Allied Data Publication 34

(ADatP-34)

NATO C3 Technical Architecture

Volume 2

Supplement 1: Domain Architectures

Version 6.0

Date: 30 September 2004

ISSC NATO Open Systems Working Group

Table of Contents

1. NATO ALLIANCE DIRECTORY ARCHITECTURE

1.1. REQUIREMENT FOR A NATO ALLIANCE DIRECTORY ARCHITECTURE

001. The requirement for a NATO Alliance directory architecture is to enable users across the NATO organisation and within individual NATO nations to share information in an efficient and effective manner. The information accessible via the NATO Alliance Directory will generally be the same for each user, subject to information access/export controls operating in the individual national Directory Management Domain (DMD)s.

002. NATO and national military communication and information systems operate at several security levels, and the NATO Alliance Enterprise Directory Architecture needs to take into account which system security levels require what kind of Directory Service. The NATO directory requirements at the Secret level, where MIS, CCIS (i.e. AIS) and MMHS systems typically interconnect across borders are quite different from the NATO directory requirement at the unclassified, public level (i.e. the Internet) where purely commercial standards are most applicable. Information exchange across the Internet typically involves many other parties and systems which are not NATO controlled, and the requirement and feasibility of an Alliance specific directory is much smaller. Again at other security levels such as Restricted, systems interconnectivity across borders today is non-existent, and an Alliance Directory System capability is thus not required. The NATO Alliance Directory is therefore primarily/initially aimed at supporting information exchange at the Secret system level. Systems at this level still exchange much information at lower classification levels, but across the “system high” infrastructure. The interoperability architecture recommended for the Secret level Alliance Directory can be selectively reused for directory solutions at other security levels for exercises, or operations involving non-NATO partners (e.g. PfP nations, Non-Nato Troop Contributing Nations (NNTCN)). The Secret level Alliance Directory is required to support exchange of directory information with AISes the NATO Secret level AISes has interfaces to. Such systems include CJTFs with NNTCN participation operating at “Mission Secret” security level. The SFOR and KFOR Secret CJTF networks are prime examples of systems the Alliance Directory will need to exchange directory information with.

003. Directory information drawn from classified systems, exposing names, organizational structure and address information, will also typically be classified (e.g. ACP-117 is NATO Restricted) and cannot be made available in a directory on unclassified/public NATO systems.

004. The way users from different nations' view shared information in the relevant systems (i.e. the classified systems) to be supported with an Alliance directory service is primarily based around organisations and roles, and the directory structure must focus on this aspect. In addition, a white pages search based on personal names and sites should be available.

005. However, the NATO Alliance directory should not only be viewed as a “white or yellow

pages" tool, but also as a global infrastructure supporting applications such as messaging (MMHS, various grades of e-mail) and storage of X.509 certificates as part of a Public Key Infrastructure (PKI).

006. For these requirements, the directory structure should globally support the following functions:

a. storing communication information (Military Message Handling System (MMHS), Message Handling System (MHS), email and general contact information for organisations, organisational role and organisational people),

b. providing access to this data through a query service,

c. exchanging this information internally through a replication service

d. providing for network interconnection,

e. offering a certificate & certificate revocation list repository,

f. management by authorised users.

007. It is emphasised that regular users will only have search and read type of access to the directory information, while authorised directory managers will be given access to add, delete and change directory information.

008. The Alliance Directory is assumed to be the Certificate Repository for the NATO PKI. Any specific requirements from this application that might affect the Allied Directory Interoperability Model have been requested from the PKI WG. In particular requirements concerning very short times for making new PKI information available to all Alliance Directory users, and/or the need to exchange very large amounts of information, are requested.

1.2. OVERVIEW OF NATO DIRECTORY ARCHITECTURE

009. The NATO Alliance Directory system is composed of:

a. the services offered to the user,

b. the information supplied by each nation and by NATO,

c. the systems in which the information is stored,

d. the protocols necessary for exchange of information between nations,

e. the means of securing the information and systems against attack.

f. access to an IP network protected at the appropriate security level for the instantiation of the Alliance Directory System, providing connectivity to all other border Directory Service Agents (DSAs) of that instantiation.

010. The NATO Alliance Directory is composed of a number of DSAs that collectively hold the NATO Alliance Directory Information Tree (DIT). The DSAs, which belong to the individual NATO nations and the NATO organization, cooperate to make the whole NATO DIT available to all users. It should be noted that within a national DMD, the distribution of information between DSAs and systems is an individual national matter, as is the amount of information provided from a nation into the NATO Alliance directory. A nation will typically have several directories exporting information to, and importing information from, its border DSA through directory filtering and synchronisation technology and techniques. Figure 1.1 below depicts a high level, generic/logical view of the Alliance Directory consisting of three tiers. It shows how information from various system/application directories within NATO and nations are synchronised and filtered before it is placed in their respective Border DSAs and exchanged with other Border DSAs, and how information from the Border DSA is provided back down to the system/application directories. The synchronisation and filtering processes may be used to populate a distinct enterprise directory that users within that nation may access, or simply just be moving selected directory data between the Border DSA and the system/application directories. The directory standards, products and methods used within the two bottom tiers are independently chosen by the NATO organisation and the nations, while for the top tier everyone must adhere strictly to directory schema, protocols and the agreed interoperability model. However, in the top tier, the use of different Border DSA products is permitted and expected, as long as they adhere to the agreed standards. Adherence to the standards is critical for the correct functioning of such a heterogeneous directory system and formalised interoperability testing will be required.

011. The set of networked national Border DSAs (including NATO as an organisation) form a distributed implementation of the NATO Alliance Directory. In order to realise an effective and efficient NATO Alliance Directory (i.e. minimise the n x n problem of interconnecting a large number of directories), the NATO organisation domain directory system may be required support certain central functions, such as holding and replicating out information replicated in from all nations, holding knowledge references, and hosting of guest entries for nations yet without their own border DSA solution.

012. In order to interoperate, national Border DSAs must support protocols defined in ACP 133 as amended by the NATO supplement to ACP 133. The following protocols, supporting information access and exchange, are supported by ACP-133; Directory Access Protocol (DAP), (Directory Systems Protocol (DSP) and Directory Information Shadowing Protocol (DISP). Additionally the Lightweight Directory Access Protocol (LDAP) as per CCEB Pub 1008 needs to be supported. Strict adherence to the ACP-133 schema as described above is also required.

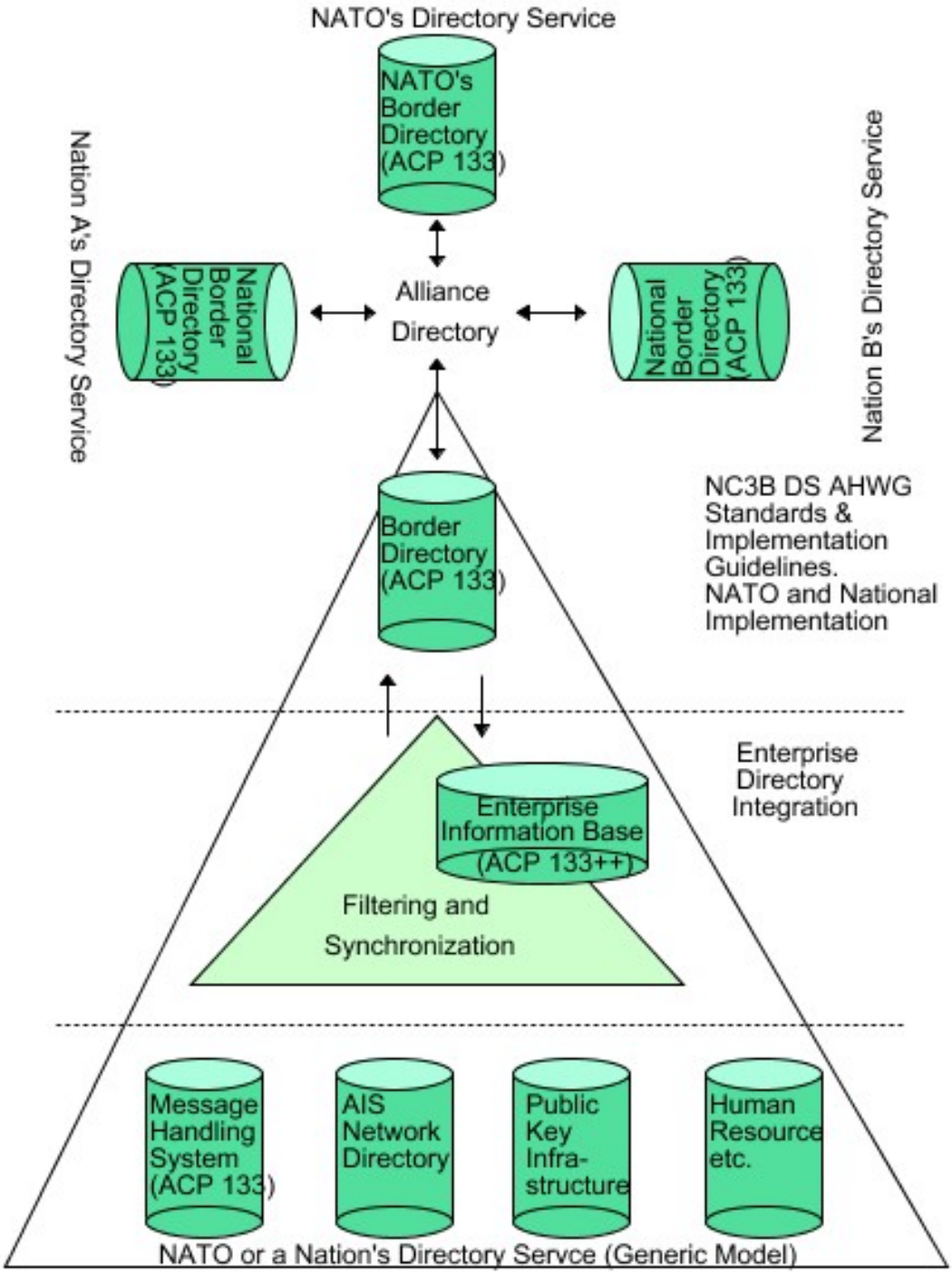

Figure 1.1. Alliance Directory, Generic Model

013. The top levels of the Alliance DIT are assumed to be as shown in Figure 1.2. The structure shows the NATO organisation at the same level in the Alliance DIT as the member na-

tions in accordance with its status as an international organisation. The Alliance DIT will also be unique in the global X.500 DIT through registration. The DIT gives a logical view of how information is structured, but does not provide a view on how information is owned, administered or physically distributed among computer systems. Each nation contributes their information to the NATO Alliance Directory via an advertised Border DSA. The root level is included the DIT figure to indicate the relative position of the Alliance DIT in the global DIT, and is commonly held among the participating Border DSAs.

014. The aim of the Alliance DIT is to facilitate easy and efficient access to shared information by providing users with a common view regardless of the organisation or country to which they belong. The NATO organisational DIT is independent of the national Directory DITs and must also be considered as a separate directory structure. The Alliance DIT will, however, hold references, links and aliases to information in national DITs, in particular for units, ships etc. that have both a national and a NATO role. It is unrealistic to standardise the Alliance DIT below the top two levels (i.e. below nation) in the short term given how far nations are with their directory implementations, and how PKI certificates lock in DITs, although this is likely to cause a lot of problems in finding information in the Alliance Directory. The DSWG recommends gaining initial operational experiences with interconnecting the current national level DITs as they are defined below level 2 before eventual standardization of DITs at these levels is initiated.

015. The complete set of information made available by and to member nations through the NATO Alliance Directory System is called the NATO Alliance DIB. The Alliance Directory Information Base (DIB) is considered to support NATO communications including MMHS, e-mail, PKI and security services, network management and general telecommunications information as defined in the NATO Requirements and Rationale document. Information held in the NATO Alliance DIB will be accessible to users via white and yellow page lookup as required.

016. Where there is an identified requirement for sharing directory information between NATO nations and across national boundaries, there must be conformance to the common directory schema agreed by all NATO nations. This common schema will be base-lined against ACP 133 and the NATO supplement to ACP 133. The requirement for full conformance to the agreed schema in all Border DSAs is showing through informal testing by the nations in the DS WG to be very critical to reliable interoperability and functioning of Border DSAs of different make (heterogeneous environment). A recommendation to conduct a formal test programme of nationally nominated Border DSAs in conjunction with the MMHS Security Demonstrator Programme (MSDP) will come from the DS WG to its parent body (SC/5).

017. Different parts of the NATO Alliance DIT will be managed by different member nations. The NATO Alliance Directory will consist of the parts of individual national directories that each nation designates to be shared within the NATO domain as a whole. The NATO Alliance Directory will contain information required to support NATO operations as appropriate. NATO operations are NATO organisation led and the (sub-) DITs representing operations will be somewhere under the top level NATO entry (o=NATO). The NATO SFOR and KFOR missions are examples of NATO operations that will be represented in the Alliance DIT. The top level command structure in such operations are NATO equipped and primarily NATO staffed, but the lower structures are national units which also need to be visible as part

of the operation structure. Some NATO operations include Non NATO Troop Contributing Nations (NNTCN) staffs and units that also need to be represented in the operation DIT, as connectivity exists from the NATO Secret to the dedicated NATO provided Operation/Mission Systems they work on. Combined Task Forces (CTF) and Combined Joint Task Forces (CJTF) are generic terms for force structures led by NATO or a nation with contributions from other nations. The aforementioned NATO operations are similar to these in structure, although the duration is longer.

018. For reasons of national security it is likely that individual nations will only wish to share a subset of their national directory information within NATO. Also providing more information than is required for Alliance use is not good information management. Separation of national domains will therefore be a primary security consideration, and the use of Meta Directory, Border DSAs, firewall and guard technology will be required within the framework of a standardised NATO-Nation AIS interconnection architecture.

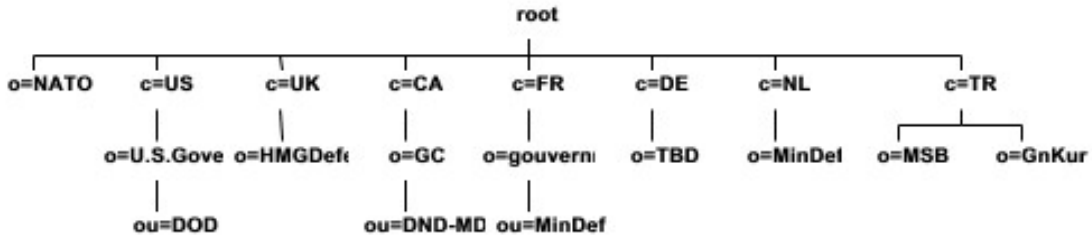

Figure 1.2. Position of NATO (as a organisation) in the Global DIT

1.3. ALLIANCE DIRECTORY SYSTEMS ARCHITECTURE

019. Figure 1.3 below shows the foreseen NATO Alliance Directory high-level architecture for the Secret network and systems environment. The Border DSAs from each NATO nation and NATO are networked over NATO s Secret WAN. Within each nation and NATO, one or more systems with directories provide information to, and get information from, the Border DSAs. NATO and Nations filter the information exported to its border DSA. The information from the Border DSA may also be filtered before it is loaded into national systems. The connectivity between the national systems and its Border DSA can be direct, an air gap, or a combination depending on security of these systems and available directory border protection devices. The Border DSAs is placed on the “Co-operative Area” LAN of the NATO NS WAN Border Protection Device where it can be reached by both from within the nation and from the NATO Secret WAN.

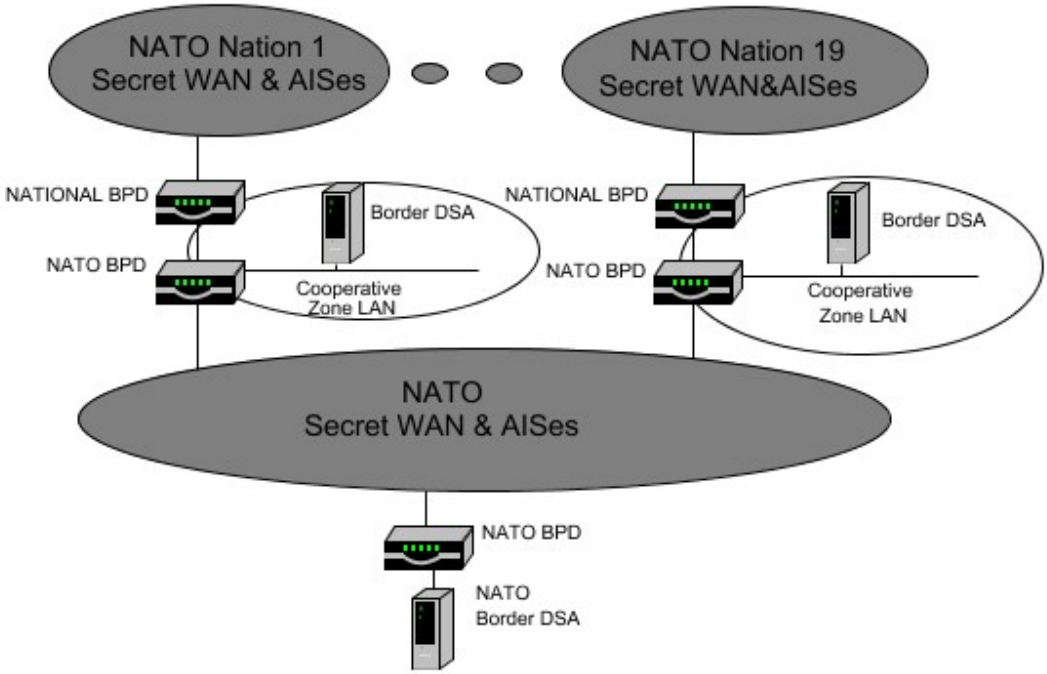

Figure 1.3. NATO Alliance Directory Network Architecture

020. The border DSAs may have to contain Meta Directory functionality if replication/shadowing with DISP between Border DSAs proves to be technically infeasible, because replication is a critical requirement in the Alliance Directory interoperability architecture to reduce loading and constant reliance of the WAN service. The Border DSAs will, unless product standardization steps are taken, be procured by the nations from different vendors, and multi-vendor DISP interoperability has not yet been fully validated.

021. The Alliance Directory will support applications that exchange information in the NATO environment. Figure 1.4 below shows how the national and NATO systems connect to the NATO WAN to exchange information. National systems communicate with NATO via corresponding proxy functions on the Co-operative Zone LAN. The proxy function again communicates with the corresponding NATO system or another nation s proxy across the NATO Secret Wan. The system configuration of the Co-operative Zones will evolve with the applications and services that are to be provided via the Zone. It is foreseen that some NATO AIS functionality (e.g. DNS server, mail gateway server, MMHS gateway server) will need to be placed in the Co-operative Zone for technical, support, availability and operational reasons. This would be procured and operated by the nation under NATO policy and guidance.

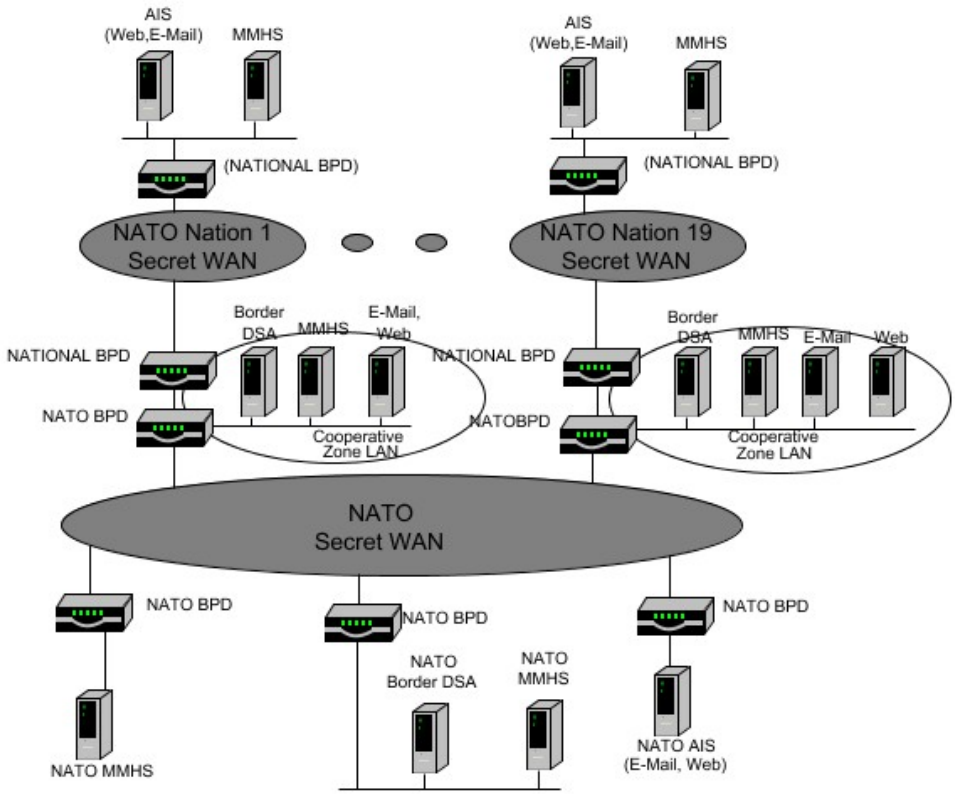

Figure 1.4. National to NATO Systems Interconnections supported by the Alliance Directory

022. Figure 1.5 below shows the directory protocols that may be used to exchange information across the NATO national interface. Figure 1.3 indicates that DISP based shadowing is foreseen to be the primary protocol used between Border DSAs, with the other ACP-133 protocols, plus LDAP, as secondary possibilities. It is not currently foreseen that national or NATO IS systems will access other Border DSAs than their own directly with DAP or LDAP, or that DSP will be used between Border DSAs for chaining or referral type of access. The solution between the border DSA and the national systems are up the nations to decide individually, however the figure indicates the possibilities of accessing information in the border DSA, bulk copy information from the border DSA via tape, floppy etc. or shadow information from the border DSA.

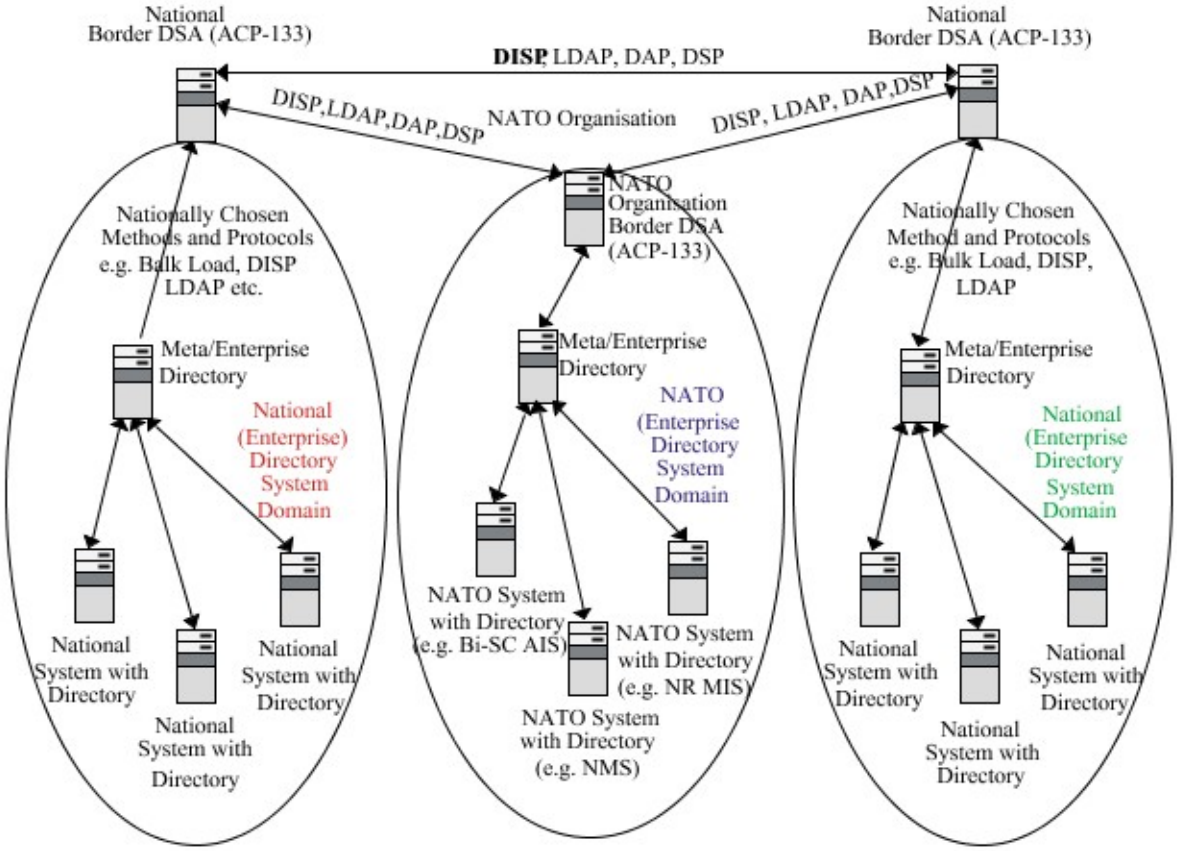

Figure 1.5. National to NATO Directory System Interface Protocols

023. Figure 1.6 below illustrates the central role an Allied Replication Hub is recommended to have in the shadowing agreements with the nations. The Allied Replication Hub is suggested to be a mandatory replication/shadowing partner for the NATO organisation and all the nations. This means that a nation will set up all its shadowing/replication agreements with one system entity and this will greatly reduce the administrative and technical effort of connecting to the Alliance Directory. The Alliance Replication Hub needs to be procured and operated as NATO infrastructure. It will receive and hold a copy of the information in all Border DSAs and be configured to replicate/shadow it all out again to all participants. In addition nations may set up other bi-lateral replication or shadowing agreements. The replication/shadowing is shown primarily using DISP. DISP normally updates the replication partner incrementally, minimising the load on the WAN, however in the case of a network or DSA server failure, a full refresh of all the directory data in that shadowing agreement can be triggered, resulting in large transfers.

024. If DISP cannot be made to reliably work in a multi-vendor environment, and as it is unacceptable to product standardize on one Border-DSA vendor, the architecture below may also be realised using LDAP and Meta-Directories on the Border-DSAs and LDAP support on

the Replication Hub.

025. LDAP based replication may also make use of “Change Log” mechanisms to minimise the transfer of data to changed data only. It is important that the Replication Hub product to be procured has a proper Change Log function available on its LDAP interface. If LDAP was the only protocol to be used, a Border DSA could be a Meta-Directory supporting the ACP-133 schema!

026. A replication scheme where a nation pushes information from its national Border DSA into the Replication Hub, and pulls back information provided by the other nations, is seen as the best replication method, based on tests conducted so far. The Replication Hub is then “passive”. Replication agreements for all other nations' sub-trees to all nations can be pre-configured regardless of whether they are actually used or not. This would greatly simplify configuration and management of the hub.

027. The integrity of the directory data in an Alliance Directory is dependent on satisfactory authentication of the replication processes, in particular those which write into the Replication Hub. Reading directory data that is released to NATO, and thus available to everyone in the Alliance network environment from the Replication Hub, should not require authentication. Each Border DSA must authenticate itself to the Replication Hub and is only allowed to write into its national sub-tree of the global DIT, e.g., the UK border DSA is only be allowed to write into the UK sub-tree of the DIT. The authentication method or methods required and available to provide the necessary authentication will be reviewed with the security authority (i.e. the NATO Security Accreditation Board (NSAB)) of the NATO Secret WAN. It is highly desirable to make use of lower layer security mechanisms, such as Border Protection Device (BPD) access control lists, Virtual Private Network (VPN), and Secure Socket Layer (SSL), in order to reduce the application layer authentication requirements on the Border DSAs and Replication Hub.

028. DISP based replication is completely dependent on equal directory schemas in the participating Border DSAs. Implementation of upgrades to the ACP-133 schema will likely require operating for a period two instances of the Allied Replication Hub directory processes, and transfer data between them using Meta Directory tools and techniques.

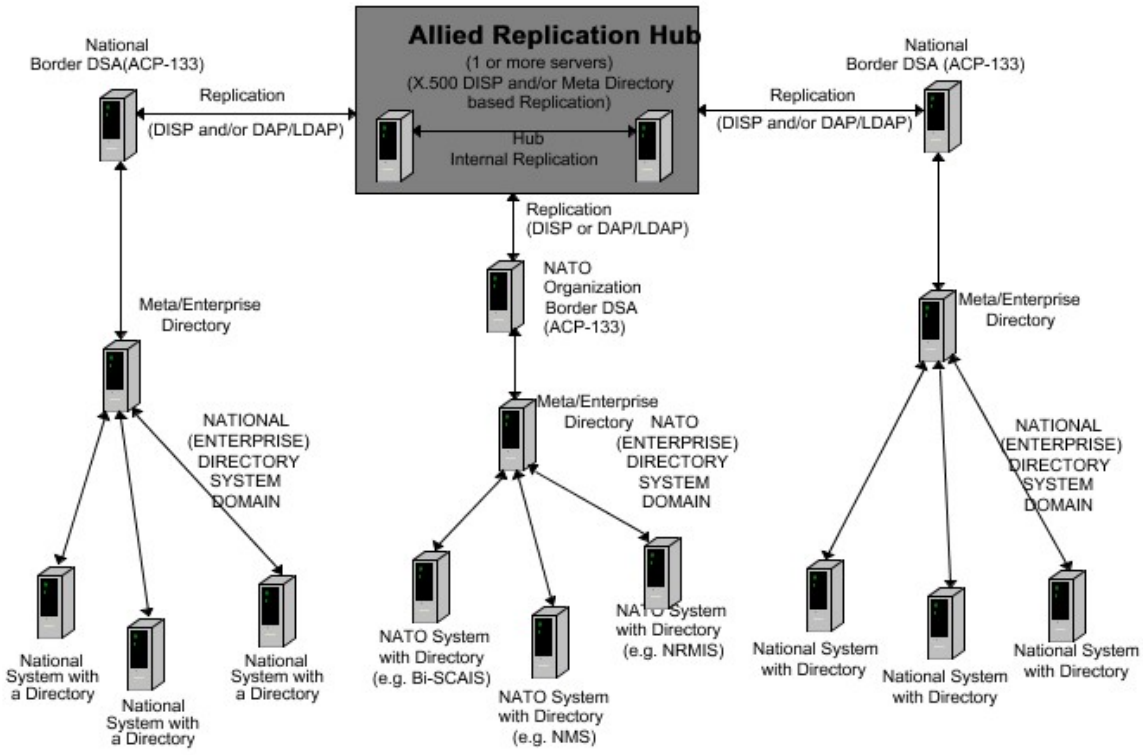

Figure 1.6. Replication between NATO and National Border DSAs

2. NATO TACOMS POST 2000 ARCHITECTURE

2.1. INTRODUCTION

029. A post-2000 NATO tactical communications architecture, TACOMS Post-2000, has been developed by the former NATO Tri-Service Group on Communications and Electronics (TSGCE), (AC/302) Subgroup 11, Project Group 6 (PG/6). The objective to develop the Tactical Communications (TACOMS) Post-2000 Standardisation Agreements (STANAGs) that will produce communications systems meeting the communication requirements of NATO operations post-2000. Participating nations include Belgium, Canada, France, Germany, Italy, The Netherlands, Norway, Portugal, Spain, Turkey, the United Kingdom, and the United States.

030. In the start-up stages of the TACOMS Post 2000 efforts, significant weight was given to the goal of providing a common system design that all nations could use as guidance to their industry to develop their national tactical networks. As time has now passed, most nations are already deep into the design and implementations of their next generation systems. This fact must clearly modify the ambition to reach this goal for TACOMS post 2000.

031. For TACOMS Post 2000, therefore, the over-riding goal of the standards must be to allow national systems to inter-operate with a maximum of coalition operational efficiency, while the elements maintain their value as national assets. Again in somewhat simpler environments, this often is achieved by defining common NATO standard information structures and formats, and then exchanging this information over dedicated gateways that are used as portals between the systems. Such standards have been successfully developed, for example for army tactical data message formats using ADAT P3 or naval messaging formats such as Link 11. For TACOMS Post 2000, however, such an approach will be insufficient due to the vast repertoire of services that are needed to be defined and the total dynamic nature of the operations that would require rapid reconfiguration of elements and systems without affecting the user services.

032. The underlaying study report [1.] proposes an alternative approach to the Architecture that permits independent decisions regarding the technology used within any network element. This approach will not define a specific technology for national elements, but will define network element performance and transfer functions that must be achieved for the whole TACOMS network to operate satisfactorily. International interoperability points are identified between national network elements. The TACOMS Post 2000 standard must define in detail whatever is necessary to ensure that a TACOMS network consisting of many national elements interconnected by these Interoperability Points may operate satisfactorily. The idea is to allow each nation to contribute elements of a TACOMS deployment based on the technology that is most suitable for each nation and at any point of time. The task of the TACOMS standardisation is then to define the interoperability requirements for a network consisting of interconnected national elements, in such a way that TACOMS appears to the users as one network, fulfilling all defined requirements in respect of QoS, capacity, mobility, ro-

bustness, security, etc.

033. The following chapters describe the principle TACOMS Post 2000 architecture.

2.2. ARCHITECTURAL VIEW

034. In this chapter, the main architectural characteristics of the redefined interoperability points are described, together with some discussions on the required transfer functionality of the new national WAS elements.

2.3. INTEROPERABILITY POINTS

035. **Single provider of Each Subsystem network**

036. Figure 2.1 shows a simplified schematic representation of the TACOMS architecture in the context of this new proposal.

037. The WAS, the LAS and the MS subsystem networks carry the services from one interoperability point (at the edge of the Subsystem) to another one.

038. In this example, each Subsystem network is viewed as deployed by a single nation or network provider.

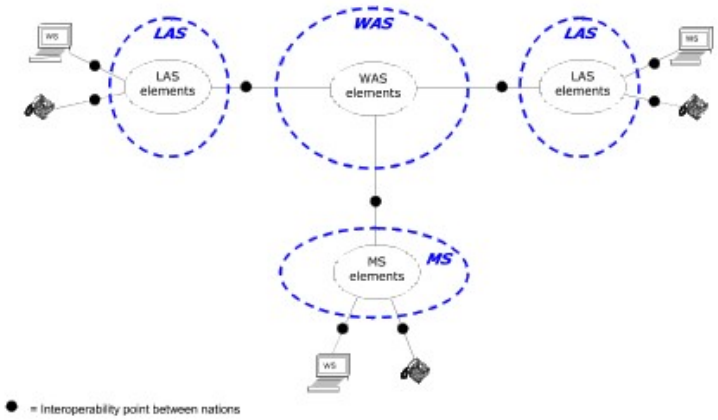

Figure 2.1. Basic Architecture

039. The basic assumption is initially to avoid having to dictate the internal technology of the national elements (e.g. IP or ATM networks or nodes). This means that each element is considered as a “black-box”, defined by the following entities:

- a transfer function
- element performance characteristics
- provision of Interoperability Points

040. **Multiple WAS network providers**

041. Figure 2.2 Multi-Element Architecture shows a more complex schematic representation of the TACOMS architecture in which the TACOMS WAS is provided by several different

nations as national WAS Elements.

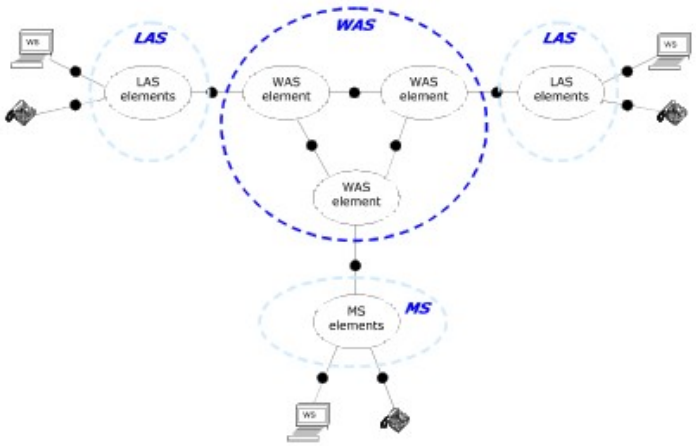

Figure 2.2. Multi-Element Architecture

042. The assumption of this concept is to avoid having to dictate the internal technology of the national elements. This means, as above, that each element is considered as a “black-box”.

2.4. REQUIREMENTS ON INTEROPERABILITY POINTS

043. **Traffic**

044. Each national element must have the necessary inter-working functions to translate between the protocols of the interconnection point and those used internally.

045. Translation between different voice encoding schemes, or any other higher level translations, should be avoided wherever possible. There is a need for negotiation of coding algorithms across the interconnection point.

046. The Interoperability Points must be able to pass traffic flows of all service- and QoS classes, typically represented as either Connection Oriented (CO) and Connectionless (CL) traffic.

047. Control flows, represented as signalling end to end must also be provided, e.g. for passing pressel signals to be used with half duplex or conference type end systems.

048. **Efficiency/Bandwidth**

049. Interoperability points are located at positions where transmission link bandwidth is not a problem. Therefore the efficiency of the local protocols at the Interoperability points is not important.

050. **Resilience**

051. As bandwidth at the Interoperability point is not an issue, but bandwidth within the national elements will be limited, there is a need to identify and control traffic flows across the interoperability point in order to avoid discarding traffic on receipt. Also, for connectionless traffic, a means of traffic engineering (such as policing) is required. This must be dynamic so that when a network element suffers degradation of capacity (due to movement, failure, attrition, etc) the traffic flows may be controlled.

052. As any network element may be subject to loss due to high transmission error rates or deliberate jamming, means must be provided to cope with this. Depending on the traffic type (voice, perishable data, high integrity data, etc) this may involve recovery, that may require additional functions at inter-working functions at the interoperability points.

053. **Call Negotiation/Precedence**

054. In order to satisfy the operational requirements in respect of interoperability, transit networks, etc, the Interoperability point protocols must allow negotiation of call parameters as part of the setup phase of connection oriented traffic. This includes bitrate, coding method, etc and also the call precedence. The negotiated call precedence must be used when shedding traffic for congestion reasons.

055. **Protocol Stack**

056. A complete protocol stack must be specified at each interface between two elements.

2.5. DESCRIPTION OF THE PROPOSED CONCEPT

057. In operational terms, the basic idea of the reorientation proposal is to include in a WAS element all interconnected WAS equipment provided by one nation. The main objective is to allow nations to choose the technology to be used inside the WAS element.

058. In technical terms, the core of the reorientation proposal is a revised definition of the WAS interoperability point W1. Starting from the current stage 1, the changes may be described as follows:

059. Currently, the standardised link protocol is used on the Radio Relay transmission links. It is carefully chosen to give a low overhead in order to utilise the limited bandwidth in the best possible way. With the TINA concept, the link is assumed to be a high capacity cable, so the need to select a protocol with a low overhead is no longer essential.

060. In the current approach, the link protocol multiplexes the Connection Oriented (CO) and Connectionless (CL) signal flows. The sharing of capacity between the two flows is administered by the link protocol itself and the CO and CL networking functions (transit switch / transit router). With the reorientation, the link protocol will not control this sharing of capacity. This must be administrated by the CO and CL networking functions.

061. The basic difference introduced by the reorientation proposal, is:

- The networking functions currently work over a standardised and unified link protocol for all links, internally within a nation, as well as on links to other nations.
- In the reorientation proposal, the networking functions must operate over two link protocols: one standardised protocol for local links to other nations, and one national remote link optimised for Radio Relay transmission, not subject to TACOMS standardisation. This dual stack concept is illustrated in Figure 3 Comparison between Stage 1 Architecture and Re-orientation proposal:

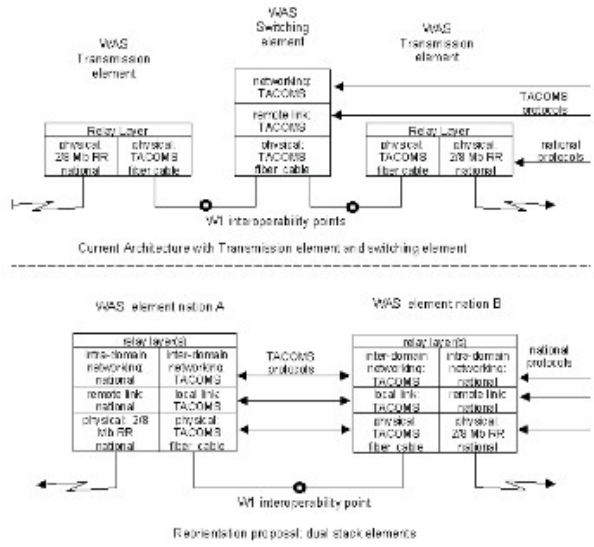

Figure 2.3. Comparison between Stage 1 Architecture and Re-orientation Proposal

062. In order to describe the policy and parameters for the sharing of capacity, the concepts of Service Level Specification (SLS) and Service Level Agreements (SLA) have been introduced. This should be regarded as a tool used for a more suitable and technology independent description of the services provided by the Elements. The basic task of sharing capacity and prioritise between traffic flows must however be solved, regardless of the reorientation proposal.

063. These tasks can be illustrated with an example. Classes of Service 1 to 10 are defined for the purpose of the example, as illustrated in the Table Example of Classes of Service.

Class of Service	Characteristics	Typical Application	Throughput	Max Delay	Max Jitter	Max Error Rate
1	Guaranteed QoS, priority 1	Voice priority 1	2.4 kb/s CBR	D1 ms	J1 ms	BER1
2	Guaranteed QoS, priority 2	Voice priority 2	2.4-16 kb/s CBR	D2 ms	J2 ms	BER2
3	Guaranteed QoS, priority 3	Voice priority 3	2.4-64 kb/s	D3 ms	J3 ms	BER3
4	Guaranteed QoS, priority 4	Vidio priority 4	n x 64 kb/s	D4 ms	J4 ms	BER4
5	Non-guaranteed QoS, priority A	Low Latency data services	1 kb/s	D5 ms	n.a.	PL-A
6	Non-guaranteed QoS, priority B	Low Latency data services	10 kb/s	D6 ms	n.a.	PL-B
7	Non-guaranteed QoS, priority C	Data services, Web, mail	100 kb/s	D7 ms	n.a.	PL-C
8	Non-guaranteed QoS, priority D	Low rate video, Data	1 Mb/s	D8 ms	n.a.	PL-D
9	Non-guaranteed QoS, priority E	High rate video, Data	10 Mb/s	D9 ms	n.a.	PL-E
10	Non-guaranteed QoS, priority F	Data, File transfer	100 Mb/s	D10 ms	n.a.	PL-F

Table 2.1. Example of Classes of Service

064. Each Class of Service can be carried by the CO or the CL service. Obviously, the classes 1 to 4 reflect telephone traffic, while 5 to 10 reflect IP data traffic. The CO service traffic across the W1 Interoperability Point could therefore conventionally be defined to carry Classes 1 to 4, while Classes 5-10 are carried by the CL service.

065. The CO service network is characterised by a signalling protocol between the switching elements on either side of an Interoperability Point. The protocol is used to handle each connection, and managing the total traffic volume across the Interoperability Point by refusing new connection if there is no spare capacity. It will also prioritise between the Classes of Service by pre-emption. The signalling protocol can be described to be an implementation of a Service Level Agreement.

066. For the CL traffic, other mechanisms like “Diffserv” and “Intserv” are used to control the flow and prioritise between Classes of Service. In general, more complex protocols are required to obtain a guaranteed QoS, compared to the conventional CO protocols.

067. Inside the national elements, there may be a different allocation of Class of Service to service networks. In an ATM based network element, the data traffic (Classes 5 to 10) may be carried as CO traffic, formatted in AAL5 across the network element. In an IP based network element, the voice Classes 1 to 4 traffic may be carried as CL traffic, supported by appropriate QoS protocols. This is illustrated in Figure 4 Cases of Interoperability.

068. In the general case, this represents an open architecture in the sense that each allocation of traffic classes to the CO/CL service networks can be subject to agreements in each case, depending on the capabilities of each of the connected networks. As an optional variation to the basic allocation of the Class of Service to CO/CL service networks, the W1 protocols could be expanded to cover different Class of Service allocations, as illustrated in Figure 2.4, c) and d). Such options would represent shortcuts between WAS elements using the same technology.

069. The definition of the protocols of the W1 interoperability point is a task for Stage 2. It is therefore not needed at this point to make a final selection. Many alternative solutions are described later in Chapter 3, and the following example is merely given to provide clarification of the concept. As an illustration and an example, the TACOMS W1 interoperability point can be described as follows:

- The physical layer is 1 Gb/s ethernet, fibre optical connection.
- The block format of the CO service is MPLS. The MPLS label is used to identify the channel in the CO service network. The MPLS format can be made compatible with the ATM cell format.
- The CO signalling protocol is ISDN based. H.323 and STANAG 4578 are both based on ISDN Q.931. Maximum capacity reserved for CO traffic is default, with override by the SMCS.
- The CL traffic uses a conventional IP protocol stack with Diffserv, where the parameters are selected to meet TACOMS requirements.

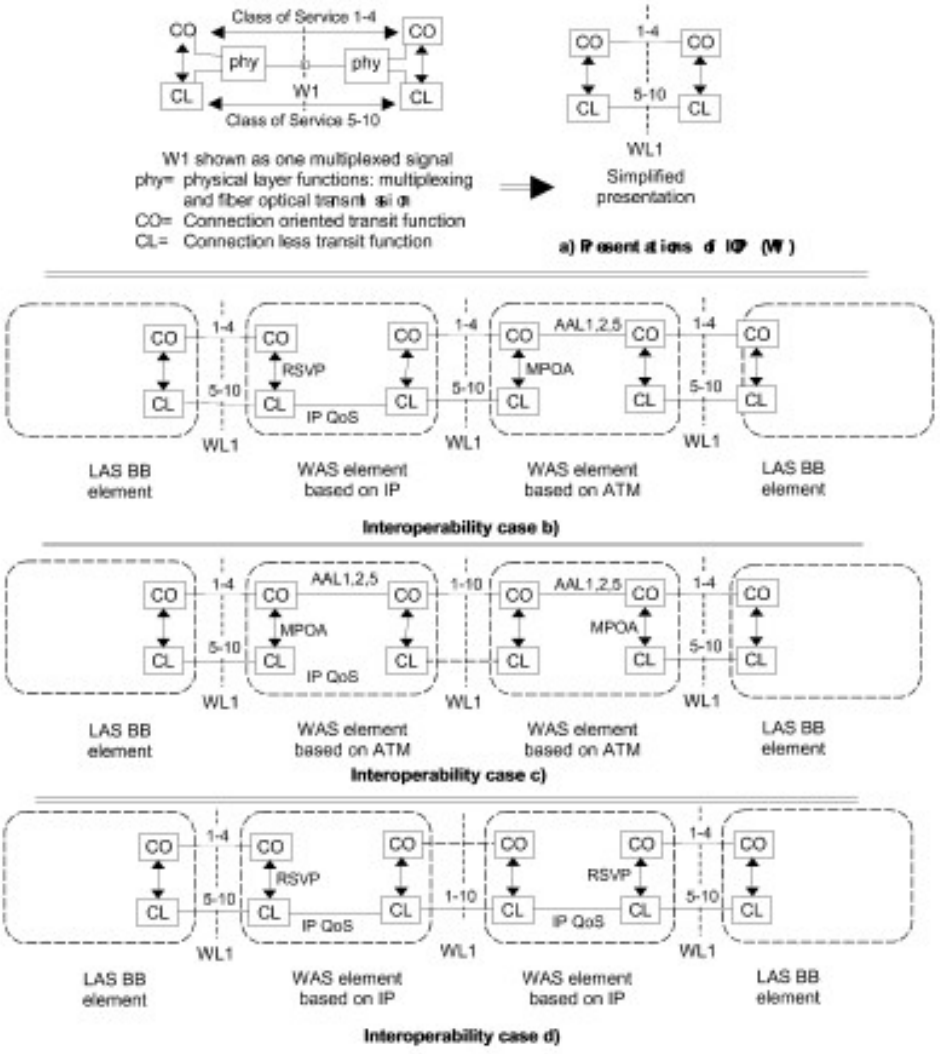

Figure 2.4. Cases of Interoperability

2.6. CHARACTERISTICS OF THE PROPOSED CONCEPT

070. This section aims to discuss some high level points related to the anticipated advantages and disadvantages (or pro's and con') of the reorientation proposal. TACOMS Post 2000 as a programme has gone through numerous stages, in which parts of its concept has been modified slightly at each juncture.

071. It is therefore important to keep the discussion of the reorientation proposal strictly with respect to the current contractual base as agreed after stage 1 of the contract.

072. The subsequent paragraphs present observations relevant to this discussion, and reflects on the impact for the nations providing elements to a TACOMS deployment, and on the operational users that will use the system to fulfil their mission.

073. **Procurement Flexibility.**

074. If a set of interoperability standards is successfully developed on this basis, the nations may achieve improved procurement flexibility in the following ways:

- If nations implement network elements with technologies chosen by the nations, in various stages of provisioning cycles, these network elements can be made TACOMS interoperable to form a complete TACOMS system provided that each national element includes an inter-working function that provides the specified TACOMS interoperability point. It is not necessary to wait until the existing systems are replaced, as long as they can satisfy stated TACOMS element performance requirements and the interface standards at the interoperability points.
- The technology used for the internal operation of the national elements can be selected from those suitable at the time of procurement. This enables an incremental acquisition policy.
- Nations are likely to use their subnets for national purposes, while at the same time serving as TACOMS elements. National use may imply specific functions for security, network management and network signalling. Such dual use is feasible when nations can choose the technology of the network functions internal to the subnet.
- This architecture is also expected to be well suited for introduction of new, as yet unknown, networking technology in the future.

075. **TACOMS System Characteristics**

076. From the perspective of the reoriented programme, a TACOMS network will have the following characteristics:

- User services will be unchanged from those previously defined.

- Subscribers will be free to move between national network elements of a TACOMS Post 2000 system keeping their same terminal equipment and directory number and without any need to change their logical address. There is no need to know the national element configuration. As in the current approach, of course, this does not apply to tactical radio-themselves, as this requires an over the air waveform which is outside the scope of the current standard.

- Subscribers may access Gateways to non-TACOMS 2000 networks without any knowledge of which national element provides such Gateways.

- The ability to pass traffic over a TACOMS network between two external networks using Gateways will not be degraded.

- The ability to pass traffic over an external network between two TACOMS networks using Gateways will not be degraded.

- Reconfiguration of a TACOMS network by changing the topology of national elements for reasons of redeployment, attrition, failure or congestion will have no effect on subscriber facilities, but may result in changed performance if, for example, lower bandwidth links are used.

077. **Impact on deployment flexibility**

078. In the current concept it is theoretically conceivable that a transmission link from one nation can be used to interconnect two transit (WAS) switches of two other nations. As described in chapter 4 this is not currently a probable situation. From a planning and network management perspective it is far more likely that nations will provide their elements in the form of sections of the network, where they can manage nationally their interconnected equipment as one contiguous network control domain, in combination for both national and coalition traffic.

079. **An integrated TACOMS System versus national networks interconnected using Gateways**

080. The nations will have the choice whether to implement the integrated TACOMS interworking functions in their transit switches or conventional “legacy” system Gateways to connect to TACOMS. As described later in Chapter 3, the first option will imply reductions in user services such as user mobility. With the reoriented proposal the users will be able to retain their logical address in the network while they move between national WAS elements.

2.7. REFERENCES

081. [1] TACOMS Post 2000, Final Study Report, WP13202, Technology Independent Network Architecture Concept Study, TACOMS/WP13202/RD/TACONE/813

3. GERMAN ARCHITECTURE FOR TACTICAL NETWORKS

3.1. BACKGROUND

082. This annex describes the aim and first results of one of Germany#s armed forces key programs for implementing modern technology into tactical communication systems using basic results from the INSC Project.

083. “The IT system of the Bundeswehr must meet the communication and information requirements at all levels, from the minister to the individual soldier on the battlefield and the employee at his desk.”

3.1.1. General Requirements

084. The target architecture must follow the following principles:

- Designed for Joint Combined Operations out of area,
- Easy to install and to maintain within different network scenarios,
- Backward connection to different WANs (Homeland, Internet, ISDN), to coalition partners and other involved organisations (e.g. UN); reduction to only a few sub network technologies (serial line, ISDN, Ethernet).

085. The network technology is principally based on IP(v6).

3.1.2. Basic Scenario

086. The following Figure contains a scenario on a schematic level which shows some configuration examples of the presented network concept.

087. The scenario does not represent a real scenario, but only outlines an overview of the complexity of the provided network concept. Based on this scenario, the following network concept is explained, but limited to the German part within a multinational operation. Other nations are connected to this network through standardised interfaces (either on an IP based BGB4 border gateway or for limited application services through an ISDN interface).

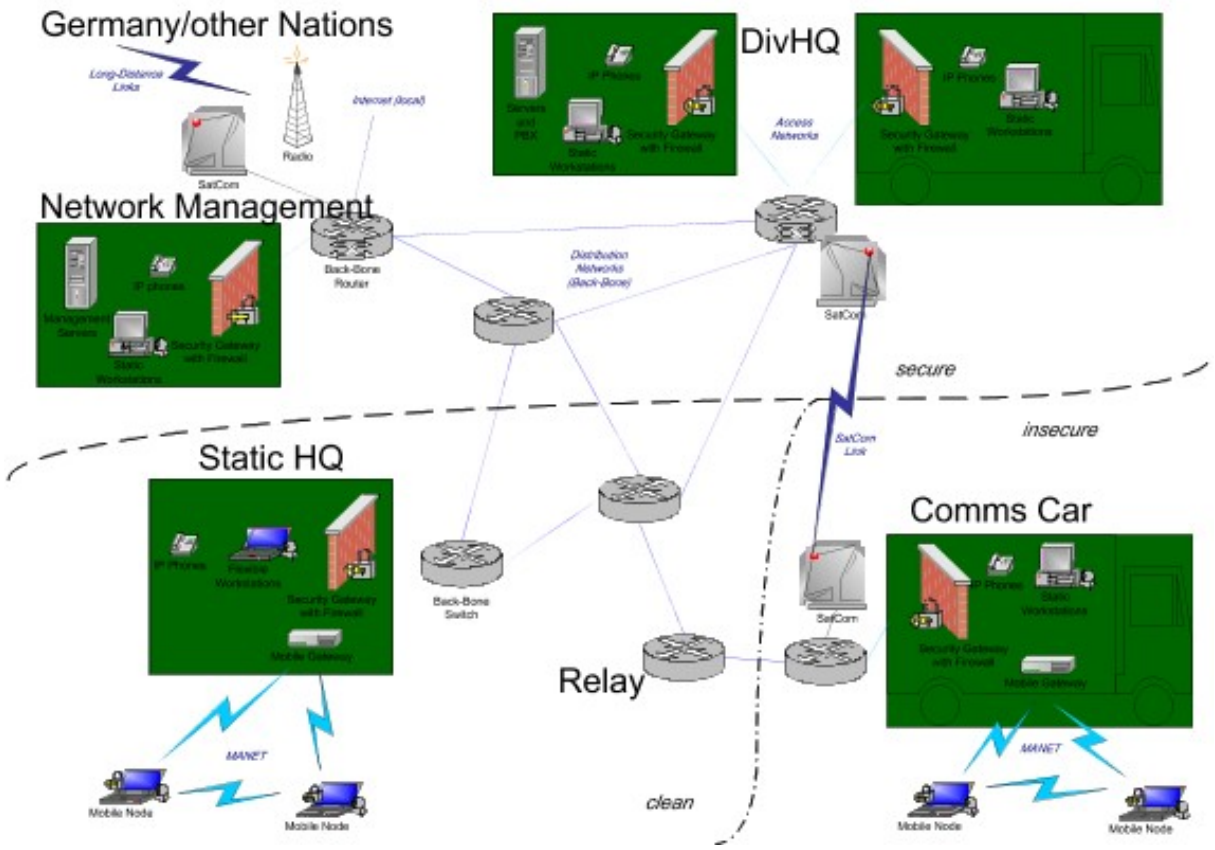

Figure 3.1. Schematic Presentation of a Possible Network (German part)

3.2. ANALYSIS AND TRANSFORMATION OF FUNCTIONAL BLOCKS

088. To allow a simpler structure and theoretical discussion, all functional blocks are identified and functional components are grouped to blocks. 11 different functional blocks could be identified (see Figure 3.2), which can be assembled to 5 groups. A detailed description of the functionalities, their interfaces and the schematic construction can be drawn from chapter 3.

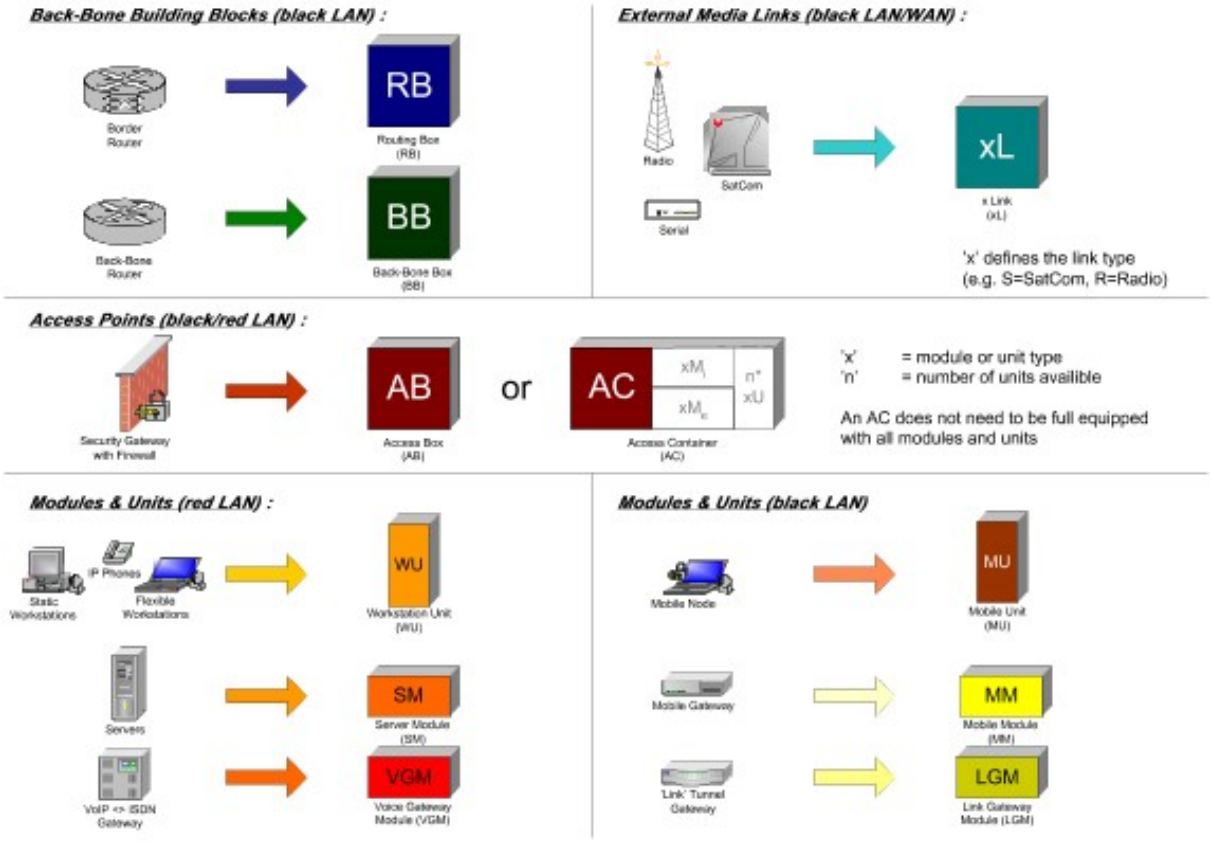

Figure 3.2. Transformation of the network components to functional blocks

3.3. NETWORK STRUCTURE

089. Using the above transformation (Figure 3.2) for the scenario from Figure 3.1, the following network structure is generated:

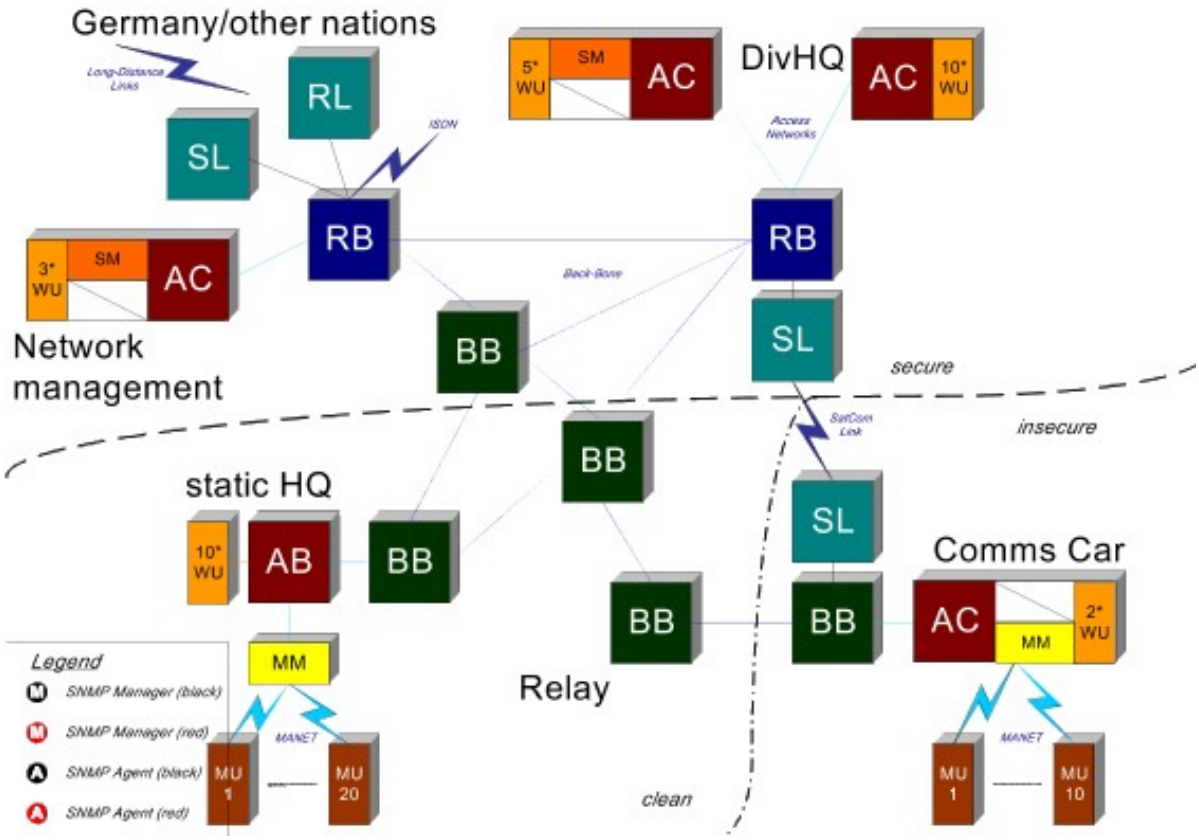

Figure 3.3. Functional display of the target architecture after transformation

090. Figure 3.4 represents the network architecture from the example scenario in terms of the network technology:

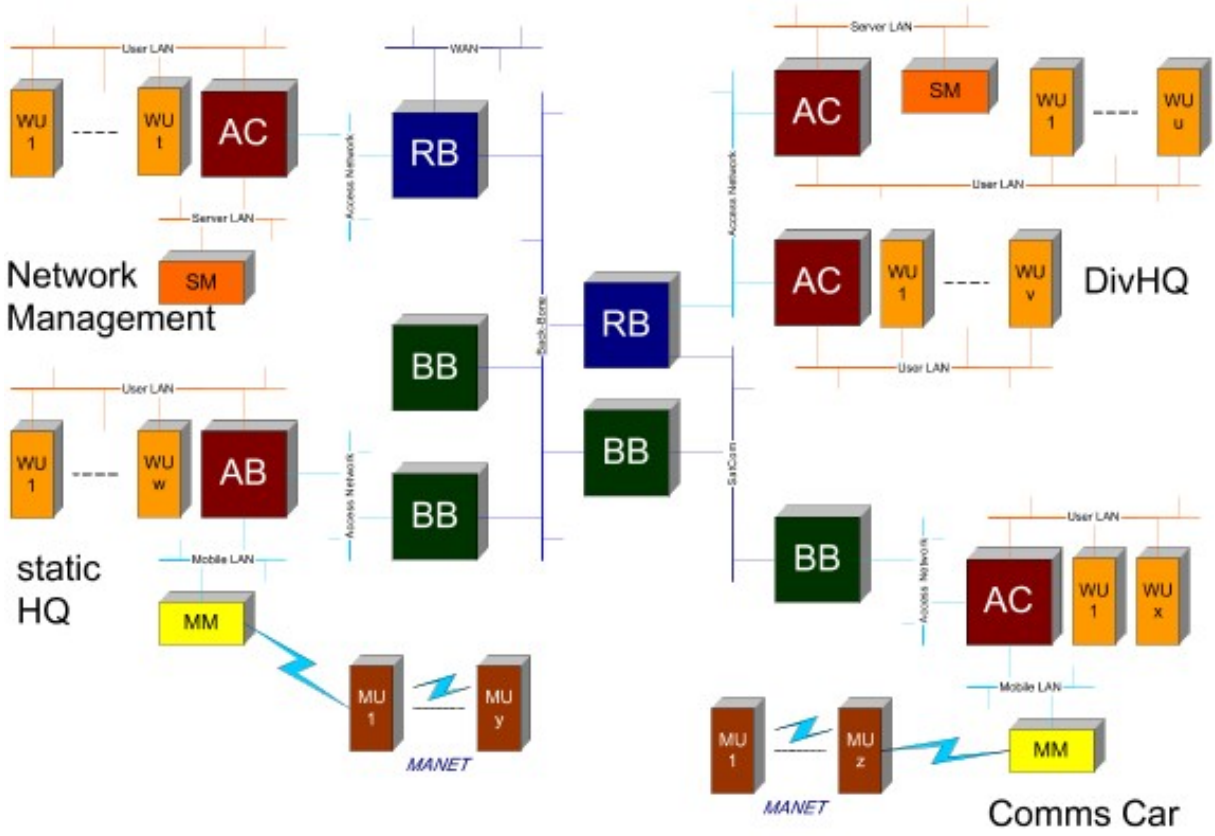

Figure 3.4. Abstracted network plan of the target network using functional blocks

3.4. FUNCTIONAL ELEMENTS OF THE TARGET ARCHITECTURE

091. For the routing methods, 3 different areas must be covered within the routing architecture:

Area	Routing Protocol	Reason
WAN e.g. Connection to Germany or other nations (coalition partners)	**BGP4**	Fast converging Widely used in other WANs=>good interoperability scalable (>1000 routers)
Backbone Network	**OSPFv3**	Fast converging Efficient bandwith usage

Area	Routing Protocol	Reason
		scalable
MANET e.g. High mobile end users (Mobile Unit, MU)	**OLSR**	Fast converging autonomous/autoconfiguration dynamical

Table 3.1. Routing Architecture

092. For the efficient usage of the limited transmission resources a dynamic management, based on ad hoc situations, is necessary. Therefore dynamic routing protocols are used, which allow a prioritised handling of different traffic streams.

093. Classification is necessary for the definition of different traffic streams. The necessary classification has to aspects:

- Technical classification (e.g. voice, email)
- User based classification (e.g. Routine, Flash)

094. A matrix can be generated based on these two aspects, where two parameters are assigned to one traffic class. To handle this matrix technically, a linearization is necessary. For this linearization, the network operator has the freedom how to do this, which also allows a modification of this linearization during network operation.

3.5. NETWORK MANAGEMENT

095. Network Management is both a “framework” and a set of processes for the planning, operation and maintenance of networks. There are a lot of management standards and concepts, how a network can be managed. The proposed one is described in the next chapter.

3.5.1. SNMP Management Model

096. The Simple Network Management Protocol is based on a manager/agent architecture, which contains a SNMP-manager, a SNMP agent, a database with management information (MIB) managed objects and management protocols.

097. In comparison to older SNMP versions a couple of security features were added to SNMPv3, e.g. integrity services, authentication services and encryption.

098. In Figure 3.5 the components of SNMPv3 are presented. In Figure 3.6 SNMP Manager

and Figure 3.7 SNMP agent the communication behaviour of the SNMP-manager and SNMP-agent are presented.

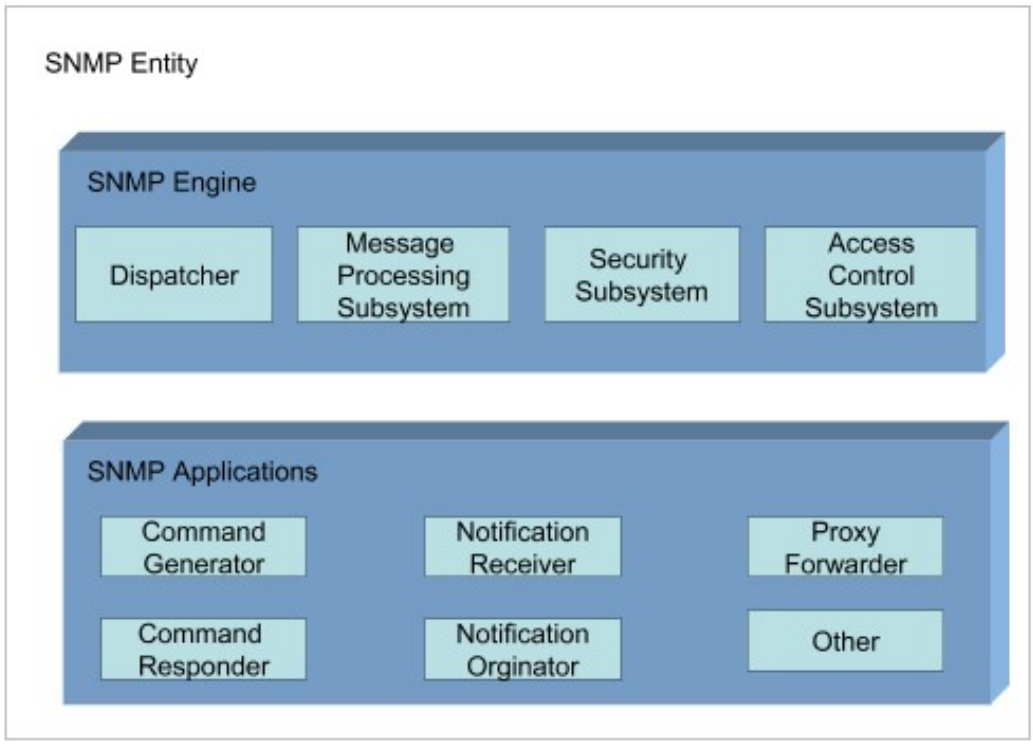

Figure 3.5. SNMP Components

099. Each SNMPv3 device contains exactly one SNMP-engine and one or more of the shown SNMP applications. The functionality of a SNMP device is defined by the implemented SNMP-applications. The components of the SNMP-engine interact with each other and with the implemented SNMP-applications. The functionality of these components is described by abstract interfaces.

100. **Engine components:**

101. *Dispatcher*

- Exactly one Dispatcher per SNMP-Engine
- Dispatcher allows the support of SNMP-messages with different versions within the same engine
- Tasks

1. Sending and receiving of SNMP-PDUs
2. Determination of the SNMP-version and interaction with the relevant Message Processing Model
3. Abstract interface for SNMP-applications fort he delivery of PDUs to other SNMP-applications
4. Abstract interface for the sending of PDUs to remote SNMP-entities

102. *Message Processing Subsystem*

- Tasks
  1. Preparation of messages for delivery
  2. Extract of data from received messages

103. Can be based on one or more Message Processing Models

104. *Security Subsystem*

- Contains security services (data integrity, authentication, confidentiality, Replay protection)
- May contain several security models for different security views

105. *Access Control Subsystem*

- Offers authentication services, based on several Access Control Models
- One Access Control Model defines a specific function for the decision support for an agreed/disagreed access

3.5.2. SNMPv3 applications

106. The SNMP-applications use the services of the SNMP engine. The different types of SNMNP-applications are:

- Command generator (monitoring and modification of management data)

- Command responder (Offers access to management data)
- Notification originators and receivers (send and receive of asynchronous events)
- Proxy forwarders (Sending of SNMP-messages to other SNMP-engines (of different type

107. In the following figures the communication between an SNMP-manager and an SNMP-agent is shown:

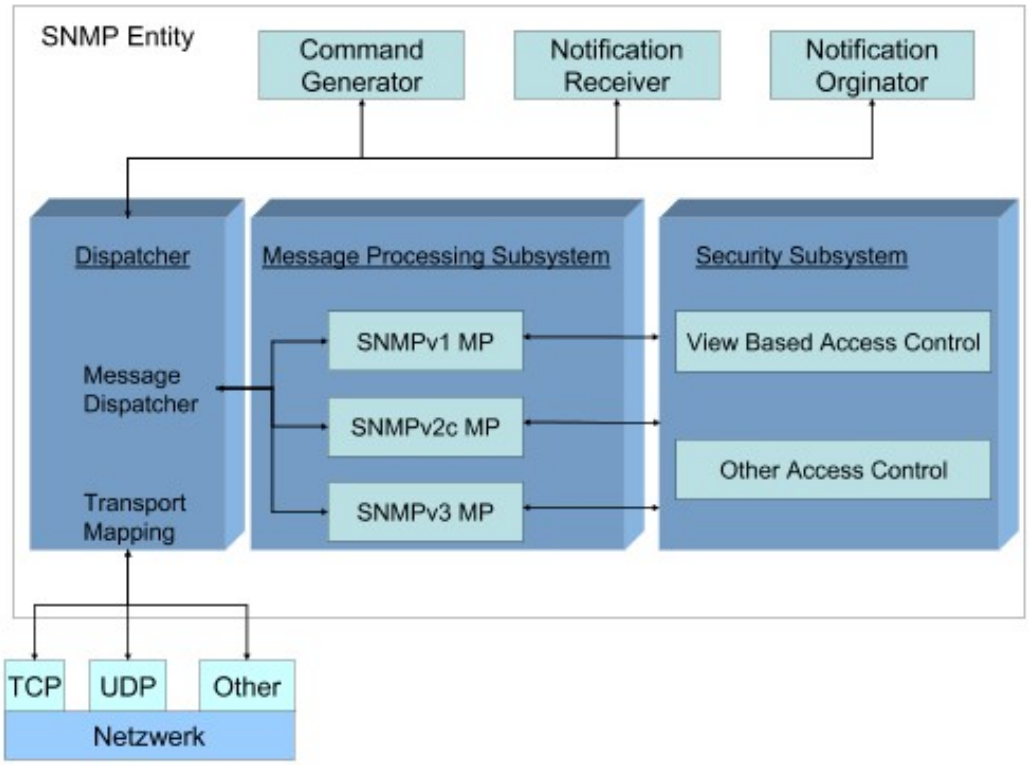

Figure 3.6. SNMP Manager

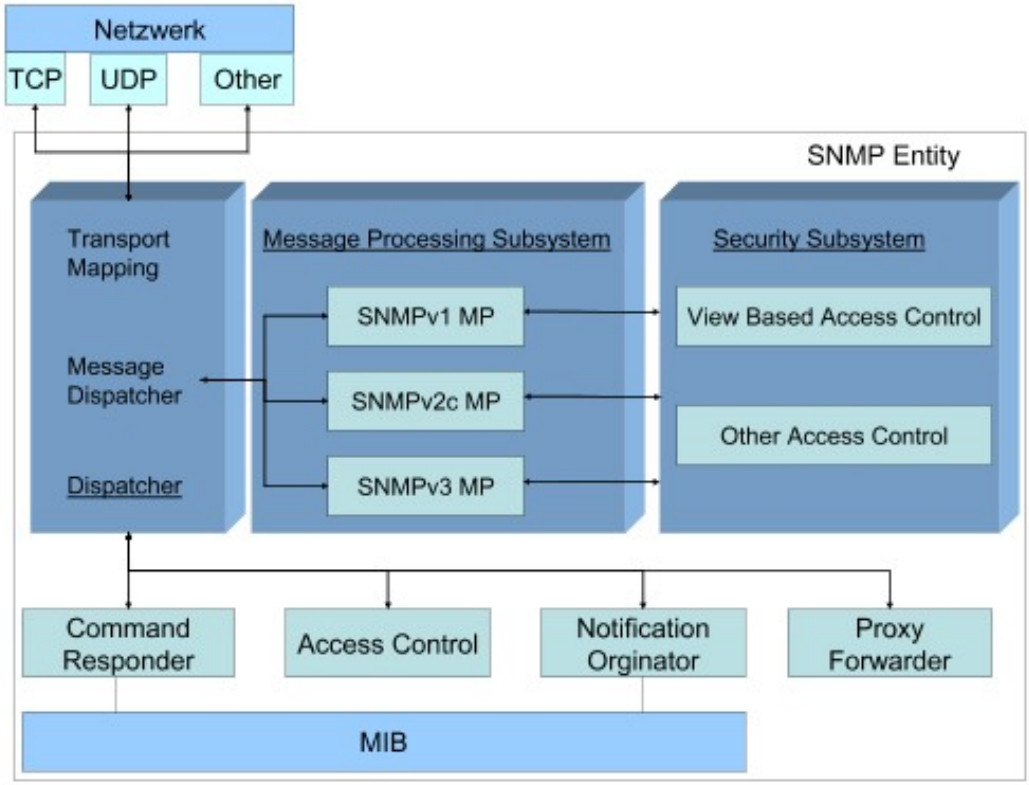

Figure 3.7. SNMP Agent

3.5.3. Technical Management Functionality

108. In this architecture, the usage of SNMPv3 (with authentication and encryption) is foreseen both within the black and the red network part.

109. The function of a manager must be implemented several times (at least twice). The geographical placement should be done near the central services (e.g. within the static HQ).

110. The following figures show as an example the placement of the SNMP manager (main and backup) and the monitored and remote controlled SNMP agents for the red and black network domain (from chapter 3). Black agents can only be managed by black managers, red agents only by red managers (hard separation between secure and unsecure network domains).

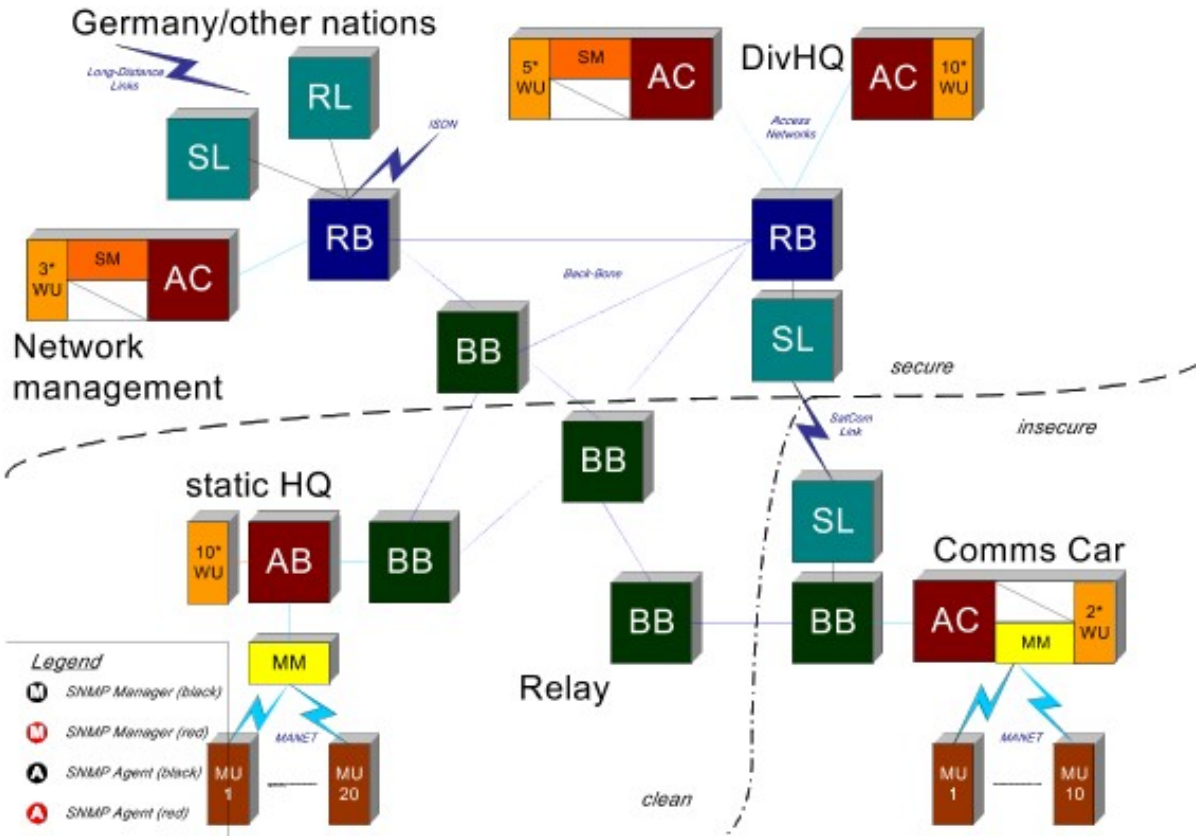

Figure 3.8. Integration and placement of the management (functional presentation)

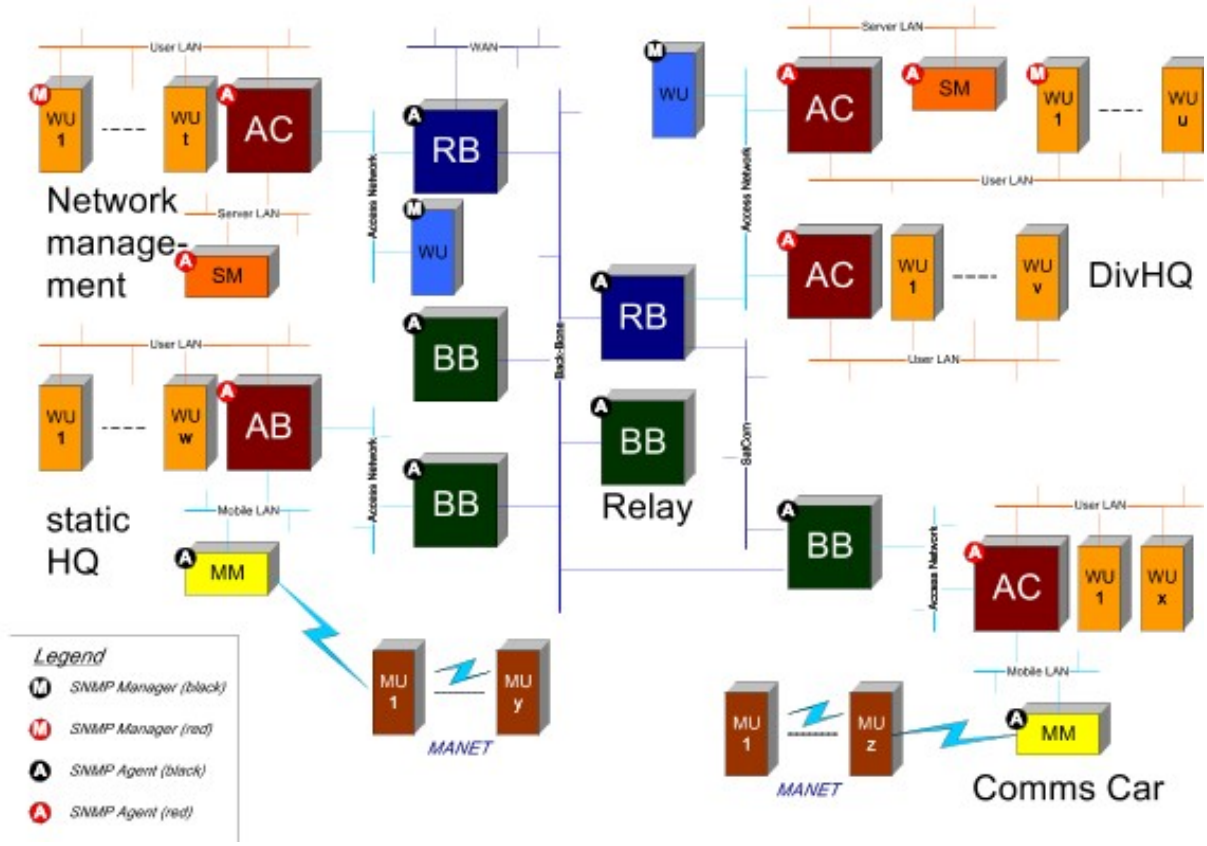

Figure 3.9. Integration and placement of the management (abstract presentation)

111. The manager both monitors different agents from remote (monitoring function), and controls (via SNMPv3) e.g. router and switches ad-hoc to adjust them to actual conditions (e.g.. IP addresses, users, routing, QoS, filter).

112. Operation centres, where red and black managers are placed, must be protected (by additional means) against access from outside. It should be noticed that principally any WU (after activation or configuration) can behave the role of a manager (assumed that the necessary access rights are given). This strengthens the redundancy and flexibility of the whole network.

3.6. IP ADDRESSING AND NUMBERING

3.6.1. IPv6 Addressing

113. Using the draft version of the AFmISBw for a military IPv6 addressing concept, the following address structure is used for tactical networks:

3	**13**	**8**	**24**	**16**	**64**
FP	TLA ID	RES	NLA ID	SLA ID	Interface ID
<--Public Topology-->				Site	
				<---------->	
				Topology	
					<-----Interface Identifier----->

FP	Format Prefix (001)
TLA ID	FTop-Level Aggregation Identifier
RES	Reserved for future use
NLA ID	Next-Level Aggregation Identifier)
SLA ID	Site-Level Aggregation Identifier
INTERFACE ID	Interface Identifier

Table 3.2. Aggregatable Global Unicast Address

114. Networks based on this architecture get a network ID based on the 6 bit of the Next-Level Aggregation Identifier (NLA), which is reserved for the various forces (e.g. 1011002 for mobile army tactical networks. This part of the address must be registered internationally. It is than within the national responsibility to structure the SLA (Site-Level Aggregation Identifier).

115. All components of the backbone (BB, RB) and access domains (AB, AC) are pre-configured with this address prefix. The following figure shows the underlying systematic:

Bit	**Part**	**Usage**	**Remarks/example**
01-03	FP	Format	001
04-16	**TLA**		
17-24		*reserved*	
25-30		NLA1	101100
31-47	**NLA**	NLA2	For additional structuring
48-51		Class	Backbone, Access Net, MANET
52-55		Typ	BB, RB, AC, AB, MM
53-56		*reserved*	
57-60	**SLA**	No.	Sequential Number
61-64		*reserved*	

Table 3.3. Address Prefix within the IPv6 Address

116. This method of the address assignment allows the pre-configuration of the prefix number within the network components and to activate them within the area of operation.

117. The Interface-ID for normal network components is regularly not pre-configured, but the hardware configuration of the device providers is used. Only in exceptional situations (where MAC addresses may be selected via software) the LAN administrator has to assign a locally unique Interface-ID

3.6.2. IPv4 - IPv6 mapping

118. To provide a connection to pure IPv4 based network from allies, a protocol and address translation is used, based on Nat-PT. This translation mechanism allows that pure IPv4 based end systems can communicate with pure IPv6 based end systems transparently. For this method a NAT-PT gateway is necessary, which transforms IPv4 in IPv6 addresses and vice versa from a pre-defined address pool. If necessary, this NAT_PT gateway also transforms protocol elements from higher layers (proxy functionality) where address translation is necessary (e.g. ftp). This NAT-PT mechanism (including proxy functionality) is now integrated in modern, IPv6 capable routers. Therefore it is assumed that the routing box (RB) can offer this NAT-PT functionality.

3.7. STRUCTURAL DEFINITION OF FUNCTIONAL BLOCKS

119. In this chapter the several functional blocks are described in detail. Both the requirements for the interfaces as a possible realisation of the internal structure is described.

120. At the beginning, the (physical) connections are described, which interconnects the several functional blocks. Both direct network links as connections to other physical transmission media (e.g. radios) are handled, in unsecure (black) and secure (red) networks.

121. Afterwards the various functional blocks are discussed. Here minimal requirements for interfaces and functionalities are listed.

3.7.1. Connection Types

122. All connections can be structured in black (unsecure) and red (secure) connections. In addition, they can be structured in reachability and area of operation.

123. In addition, the following table contains possible technologies and protocols, requirements for minimum distance and theoretically possible bandwidth. Based on these criteria, the different connection types can be classified:

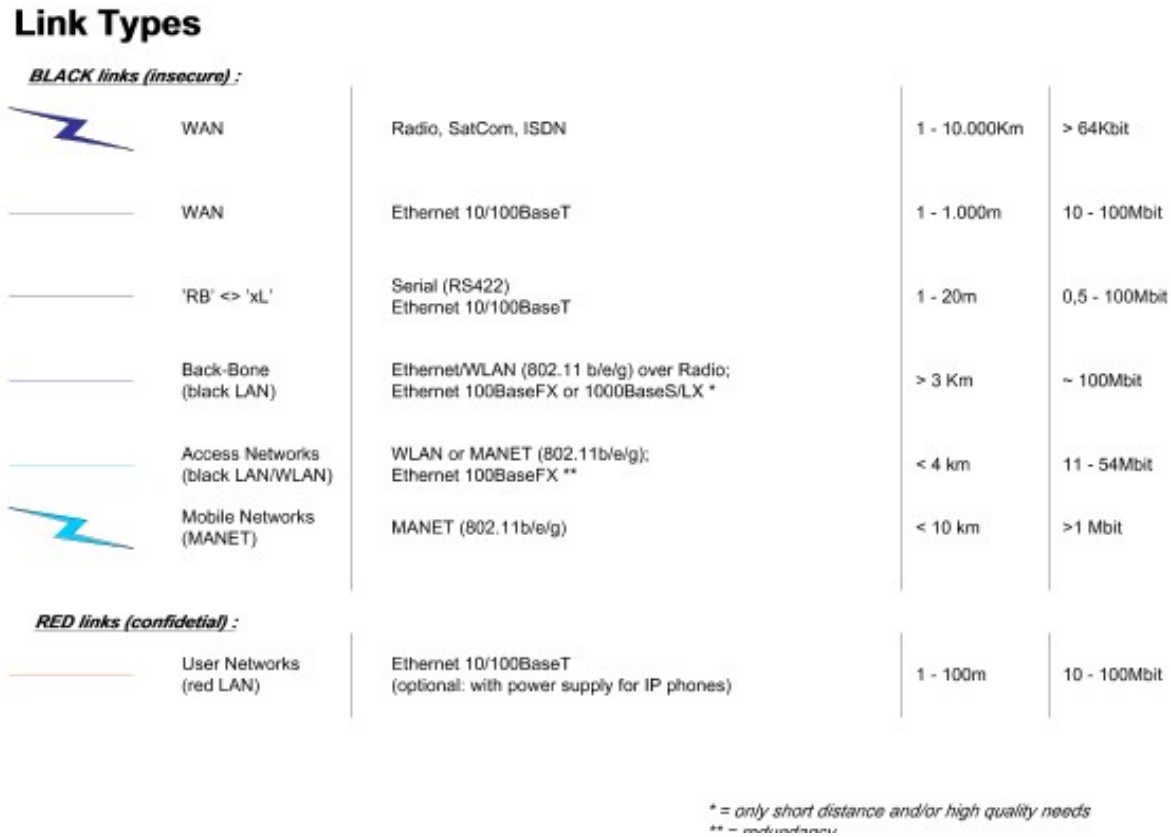

Figure 3.10. Specification of connection types for the interconnection of the several function blocks

124. In the following, the main terms are explained:

125. **MANET (OLSR)**

126. The forwarding of PDUs is done in packet switches (routers). This is done on a store-and-forward basis. This principle is also used in mobile networks for the extension of the radio range of classical combat net radios. A previously used radio system as a pure end system will now be used as an automatic radio relay. Based on the IP addresses within the PDUs, a radio relay will recognise whether this PDU is determined for the own interconnected end system or it is determined for another, remote end system. The radio system transmits this PDU again on the radio channel. In consequence, this method maps the INTERNET behaviour to radio networks and is known under the term “Mobile Ad-Hoc Network (MANET)” . Within this method, a specific routing algorithm (Optimized Link State Routing, OLSR) calculates periodically a unique routing tree across the physically interconnected remote radio systems which are allowed to be operated in the radio relays mode. The result is the extension of the radio range of all interconnected radio systems.

3.7.2. Backbone Nodes

127. The different backbone nodes allow the communication between different access networks (access container / box), to Germany and to other nations. Two different nodes are defined, expressed in the available functionality and interface types/numbers. The most flexible type of node is the Routing Box (RB). It will be used mainly in clean areas and will be used for special and complex operations (e.g. fort he interconnection with Germany or other forces). Instead of this, the Backbone Box (BB) will be used primarily fort he interconnection with Access Containers (AC) or Boxes (AB) and as a relay within the backbone network.

3.7.2.1. Routing Box (RB)

128. The Routing Box (Figure 3.11): can be separated into the network areas WAN, backbone and access network. The WAN interface is used for the interconnection with Germany, other forces or ISPs. But the necessary interfaces may also be used within the backbone for specific devices (HF radio, SATCOM). The interface types for the backbone are either Ethernet (2 - 4) or point-to-point connections (802.11 over radio) which allows the direct interconnection with a radio-LAN. Additional 4 interfaces are available for redundancy purposes. The access network interface is realised through WLAN (infrastructure mode), which is adopted for military purposes. 4 additional Ethernet-interface are available here for redundancy or fall back purposes, too.

129. The functionality of the RB is realised via routers and VLAN switches. Router and VLAN switch are available two times for redundancy purposes (using HSRP) and can be managed through SNMPv3.

130. In addition, the RB is equipped with military connectors (Military Field Connector Panel), directed radio antennas, WLAN antennas and several bases for CNR antennas. The RB can be used as the interface point to other autonomous systems (using BGB4 as the necessary routing protocol).

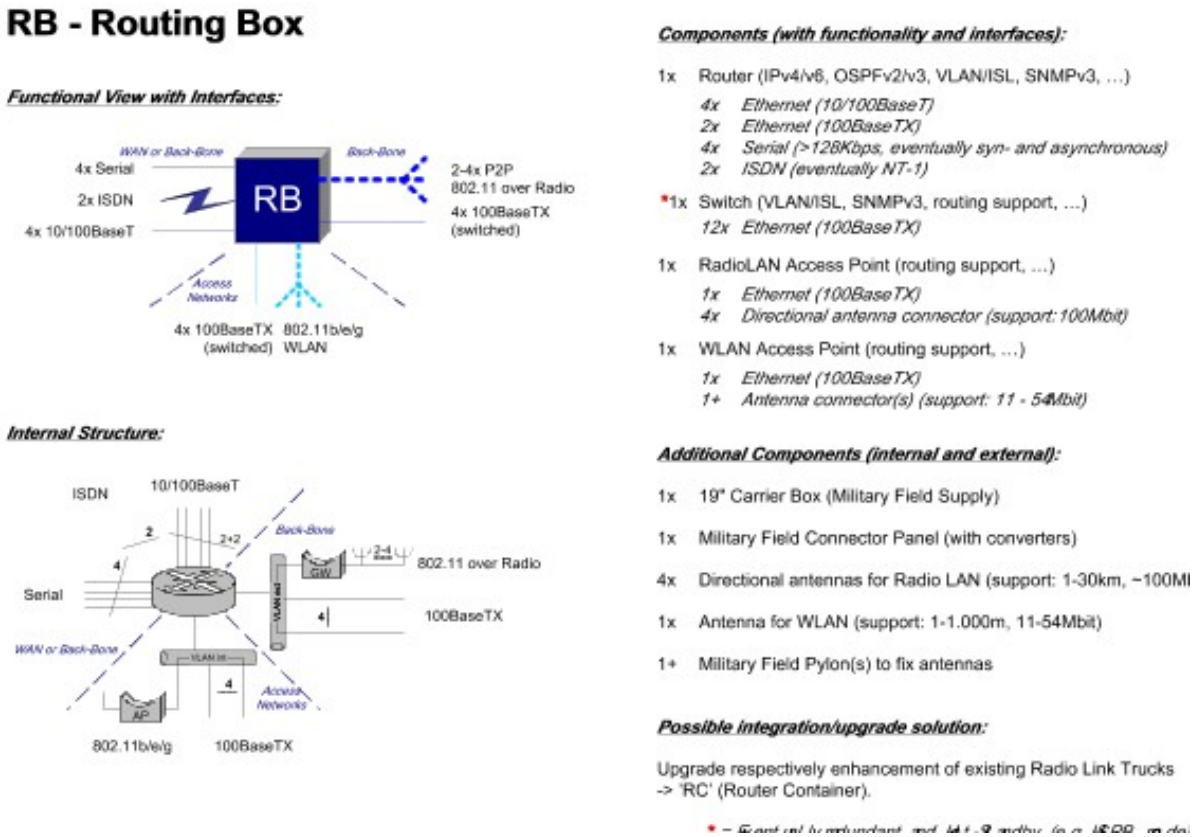

Figure 3.11. Specification of the functional block “Routing Box” (RB)

3.7.2.2. Backbone Box (BB)

131. The Backbone Box (BB) is used both as a Relay to the backbone Network and as an access point to access contains and boxes. It offers the functionality of a routing box, but has less interfaces and configuration possibilities. The AB should be pre-configured, so that only the interconnection with radio devices and cables must be done out-of-area. This pre-configuration is done using the information from the DAKIS database. As available within the RB, the BB 3 interface areas for the WAN, the backbone and the access networks. The WAN area of the BB is used for the interconnection with proprietary connection devices (e.g. HF radios, SATCOM). As the BB is realised as a small and simple functional block, redundant equipment is not necessary, but, if necessary, a RB can be used instead of a BB.

132. The additional components are identical with the RB. The necessary protocols are described in the previous chapter.

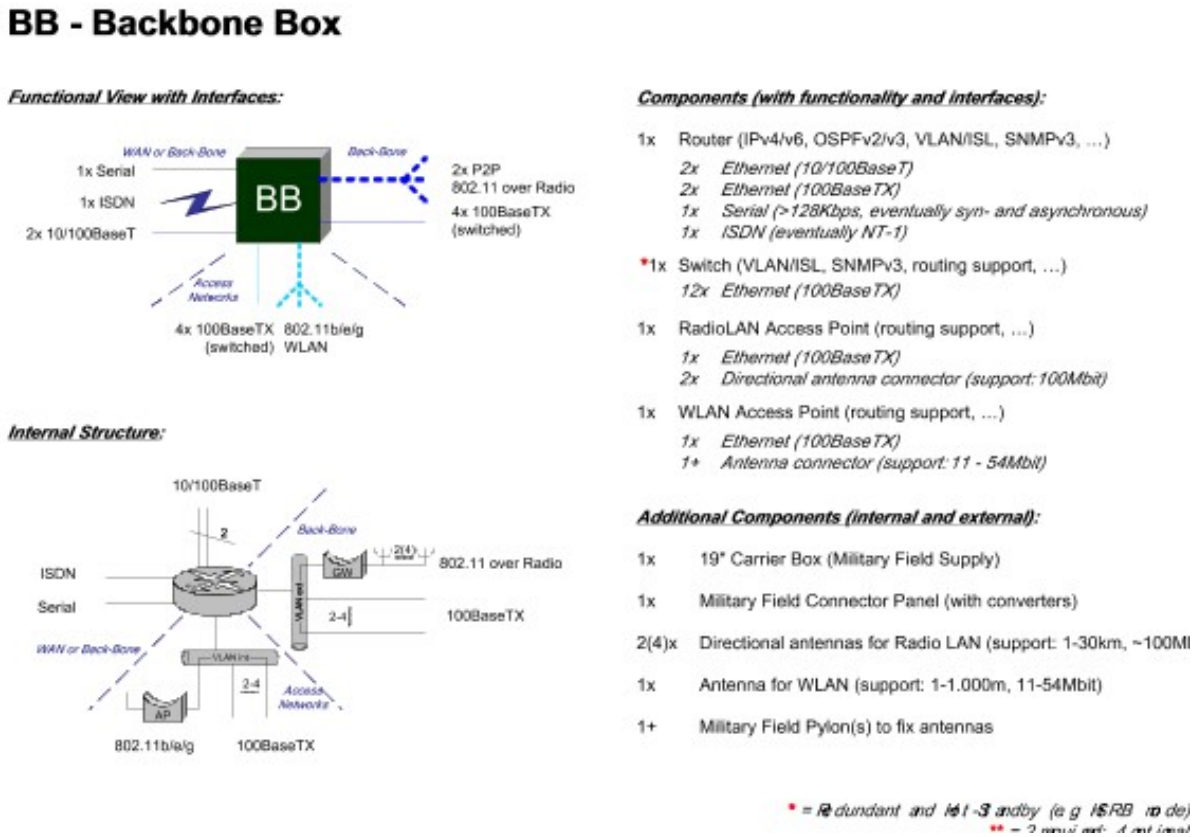

Figure 3.12. Specification of the functional block "Backbone Box" (BB)

3.7.3. Access to the Backbone (red-black interface)

133. Access Container (AC) and Access Box (AB) are the access nodes to the backbone. Based on the operational requirements one of them can be selected. The Access Container offers more flexibility for necessary extensions (e.g. server module), while the Access Box is optimised for ad hoc integration.

3.7.3.1. Access Container (AC)

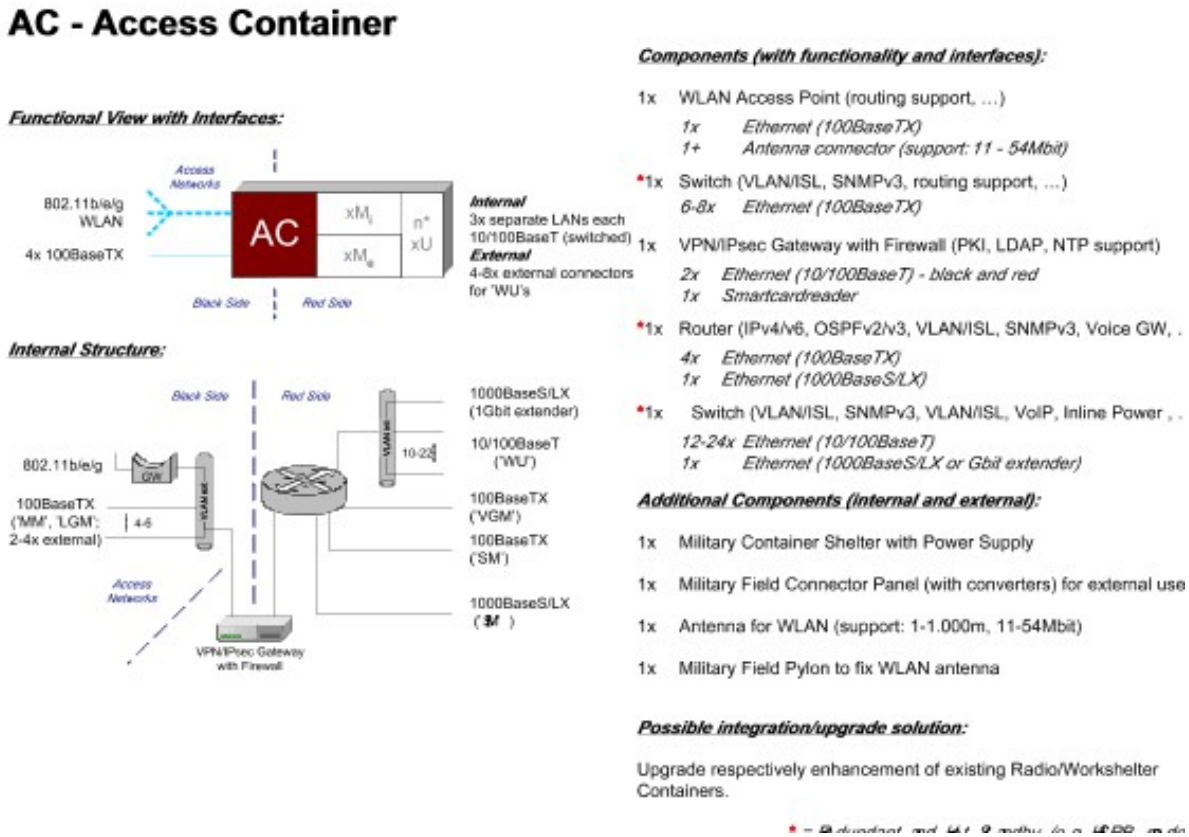

Figure 3.13. Specification of the functional block "Access Container" (AC)

134. In principle, the Access Container (AC) is separate into a black and a red network area. The separation is done through a VPN gateway. Therefore all data from the red domain to the black domain is encrypted at the IP level. In the other direction, it is only possible to communicate with a system in the red domain if the incoming PDUs follow the security policy of the VPN gateway. The Access Container can be separated into three interface areas: Access Networks, Black Modules, Red Modules and Units. Within the Access Networks area it supports AC WLAN (Infrastructure mode) for the interconnection to RB or BB, but it also offers Ethernet interfaces (100BaseFX) for redundancy. On the other side, it offers interfaces to black modules (e.g. MM, VGM). These external modules are not protected by VPN gateways and located within the black network. Platforms within this area must install own security features (see MU). Other modules (e.g. routing modules, SM, LGM) and devices (e.g. WU) are within the red domain. The physical interfaces, which realise these interconnections, are available within the AC description.

3.7.3.2. Access Box (AB)

135. The Access Box offers principally the same functionality as the Access Container, but is

designed for another area of operation, which means that other modules and devices are involved. Within the black network domain, as an option only the interconnection with Mobile Modules (MM) is foreseen. On the red side only WUs are recommended and supported. For this side, in addition a Gigabit Ethernet is available (e.g. for cascading LANs).

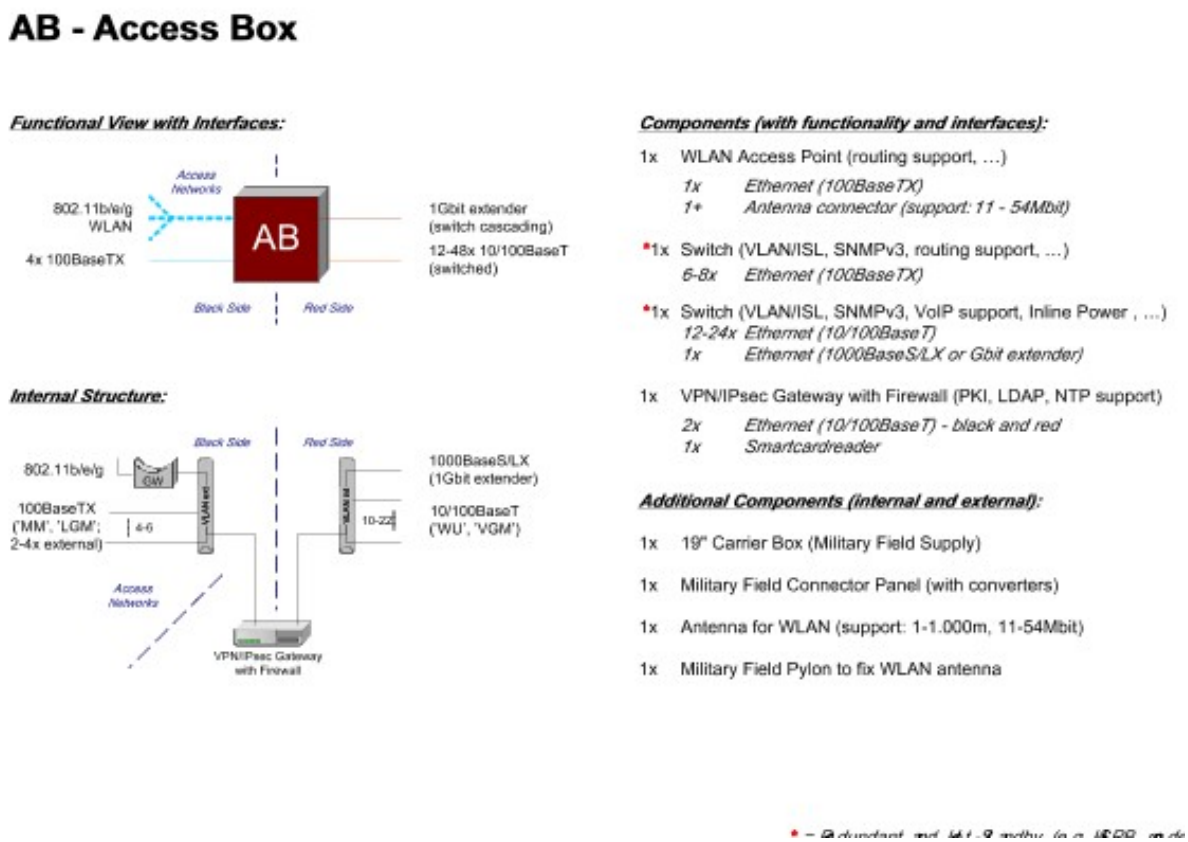

Figure 3.14. Specification of the functional block "Access Box" (AB)

3.7.4. Black Functional Modules and Units

136. The following units and modules (Mobile Unit MU, Mobile Module MM; Voice Gateway Module VGM) offer the possibility to interconnect mobile users (platforms) with Access Networks (via Access Container or Box).

3.7.4.1. Mobile Unit (MU)

137. The Mobile Unit (MU) is the counterpart to the Mobile Module (MM). It realises the interconnection of platforms with the MANET interface of the MM. The MU consists of a MANET and a VPN gateway and a switch, which supports the connection with workstations, IP phones and other devices (e.g. sensors), which offers an Ethernet interface. The VPN gateway is mandatory, as the MM is interconnected with a black, unsecure network (Access Net-

work).Therefore, each platform must be equipped with a VPN gateway to establish a secure and encrypted communication.

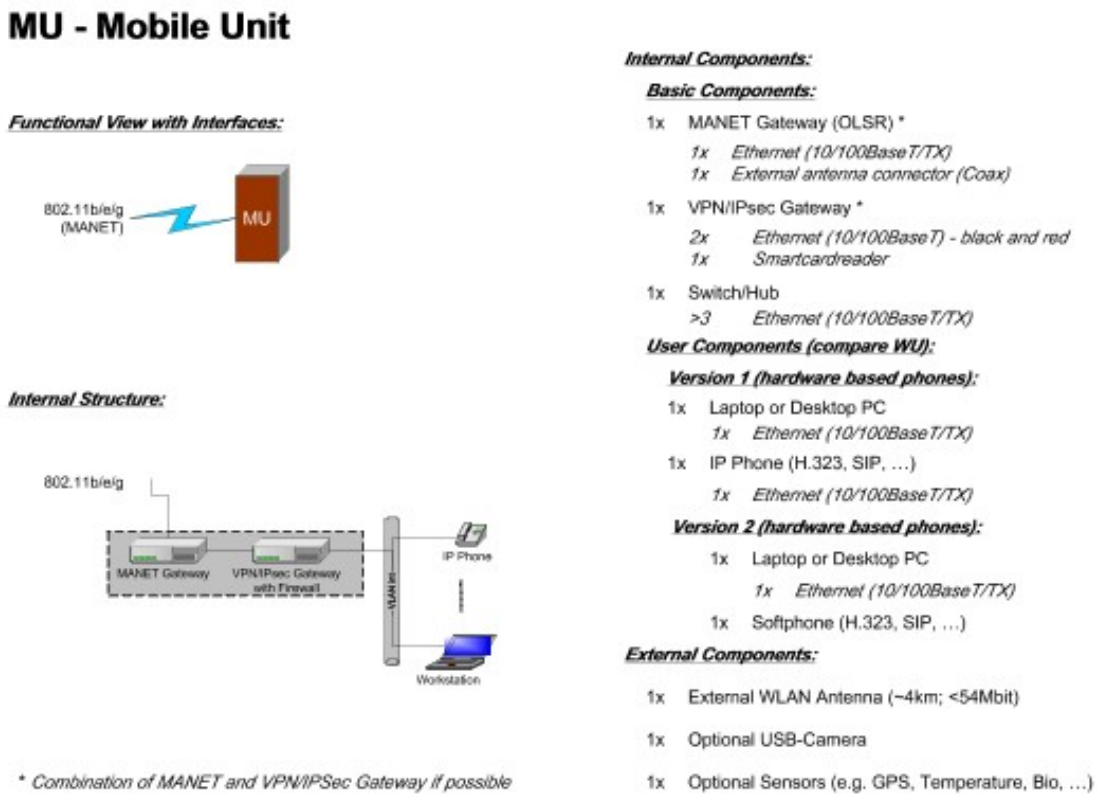

Figure 3.15. Specification of the functional block “Mobile Unit” (MU)

3.7.4.2. Mobile Module (MM)

138. The Mobile Module (MM) is connected directly (wired connection; Copper Side) with the black side of the Access Container or the Access Box and offers a WLAN or MANET interface (Wireless Side; 802.11 a/b*/e/g).

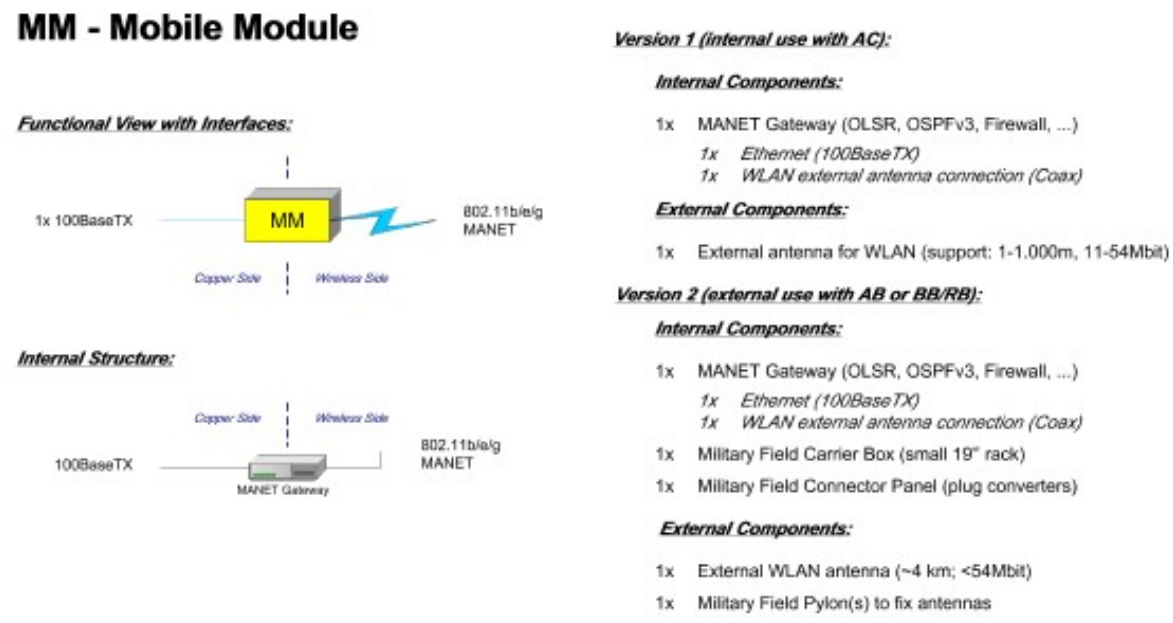

Figure 3.16. Specification of the functional block "Mobile Modulet" (MM)

3.7.5. Red functional Modules and Units

139. Red modules and units are placed in the red area (behind a VPN gateway). These are: Workplace Unit (WU), Server Module (SM) and Link Gateway Module (LGM).

140. **Workplace Unit (WU)**

141. The Workplace Unit can be realised as a IP Phone, a Workstation or a sensor end system (e.g. USB camera) or a combination of all of them. The Workplace Unit is connected through a 10/100 BaseT Ethernet.

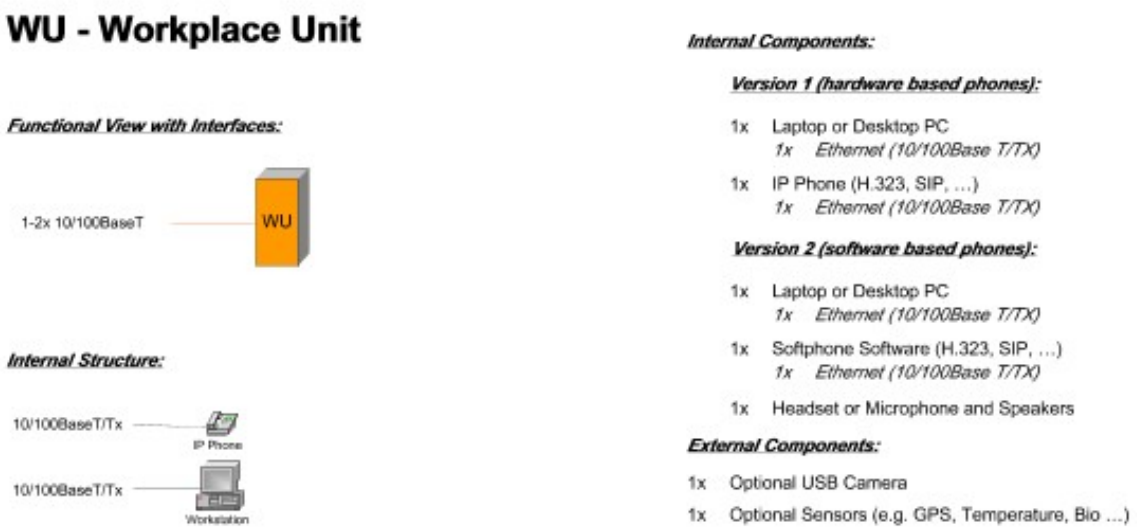

Figure 3.17. Specification of the functional block “Workplace Unit” (WU)

3.7.5.1. Server Module

142. The Server Module can be equipped with different elements: Mandatory parts are a server for basic services (e.g. DNS, DHCP, NTP, GPS), an application server (e.g. databases, command and control systems) and a Storage Server (RAID-System). Additional servers can be a VoIP or PKI server. The server module uses a FastEthernet (100BaseTX) connection. The additional Gigabit Ethernet (1000BaseS/LX) is used for an internal server to server communication.

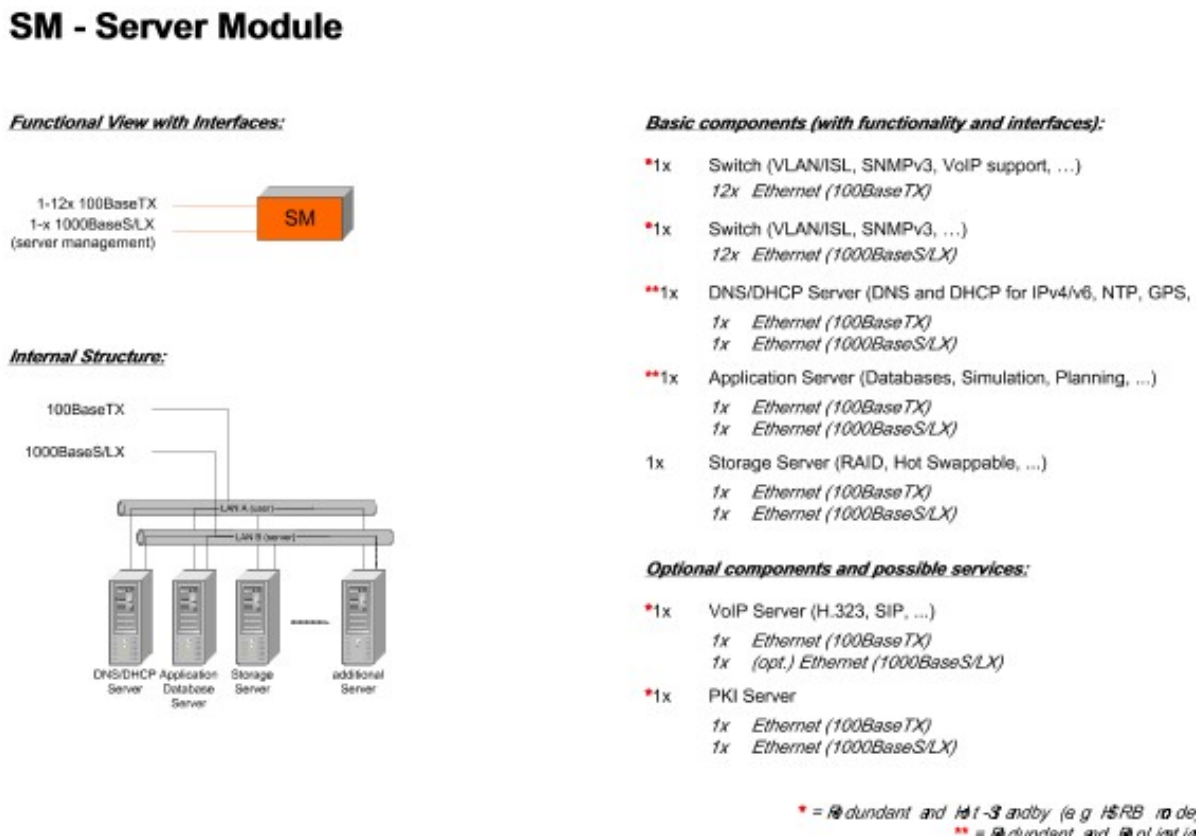

Figure 3.18. Specification of the functional block “Server Module” (SM)

143. A special variation of the server module is he interconnection to external systems (e.g. command and control systems of allies within joint combined operations). Here the NATO model of the #Cooperative Zones#, CZ is used.

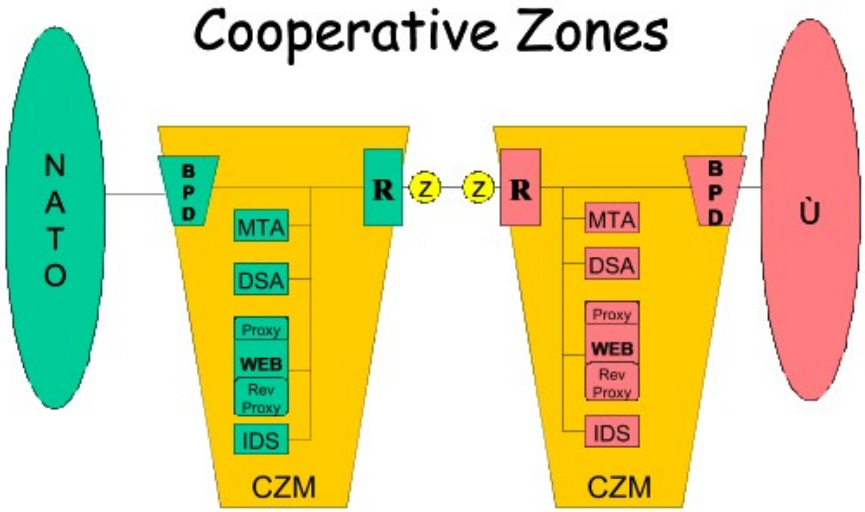

Figure 3.19. Model of the Cooperative Zone within the Server Module

3.7.5.2. Voice Gateway Module (VGM)

144. The Voice Gateway Module (VGM) is directly connected to the red side of an Access Container or an Access Box and offers a translation from VoIP (H.323) to PCM for ISDN-based networks (n * S0). The call handling for VoIP and the translation H.323/PCM may be handled in different modules or integrated within one module. As technology changes here, an additional ISDN crypto module is necessary.

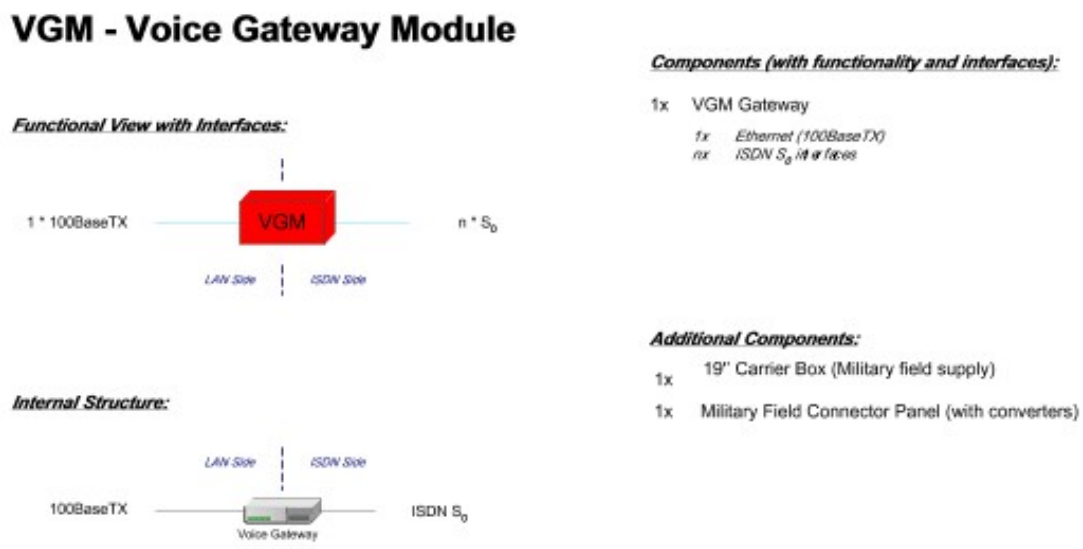

Figure 3.20. Specification of the functional block "Voice Gateway Module" (VGM)

3.7.5.3. Link Gateway Module (LGM)

145. The Link Gateway Module is able to tunnel different Link types across an IP network (backbone network) to another LGM Mandatory part of the LGM is an NIRIS server for basic services (e.g. tunnelling of Link1, Link11B, Link16 over IP.

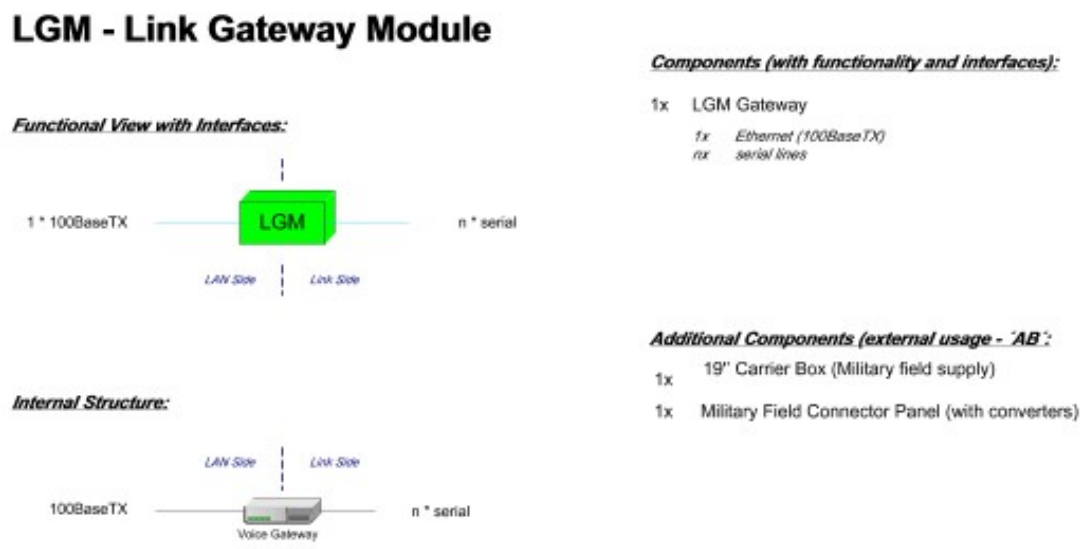

Figure 3.21. Specification of the functional block "Link Gateway Module" (LGM)

146. The solution of the NC3A for an LGM is used here (NATO Interoperable Recognized Air Picture Information System # NIRIS, Version 2).

147. NIRIS2 allows the tunnelling of Link1-, Link11B-, IJMS-, Link16- and ASTERIX data across different network technologies, including IP networks.

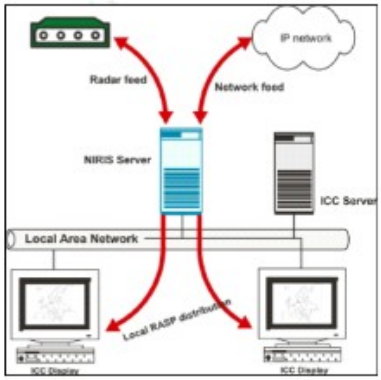

Figure 3.22. Principle figure for the usage of an NIRIS2 server

4. IDENTIFICATION ARCHITECTURE

148. The NATO Identification Reference Architecture (NIRA) was developed in accordance with the NATO C3 Systems Architecture Framework (NAF). It has been developed in a manner unrestrained by any solution or presupposition in the technology, which might be used to support the requirement.

149. The purpose of the NIRA Operational View is to serve as a single document which describes aspects of identification in operational terms to aid NATO nations in procurement of systems which will meet their requirements. The Operational View will be used by systems architects to help determine compliance of alternative systems architectures as they are being evaluated.

150. The scope of the NIRA Operational View includes processes, mission areas, operations, organisation, operational elements and identification information exchange requirements and attributes for air/space, land, maritime and combined joint operations in peace, crisis and conflict. The Operational View accords with the Military Operational Requirement (MOR) for Identification in NATO, and supports fulfilment of the Military Functions as defined in MC 299/5 and amplified in MC Guidance for Defence Planning.

151. Identification requirements generally vary from operation to operation and are addressed based on the definition for identification, which is the determination of friend, foe or neutral and may require distinction as to military or civil nature and determination of class, type, nationality or intent. All identification information, determinations and indicators must be correlated with a track or position to have value at the tactical or operational level.

152. Within the Operational View each mission area is described illustrating common command relationships and critical operational elements. These two aspects are summarised by the Command Relationships Chart and High-Level Operational Concept Diagram. Subsequently, each operation type is analysed with regard to the nature of identification information and is summarised with an Operational Node Connectivity Diagram that shows the connectivity and relationships among operational elements needed for successful execution. Lastly, specific identification information needs, in terms of identification determinations and identification indicators are considered and summarised.

153. The purpose of the NIRA Systems View is to serve as a single source describing system and standardisation needs for nations to develop and field interoperable joint identification systems covering all aspects of the air/land/maritime battlespace. It allows SC/7 and the nations to better determine identification capabilities and deficiencies relative to requirements, where and how to achieve interoperability, and a set of priorities for improving the identification capabilities of the Alliance.

154. The scope of the NIRA Systems View is to provide a description of systems and interconnections providing for and supporting NATO identification. The Systems View includes technologies/systems and standards (non-co-operative and co-operative identification, data

links, sensors, and identification fusion) necessary for all operational elements to fulfil identification requirements for air/space, land, maritime and combined joint operations in peace, crisis, and conflict in accordance with the Military Operational Requirement for identification in NATO and the NATO Identification Reference Architecture - Operational View.

155. The NIRA Systems View has been developed in accordance with the NAF and includes templates which have been constructed for military operations requiring identification. Identification requirements and solutions generally vary from operation to operation and are addressed based on the definition for identification, which is the determination of friend, foe or neutral and may require distinction as to military or civil nature and determination of class, type, nationality, or intent. Identification characterisation must be correlated with position or a track to have tactical value.

156. Within the Systems View each operation is addressed emphasising the technologies, systems, or standards most likely to fulfil the identification requirements as described in the Operational View.

5. RECONNAISANCE AND IMAGERY

5.1. GROUND STATION IMAGE SERVER

157. The NATO Imagery Interoperability Architecture (NIIA) defines the overall structure of the elements of the Intelligence, Surveillance, and Reconnaissance (ISR) community.

158. The objective is to achieve data exchange interoperability between NATO reconnaissance and surveillance assets levels of interoperability, as defined in NATO interoperability publications.

159. The level of interoperability is currently:

- **Degree 2:** Structured Data Exchange. Involves the exchange of human-interpretable structured data intended for manual and/or automated handling, but requires manual compilation, receipt and/or message dispatch.
- **Degree 3:** Seamless Sharing of Data. Involves the automated sharing of data amongst systems based on a common exchange model.

160. Main focus of the NIIA is on the imagery interfaces between airborne and surface-based elements and between the output of the surface-based elements and the rest of the ISR community.

161. In this document interoperability targets to the output of the ground station with each nation accessing imagery, text, and graphics from all other nations.

162. The following Standards are relevant:

163. **STANAG 4545, #NATO Secondary Imagery Format# (NSIF)**

164. This STANAG establishes the format for exchange of electronic secondary imagery. Secondary imagery is sensor data that has been previously exploited and/or processed into a human readable picture.This format enables an operator at one workstation to compose and capture a multimedia image on his workstation, and send it to another workstation where it is capable of being reproduced exactly as it was composed on the origination workstation. The NSIF format can be composed of images, graphics and text. Because of the wide variety of display capabilities, the implementations of NSIF readers and writers are classified by their level of complexity, where the highest level will handle very large images with many bands of data, and the simplest level will only handle small, single band images. For interoperability considerations, a reader of an NSIF file must be greater than or equal to the complexity level of the image it is reading in order to display it. There are reserved segments at the end of the NSIF file and within the different segments of the file for other types of information not cur-

rently defined in the baseline standard (e.g. GMTI data or motion imagery). For example a reconnaissance exploitation report (RECCEXREP) formatted in an ADatP-3 format could be attached to an image segment through a text segment.

165. **STANAG 4559, "NATO Standard Imagery Library Interface" (NSILI)**

166. This STANAG is to provide interoperability between NATO nations" reconnaissance databases and product libraries by defining an interoperable interface to each nations" image library systems, without altering the internal architecture each individual system. This STANAG standardizes on the commands that pass back and forth between database systems and the clients as well as the parameters that can be used to search for a particular image in a remote database (e.g. date, time, and location).The interface relies on facilities and services to collaborate database request, reports and orders. The STANAG does not cover the delivery of the requested images to the requestor. It does recommend that products be delivered in STANAG 4545 format.

167. **STANAG 4575, "NATO Advanced Data Storage" (NADS)**

168. This STANAG defines an interface for advanced digital storage systems, such as solid state memories or disk arrays, with the aim of providing cross servicing capabilities for "NATO nations" reconnaissance and surveillance assets as well as the exploitation of the imagery data in any reconnaissance ground station. The interface will be a high data rate port to allow direct download of the imagery and auxiliary data, either at the air platform or at the ground station. Once the memory has been transferred to a reconnaissance exploitation ground station, it can be exploited using normal tools.

169. **STANAG 7023, "ATO Primary Imagery Format" (NPIF)**

170. This STANAG establishes a standard data format and a standard transport architecture for the transfer of reconnaissance and surveillance imagery and associated auxiliary data between reconnaissance collection systems and exploitation systems. The concept behind STANAG 7023 is to describe the sensor data structure in a space-time domain. This enables STANAG 7023 to describe any sensor data structure without modification to the STANAG. STANAG 7023 is capable of handling any type of sensor. It is simply a shell for capturing multi-source data for the purpose of data correlation at a later time and place. It is also possible from a STANAG 7023 data stream to replicate events in precisely the same order in which they occurred at acquisition.

171. **STANAG 7024, "Air Reconnaissance Tape Recorder Interface"**

172. This STANAG establishes the physical format for the exchange of magnetic tape cartridges for 4 different technologies of recorders. All the recorders in STANAG 7024 are sequential access. The four technologies are each listed in a separate annex as shown below.

- **Annex A** - 19mm helical scan ANSI ID-1 digital instrumentation recorder with large, medium and small tape cartridge formats

- **Annex B** - 8 mm, helical scan Hi-8 digital, and 8mm analogue
- **Annex C** - 12.65 mm helical scan SVHS analogue recorder
- **Annex D** - 25.4 mm transverse scan AMPEX DCRSi digital instrumentation recorder

173. **STANAG 7085, "Interoperable Data Links for Imaging Systems"**

174. This STANAG provide the interoperability standards for 3 classes of imagery DL used for primary imagery data transmission: analogue links described in Annex A, point-to-point digital links described in Annex B and broadcast digital links described in Annex C. Command and control of the sensors and platform is an auxiliary mission. Annex B is organized in 2 chapters #General Requirements# and #Implementation Directives# which describe point-to-point digital links. Different implementation profiles are possible : the U.S. Common Data Link (CDL) is described in Implementation 1. Further study continues to update the Annex C Digital Broadcast configuration. The STANAG is structured such that it provides a number of options for the specific data link configuration, such as simplex or duplex operation, data rate, carrier frequency, channel multiplexing, interleaving, encryption, and many others that must be matched prior to passing data from transmitter to receiver. STANAG 7085 data links can handle any form of data (e.g. 7023, 4545, or GMTI), and can operate in different configurations, including two way (half or full duplex) modes.

175. **STANAG 4586, "AV Control System (UCS) Architecture"**

176. The objective of this STANAG is to facilitate communication between a UCS and different UAVs and their payloads as well as multiple C4I users. The implementation of the standard UCS architecture and the interfaces will also ease the system integration process of subsystems from different sources. This standardization will allow the continued utilisation and the integration of legacy systems. This STANAG is under the control of the NATO Naval Armaments Group (NNAG).

6. GIS ARCHITECTURE

177. The NATO GIS Target Architecture provides the Geographic Information System functionality to the Bi-SC AIS. This Project will eliminate proprietary geospatial data file formats from the integrated Bi-SC AIS and implement within the Core GIS Services, an open GIS structure based on a spatially enabled Database Management System (DBMS) storing information in a geospatial neutral format. The Bi-SC AIS Functional Services will exclusively utilise geographical information services as described in the GIS Target Architecture (NC3A-BE/ACQ/ISB/20.20.05/02/04 Dated November 2002 - GIS Target Architecture Ver. 1.3).

7. INFOSEC ARCHITECTURAL VIEWS

7.1. INTRODUCTION

178. The NATO C3 Overarching Architecture has provided the base elements for the development of specific InfoSec Views for NATO PKI, the NATO General Purpose Segment Communications System (NGCS) Reference Architecture, the Bi-SC AIS Reference Architecture, the INFOSEC Reference Architecture for NATO Capability Package CP 0A0155, and the Deployable CIS Module INFOSEC Functional View (DCIS IFV). An INFOSEC View for the Overarching Architecture itself is still under development.

7.2. INFOSEC FUNCTIONAL VIEW OF THE NATO GENERAL PURPOSE SEGMENT COMMUNICATIONS SYSTEM (NGCS) REFERENCE ARCHITECTURE AC/322(SC/4)N(2003)052 DATED 25 AUGUST 2003

179. The INFOSEC Functional View of the NATO General Purpose Segment Communications System (NGCS) Reference Architecture derives the pertinent requirements from the existing agreed upon guidance and policy documents; identifies the services / mechanisms that can be used to meet those requirements; and, illustrates the placement of selected services / mechanisms. NGCS capabilities are driven by mission requirements and the establishment of the INFOSEC components must be integral during the design and implementation of NGCS. A Risk Management approach must be applied to implementation of these specific INFOSEC mechanisms or countermeasures. The exact INFOSEC mechanisms are still to be defined following completion of a detailed Risk Assessment and Target Architectures.

180. The NGCS reference architecture relies on the provision of the security services and mechanisms defined in Infosec Functional View. A complete and detailed Risk Assessment will determine the level of security required. These services and mechanisms interact to provide the required security; it is not possible to delete or reduce any one of the services or mechanisms without impacting the overall security. For example, if robust connectivity is reduced due to cost, then availability will be impacted. It is therefore paramount that the reference architecture be re-examined if some mechanisms or services are not implemented due to cost or other reasons.

181. At this point in the development cycle of the NGCS reference architecture, it is not possible to provide all the detail and precision that can be anticipated as an outcome of the development of the NGCS Target Architecture and the detailed Risk Assessment. It is evident that modern INFOSEC mechanisms, with growth potential to counter future threats, must be implemented to thwart known and projected threats. Further detail and refinement shall be reflected in an INFOSEC Functional View to be developed to accompany the NGCS Target Architecture.

7.3. INFOSEC FUNCTIONAL VIEW OF THE NATO PUBLIC KEY INTERFACE (PKI) REFERENCE ARCHITECTURE, AC/322(NPMA-PAC)WP(2003)002 REV 1

182. This document provides a Reference Architecture for the NATO Public Key Infrastructure: deriving the pertinent requirements from the existing agreed upon guidance and policy documents; identifying the services/mechanisms that can be used to meet those requirements; and, illustrating the placement of selected services/mechanisms. Public key technology capabilities are driven by mission requirements and the establishment of the public key technology components must be integral during the design and implementation of the NPKI. A Risk Management approach must be applied to implementation of these specific public key technology mechanisms. The exact PKI mechanisms are still to be defined following completion of a detailed Risk Assessment and the development of a NPKI Target Architecture.

183. The NPKI security architecture relies on the provision of the security services and mechanisms defined in this document. A complete and detailed Risk Assessment will determine the level of security required. These services and mechanisms interact to provide the required security; it is not possible to delete or reduce any one of the services or mechanisms without impacting the overall security. For example, if robust connectivity is reduced due to cost then availability will be impacted. It is therefore paramount that the security architecture be re-examined if some mechanisms or services are not implemented due to cost or other reasons.

184. At this point in the development cycle of the NPKI Reference architecture, it is not possible to provide all the detail and precision that can be anticipated as an outcome of the development of the NPKI Target Architecture and the detailed Risk Assessment. It is evident that modern public key technology mechanisms, with growth potential to counter future threats, must be implemented to thwart known and projected threats. Further detail and refinement shall be reflected in the NPKI Target Architecture.

7.4. BI-STRATEGIC COMMANDS AUTOMATED INFORMATION SYSTEM (BI-SC AIS) REFERENCE ARCHITECTURE INFOSEC FUNCTIONAL VIEW (IFV) (VOLUME 2),VERSION 0 PUBLISHED 18 AUG 2003

185. This document provides an INFOSEC Functional View of the Bi-Strategic Command Automated Information System Reference Architecture: deriving the pertinent requirements from the existing agreed upon guidance and policy documents; identifying the services / mechanisms that can be used to meet those requirements; and, illustrating the placement of selected services / mechanisms. Bi-SC AIS capabilities are driven by mission requirements and the establishment of the INFOSEC components must be integral during the design and implementation of the Bi-SC AIS. A Risk Management approach must be applied to implementation of these specific INFOSEC mechanisms or countermeasures. The exact INFOSEC mechanisms / products are still to be defined following completion of detailed Risk Assessments of the Bi-SC AIS Target Architectures.

186. The Bi-SC AIS security architecture (actually the IFV) relies on the provision of the se-

curity services and mechanisms outlined in this document. A complete and detailed Risk Assessment will determine the level of security required. These services and mechanisms interact to provide the required security; it is not possible to delete or reduce any one of the services or mechanisms without impacting the overall security. For example, if robust identification and authentication services are reduced due to cost considerations then the relative strength of the need-to-know separation service may be impacted. It is therefore paramount that this IFV be re-examined if some INFOSEC mechanisms or services are not implemented due to cost or other reasons.

187. At this point in the development cycle of the Bi-SC AIS architecture, it is not possible to provide all the detail and precision that can be anticipated as an outcome of the development of the Bi-SC AIS Target Architecture and the detailed Risk Assessments that will be accomplished under CP 0A05020. It is evident that modern INFOSEC mechanisms, with growth potential to counter future threats, must be implemented to thwart known and projected threats. Further detail and refinement shall be reflected in an INFOSEC Functional View to be developed to accompany the Bi-SC AIS Target Architecture.

7.5. REFERENCE ARCHITECTURE FOR ELECTRONIC INFORMATION SECURITY SERVICES (INFOSEC) NATO CAPABILITY PACKAGE CP 0A0155

188. This INFOSEC Reference Architecture describes the security functionality required in the NATO Command and Control environment to meet the anticipated user requirements in the subject time frame. This Reference Architecture applies in principle to all NATO common funded Command and Control Information Systems (CCIS) and their supporting communications bearer sys-tem. It provides the framework for the delivery of the security tools, organization and prin-ciples to the users, the systems and the management systems to achieve these. In particular this RA provides rationale, and documents the current thinking, for the projects under Capability Package 0A0155. As the document is under development at the NC3A there is no reference yet.

7.6. DEPLOYABLE CIS MODULE INFOSEC FUNCTIONAL VIEW (DCIS IFV)

189. The Capability Package (CP) 5A0049/9B0019, “Provide a NATO Deployable CIS Capability”, is intended as the vehicle for completion of a deployable CIS module (DCM) capability. With DCMs NATO will be able to deploy and provide CIS (Communications and Information System) support to the strategic level of both Article 5 and Crisis-Response Operations (CRO) in a Combined Joint Task Force (CJTF) context. DCMs are organised into two regional DCM battalions and are manned during peacetime. Each DCM troop is able to split into two DCM elements. The calculations of amounts of equipment to be provided through the Capability Package reflect the overall requirement for each DCM element to be able to deploy and establish a CIS infrastructure for a number of staff using self-contained assets. The DCIS IFV will describe the INFOSEC aspects related to the implementation of the assets of the DCIS Module. As the document is under development, there is no reference yet.

190. The DCMs are intended to be part of the NATO CIS Contingency Assets Pool (NCCAP) and Initial DCM capability is to be provided through ongoing procurements supported by CP 5A0001: “Provide an ACE CIS Contingency Assets Pool (ACCAP)”.

8. AN MLSA SECURITY MODEL

8.1. INTRODUCTION

191. A Multi Layer Security Architecture (MLSA), provides a Security System View identifying a complete set of security components required to set-up secure IT systems in general and in particular for inclusion in the NCOE component model. The individual security components are grouped in domains according to their role within a holistic security system approach.

192. A MLSA security view of the IT system is considered as important to derive an appropriate overall security policy and to facilitate the definition and implementation of secure NCOE-CM structured IT systems. The MLSA approach helps to identify security components also, which are intentionally not covered by the existing component model, i.e. personal security environments, security services for FAS applications or lower layer security protocols.

8.2. SCOPE

193. The modelling of infrastructures for the generation, sign, encrypt, storage and communication of data objects (information), as well as the protection of the infrastructure itself is based on state-of-the-art architectures, methods, security services and protocols. MLSA is an approach to provide a top level and compact view of the security aspects of the information and communication technology. It takes care for nowadays dimensions of threats and is adopted as a framework for the conception and implementation of secure information systems. The purpose of MLSA is:

- To provide a top level and compact view of the security aspects of Information and communication technology (ICT) in an Open Systems environment;
- To identify the state-of-the-art security services, protocols and technologies and their placement in multi-layer IT systems;
- To draw the management aspects in the perspective of secure systems and services and security management;
- To evolve and place generic security services in IT systems;
- To take into account the Personal Security Environment (PSE) including required security services at the man-machine interaction point; and
- To provide the methodology for set-up of secure IT systems.

8.3. MLSA SECURITY SERVICES MODEL

194. The MLSA security services model is based on the ISO Open Systems Interconnection Reference Model international standards. These international standards are recognised world-wide as the applicable architectures according to which communication system, including the Internet, and data processing systems can be built, used and maintained. The MLSA model uses the concept of domain to portion the IT security system into meaningful and manageable parts. It is compatible with the NCOE component model, however, taking care for the security aspects of IT systems only. The concept domain denotes an architectural construct for dividing complex IT security technology into smaller, more manageable portions. A domain delimits individual parts of an IT system and makes it easier to see and consider them individually, in context of the entire system. This allows grouping the required security services and security functional elements into individual domains, namely user domain, services domain, transport domain and management domain. It also allows the creation of a generic security services aspect for the purpose of grouping the security services and elements of generic nature, for use by all other domains. The security services model identifies all the required services and elements necessary to build a secure ICT environment. It may be seen as a construct toolkit for setting-up of modular and scalable security systems to user requirements according to agreed security policies.

8.4. MLSA DOMAINS

8.4.1. User domain

195. The user domain includes all security aspects required for the local user requirement and security aspects for peer-to-peer interactions between users (persons). I.e. data objects, operational processes (work-flows), in particular the process to sign data objects (sign process) and end-to-end security mechanisms, authentication procedures for users and to access the system. E.g. the confirmation to agree with a message content belongs to the user domain - the receipt confirmation of a message belongs to the communication services domain. Operating systems, computer, user and applications for the data processing are the determining factors. The service access point to communication services represents the interacting interface to the outside world. The scope of security is persistent, i.e. security for data objects through their entire lifecycle.

- Local, person and role related security aspects of data processing;
- Security related interactions (peer-to-peer) between producers and consumers of information;
- Residences of secure data objects;
- Persistent security of data objects.

8.4.2. Communication Services Domain

196. The services domain includes all security aspects required for communication services and protocols, e.g. messaging, web, enclave protection. The scope of security is transient , i.e. security for data objects during an instant of communication. Communication services and the protocols providing them are the determining factors. This domain is responsible for the interoperability between partner entities, which can only be guaranteed if agreed sets of profiles are used.

- Security aspects of communication services and protocols;
- Security related interactions (peer-to-peer) between communication service provider entities;
- Security aspects of application layer gateways for enclave protection;
- Transient security of data objects.

8.4.3. Transport Domain

197. The transport domain includes all security aspects required for transport, network, data link and physical layer protocols, i.e. SSL, VPN, IPSec, IP filtering, Kryptos. The scope of security is transient, i.e. security for data object components during an instant of transportation. The transport and network protocols and the used subnetwork technologies are the determining factors. This domain is responsible for the interoperability between partner entities, which can only be guaranteed if agreed sets of profiles are used.

- Transport and networking aspects of secure data processing;
- Locally constrained security functions for protection the enterprise enclave against penetration of malicious IP packets;
- Security protocols for bridging of insecure subnetworks;
- Data encryption at the physical level;
- Transient security of data.

8.4.4. Management Domain

198. The management domain includes all security aspects required for the support of user, communication services and transport domains, i.e. system, network and security management, in particular monitoring and public key infrastructures. The scope of the management are supporting services. Security of information and communication technology is determined by such system properties as robustness, availability, and reliability. These properties can be made visible by the management system, made controllable, and be regulated, and thus can be

matched to the requirements of a given security policy. An important aspect to pay attention to when choosing a security system is the heterogeneity of the IT system to be managed. The decisive criteria for management functions are distribution, portability, and effectiveness:

- Management aspects of secure data processing;
- Management infrastructure;
- Key management;
- Monitoring;
- Influence of system and network management on security;
- Secure management.

8.4.5. Generic Security Services Domain

199. The generic security aspects domain includes all generic security issues required for the support of user, services, transport and management domains, i.e. generic methods, services and technologies. The scope of the generic security aspects are supporting services, e.g. Risk ' thread assessment, generic krypto service providers and the formulation of security policies.

- Key management;
- Monitoring;
- Influence of system and network management on security;
- Secure management.

8.4.6. Generic Security Services Domain

200. The generic security aspects domain includes all generic security issues required for the support of user, services, transport and management domains, i.e. generic methods, services and technologies. The scope of the generic security aspects are supporting services, e.g. Risk ' threat assessment, generic krypto service providers and the formulation of security policies.

201. The majority of security functions and mechanisms are based on cryptographic techniques. For an economic and secure information technology they should be implemented and accessible in a standardised way and be generic in nature. The generic security services (GSS) are implemented and are also accessible in a standardised way at the GSS-APIs. Moreover, GSS-APIs are independent of the algorithms being used. The generic security services domain groups all the security services, also those that might be present in the operating system:

- Generic krypto provider;
- Operating systems;
- Security related aspects of the local system (compusec, safety - robustness of equipment);
- Methodology (set-up process);
- Krypto algorithms;
- Generic security services APIs;
- Security policy.

202. The methodology to perform threat and risk analysis and to define appropriate security facilities and components for a domain, to build and set-up security domains and secure ICT environments is an important element of this domain.

8.4.7. MLSA Covering Security Aspects of the NCOE-CM

203. The NCOE Component Model includes security services in all component levels as well within the Support Services component level. So, the MLSA may be seen as holistic security system view of NCOE component model, contributing security components required to all levels of the component model.

204. The following table draws a secure IT system conformant to the Multi Layer Security Architecture - MLSA. The figure includes also the correspondence with the NCOE component model (NCOE CM) and where the security services are applied.

User domain - persistent security. NCOE CM user, mission applications	**Management domain.** NCOE CM support services
• Secure data objects (documents, maps,..) • End-to-end security (request/confirmation dialog) • Encapsulation/sign process (policy enforcement) • Authentication (access control, peer-to-peer) • Personal security environment (SmartCard,..)	• Security management (PKI, directories) • System management • Network management • Monitoring • Auditing • Intrusion detection • Secure management

<table>
<tr>
<td>Communication Services domain - transient security. NCOE CM common support application services

• Secure communication services (email, Web,..)
• A-Layer proxies (Firewall)
• A-Layer Filtering (Virus Checker)
• Semantic related filtering
• Secure platforms (CORBA,..)</td>
<td>Transport domain - transient security. NCOE CM network services

• Transport security services (SSL, SHTTP)
• Network security services (VPN, IPSec)
• Kryptos</td>
</tr>
<tr>
<td colspan="2">Generic security aspects. NCOE CM support services, kernel services, APIs, DATA.

• Methodology (NC3TA-IHB, ICT set-up process, templates,..)
• Risk ' threat assessment
• Security policy (certificate policy, certification practise statement, verification policy,..)
• Generic krypto services provider (GSS-API, krypto algorithms)
• Secure operating systems (file encryption, file access control, local system access control,..)</td>
</tr>
</table>

Table 8.1. MLSA structured NCOE Security Services