iTRINEGY

DE-RISKING THE DEPLOYMENT OF APPLICATIONS OVER MILITARY NETWORKS

INTRODUCTION

The adoption of network centric warfare has made the timely delivery of data to front line forces a critical requirement. Failure to achieve this could have potentially fatal consequences.

iTrinegy has been working alongside its military customers and leading defence contractors for over a decade to perfect the most accurate and realistic test network environments available from extremely low bandwidth, high latency environments through to high speed, high volume set-ups in order to ensure application and systems performance is thoroughly tested prior to deployment.

Drawing on our experience, we have developed a range of customer-extensible Network Emulation (Virtual Test Network) products that enable you to develop & test software, systems and devices in accurate replications of different types network with many different communications links (Satellite, Mobile, Wireless, WAN, Cloud etc.) prior to release. These products are also applicable to the testing of IoT systems and cyber defences.

The iTrinegy INE Range can quickly recreate realistic facsimiles of complex military networks

Given the complex nature of the networks our military customers are often trying to recreate, our engagement with them typically involves a comprehensive consultation to ensure their requirement is fully analysed, understood and deliverable.

Our products are already proven in many defence (and commercial) environments including the MOD, numerous branches of the US military, the Australian Government Department of Defence and leading global defence contractors.

MILITARY NETWORK CASE STUDIES

Case Study 1: Soldier-Carried Situational Awareness System
A leading defence systems supplier produces a situational awareness system for use in-vehicle and solider-carried where effectively the user can look into a scope or at a screen which, using symbols (squares, triangles and similar objects) displays data such as enemy locations, the position of their own troops and target designation for airstrikes etc.

When a solider enters a new input into their situational awareness device, the updated information needs to propagated across all other devices. This is achieved using ad-hoc wireless networking, the quality of which can be highly variable owing to factors such as terrain and weather.
The systems supplier needed to test the devices in a network that is a realistic facsimile of the wireless network, ranging in quality from desired, disadvantaged to disrupted.

MILITARY NETWORK CASE STUDIES (CONT.)

Case Study 1: Soldier-Carried Situational Awareness System (Cont.)

They selected iTrinegy's network emulator as it was capable of cost-effectively connecting 30-50 devices simultaneously and creating the different ad-hoc networks required in a typically fully meshed wireless set up. This allowed the contractor to realistically test these devices long before any field tests needed to be conducted, thereby accelerating systems development and greatly reducing the cost of having to correct any potential failures that may not have come to light until the field trial stage if this approach had not been adopted.

Case Study 2: Government Communications Research Centre

A national government scientific laboratory with responsibilities for research and development in wireless technologies needed to simulate a wide range of communications involving vehicles, solider-carried devices, aircraft etc., across wireless networks. Network conditions in this environment could change rapidly, for example as two aircraft initially approach and then pass each other.

Therefore, it was important that, not only could they connect multiple devices (in this case up to 17 simultaneously) in a fully meshed wireless set up but also that they could vary the various network properties millisecond by millisecond. iTrinegy's network emulator was selected as it was capable of accurately meeting both the network and the high speed changes in this requirement.

Case Study 3: Army Information Systems Proving Centre

A leading European army uses iTrinegy's network emulation technology as an integral part of its test and reference facility to ensure the resilience of military communication and information systems throughout their lifecycle.

Every application destined for use across for the army's core network needs to be proven as being safe to deploy in the live environment. Using the facility, applications are effectively "certified" as being fit for purpose in this environment and iTrinegy's network emulators provide a synthetic version of the army's network in which to conduct these tests.

Any applications or systems that fail are sent back for reengineering or modification. Our emulators have to faithfully reproduce the conditions of the live Army network including changeable or varying quality experiences as they are tried in different scenarios/theatres.

ITRINEGY NETWORK EMULATORS

The iTrinegy range of network emulators (software, hardware and virtual appliance-based) simulate a wide range of network impairments such as packet bursts, latency, congestion, jitter, bandwidth restrictions, packet loss and errors that IP-based applications could encounter over different military networks.

All of iTrinegy's Network Emulators provide an easy-to- use interface for the creation of Wireless, Satellite, Mobile, WAN, Cloud, SD-WAN, LAN or other types of networks. Users can easily adjust settings to reproduce different levels of network quality (Desired/Disadvantaged/Disrupted) to accurately reflect the state of network connectivity as operations evolve over time. Extreme impairments, used to represent degradation in network availability due to terrain or enemy activity can also be created on demand.

NE-ONE EMULATOR RANGE

With iTrinegy's NE-ONE Network Emulator you simply select and run the type of point-to-point or point-to- multi-point Network scenario you require.

With NE-ONE you can also adjust the order and duration of each scenario dragging and dropping the scenarios onto a timeline and then, simply playing them in the order you select. You can even select automated intelligent transitions.

INE ENTERPRISE / ULTRA

Where you need to map multiple communications links or large numbers of devices in a more complex network environment, our INE range (INE Enterprise and INE Ultra) with their network drawing interfaces and ability to connect 200+ devices are the ideal choice.

VIRTUAL APPLIANCES

Both the NE-ONE and INE Enterprise are also available as part of our Flex virtual appliances range, certified to run on VMware's ESXi Server.

SUMMARY

Military organizations are increasingly reliant of data communications to provide them with battlefield advantage. Whether it is to achieve superior situational awareness or improved resilience, systems that are required to be delivered over networks need to be thoroughly tested.

iTrinegy Network Emulation products provide highly realistic facsimiles of a wide range of military communications networks to identify and mitigate the risk of application performance issues or failure.

They can be used to accelerate systems development and delay any real live network trials until much later in the project lifecycle, leading to significant cost savings.

iTrinegy is an established world leader in Networked Application Risk Management and is trusted by governments, military organizations and enterprises across the globe who have drawn upon our proven expertise in effectively verifying application performance over Wireless, Satellite, Mobile, WAN, Cloud, SD-WAN, LAN as well as other types of networks.

www.itrinegy.com · T: (USA): +1 888 448 4366 · T: (UK): +44 (0)1799 252 200 · E: info@itrinegy.com

ref: ITRINEGY-MILTECHBRIEF-02142018