A COTS based Testbed to Develop Mission Tailored Solutions: Versatile Communications Backbone Network

Dr. Alberto Domingo, Dr. Hermann Wietgrefe*
NATO Consultation Command and Control Agency,
P.O-Box 174, NL-2501 CD The Hague (The Netherlands)
* Member IEEE

and

Mr. Miguel Angel Rico
MARM Desarrollo de Sistemas, Asesoría y Consultoría S.L.,
Madrid (Spain)

Abstract – **The NATO Response Force operational concept is based on the rapid deployment of expeditionary forces at a number of locations with mission tailored capabilities. Commercially available products fail on key NATO requirements for various reasons, e.g. form factor, types of supported interfaces, and resilience, to name a few. Therefore a commercial-of-the-shelf (COTS) technology based testbed for the development of mission tailored communication functions has been drafted. As a first application of this testbed, a tailored, multi-service, highly redundant LAN/MAN ring communication system for deployed military CIS infrastructure, the so called Versatile Communications Backbone Network (VCBN), has been developed by the authors. The VCBN concept provides a very-high reliability backbone ring, made up of two dual-redundant IP rings. The rings can be implemented using different media, and therefore support very well the phased deployment of communications into theatre. To ease industrialisation, the VCBN nodes are implemented using COTS products: Intel-based single board computers, standard Ethernet interfaces, and a ring logic and node management application running on Linux. The system incorporates the functionality required for expeditionary deployments, and the strictly needed interfaces, without the complexity of commercial systems that, in general, render suboptimal solutions in terms of space complexity and cost. Each VCBN node can be fitted into a 2U, 19 inch rack-mount. Initial analysis has proved that VCBN nodes are operationally and commercially feasible, at an affordable cost. While established with the VCBN application in mind, the test environment used for the development is well suited for the development and mission tailoring of other communication functions.**

Keywords: NATO Response Force, NNEC, redundancy, availability, survivability, IP convergence, phased communication deployment, COTS.

I. INTRODUCTION

The NATO C3 Agency is NATO's technical research centre for Command and Control, Operations Research and Communication and Information Systems. Consequently, NC3A develops various prototypes and proof of concept devices. The authors' area of activity is Deployable Communication and Information Systems (DCIS). The DCIS Scientific Programme of Work studies concepts to provide deployable and mobile CIS solutions tailored to the special needs of expeditionary forces, including operation and maintenance, network planning and network management.

Addressing the above, DCIS research work concentrates on developing lightweight DCIS components and improving CIS performance. The aim is to design modules that can finally constitute the deployable element of NATO Network Enabled Capability (NNEC), the future network centric warfare enabled CIS components. In the NNEC concept, all CIS infrastructure is expected to converge to an all-IP infrastructure, interconnected by a Quality of Service (QoS) enabled IP backbone.

NC3A has developed a number of prototypes, integrated into a DCIS test laboratory environment and interconnected with the other NC3A internal testbeds. To prove the suitability of the prototypes and testbeds, both are involved and tested during various events, ranging from CIS interoperability exercises to live exercises, conducted under operational conditions.

A large portion of prototypes and testbeds are based on Commercial Of The Shelf (COTS) technologies. However, commercially available solutions do not fully address all requirements for military CIS systems to support expeditionary and mission tailored deployments, e.g. form factor, types of supported interfaces, and resilience, to name a few. An example of a COTS based NC3A prototype and its application in Testbeds for mission critical CIS systems has been introduced in [1].

This paper discusses a COTS based testbed for the development of mission tailored communication functions. As a first application of that testbed, a highly redundant LAN/MAN ring communication system for deployed military CIS infrastructure, the so called Versatile Communications Backbone Network (VCBN) is discussed in detail.

The paper is structured as follows. First, future NATO transformational objectives are introduced, and some key aspects of typical expeditionary mission are discussed. From these high level requirements, the operational requirements for backbone network are derived. Commercially available products and technologies are introduced and discussed. As a tailored COTS based solution is identified as the solution best matching the requirements, this technical solution is elaborated in detailed, with special attention being paid to the ring logic proposed to meet the operational requirement. Finally, implementation aspects are addressed, and production costs for a final production are assessed.

II. NATO OBJECTIVES AND MISSIONS

NATO's Expeditionary Operations are characterised by deployed operations of the NATO Response Force [2] supplemented by units from many national Armed Forces. To be credible and effective, these types of missions require NATO CIS assets to deploy, be set-up and be ready for operation with only a few days notice to locations where little or no existing infrastructure can be expected. In the NATO Network-Enabled Capability (NNEC) era, Command and Control (C2) capabilities should be comparable to those available in the static domain. This requires deployed users to have at their disposal sufficient Communications and Information Systems (CIS). Also, effective reach-back between the static and deployed domains is necessary.

A typical NATO operational scenario would involve a number of deployed locations, interconnected among themselves and with the static headquarters using a Wide Area Network (WAN). A key element of the supporting CIS is the distribution of voice and data services between the WAN anchor point at a deployed location and the users in that location. While there are many technical options to support capillary distribution of scalable connectivity between the anchor point and the users, there are not many Commercial-Off-The-Shelf (COTS) based technologies able to cope with the functional, performance, operational, INFOSEC, interoperability and reliability requirements of a military operation. Commercial technologies are either focused on the industrial market (often lacking flexibility, performance or interoperability) or target the telecoms operators, with complexity, size and environmental hardening characteristics not matched to the requirements of a military mission.

The semi-COTS solution proposed in this paper offers a converged (all-IP) backbone, able to satisfy all the identified military user requirements, including rapid deployment (in a phased approach) and very high availability. In addition, the proposed solution easily adapts to embrace different information dissemination logics, constituting a very good test-bed to develop, test and experiment with NNEC-enabling concepts and technologies.

III. OPERATIONAL REQUIREMENTS

In a military operation the backbone should support all required services, including voice, teleconference and data, in several security domains. It should then support not only packet transport-based services (IP), but also traditional military voice and videoconference services, based on ISDN, analogue and tactical networks [3]. To minimise operation and maintenance complexity and cost, technology convergence to an all-IP solution is desirable.

Rapid establishment of services require a very fast initial CIS set-up and operation, which is best provided using a small number of user-nodes interconnected through wireless links. This enables provision of basic services within a few hours of arrival on-site. After the initial entry phase, the deployment is scaled-up by simply adding additional identical nodes as the operation grows in size. That is the moment when wireless links can be augmented and/or replaced by wired ones, to enable more secure, higher performance operation, as soon as battle rhythm allows doing so.

Because the backbone carries all traffic within the deployed location, it can become a single point of failure. High availability and reliability is required, including path and media diversity. Therefore ring topologies are suggested, but based on dual redundant rings rather than on single-redundant solutions that industry normally offers. Finally, to comply with the potentially adverse environmental characteristics of deployed missions and the limited availability of logistic support, the selected solution should allow ruggedization, be small in footprint, limited in weight, provide only those functions and interfaces required for the mission, be based on technologies requiring limited training and expertise on the support CIS companies, and should preferably be based on identical (and therefore interchangeable) low-cost nodes.

IV. TECHNICAL SOLUTION

To satisfy the above requirements, an initial feasibility analysis was performed, including a comparative analysis of potential solutions. The comparison criteria are categorised as follows:

- Functional requirements
- Interface requirements
- Performance requirements
- Operational requirements
- Implementation requirements
- Network Management requirements
- Environmental requirements
- INFOSEC requirements

and included for example: a) feasibility of implementation using mainly COTS, b) compliance with open industry standards, c) feasibility of tailoring to specific military requirements, d) high availability/reliability and fast recovery upon (node or link) failures (less than 50 milliseconds), e) support for phased deployments (including support for initial wireless based operation), f) converged (all-IP) solution, g) support for remote management, h) reduced footprint, i) feasibility of ruggedizing the solution, j) cost per node, and k) compliance with the rest of the overall requirements as described in previous section.

In total five options were explored, and scored in terms of their ability to satisfy the above criteria. The results of the ranking (in normalised percentage with respect to the best identified solution) were:

- Backbone based on a next-generation of current product family (optical transport network) (35%);
- Backbone based on layer-2 frame repeaters in a dual ring configuration (41%);
- Backbone based on Resilient Packet Ring (RPR, IEEE 802.17 standard) nodes (53%);

- Redundant backbone based on standard IP routers in a dual ring configuration (59%), and
- Tailoring of an integration of COTS-based products (100%).

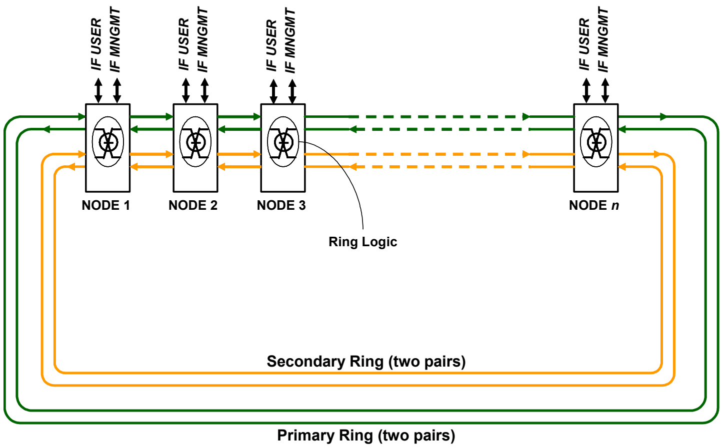

Figure 1. Backbone ring structure in VCBN

Based on the above, a technical solution based on a tailored integration of standard COTS was selected. This option proved to be the only one able to comply with all functional and interface requirements for the backbone and user interfaces to access the backbone. In addition, the solution is

- able to combine the ability to use open-standards,
- provide a converged (all-IP) solution,
- able to tailor the design to different deployment scenarios (including support for phased deployments),
- feasible to end-up in a low-cost, small and lightweight, easy to environmentally-harden product.

The proposed solution, called *Versatile Communications Backbone Network* (VCBN), is based on a variable number (in principle unlimited other than for total ring delay aspects) of identical nodes. The nodes are connected using a dual redundant ring structure, as shown in Figure 1.

Every node in the backbone is connected to each of the two adjacent nodes using two Ethernet interfaces (primary and secondary). Each interface is bidirectional, and uses different media for each direction, actually resulting in four possible transmission paths between any two nodes. Each of the interfaces can be of arbitrary media type (fibre, copper, wireless, etc.) and capacity. All the links in the backbone connecting the primary interfaces of the nodes make up the Primary Ring (or Ring A), while all the links connecting secondary interfaces compose the Secondary Ring (or Ring B). No links interconnect primary and secondary interfaces.

The ring logic determines which of the four outbound port available in any node should be used to transmit a frame on the ring. To enable different link capacities in the same ring, nodes implement buffering while forwarding packets between the different interfaces.

At node level, each VCBN node consists of a set of building blocks (depicted in Figure 2), which implement the required functionality.

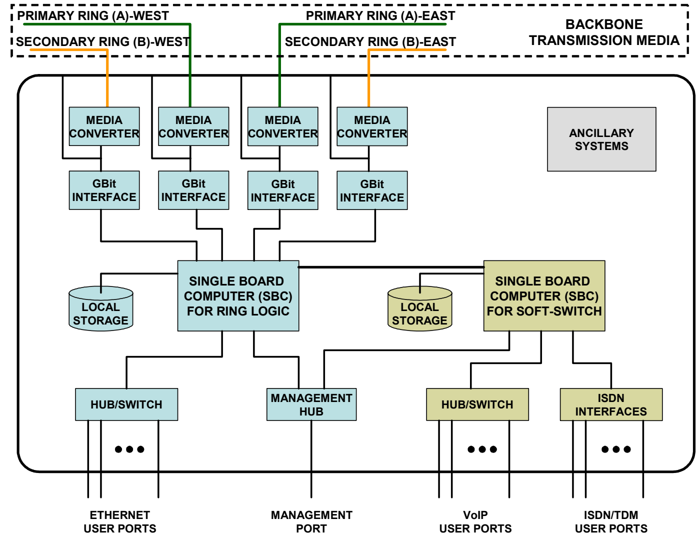

Figure 2. VCBN node HW architecture

The Single Board Computer (SBC) for ring logic implements the logic of the network bridge/switch, including packets capture, bridging/routing function, filtering, monitoring and control of system, management functionality, etc. The network interfaces provide at least four 1 Gbps Ethernet ports for the backbone rings, plus a number of Ethernet interfaces (auto-sensing) for user traffic, and at least one Ethernet interface for management purposes. The media converters provide conversion between the copper interface of the Ethernet ports and the fibres and/or wireless devices used for the actual transmission. The local storage hosts the soft-bridge operating system, the bridge application and libraries, and the system configuration and status parameters. The single board computer for the voice switch implements a basic PABX-like function for VoIP phones, ISDN and analogue devices. The voice switch will provide local switching for calls between local (to the node) users, but also switching for calls to/from users in other nodes. In any node provided with this functionality, one or several user ports can be used as a gateway to other voice networks, including those based on ISDN or PTT technology. The line between the two single board computers in the figure represent the logical connection for voice calls routed through the backbone ring(s) to users in other nodes/remote networks, while physically this connection can be realised using the management hub shown in Figure 2. The ancillary systems include a common power supply, KVM switches, cabling, patching and mechanical fixtures, as required. Additionally tools like a traffic monitoring and analysis platform [4] can also be embedded to facilitate traffic management and enforce security in the deployment site.

The architecture described above is able to deal with both data and voice applications. In the latter case, both existing circuit-switched implementations (ISDN, legacy POTS and tactical systems, mainly) and packet-switched solutions (such as VoIP) can be supported. This is achieved by embedding a soft-switch platform in each of the VCBN nodes. If only a subset of nodes connect to users of voice/VTC and other Time Division Multiplexing (TDM), the system developers could opt to implement two different VCBN node types.

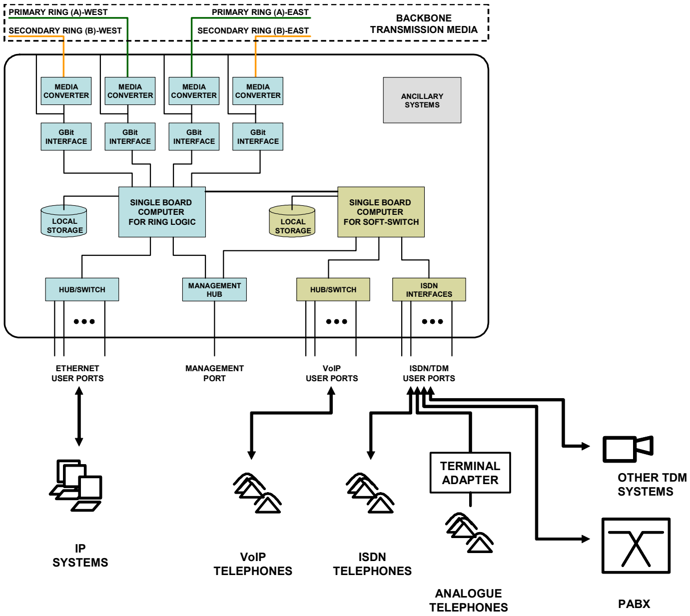

Figure 3. Connection of users to a VCBN node.

At the user side, the soft-switch platform offers standard IP ports to which users can attach standard IP phones. In addition, the Single Board Computers (SBC) can be fitted with interface cards implementing POTS, ISDN PRI and BRI ports, to connect to ISDN or analogue phones, to interface with an existing ISDN-based system (such as a PABX, including those of the local Telco), or to provide transparent PRI or BRI channels. Internally to the soft-switch, ISDN and analogue calls are converted to VoIP before being forwarded to VoIP users on the same node or any other user in any other node. Figure 3 shows the described interconnection of user terminals and VCBN nodes, with particular emphasis on voice terminals.

On the backbone side, the soft-switch platform connects to the routing platform in the VCBN node, and uses the high-speed Ethernet interfaces to exchange voice conversations with other users/systems attached to other nodes. Voice conversations are transmitted as VoIP traffic, interleaved with data traffic. To preserve voice quality, QoS mechanisms are enabled in the backbone (using path diversity or other mechanisms) under conditions of expected high load. QoS for IP voice and/or transparent PRI/BRI channels can be provided using several techniques, including reserving specific paths (e.g., the signalling direction of a ring, or the secondary ring) in the backbone, implementing DIFF services (RFC 3260) on the VCBN switch, etc.

To complement the above building block diagram, a software architecture based on different layers is used to manage and control the ring, the nodes, and the node interfaces. This software architecture is shown in Figure 4. It shows both hardware elements and the overlaying operating system and tools used to manage it. In addition a number of COTS software elements are used to implement generic network and traffic related functionality. Finally, boxes above the dotted line depict additional in-house effort that needs to be done to implement (on top of existing COTS tools) the required VCBN functionality.

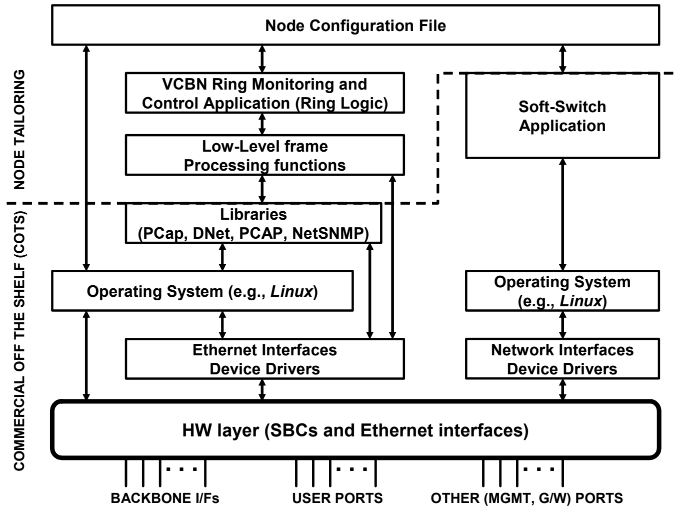

Figure 4. Software architecture of VCBN

In the Figure 4, the HW layer comprises the two SBCs, network interfaces and other HW items used to build the system barebones. The interfaces device drivers provide to the operating system and tools a unified application program interface (API) to isolate network functions from the specific interface types and media. The Operating System provides generic functionality to operate the underlying hardware.

For the backbone control, standard libraries of low-level communication functions are used to simplify the implementation of the ring logic. These functions include basic routines to configure the interfaces, to transmit and receive frames, to process the frames, to manage the system, etc. on top of these basic routines, a number of functions need to be developed specifically for VCBN. They mainly determine the behaviour of the node upon reception of frames (from the backbone and/or the user ports) plus the overall node signalling strategy. This is referred as the *Ring Logic* (or Ring Monitoring and Control Application). Above the ring logic, identical for all nodes in a ring, a small overlay element determines the specific configuration details of each node, describing specificities such as the node number, number of interfaces, node addresses, voice configuration details (like numbering and dialling plan), etc. This element of the node SW architecture is referred to as the *Node Configuration File*.

On the voice side of the VCBN node, and on top of the hardware, the drivers and the operating system, a COTS soft-switch application is used. The Node Configuration File described in the paragraph above can be used to store the specific details (numbering, dialling, routing, access control mechanisms, etc.) of the voice part of the system.

V. RING LOGIC

The ring logic determines the process to be followed to route each frame arriving to any ring node through any of the available interfaces. It also describes which strategy is used to detect a node/link/port failure, and which actions are triggered upon failure detection (of any node, link and/or port). The concept of implementing VCBN over a set of SBCs plus an overlying software/firmware ring control function allows implementing almost any type of ring logic. Different ring logics can be implemented to achieve different ring behaviours, in principle linked to the intended operational use of the network.

The ring logic of the first VCBN prototype focuses on easing *phased deployments*. A phased deployment is understood as a set-up where initially VCBN nodes are interconnected using wireless links, in whatever technology available (e.g. WiMAX (IEEE 802.16-2004) point-to-point Line-of-Sight radio links, IEEE 802.11, etc.). This typically happens when there is little time or resources to implement a wired backbone.

In a second phase of the deployment, as time permits, wireless links are augmented and/or replaced by more reliable, typically higher capacity links, based on wired (fibre or cable) technology. As soon as the first of those wired links is deployed, the concerned nodes detect the presence of the new link and start routing traffic between the two of them using the primary (wired) link. As more wired links are deployed between other nodes, those primary ring links become active while the wireless (secondary) ones become idle. Wireless links might also remain operational as backup, for traffic balancing, or be gradually phased out, as the ring logic supporting the operational needs deems appropriate.

To implement this logic, the ring monitoring and control application implements the following principles of operation:

- Primary ring (ring A) shall operate clockwise (East-to-West) for data traffic, and in the reverse direction for ring monitoring and control purposes (such as heartbeat frames transmission and other mechanisms to detect ring failures). Secondary ring (ring B) shall operate in the opposite manner: counter-clockwise (West-to-East) for data traffic, and in the reverse direction for ring monitoring and control.
- Each node will have at least ten interfaces. Four of them will connect the node to the adjacent node to the west (PRW1, PRW2, SRW1 and SRW2), other four to the corresponding to the East (PRE1, PRE2, SRE1 and SRE2), one (or more) is dedicated to node users and the last one is reserved for node management purposes.
- Whenever possible, user traffic shall use the primary ring (A), and only resort to the secondary ring (B) upon primary ring failure detection in one or more nodes and/or links.
- Heartbeat frames shall be independently generated and processed for each ring.
- Each node shall process all data frames arriving on any of the interfaces of any of the two rings. Any data frames for which the destination is a user locally connected to the node shall be forwarded to the local port where the user is connected. Data frames addressed to a user connected to another node shall be sent to the forward direction on the primary ring (if possible). Data frames with unknown destination shall be broadcasted to all the local ports and to the reverse direction on the primary ring (if possible). Routing/bridging tables shall be updated accordingly.

A ring monitoring and failure detection algorithm is implemented in a manner that failures are detected within a few milliseconds. Upon failure of one link/port in the primary ring, the secondary ring shall be set as the active link/port in that segment. Upon restoration of communications in the degraded primary ring link/port, the primary ring becomes active, and the secondary ring is set as back-up again. In case of double link/port failure in the nominal rings data traffic direction, ring folding on the primary ring is activated if possible. In case of triple link/port failure (in the nominal rings data traffic direction and in reversal primary ring direction), ring folding on the secondary ring is activated. Upon restoration of link/port communications in the nominal ring data traffic direction, the nominal direction becomes the active direction. Switching to redundant ring and folding is done in such a way that no significant impact on the user applications is observed. This includes fast recovery time for time-sensitive applications, and normal provisions to cope with lost and duplicate frames.

To implement the above, VCBN nodes will operate at layer 2 (link layer) of the ISO-OSI reference model. They will be then, transparent to higher level protocols, such as IP. Each node interface has its own (MAC) address. Data is transmitted with a source address (sender) and destination address (final receiver). A "*time to live*" (TTL) parameter is added to avoid that a frame that does not reach its final destination perpetually circulates through the ring.

The ring supports unicast, multicast or broadcast (flooding) addressing. The different types of addressing are supported by the standard protocols and not considered hereafter. Multicast and broadcast need support from the ring logic, to manage multiple transmissions/receptions of identical frames.

To gain awareness of the VCBN topology and status, a *Topology Discovery Frame* (TDF) is used to describe the current status of the backbone. The TDF is retransmitted periodically, or when a change in the topology is detected, by any node in the ring. The TDF is built with the MAC addresses of each of the nodes and their position in the ring. Each node sets the known part of a TDF. In addition, each of the nodes in the ring announces its state to the adjacent nodes using a heartbeat data frame.

By knowing the ring topology, in case that several paths are possible to forward a packet, each node will implement the logic to transmit the data in the more convenient ring/direction. The implementation processes of each node considers the following tasks in the given order of priority in order to allow fastest topology changes detection and recovery actions:

- Heartbeat frame transmission.
- Heartbeat frame acknowledgement.
- Interface status update.
- Topology frame acknowledge.
- Topology frame transmission.
- Node/network management commands.
- Data packets acknowledge and dispatch.
- Node/network management background tasks.

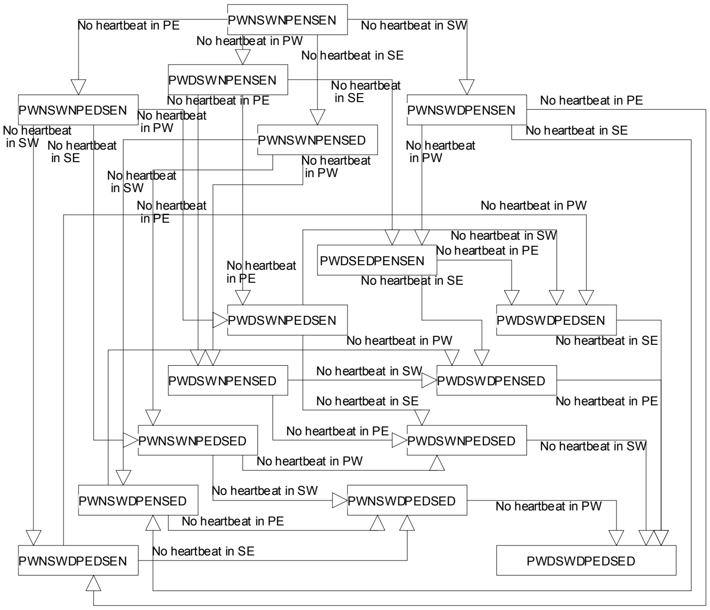

Figure 5. Nodal state transition diagram

One fully deployed ring allows recovery from a single point of failure. With two completely deployed rings the system is able to survive three failures. The mechanisms to allow this is described in the node transition diagram depicted in Figure 5. A state transition takes place when the node detects the lack of a heartbeat signal on one of its interfaces. Depending on the state, the ring logic forward traffic taking into account the current status of the interfaces as indicated by the heartbeat signal, or the lack thereof.

VI. IMPLEMENTATION

To implement the above technical solution a number of COTS-based options were evaluated, and finally a configuration was selected for the prototyping effort. The configuration is based on Intel-based single-board computers, on for the ring logic, and a second SBC for the soft-switch. Backbone ports are implemented using Intel pro1000mt quad port server Gbit Ethernet adapters [5], while a number of 100 Mbps Ethernet interfaces (provided by the SBCs and two hubs) are used for the user and management ports. Standard media converters with sufficient output power to reach distances of up to 2 km per link on military fibres (up to 15 dB between any two ports) are applied, and LinkSys Ethernet bridges simulate wireless links between nodes. S-ATA hard disks are used for local storage during prototyping phase (a Flash memory embedded system will be used for production units), and Digim and Beronet PCI E0/E1 interface cards (for the ISDN and POTS interfaces for non-VoIP voice users and other TDM applications) complement the configuration.

On the software side, the selected configuration is based on the SUSE Linux operating system, which provides the generic functionality to operate the underlying hardware, including the device drivers for the Ethernet interfaces. For the backbone control, the standard libraries of low level communication functions Libdnet [6] and LibPCAP [7] are used to simplify the implementation of the ring logic. They include basic routines to configure the interfaces, to transmit and receive frames, to process the frames, to manage the ports and interfaces, etc. The ring logic is developed in C++ and JAVA as a software application built over the hardware-level function libraries, implementing a set of APIs which provide a number of simple functions to control the backbone. Those functions are generic, and valid for any ring logic that might be implemented. The different ring logics are then a result of the specific combination and sequence of calls to those functions, allowing easy modification of the ring algorithm. The specific configuration details of each node are stored in a plain text file. For the soft-switch, the open-source Asterisk [8] has been used. Finally, the Net-SNMP [9] library is used to implement the overall VCBN management and control layer.

VII. DEVELOPMENT EFFORT

Implementing the above dual-backbone ring architecture only makes sense if (in addition to meeting the operational requirements) it does so at a reasonable cost. By "*reasonable cost*" we understand that it is in the order of magnitude of the current in-use technologies, when a purchase volume of nodes of about a hundred is considered.

To verify the above, a cost analysis has been done, which considers the one-time development cost of the first-node, and prototype costs for follow-on nodes two to five. After successful testing, the cost of industrializing the design is assessed, and finally the cost of producing 100 industrialized nodes. The resulting cost per node is depicted in Figure 6. It turns out that cost for a first node would be in the order of 50 KEUR, and that it would gradually decrease to 15 KEUR for productions quantities of about a hundred nodes, showing that the VCBN solution is also commercially viable.

VIII. DEVELOPMENT STATUS AND FUTURE WORK

At the time of writing this paper NC3A has procured and integrated the hardware required to implement three VCBN nodes, which is the minimum number required to test compliance of the architecture with the operational requirements in a single security domain [10]. First testing results show that the functionality can easily be achieved, and that the system is flexible enough to accommodate a large variety of ring logics, tailored to a number of different deployment scenarios. The preliminary results also show that the prototype and the developed test environment are an extremely flexible and appropriate tool for test-bedding other concepts of interest for CIS in deployed expeditionary operations, including Quality of Service (QoS), VoIP add-ons, interoperability solutions and NNEC-related concepts and experiments.

Further work on VCBN includes finalising the prototype to fulfil the requirements of a product ready for industrialization. This includes improving the software reliability and maturity, but also hardening the hardware for compliance with potential harsh environmental conditions. Finally, some optimisations like using solid-state memory only, additional backbone and user interfaces, or better user operation and management tools are also expected short-term improvements.

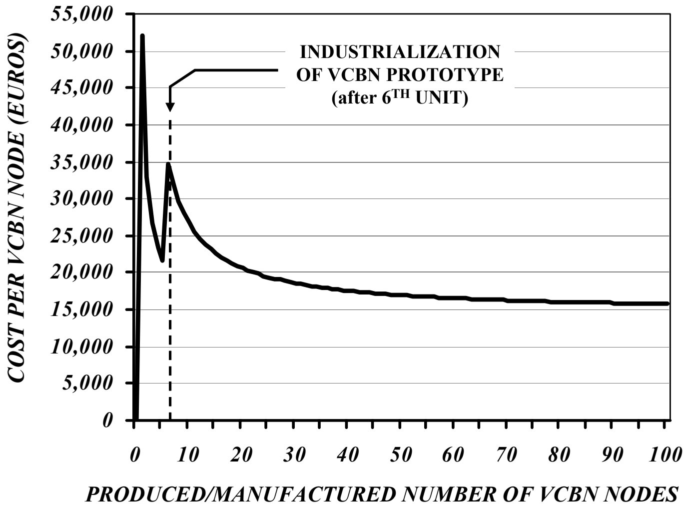

Figure 6. Cost per no. of VBCN Node produced

In a more long-term basis, other ring logics will be implemented to reflect alternative operational needs (like reliable split-up of strategic and tactical networks, secure separation of communities of interest, stand alone reach back support, etc.), to favour one type of traffic over another, or to ensure that some traffic flows always receive a given amount of bandwidth (QoS oriented logic). Also, ad-hoc networks principles will be investigated to implement low-cost traffic delivery mechanisms and to optimize service to mobile users, while spread ring logic techniques will be analysed to improve guaranteed reliable delivery of frames to adjacent nodes connected by unreliable links.

IX. CONCLUSIONS

The development of prototypes and their interconnection to testbeds is a pivotal activity in the NATO's development cycle of mission tailored CIS solutions. Main research and development activities are directed towards is the use, adaptation and customisation of Commercial Of The Shelf equipment to meet NATO's requirement for mission tailored, flexible, robust and reliable CIS. One outstanding example, the Versatile Communications Backbone network, and the related prototype and testbed activities, have been discussed and analysed in detail in this paper.

Out of the performed analysis it seems that 100% COTS solutions might not be optimal for today's highly specialized military CIS needs. Network-enabled capabilities demand functionality and performances at very high reliability rates that cannot be entirely achieved using standard industrial or telecoms operators' technologies and product lines. Instead, with the availability of low cost, high performance, highly programmable boards and associated tools, tailoring is becoming a good solution to enable full-functionality adaptation, while allowing reduced footprint and less dependency from specialized commercial suppliers.

One of the examples of the above is the provision of all-IP high-availability CIS backbones, with the functionality and interfaces required for military deployed operations. While commercial products today do not meet all NATO's operational requirements, the tailored device proposed in the paper can be produced in quantity for a price equivalent to (or slightly less than) the currently available products. In this area, tailoring can overcome the functionality limitations of off-the-shelf products and the relatively low reliability and low deployability of telecommunication products, while keeping the low costs associated with COTS products.

In addition, this paper shows that such tailoring allows implementing backbones able to incorporate specific needs, such as phased deployment logic, which is a versatility and flexibility not provided by standard, commercial and operator-oriented COTS products.

Finally, the proposed design has also been shown to be an excellent testbed platform for development of future NNEC solutions, including network convergence, QoS and VoIP, mixed-hybrid networks, network management and ad-hoc networks.

REFERENCES

[1] H. Wietgrefe, A. Domingo, T. Rogula: Monitoring, Capturing and Analysis of Mission-Critical Traffic in Experimental Communication Networks, IEEE TridentCOM 06, March 06, Barcelona

[2] A. Domingo, Operational View of NATO Response Force (NRF) CIS, NC3A Technical Note 1096, December 05. NATO Restricted

[3] Alberto Domingo, Hermann Wietgrefe. "NATO Deployable CIS Target Architecture" NC3A Technical Note 1009. Edition 3.0. March 2005. NATO Restricted.

[4] Alberto Domingo, Hermann Wietgrefe "Minimal-Intrusion Traffic Monitoring and Analysis in Mission-Critical Communication Networks", Journal of Systems, Cybernetics and Informatics, Vol 1, Nr 5, Dec. 03, ISSN 1690-4524

[5] Intel Quad Gigabit Ethernet Adapter. http://www.intel.com/network/connectivity/products/pro1000mt_quad_server_adapter.htm.

[6] http://libdnet.sourceforge.net/dnet.3.txt for the manual page of the library

[7] Library Lib-PCAP user manual http://www.tcpdump.org/pcap3_man.html.

[8] Asterisk soft-switch information page http://www.asterisk.org.

[9] General information on Net-SNMP library http://net-snmp.sourceforge.net. Comprehensive FAQ on Net-SNMP http://www.net-snmp.org/docs/FAQ.html.

[10] Alberto Domingo, Miguel Angel Rico. "Feasibility Analysis of a Multi-Service, Versatile Network Backbone" NC3A Technical Note 1170. in editing. NATO Unclassified.