microwave or satellite communication terminals. The VadEDGE device also interfaces with other external communications equipment, including radio equipment and modems, supporting concurrent, simultaneous transmissions over multiple WAN interfaces to maximise the available bandwidth and is able to roam between bearer networks for seamless data communications without needing to re-submit transactions or re-connect any sessions.

The use of application acceleration and compression maximises the throughput of low bandwidth links, such as Tetra, providing an effective virtual speed many times greater than the raw data rate.

Approved by the UK Government's CESG Assisted Product Scheme (CAPS) to Enhanced Grade, assured to ITSEC E3 standards and accepted by the HMG's Defence INFOSEC Product Co-Operation Group (DIPCOG). The AEP Net Remote device is approved to separate data traffic from multiple user organisations over a single bearer e.g. Tetra.

The device meets the highest standards for a Commercial Off-the-Shelf (COTS) encryptor.

Command and control (Core) element

The VadIX multi-bearer router routes traffic to and from the bearer network and is scalable to meet customer's requirements and operates in a fully resilient architecture. The AEP ED100 encryption device provides both data confidentiality and source authentication for network traffic enabling high confidence Virtual Private Network (VPN) Communications.

Network management and network acceleration element

To manage routing policies, display and analyse the network connections, connected devices and traffic, the In-Vehicle solution uses the MegaWATCH SNMP management product, which is installed within the core network at Command and Control Centres, HQs or similar.

Delivering specialist secure communication solutions

The VadEDGE platform supports a wide range of protocols, WAN and user interfaces. This enables customers to aggregate and effectively deliver multiple service streams over almost any bearer communications network. This ability to carry all services across so many different interfaces and the ability to auto detect the available circuits, makes the VadEDGE platform flexible, resilient and extremely user friendly. The core component throughout the entire AEP Ultra Communicate Systems product range is the VadOS operating system. VadOS recognises the importance of each data stream as dictated by business need and assigns a level of service integrity and quality of service while dynamically managing bandwidth for optimal use. This approach to aggregating and delivering voice and other mission critical application data streams over the most efficient transport mechanism enables our customers to intelligently handle multiple protocol communication requirements with ease.

The proven AEP encryption devices are designed to seamlessly integrate into any network architecture providing a central management capability that enables "fit & forget" installation of the encryption devices. The devices are widely used by Government departments and agencies, local authorities, public health and public safety and criminal justice organisations that need to protect sensitive information across networks. Today many of these organisation use AEP network encryption devices to protect voice and data services across the Internet and other commercial communications infrastructures.