NETFORCE PRINCIPLES
An Elementary Foundation of NEC and NCO

Hans E. Keus
TNO Defence, Security and Safety
Oude Waalsdorperweg 63
P.O. Box 96864
2509 JG The Hague, The Netherlands
+31 70 3740022, hans.keus@tno.nl

Keywords:
Network Centric Warfare, Network Enabled Capabilities, Netcentric, Netforce, Reference Model, Foundation, Nodes, Functions & Services, Interoperability

ABSTRACT: *The debate on NCO and NEC continues to suffer from definitional and conceptual imprecision. This paper introduces a modelling framework that provides elementary netcentric principles with which NCO and NEC concepts can be constructed and derived. In a stepwise derivation process, starting with a simple network-node paradigm, a set of elementary modelling concepts is defined. This set, which we call the Netforce Reference Model comprises the basic notion of netcentric nodes, a description of the elementary properties of nodes, node integration properties with a network, interacting nodes and resulting multi-node behaviour like functions and services. These so-called Netforce Principles (NP) can be used to derive and design systems and procedures in a netcentric environment. It allows commonly used NEC and NCO concepts to be explained by their fundamental underlying principles. Examples of these are situational awareness, synchronized decision making and agile mission groups (AMG). By adopting NP for modelling NEC, NCO and systems in the netcentric environment, interoperability on the information and especially the procedural levels can be substantially improved. This paper describes the current status of the Netforce Reference Model.*

1 Introduction

1.1 Background

One of the major areas of interest and discussion today is the formulation and introduction of netcentric principles in modern warfare and in crisis response operations. From the moment of introduction of the term netcentric warfare (NCW) [1] the topic has undergone a fast evolution and it became the major trend of contemporary military developments. The terminology itself has also evolved and we now also speak about NCO (network centric operations), NEC (network enabled capabilities) [2], etc. We will use the UK term NEC in this paper, as it is now firmly adopted in NATO.

In many discussions on NEC the specific netcentric concepts are just loosely defined. Terms like synchronisation, agile mission groups, real time shared situation awareness, effect-based planning are often ambiguously understood. This is caused by the fact that underlying netcentric principles that construct those higher level concepts are not precisely known or defined. In discussions on how to create net-centricity, how to evaluate the effects of netcentric developments, how to introduce NEC in organisations, or how to perform the netcentric transformation, the lack of a fundamental understanding of the basic building blocks of NEC is felt even more.

1.2 Context and Purpose

In this paper we address fundamental work in solving this lack of understanding. In a stepwise process, starting from a small set of basic assumptions, a framework of NEC concepts is built;

from very elementary and fundamental building blocks till higher order more complex concepts, like services, operational functions and generic warfare models. This framework is called the *Netforce Reference Model (NFRM)*, with the *netforce* defined as *the total collection of all netcentric elements that constitute the complete operational netcentric force*. The purpose of the NFRM is to offer a generic framework providing a complete set of elementary NEC building blocks with which higher-level NEC concepts can be modelled and defined. It offers a means to harmonize NEC terminology, to understand the nature and complexity of commonly used netcentric concepts, and it increases interoperability between organisations and systems when they are defined and designed based on these netforce principles.

1.3 Overview

In section 2 we shall introduce, by using a network-node paradigm, the basic building block of the netforce framework: *the netforce node*. It is this node concept, together with its set of elementary properties, that the netforce framework will be constructed from. The basic netforce concepts that can be derived from the nodes and their properties are discussed in section 3. Section 4 deals with the different interactions between the nodes and they are the basis of the functions and services, and especially the generic netforce functions that are discussed in section 5. In section 6 we will apply the netforce concepts to the modelling of warfare areas. We will conclude with some of our conclusions and identify some promising lines of further development.

2 The Network-Node Paradigm and the Basic Nodes

2.1 Starting Points

In the netcentric approach we talk about achieving self-synchronisation of decision making and actions, about the necessity of shared awareness, of the provision of adequate data and information. For NEC to become that reality we need NEC capable systems, communication networks, NEC-based CONOPS (Concept of Operations) and substantial support in the areas of training, leadership, doctrine, logistics, etc. Current and future operations are more and more of a coalition nature. This means that interoperability between systems and procedures (command procedures, CONOPS) of different nations is only gaining in importance. To enhance interoperability between these systems and procedures it is advantageous when they are being conceived, designed and developed according to a set of standard principles.

However, a good understanding of the underlying principles of netcentric behaviour, netcentric systems and procedures is not common knowledge nor, in the best case, based upon a common shared model. This paper therefore adopts a set of starting points to create such a common shared model or reference model.

Description of the starting points.

- The framework shall create a solid description of the basic building blocks for netcentric concepts, functions, systems and operations.
- The framework of netcentric principles shall be able to relate the netcentric concepts over the whole spectrum, from the lowest netcentric building blocks till the high level of the netcentric operational functions and the operations themselves.
- The framework of netcentric principles shall be applicable to all types of military operations.
- The netcentric principles approach must allow for legacy systems to be incorporated in the netcentric system of systems.

To derive this framework we will look at netcentric operations from a basic point of view. We will regard netcentric operations from a *system of systems* point of view. The netcentric System of Systems (SoS) is a collection of nodes which interact with each other through a network in order to carry out the netcentric operation. All entities in a netcentric operation,

from organisational elements, systems, combat assets (tanks, jets, ships, soldiers), sensors and weapons or support units are regarded as nodes in a network.
This we will call the *Network-Node Paradigm.*

The Network-Node Paradigm: all entities in a netcentric operation can be regarded as nodes interacting with each other through a communications network.

To establish an unambiguous terminology the following definitions will be used:

Node	an entity in the NEC environment that performs one or more basic netcentric actions and is able to interact with other nodes in the NEC
Node types	the characterisation of a node according to its main basic netcentric action
Netforce	the total collection of connected nodes that work together to perform a specific NEC. This is the total netcentric system of systems
Network	the collection of nodes that perform communication and data distribution actions

By adopting these definitions it is unambiguous what we mean by *network*. In our definition it is restricted to the infrastructure of the whole netcentric environment while the term *netforce* stands for the total netted force.

2.2 Netforce Basic Actions and Node Types

In our netforce concept it is intuitive that there will be different types of nodes performing different types of actions. These node types will reflect the elementary actions or processes that take place in the netcentric SoS. To identify the basic netforce actions we will look at NEC from an operational point of view. In Figure 1 we have the basic notion of NEC according to the UK MoD [2]. It is based upon the OODA loop concept, which is the basic observe, orient, decide and act cycle, and the timely and adequate provision of quality information. This abstraction characterizes NEC as a handling of information in such a way that the desired results are being achieved. These results are to co-ordinate goals and to achieve synchronized actions. NEC in this approach is an information driven process where network enabled sharing of information, intentions, decisions and actions (self-synchronisation) are the resulting processes in the physical, information and cognitive domains. Many other NEC benefits can be derived from these basic characteristics.

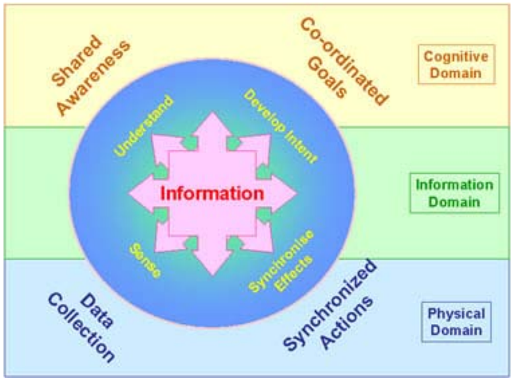


Figure 1 The UK Model of NEC (source UK MoD)

In Figure 2 we have another representation of the major NEC aspects. Here we also see the elements of the OODA loop and some of the most essential NEC capabilities or functions, like shared awareness, synchronized decision making. Many of these concepts can be directly related to equivalent concepts in the UK and NATO NEC [3] approach. In Figure 2 the network is regarded as the enabling 'asset' for the netcentric approach. Important is that in Figure 2 supporting areas are being identified that also need to be addressed in order for NEC to become a success and reality. NEC can only be a sustained success when it is adequately supported by a number of areas, like doctrine, human factors, training, technology, services, the network.

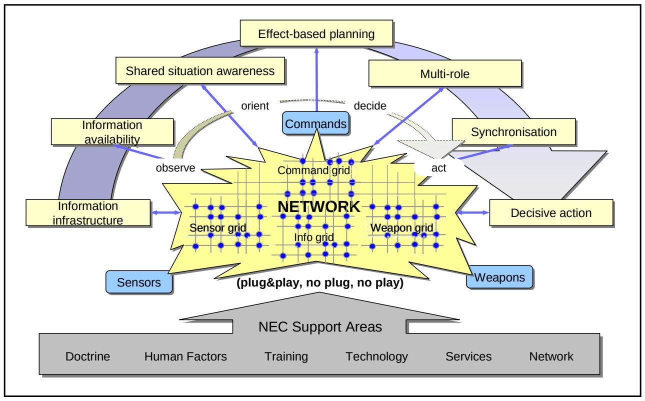


Figure 2 A Basic Model of NEC

When we combine the common set of characterisations of both NEC models and take an operational point of view, we can define a small set of descriptions to characterize NEC:

1. the collection, processing, interpretation of data/information,
2. the provision through the network of quality information to all decision makers,
3. the ability of co-operative and synchronized decision making to create tailored measures,
4. the ability to execute these tailored measures in a timely, accurate and synchronized way.

This set is both information and network driven. It is our key NEC characterisation. In analyzing these key characteristics we derive 6 elementary NEC actions. Five of which are operational and one arising from the necessity of a netcentric support of the operational NEC actions.

The six elementary NEC actions are:

data collection — the action of collecting data and information for use in netcentric operations

information processing & provision — the action of data and information processing, interpretation, association, correlation, fusion, and the provision of that information in the right format to information requestors

communication — the transportation of data and information using various means of transport media

decision making — the action of using the available data and information to decide on possible courses of action

taking action — the action of effectuating the decisions made by the decision making processes

providing support — the action(s) of providing support for the netcentric operation to be carried out and sustained. This class of elementary actions consists of a variety of different support actions.

In our netforce approach we will apply the axiom that these elementary actions can be produced in the netcentric environment by entities or nodes capable of performing one or more of those actions. Consequently we arrive at the following set of basic netcentric nodes with which we will model NEC:

Netforce Actions and Node Types		
Basic actions	*Node types*	
data collection	C	collector
information processing & provision	I	information provider
decision making	D	decider
taking action	E	effector
communicating	Com	communicator
providing support	S	supporter

Table 1 The Basic Netforce Actions and Node Types

Each node in the netforce can be characterized according to the major action it performs. The choice has been made for one information provider node instead of a processor and a provider type. The rationale for this is that in the real world information processing and provision is usually done by an information system combining both functions. And we have chosen for the name ‘ Information provider’ or ‘I provider’ since that reflects the best the information provision towards decider nodes. We have also defined a node type effector for the basic action ‘taking action’. This node type is for all effects that require special effectors, like weapon or task forces. It is obvious that an action can also be to guide or control for instance a collector or a decider node. But for all actions that do not involve C, I, D, S or Com nodes we need to have the concept of the E node.

Node types	**Collector**	**I-Provider**	**Decider**	**Effector**	**Communicator**	**Supporter**
instances	**C**	**I**	**D**	**E**	**Com**	**S**
Node examples Nodes can be basic or composite nodes, persistent or temporal.	space-based	sensor data fusion	governments	weapons	Lk11,16,22	netforce manag ement cell
	MFR nav	SIAP, RAP JCOP	JFC JFACC	task forces	bi-directional LoS	communication management
	IR EO temp	info cell	CAOC	agile mission groups	Satcom, radio HF/UHF	maintenance repair
They can exist on hierarchical levels (strategic, operational, tactical)	human observer	data mining	platform command	viruses, worms (info ops)	internet connector	
	intelligent agent	info system	automated system	pamphlet (psyops)	ATM	

Table 2 An example of Netforce Node Instances

Some examples of nodes are given in Table 2. As can be seen node instances can vary greatly and include human controlled objects as well as fully automated ones, like software agents or viruses in the case of information operations.

Many real world objects exhibit more than one basic netforce action. For instance a naval combatant exhibits all six basic netforce actions. Such objects will be called *composite nodes* in the netforce. They are nodes which consist themselves again of nodes. We will discuss composite nodes in section 3.3.

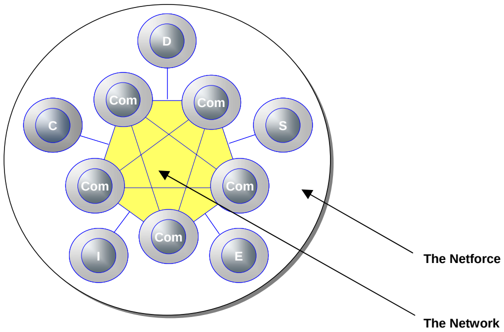


Figure 3 A Schematic View of the Netforce and the Network

A schematic picture of the netforce is given in Figure 3, where we have pictured the network as being built up by a number of communication nodes and the whole netforce as the total collection of all nodes. For graphical reasons we have depicted the non-Com nodes connected to the network made-up by the Com nodes. The actual interfacing mechanism will be discussed in section 3.1

2.3 The Elementary Node Properties

Nodes are the basis of the netforce reference model. The property 'type' of a node is only a part of what we need to know about nodes in order to use them for understanding the NEC concepts we referred to in section 1. For modelling we need to know a complete set of properties associated to nodes. In this section we will discuss this set of elementary node properties.

In describing nodes in a netcentric environment we have to be able to fully characterize and specify the nature and behaviour of nodes. Some of these characteristics or properties are static and others are dynamic of nature. There are properties specifying the nature of the node, like its identity and its structure properties. The node type is part of such an identity property. Other properties involve control and behavioural aspects of the node, like status, capability, control, security, integration capability into the network and interactions with other nodes. Consequently the specification of a node is a function of its elementary properties:

$$Node_{spec}=f(P_1, P_2, P_3, \ldots, P_n),$$

where P_1 till P_n are the elementary node properties. In Figure 4 a characterisation of these properties is shown.

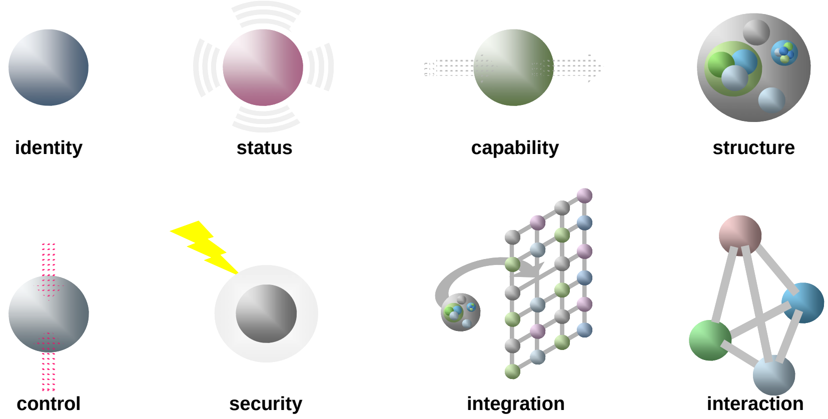


Figure 4 The Elementary Node Properties

Node properties are not necessarily singular values. On the contrary, a property will often exist of sub-properties. They can be a complex specification, like specifying the capability of the node in terms of quality of service. For the sake of simplicity and understanding we have grouped the sub-property characteristics into the set as displayed in Figure 4 and as discussed briefly in the list below.

- $P_{identity}$: this property uniquely identifies a node from all other nodes in the network. It has identification, type and localisation sub-properties. The identification can be an IP address, the type is the node type as we discussed before, while its location may for instance be in GPS format.
- P_{status}: the status property involves the specification(s) about the operational status of the node. It indicates whether a node is operational (or the operational readiness level), in training, in maintenance or repair, in transit, etc. For different node types this property can have different specifications tailored to the specific node type.
- $P_{capability}$: this property is a specification of the operational capability of the node and consequently very much related to the specific node type. It is obvious that each node type will have its own specific capability specification. In later sections in this document we will address the capability specification in more detail. We will adopt a *Quality of Service* (QoS) approach to specify the node capability property.
- $P_{structure}$: many nodes have a composite structure, which means they consist of several sub-nodes. The structure property specifies the internal structure of the node. By introducing the notion of composite nodes we allow nodes to be described on more than one level of detail as may be required by specific applications.
- $P_{control}$: the behaviour and especially the capability of the node needs to be controllable, sometimes even from outside the node. The control property describes the mechanism and formalism that controls the capability of the node. It can be regarded more or less as the node interface. It allows for specific node types, like collectors (e.g. a radar) or effectors (like weapons) to have generic interfaces. In later sections we will address this in more detail.
- $P_{security}$: in the netcentric environment the concept of security is of vital importance. In the NFRM security specification starts already on the basic node level. The security aspect can differ substantially for different node types. It can be absent when no security aspects are applicable for a specific node or it can be a complex property describing under what conditions specific authorized users (other nodes) may have access to specific parts of the node. In the case of composite nodes (see section 3.3) we can even have multi-layered security when going from the node to the sub-node level.
- $P_{integration}$: one of the most essential concept in the network-node based approach is how nodes interface with the network. Nodes need to be able to integrate into a network, make themselves known to the network and must be able to co-operate with other nodes. The integration property contains the integration function of a node. The mechanism used in the netforce approach is described in detail in section 3.1.
- $P_{interaction}$: the last property deals with the relations between a node and other nodes. There is a number of different interactions a node can have with other nodes, much depending on the type of nodes involved. It allows us to specify hierarchical interactions (e.g. between organisational elements, or client-server type of interactions). In section 4 these different interactions will be discussed.

3 The Basic Node Related Concepts

In section 2 the nodes and their elementary properties were introduced and shortly described. It gives a basic understanding of the direct consequences of applying the network-node paradigm: it provides us with the concept of the netforce node and its set of elementary properties for nodes. The netforce node is the starting point to derive and define the basic concepts from which the netforce reference model is constructed.

This section discusses the basic concepts directly related to single nodes and their properties. Multi-node behaviour arising from interacting nodes will be discussed in sections 4 and 5. We will start here with the most important concept: *how does a node interface with the netforce and with the network?* Having defined this mechanism many of the other properties are more or less automatically addressed and discussed too.

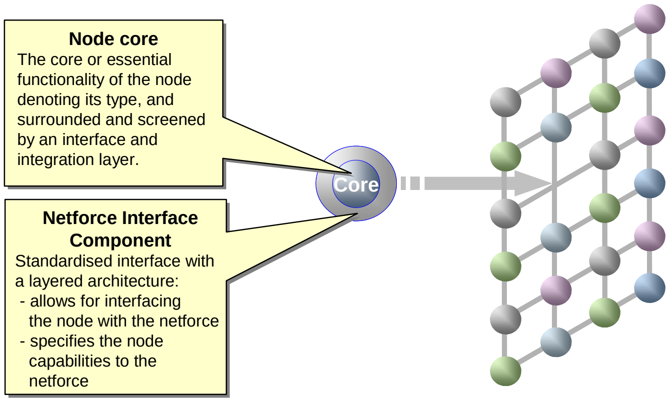
3.1 Node Interfacing and the Netforce

In a netcentric environment one of the most important concepts is how nodes integrate and interface with the netforce. To derive the formalisms that perform the interfacing and integration we will define a number of high level requirements regarding node interfacing with the netforce. The following set of high level requirements is formulated:

Netforce Interface Requirements

- In line with the dynamic nature of NEC each node must be able to dynamically plug & play in the netforce structure. This may be realized with a logon/logoff protocol or registration service.
- In order for the node capabilities or services to be used in an effective and efficient manner, they must be known to specific other nodes in the netforce. This can be realized with a node resource management service.
- Changing capabilities of nodes need to be promulgated to the netforce. This may be realized with a status reporting function or protocol.
- Node access, node control and node use is to be regulated. This may be realized with a node access control, authentication and security function.
- Legacy systems must be able to 'connect/integrate' with the netforce also. In other words: it must be able to make legacy systems netforce compliant. This may be realized with a kind of encapsulation mechanism.

The way we have met all these requirements is to define a layered model of the node architecture as is shown in Figure 5.



Node core
The core or essential functionality of the node denoting its type, and surrounded and screened by an interface and integration layer.

Netforce Interface Component
Standardised interface with a layered architecture:
- allows for interfacing the node with the netforce
- specifies the node capabilities to the netforce

Figure 5 The Node-Netforce Integration

A distinction is made between the *node core functionality* (one or more basic netforce actions) and the functionality required to function in a netforce environment. Conceptually this functionality can be regarded as residing in a *node interface layer* surrounding the node's core functionality. This layered approach is also conceived to fulfil the last of the netforce interface requirements of enabling legacy systems to be integrated to a netforce environment. By adopting a layered structure we can shield the internals of a node from the outside world and allow for the outer layers to exhibit the required netforce behaviour. The netforce shell around the node's core consists of three layers. This layered structure is shown in Figure 6.

The netforce interface comprises three distinct layers:

- *the network communications component*: this component provides the node with the means to connect itself to the network.
- *the node interface component:* the component which provides the translation of external node commands (e.g. sensor settings) to internal node commands, and consequently controls the node's capability (associated with the node control property)
- *the node specification component:* the component that specifies the node identity and its services to the netforce.

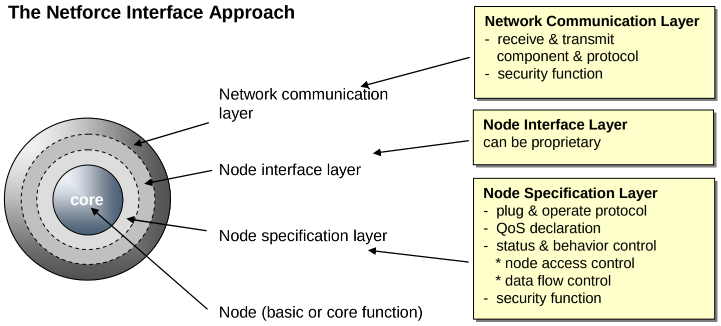

The Netforce Interface Approach
core
Network communication layer
Node interface layer
Node specification layer
Node (basic or core function)
Network Communication Layer
- receive & transmit component & protocol
- security function
Node Interface Layer
can be proprietary
Node Specification Layer
- plug & operate protocol
- QoS declaration
- status & behavior control
* node access control
* data flow control
- security function

Figure 6 The Layered Node Structure

Figure 6 is a functional view of the node structure, where we have regarded the three components as layers around the core functionality. We can also represent this layered structure in a component or modular view, where it better resembles the architecture of the node structure.

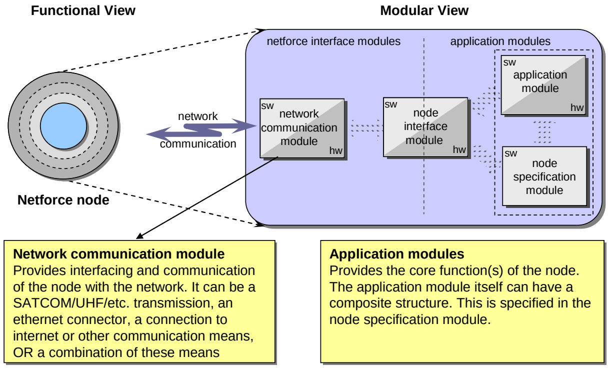

Functional View
Modular View
netforce interface modules
application modules
sw
application module
hw
network
communication
sw
network communication module
hw
sw
node interface module
hw
sw
node specification module
Netforce node
Network communication module
Provides interfacing and communication of the node with the network. It can be a SATCOM/UHF/etc. transmission, an ethernet connector, a connection to internet or other communication means, OR a combination of these means
Application modules
Provides the core function(s) of the node. The application module itself can have a composite structure. This is specified in the node specification module.

Figure 7 The Modular Architecture of Netforce Nodes

In Figure 7 we have given a modular view on the internal architecture of netforce nodes. The modules are equivalent with the layers described in Figure 6. In the next sections we will give a description of these node interface components or modules.

3.1.1 The Network Communications Component

The *network communications module NCom* controls the actual connection of a node with the netforce environment or more specific *the network.* It enables the transfer of data between a node and the network. It can do that, if required, in a secure way. Therefore security features can be part of the NCom module. The NCom component or module can provide the network connection in different ways. It can be a simple internet connection, a Bluetooth connection or as much as a full-blown transceiver (HF, VHF, UHF, SATCOM, laser, etc) component. In the latter case we can then speak of a composite node, where the NCom component is actually a sub node of the type ‘Com’.

3.1.2 The Node Interface Component

To enable the node core functionality to be addressed from the outside, the *node interface component/module NInt* provides an interface for accessing and controlling the node specific functions. The NInt can be a proprietary interface and/or a generic one, defined by a public organisation. This approach is compatible with several existing initiatives to define generic interfaces for specific objects. We mention the MTMD Open Architecture Working Group [4] and the initiatives of the OMG (Object Management Group) [5]. The NFRM provides a placeholder for this external work to be fitted into the reference model.
In the case of composite nodes the NInt can allow underlying sub node functionalities to be accessed.

3.1.3 The Node Specification Component

There is a strong relation between the node interface and the *node specification component NSpec*. The NSpec component specifies the node capabilities according to a Quality of Service (QoS) approach. This means the node interface and the node specification component must be consistent with respect to these capabilities. The NSpec component not only provides a complete specification of the node capabilities but also with respect to security, access control and some other functions to be mentioned in this section.
For node specification we have chosen for a Quality of Service (QoS) approach in the NFRM since it enables nodes to make their capabilities known to the netforce in a formalized way and to allow those capabilities to be shared in a controlled way.
The NSpec component declares several essential node properties to the netforce. This is done in the logon/logoff or registration function. This function is activated when a node enters or leaves the netforce structure. Also, when the node is already embedded or integrated into the netforce, the node properties can be requested by specific netforce or network functions (to be discussed later in this paper). The security part of the NSpec has to verify that only properly authorized requests are serviced.
Specific tasks of the NSpec component are:

- the logon/logoff or registration function;
- the node structure (composition) specification;
- the QoS specification of the node capabilities that are available to the netforce;
- the security function, including node access control.

Since nodes can differ substantially from each other (in type and capability) the NSpec will differ accordingly. It provides a complete specification of the node, its behaviour and its capability to the netforce to enable optimized and controlled use of the node by the netforce. See section 4.2 for a discussion on QoS.

3.2 Node Security, Access Control and Ownership

Node security and access control have been mentioned in the preceding sections a couple of times. In a network environment security is of the utmost importance, which is why we have treated security as an elementary property of nodes. In our discussions about security and control in the netforce environment we distinguish security, access control and ownership of a node.

Security is part of the NCom component of the node interface, where it can provide a secure connection of a node to the network. It is also part of the NSpec component where it can specify which users are authorized to use, under what conditions, specific parts of the node’s capabilities. In this way security is focussed on access control. The security property however can also be a simple security classification of the node, like NATO Confidential or SECRET, or a national security classification. In the case of a composite node security can be specified for the node as well as for the sub nodes (see section 3.3) creating multi-layered security.

In dealing with the security and access control properties of nodes it should be realized that these properties must receive an initial setting. Even more, these values can sometimes change too. For this reason we have introduced the concept of *node ownership*. By *ownership* we mean to specify who has control over the security and access control settings of a node. In netforce terms this will be a node, not necessarily the node itself but it can also be another node where the ownerships resides. The concept of ownership allows for mechanisms of changing the classifications of specific nodes (the security and access control properties) according to changing needs in the operational environment, and it provides a mechanism where ownership can be transferred too. *Ownership handover* can be convenient for instance in the case of UAVs (unmanned air vehicles) in a theatre where the control of a UAV is transferred from one node to another.

The management of security and access control is performed by a netforce or network service 'Security Management'. This is discussed in some more detail in section 5.2.

3.3 Composite Nodes

An elementary property of each node is its structure. A node is not necessarily a monolithic, unstructured node. In fact, most real world nodes have multi-nodal capabilities and they consequently have a structured nature, implying they exist of other sub-nodes which together make up the overall node. An example is a naval combatant. It has observation, I-provider, effector, communication and decision capabilities. Some of these capabilities are in themselves again of a composite nature. Thus, a combatant can be thought of as being constructed by its specific sub-nodes. Other examples are a brigade, a jet fighter, or even an optically guided bomb (collector and effector functions) can be regarded as a composite node.

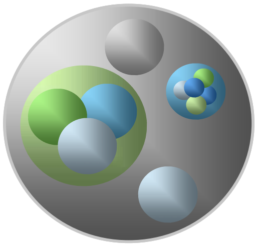


Figure 8 The Notion of Composite Nodes

In *Figure 8* this is conceptually shown as the little spheres residing inside the larger sphere. Each of the sub nodes can be regarded again as a node. This means that we have a nested structure of interface layers the deeper we go into a node structure. This allows for node access control and security to be specified at the level of the sub-nodes itself.

A number of issues are important with respect to the treatment of composite nodes. These are the declaration of the node structure to the netforce, the access control to the sub-nodes, and the maintenance of the netforce integrity with respect to node composition.

Logon/logoff function for composite nodes:
In the logon/logoff (registration) procedure for composite nodes the internal structure must be specified. This can be done in several ways. When no permissions will be given to other netforce nodes to access the components of a composite node, or when it is required to screen node internals from others, it is not required to specify the node structure in terms of its components. However, when it is allowed that (part of) sub-node capabilities can be accessed or even controlled by other nodes or netforce functions, then it is required to declare these sub-nodes to the netforce. Thus we have the following options for composite node specification:

Composite Node Registration Modes
1. As a composite node fully decomposed into its constituent sub nodes;
2. As a composite node partially decomposed into only those sub-nodes to which access will be granted;
3. As a non-decomposed node but with QoS declaration of its multi-function capabilities.

When a composite node logs off from the netforce all its sub-nodes need to be logged off as well in order to maintain the integrity of the netforce structure. This integrity maintenance is handled by the netforce node management function, which uses the so-called Netforce Structure database (NFSdb) in which all data from the logon/logoff procedures is stored. The netforce management function and the NFSdb are discussed in section 5.2.

The mechanism of multi-layered security and access control allows for a flexible means of using specific sub-node capabilities. Some of these means are necessary for force level functions, like collector or effector management (see section 5.1). For instance, in the case of a naval combatant, it can be specified in the NSpec layer of the node whether access and control is allowed for other nodes to the combatant’s collector and effector sub-nodes. Not in all situations it is permitted or even advisable that a ship’s sensors or weapons can be controlled from the outside. The NSpec layers of the node and its sub-nodes provide a mechanism where this access and control can be regulated.

3.4 Node Types

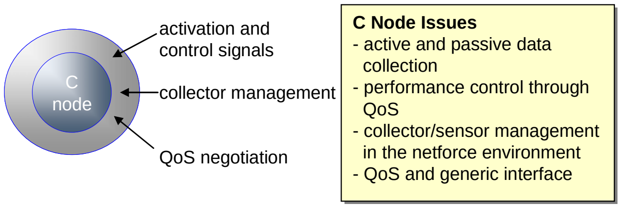
To illustrate some of the node types we will in this section focus on those node types that are primarily involved in the process of creating situation awareness (SA) which is required for decision making. In the SA process the following node types are involved: the collector node that gathers data and information, the I-provider node that processes and provides information and the decider node that uses the information to create the situation awareness upon which decisions are based. This is the C-I-D chain. The Com nodes are also involved in this process, since they distribute data and information.

3.4.1 C nodes

C nodes are collectors of data and information. They provide the basic NEC action of data collection. They can do this in an active or passive or mixed way. In the remainder of this document we will usually not make the distinction anymore between data and information as it is not really relevant for our purposes here.

C nodes can vary from sensors (radar, MRF, IR, EO, pressure, temp, movement) to data collectors like intelligent data collecting agents, data mining programs, etc. All data or information collection entities in the netforce environment can be regarded as data collection nodes. This means that the NFRM is not restricted to the conventional notion of data collection devices like a radar, but it also allows for different kind of collector nodes encountered for instance in information operations or agencies (e.g. for Intel).

The behaviour and performance of C-nodes can be controlled through the NSpec module (see 3.1.3). Performance and control needs to be specified in the QoS specification of a C-node. This is part of the overall node interface and is accessed through the NInt component (see 3.1.2). For some C-nodes even a generic interface can be defined with respect to activation and control and with respect to the quality of the data they provide (see also the NInt discussion).



C Node Issues
- active and passive data collection
- performance control through QoS
- collector/sensor management in the netforce environment
- QoS and generic interface

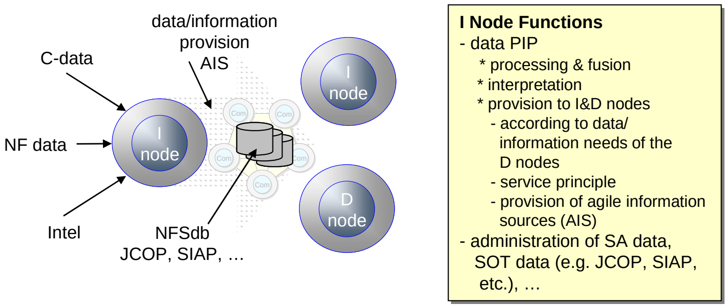
Figure 9 The C Node

If applicable to a collector, specific modes of the data collection function can be requested or controlled through the QoS mechanism. This can be a part of an overall sensor management function, which manages and controls the functioning of specific C nodes. Sensor management is a generic netforce function and will be discussed later in this document. Sensor management works through the NInt onto the NSpec of the C nodes.

Access to a C node from somewhere in the netforce is controlled by the security part of the NSpec. This is the managing mechanism for access and control of the node for authorized users of that node. This is not only valid for C nodes but for all node types. The use of the full potential of the node interface concept with respect to access control is only necessary when a particular node is accessible from the netforce by other nodes than the node itself. When a node is a dedicated node in a specific system and only accessible by that system (this will usually be the I-part of a system) then it is not necessary to use and specify all related interface parameters.

3.4.2 I nodes

The C nodes provide their data to the network and in particular to I nodes (using Com nodes). The I-node is a key concept in the whole netforce approach. The I-nodes are directly related to the essential mechanism of providing relevant and accurate information at the right moment in the right way (level of detail, timeliness, etc.) to the right decision makers. I-nodes are functioning as information processing & provision centres for the netforce. In an optimized netforce architecture the I node capability should ideally be distributed in such a way that the information needs of D-nodes can be fulfilled in an optimal way (speed, latency, accuracy, level of detail, format, etc.). The distribution and functionality of the I nodes is part of the design and configuration process of the architecture of the environment.



I Node Functions
- data PIP
  * processing & fusion
  * interpretation
  * provision to I&D nodes
    - according to data/ information needs of the D nodes
    - service principle
    - provision of agile information sources (AIS)
- administration of SA data, SOT data (e.g. JCOP, SIAP, etc.), …

Figure 10 The I node

I nodes and Situational Awareness (SA)

The I nodes are the netforce mechanism to create and maintain dedicated situation awareness information sources required for the decision making process (D nodes). I nodes create and maintain for instance the Joint Common Strategic Picture (JCSP), the Joint Common Operational Picture (JCOP) (like the SIAP [6] for the air component) and the Joint Common Tactical Picture (JCTP). These pictures distinguish themselves from each other by the level of detail and the timeliness of the information contained in those pictures. We will see in later sections that the I nodes also provide the mechanism that maintains the Netforce Structure Database (NFSdb), which contains the data about the netforce structure and its components (nodes, QoS, access control, security, services and functions).

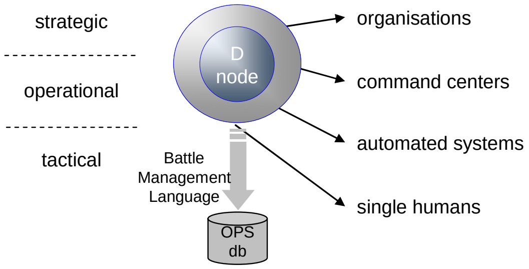
There are several classes of I-nodes since not all I-nodes will or need to have full capability. Data fusion centers or systems are an example of I nodes, but also the systems that create a JCOP. In general I nodes in the netforce concepts are information systems that store, fuse, correlate, and process data and information in such a way that it can be presented to users (D nodes) in the format required for fast and efficient decision making. I nodes can be on the strategic, operational and tactical (SOT) level. The information processing and providing capability in the netforce can vary from a generic ‘publish and subscribe’ mechanism available for all authorized users in the netforce, till very dedicated systems for a specific D node only, like a combat management system (CMS) for a fighter aircraft, a tank , a ship, etc.

Agile Information Source (AIS)

One of the NEC concepts is the Agile Mission Group (AMG) [7]. An AMG is the result of the ability to assemble a collection of assets in the operational arena to obtain a specific objective in a short time and in an effective and efficient way. An AMG may have a lifetime of just the mission it is created for. Because of the ad hoc nature of an AMG (either with respect to its creation or its mission) the information need will also be of an ad hoc nature. It is therefore not sufficient to only identify the AMG as a NEC concept, but we also have to acknowledge its natural counterpart in the NFRM: the Agile Information Source (AIS). A true netcentric environment should allow for the information needs of an AMG to be serviced in the same creative and ad hoc way as the AMG is created or its mission assigned. This means that I node capability must be able to be dynamically configured in the same way as a AMG is created. An AMG can be seen as a composite node having D node capabilities in order to decide on the right actions (see the discussion on D nodes). The D node capability of an AMG has its own specific information needs. This means that in a netcentric environment, which allows for the creation of AMGs, it should also be possible that specific nodes can be configured in such a way that the information needs of an AMG can be fulfilled. This will usually be a C-I-D chain since the C-I combination provides the situation awareness for the D part of the AMG. Using the already identified concept of AMG we have derived from that an equally essential concept of AIS.

3.4.3 D nodes

D nodes exhibit command & control behaviour or more specific *decision capability*. The associated basic NEC action is *decision making*. A D node is therefore predominantly characterized by the decision process it stands for. As such, a D node can be human decision making or machine decision making or a mix of both. In principle, a D node can even be an automated system performing decision making tasks without human supervision. With D nodes we can model organisational structures (CJTF, HQ, CAOC, ship-based ops centers, or even a single human (like a FAC: forward air controller)) on strategic, operational and tactical levels. Collaborating D nodes can result in polarisation and synchronisation. That means that D nodes can work together to obtain a common goal and synchronize their actions in time (self-synchronisation). The information demand of D nodes drive behaviours of specific C, I and Com nodes that can fulfil that demand. The I-D interaction is the mechanism that creates the situation awareness for the D nodes (see previous section). The results of decision making can influence all nodes. D nodes generate policies, operational goals (commander's intent), RoE, weapon deployment decisions, etc.



D Node Issues to be addressed
- projection on organisational and systems views
- human-machine interfacing
- organizational levels, organizations
- decision making:
  * polarisation and synchronisation
  * collaborative decision making
- d/I requestor: link to generic operational interfaces
- generates the OPSdb and BML

Figure 11 The D node

An important concept in NEC is collaborative decision making and synchronisation of decision making. In netforce terms this is the collective behaviour of sets of D nodes using a shared I node system through a dedicated part of the network (involved Com nodes). This is the I_nD_m interaction, to indicate that multiple D nodes and I nodes (it might be just one I node) are involved. See the next section for a discussion of the netforce interactions.

3.4.3.1 Formalisation Aspects of the C2 process

With the association of the decision making or the command & control process with a node in the netforce environment and by adopting the QoS formalism for them as well, the need for formalisation of the decision making or C2 process becomes more and more urgent. D nodes may for instance be used in the netforce as resource, just like the other node types. To be able to do that in a proper way it is necessary to know the quality and specific characteristics of a D node. In order to make the decision process of a D node function correctly it would help when the information needs of a D nodes can be described in such a way that automatic information provision could be facilitated. Also a netcentric concept like self synchronisation benefit from a more formal understanding of underlying principles.

As a result of netcentric thinking and adopting the netforce principles there exist a number of areas where formalisation of the C2 process can be applied. Based upon a simple 'input-process-output' model for a D node, we identify the following categories:

Formalisation categories of C2 processes:
- the task description (scope and type of decisions) of a D node (the process itself);
- the information need description of a D node, based upon its tasks (the input part);
- a description of the decisions resulting from the decision making process (the output part).

The task description of the node can be used in two ways: to derive and specify the information set it needs in order to create its situational awareness from, and to derive the decision space for that node in which its decisions take place.

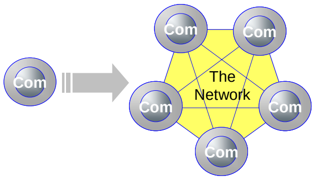
The information need can be regarded as a function of the D node tasks and has a relation to specific information providers and collectors.

When we have a formalism to describe the decisions or actions, we can use that for instance in synchronizing decision making processes. A current area of exploration is *Battle Management Language (BML)* [8]. Until now the decisions made by deciders are usually not strictly formalized (except for some exceptions like an ATO (air tasking order)). This means they are not according to a generalized format in which command decisions can be formulated. A current area of investigation is how to formulate command decisions in a generalized formalized way. In achieving such a formalisation it can also be used for modelling & simulation as is demonstrated in [8].

Current work in the NFRM deals with these formalisation aspects of the NFRM and will be applied to create semi-automatic management functions and services in the netforce environment.

3.4.4 Com nodes

The Com node in the netforce is the entity that transports data from one place to others. In its simplest form a Com node has two basic actions: receive and transmit. Examples of Com nodes are radio transmitters, SATCOM, laser communication, etc. In principle even the combination of the human ear and mouth can be regarded as a Com node, provided we could address it in the netforce. Collaborating Com nodes create the communication network, or network for short. This can be a multi-segmented network with gateways and bridges, with segments dedicated to special users. Network configuration heavily depends on available means, bandwidth and security requirements. The network in the netforce is the means through which all data is transported. Also internet can be regarded as a Com node; actually internet is a composite node with I and Com capabilities.

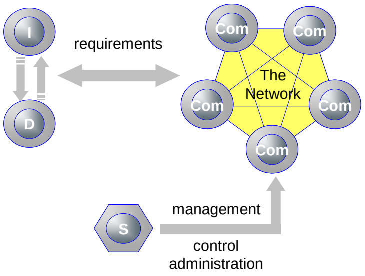


Com Node Issues
- two basic actions: transmit & receive
- transmission media (VHF, UHV, Satcom, laser, acoustic, electric, etc.
- does not interact with the data
- collections of Com-nodes create networks or communication grids
- security: encryption capability
- the network need network management functions

Figure 12 Com node create the network

A characteristic of a pure Com node is that it does not interact with the data: this means it does not semantically change the data like an I node does (it does allow for encryption though). Its function is to receive and transport data without processing it. This principle makes a data link a composite node, with I and Com capabilities. The transmission part of a data link, like Link16 for instance, is the Com part of the link, while the link processor is the I part. This is according to the current situation where different processors are used for a data link.

As said before an intrinsic property of each node is security. This is particularly true for Com nodes: in a networked environment the security properties of the Com nodes are a crucial element to ensure that data is only available to authorized users (i.e. nodes) and can not be altered or tempered with. Encryption and multi-layered security are key concepts for Com nodes. It is outside the scope of this paper to go into more detail on the security aspect of Com nodes in the netforce environment since we focus here only in explaining the netforce principles at a high level. (See also section 5.2 on security management.)



Network Issues
- service requirements from predominantly the I-D interaction
- network management
- network optimisation
  * static and dynamic
  * service negotiation
- network security, resilience

Figure 13 Network configuration

The collective behaviour of Com nodes, the Com-Com interactions, need to be managed in order to provide the netforce with the required communication capability. The capability of the network depends heavily on the information needs of the D nodes. Therefore the I-D interaction is the guiding mechanism to optimize the network configuration, where static as well as dynamic information demands needs to be taken into account. This is done by the communication management services (see section 5.3).

4 The Netforce Nodes and their Interactions

In section 3 we discussed some of the basic netforce principles directly associated with the node concept itself. By starting with the node interfacing to the network we dealt with node properties like node ID, capability, structure, security, access control.
In this section we will extend the netforce principles by looking at the node interactions. This implies a transition from single node to multi-node concepts. In the previous section during the discussion of the nodes we already touched some specific interactions (like the I-D interaction), but we will introduce them here in a more formalised and structured way.

The netcentric environment is a dynamic system of system in which interacting nodes create the desired results with respect to shared situation awareness, synchronized decision making and resulting synchronized actions. To understand the multi-node interactions we will start by examining node interactions in a simplified way, and then extend the concept in section 5 to multi-node interactions where we will look at functions and services.

4.1 Simple Node Interactions

In the netcentric environment interacting nodes exchange information, and this information exchange occurs through the network. This is the starting point we adopt for node interactions. This implies that when we look for instance at a D-node interacting with a I-node, the network, or to be more precise one or more Com-nodes, always plays a role as the intermediate transmission medium. In its simplest form a node-node interaction can be represented as two nodes exchanging information through the network as is shown in Figure 14.

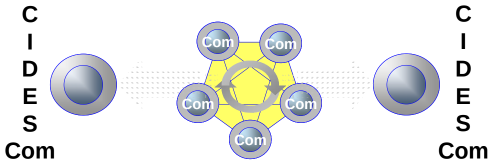
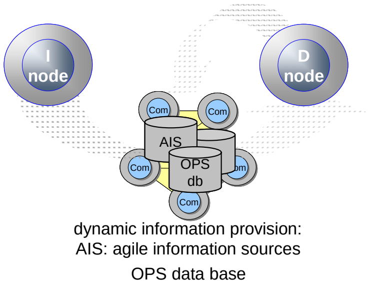


Figure 14 Representation of node interaction

The (non exhaustive) list below gives some of the most characteristic interactions between node and illustrates what real world processes can be associated with that interaction.

-	C-I	information creation
-	I-I	information processing & availability
-	I-D	(shared) situation awareness
-	D-D	synchronized decision making
-	D-E	effector assignment
-	E-I	guided action, engagement
-	E-E	synchronized engagement

For simplicity we left out the Com nodes since they are always involved in the interactions. We will briefly review these basic node interactions to understand their meaning. We start with one of the most important interactions in the netcentric environment: the interaction that provides decision makers with the necessary information to make the right decisions: this is the I-D interaction (see Figure 15).


I
node
D
node
Com
Com
AIS
OPS
db
Com
Com
Com
dynamic information provision:
AIS: agile information sources
OPS data base

I-D Interaction
- pre-defined and ad hoc data and information demands (adaptation to situation)
- static and dynamic data distribution functions: so called “agile information sources (AIS)”
- I-D interaction generates operational information requirement for the C-I interaction

Figure 15 The I-D Interaction

The I-D interaction

Obtaining the right information for decision making is a key in any operation. The ‘right’ information depends strongly on the specific tasks the decision makers have to perform. A decision maker needs to obtain the right situation awareness to be able to asses alternative courses of action (CoA) and to evaluate possible consequences of the decision. As we have seen in previous sections the creation of situation awareness is a result of the interaction of a D node with its supplying I nodes (with respect to information). The associated I nodes provide the information processing power the D nodes requires. The formalized descriptions of the C2 process can be applied to this interaction (see section 3.4.3.1).

The C-I interaction

The C-I interaction is a process of creating the information sets for decision makers in the netforce environment. This interaction plays a significant role in well-known processes like picture compilation and sensor data fusion. An important process like sensor management involves this particular interaction (see section 5.1). A specific C-I interaction can be a result of a need of a D node. An example of this is the creation of an AMG which may require an AIS (see section 3.4.2).

The I-I interaction

The interaction between I nodes comprises updates of databases and also data replication mechanisms. Different replication mechanisms can be applied and are not prescribed by the NFRM. An example is the data replication mechanism used in MIP [9]. The I-I interaction is also the mechanism for providing AIS as discussed in section 3.4.2. A combination of information from different I nodes can fulfil the information demand of an AMG.

The D-D interaction

The D-D interaction takes place between different decision nodes. This can be *vertical* (usually *hierarchical)* interactions (like authorisation of command decisions and dissemination of operational plans) or *horizontal* interactions, involving consultation or synchronisation, or a mix of both. Common netcentric terms associated with this interaction are (self) *synchronisation*, *co-operative decision making* and *BML*.
Techniques which can be applied to establish a D-D interaction are for instance *VTC* (video teleconferencing), *chat rooms*, or *collaborative virtual planning environments*. In the netforce environment these techniques are represented as the capability of an I node.

The D-E interaction

The D-E interaction links decision makers with selected effectors and is usually a direct result of the decision making process. This can range from creating a AMG till the selection and activation of a missile. As such, *weapon assignment* and *co-ordinated engagement* are part of this interaction.

The E-I interaction

The E-I interaction takes place between an effector and one or more information sources that provide the effector with the latest data updates to effectively execute the effect. This is the so-called *guided action*. The uplink to a guided missile is an example of this interaction. Another example is *co-operative engagement*, where data sources and effectors work together to create the desired results.

The E-E interaction

This particular interaction takes place between effectors themselves. It is the actual carrying out of a synchronized action by effectors. In order for effectors to exhibit this kind of behaviour it is required they are able to sense the actions of other effectors and therefore need to be composite nodes, with C, I and D capability. They are however predominantly characterized as E nodes. Concepts like *swarming* [10] are part of the E-E interaction. The E-E interaction can take place in the *physical* domain as well as in the *information* domain (e.g. as part of information operations).

4.2 Quality of Service

One of the mechanism that is used in the node interactions is the Quality of Service (QoS) principle. In Figure 16 we have depicted the concept of QoS.

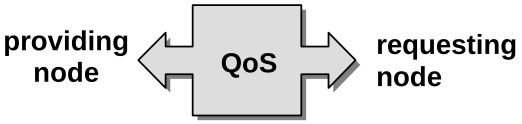


Figure 16 The Quality of Service Principle

The purpose of the QoS mechanism is to provide a means to optimally use the capabilities of nodes by the netforce (other nodes), static as well as dynamic. The QoS can be used as the negotiation mechanism to (partially) optimize parts of the netforce environments according to dynamic operational needs. In the NFRM the QoS mechanism can in principle be used for every node type. A lot of QoS work is carried out for network optimisation [11], but with respect to QoS. In the NEC environment this work is just starting.

The QoS specification of a node contains the following data:

- the node identification;
- the type of services provided by the node. The service declaration is stored in the NFSdb, where the administration of available services to the netforce can take place (see section 5.5.1);
- the specification of the provided services. This means that for specific node types we need to be able to specify in a manageable way the service it provides (see the discussion below);
- access control parameters, specifying the condition under which other nodes or services of functions can use or control the provides services. This also comprises the notion of ownership as discussed in section 3.2.

For each node type there are specific QoS related issues that need to be specified, studied or yet to be solved. Some of these are:

C nodes	the C_QoS specifies the collector quality, like accuracy and timeliness of the data provided. It is also be used in a function like collector (sensor) management, which will be discussed in the next section. The development of standardised collector interfaces [4], [5], can contribute to defining C-QoS.

I nodes specification of the quality of the information processing and provision mechanism. This can consist of many aspects, like the quality of information distribution, replication, the quality of the information itself, etc. D node can use the I_QoS to optimize their information demands. The I_QoS and the D_QoS are strongly related and a more formalized way of describing these QoS is needed (see section 3.4.3.1).

D nodes for D nodes the QoS means a specification of the decision making process. To be able to do that in a standardized way requires still considerable study and effort. There is a strong relation with the formalisation of the C2 process we already discussed in section 3.4.3.1. The whole concept of D_QoS in the netcentric environment still requires a substantial amount of R&D. Nevertheless, in the NFRM we have created the placeholders and handles for the QoS mechanism.

Com nodes for the Com nodes the QoS mechanism provides a means of negotiating bandwidth and quality of communications according to operational needs, either for a single Com or for a network (segment).

E nodes for specific effectors one might wish to specify precision, amount of effect, time of effect, etc. Here too no standardized QoS specifications have yet been agreed upon.

S nodes support nodes occur in the NFRM in a large variety and consequently this is also valid for the S_QoS. Because of the many aspects related to S nodes this requires a separate discussion.

5 Netforce Functions and Services

In our stepwise derivation process of defining the netforce principles we have completed the first steps which dealt primarily with the static principles of the netforce: the node definitions with their types and properties, their structure, the interfacing and the relations between them. We are now ready to take the next step in going to the dynamic netforce principles. We will use the elementary building blocks to derive those principles that describe the behavioural aspects of NEC. In netforce terminology these are the functions and services (F&S) which manage and control the netforce and which prevent the netforce from becoming a chaotic behaving system of nodes.

A function or a service is the management, control of multiple node capabilities to collectively and coherently achieve a specific purpose. In our discussion we will use the term *function* for a more operational oriented node interaction and the term *service* for a more support oriented interaction.
A difference can be made between *network* and *netforce* functions or services. For the netforce we distinguish between the *operationally oriented functions* and *support services*. Because we regard the network as the enabler for the netcentric concept we will predominantly use the term *'service'* for the network.

Functions and services can be described in two different ways. When we consider a function or service from the level of the participating nodes, we can talk about a *inter-node function* or *service*. In that case all interactions and interfaces with the involved nodes need to be specified. When we consider a function or service from a higher level, like a function or service occurring inside a composite node, then we can talk about an *intra-node function or service* and a black box type of specification suffices on the composite level. The difference between an *inter-node* and an *intra-node F&S* is therefore the level of abstraction and the required level of specification. When we treat a set of nodes as a composite object, then the F&S inside that set become intra-node F&S at the composite level, and a different way of specifying them can be used. An example is a CMS (combat management system) of a naval combatant. At the level of a naval task force a ship CMS is an intra-node function (also called a platform function). A so-called force level TEWA (threat evaluation and weapon assignment) function is an inter-node function. here the interface and behaviour specification with each node is required. In our situation today we still have many intra-node functions for all kind of platforms (nodes), like tanks, ships, aircrafts. Although the same, these functions of similar platforms are often not connected to each other yet, or at best only in a rudimentary way. We are in a transition process where these intra-node functions become connected to each other and thereby creating an inter-node function. When dealing with F&S we therefore have to take into account existing intra-node F&S and how to interface with them or how to integrate them into an inter-node function. In our netforce discussion here we will only address the inter-node F&S.

An (non exhaustive) indication of the netforce functions and services is given in Table 3.

Netforce Functions and Services	
Netforce Functions	*Network Services*
Operational Functions	“Standard” Communication Services
Support Services	Network Optimisation
Node management	Security Management
Data Management	
Security Management	

Table 3 Examples of Netforce Functions and Services

5.1 Generic Netforce Functions and Services (GF & GS)

An agreed set of generic netforce functions (GF) and services (GS) with ‘standardized’ interfaces and architecture would considerably increase interoperability between different national systems. In a step towards deriving more operationally directed netforce principles like GF&GS we adopt the same operational view as we already did in section 2. In the derivation of these netforce GF&GS we use the following set of guidelines:

GF&GS Guidelines

- focus on the operational process and on the support of the operational process;
- based on the elementary OODA loop concept: observe, orient, decide and act;
- based on the netforce node types;
- taking into account real world concepts and systems like SA (situation awareness), TEWA (threat evaluation and weapon assignment) and CEC-like systems (co-operative engagement capability);
- remain as generic and independent of warfare area or operation types as possible;
- a GF or GS can be multi-nation (a coalition) function or service.

Applying this list of guidelines (except the last one) we have formulated the following set of eight GF&GS, six of which are operational oriented and two are support oriented.

Netforce Generic Functions and Services

- Collector Management (CM)
- Picture Compilation (PC)
- Situation Evaluation (SE)
- Effector Assignment (EA)
- Effectuation (Eff)
- Planning and Coordination (PLC)
- Resource Management (RM)
- Netforce Management (NM)

In Figure 17 we have shown these GF&GS in a diagram where we have illustrated the major interactions between these functions with arrows. It is noted that the defined GF&GS differ in some ways from currently used terminology, like situational awareness, Force TEWA (threat evaluation and weapon assignment, etc.) The set of GF&GS is more fundamental than for example TEWA, since that is a combination of two underlying functions. In Figure 17 we have shown some of the commonly used term in different colours and projected them behind the corresponding GF&GS. In section 6.2 we give a more elaborate diagram of these functions with their relations.

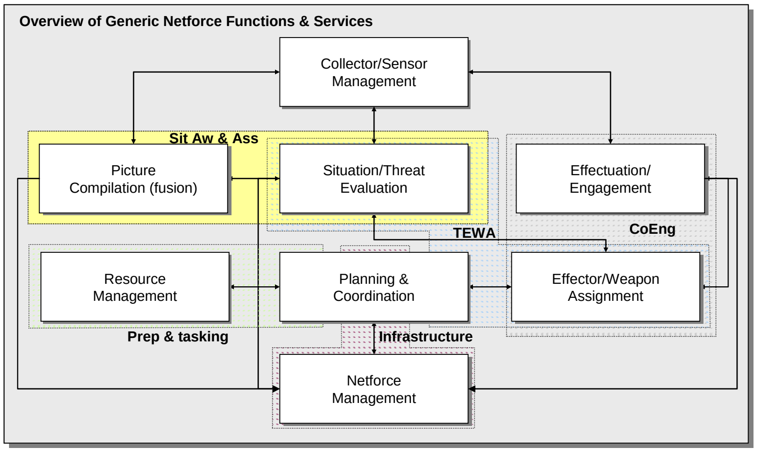

Overview of Generic Netforce Functions & Services
Collector/Sensor Management
Sit Aw & Ass
Picture Compilation (fusion)
Situation/Threat Evaluation
Effectuation/ Engagement
TEWA
CoEng
Resource Management
Planning & Coordination
Effector/Weapon Assignment
Prep & tasking
Infrastructure
Netforce Management

Figure 17 The Generic Netforce Functions and Services

In the following text we will give a short characterisation of each of the GF&GS, but will refer to later papers for a more elaborate discussion on GF&GS.

GF CM: Collector Management

Employment of collectors (like sensors) and control of their configurable characteristics (such as frequency, PRF, scan rate, frame time, waveforms, power, etc.) such that activities like picture compilation, threat evaluation and engagement are optimised. A GF CM uses interactions in the C-I-D-E chain to optimize the configuration of the contributing collection of C nodes.

GF PC: Picture Compilation

Process leading to coalition common pictures (CCP) at the strategic (CCSP), the operational (CCOP) and the tactical (CCTP) levels through taking input from all contributing collectors and compiling the picture or situation representation (not necessarily a picture in all cases). We use the commonly used term ‘picture’ for the representation of the relevant operational situation. A common ‘picture’ facilitates collaborative planning and assists all echelons (D levels) to achieve situational awareness. A Single Integrated Air Picture (SIAP) [6] - consisting of real-time or near real-time common, continual, and unambiguous tracks of airborne objects of interest in the surveillance area – is part of the GF PC results.

GF SE: Situation Evaluation

Based upon available information (usually provided by the GF PC) the analysis and subsequent prioritisation of specific *entity* (like targets) in the operational theatre, based on their potential to do harm and includes the post effectuation evaluation. In a coalition setting the harmonisation of the evaluation and assessment criteria is important here.

GF EA: Effector Assignment

Using the results of the GF SE the process by which available effectors are analysed and subsequently assigned to engage a designated contact (like an air target, a C2 system or a program (information ops)). An inter-node scheduling mechanism for engagement (a DDE interaction) is part of a coordinated engagement capability.

GF Eff: Effectuation

This is the actual action (like the execution of a fire control order) by one or more effectors (more in the case of synchronized engagement) aimed at bringing about the desired effect decided upon by a decision process of a D node. It comprises for instance all actions needed to direct or authorize nodes (units and/or weapon systems) to engage a designated target, and the effector's subsequent path to intercept. It includes coordination necessary to execute cooperative and synchronized engagements (the D-E and E-E interactions).

GF PLC: Planning & Coordination

In the pre-operational phase the GF PLC covers pre-mission preparations, battlefield preparation and shaping, RoE establishment, operational planning (OPLAN). In general it involves predominantly strategic and operational planning & preparation tasks. We made the decision to identify these activities as a generic inter-node function because of the importance of these tasks in a coalition setting. The preparation and shaping of the netcentric environment out of multi-national contributions is of paramount importance for the correct and smooth functioning of the netcentric operation.

GS RM: Resource Management

This is predominantly a support function for the complete operation. Logistics, maintenance and repair are part of this GS. There is a strong relation with the netforce/network management function since they contain data directly related to the netforce and network nodes.

GS NM: Netforce Management

Netforce Management comprises a number of services. It contains the netforce support services and the network services. The netforce support services maintain and control the architecture, the interconnectivity, the integrity and security, while the network services are the 'standard' data communication services, but also network security to ensure and the timely passage of seamless data/information between nodes required to fulfil mission requirements. We have grouped all these support services in one single GS just to limit the number of high level functions.

5.1.1 Netforce GF&GS Design Issues

We are aware that we have only addressed the concept of the netforce GF&GS on a very general and high level. It is clear that in subsequent work we have to address the application of the netforce node principles for the design of GF&GS architectures: how to use the nodes, the node types and the node properties to design GF&GS. At the level of GF&GS architecture there also exist common concepts just like the ones we have identified at the underlying netforce level discussed in this paper. We mention for instance: GF&GS initialisation and control principles: centralized or distributed, localized control to enhance self synchronisation capabilities, a levelled capability approach to allow nations to select their own level of ambition they can operate on, techniques for automated data distribution and replication between participating nodes in a GF&GS, bandwidth reduction mechanisms, graceful degradation, interaction between GF&GS on SOT levels, etc. These topics go too deep for the scope of this paper and will be addressed later.

5.2 Netforce Management Services

In the introduction of section 5 we mentioned the netforce support services. They are a set of services aimed to manage, maintain and protect the netforce as a netcentric environment. As shown in Table 3 we have identified a set of three variants of these services. We will give a brief description of each one of them.

Node Management
The netforce approach assumes that the collection of nodes called *the netforce* is a well known and defined entity. This means that a mechanism is needed to keep track of participating nodes (entry and leave), their status, their capabilities and their mutual relations. Node information is required to provide and maintain the netforce security, but also to provide information to requesting services about what kind of capabilities are available for specific actions. A part of the Node Management service is the earlier mentioned logon/logoff function for nodes. Netforce node information is stored in the Netforce Structure Database NFSdb (see section 5.5.1).

Data Management
The second of the netforce support services is the netforce data management. The data management service has two major tasks: one is to establish the common data sets for the (coalition) operation and the other is management of information provision for the decider nodes (like organisational elements) in the netforce. The latter one is obviously a function of the I nodes working together to ensure optimal information provision to C nodes in the netforce. In addition to more or less ‘local’ I node systems (information systems) which already exist for ‘local’ D processes (like existing command centers of platforms) we envisage in a true netforce environment also inter-node level information distribution and provision systems. These kind of data management services are part of the information layer in an architecture as described in section 5.4 and shown in Figure 19.

Security Management
The last but not the least of the netforce support services we discuss is *Security Management*. We have stated before that security is a key aspect of the netcentric environment, and it is therefore modelled as an elementary property of all node types. We have also identified security as one of the netforce support services. During the pre-operational stage the netforce Security Policy needs to be established and enforced, for the whole coalition as well as for national interests. Although the emphasis in the netcentric environment will be to have a maximum degree of openness and accessibility, there will always be national interests to be taken into account. To minimize unwanted interruptions during the operational process many of the national security issues need to be established during the pre-operational phase. Another important issues in netforce security is intrusion detection. This function is strongly related to the equivalent one for the *network*. Sufficient is to say here that adequate means (on several levels and distributed and coordinated) need to be available in the netforce environment. For an overview of the specific security aspects in a NEC environment we refer to [12].

The execution of most of the netforce support services can be allocated to the tasks of the Netforce Management Cell as discussed in the next section.

5.2.1 The Netforce Management Cell

In the preparation and execution phase of operations the netforce environment needs to be defined, set-up, prepared and managed/controlled. This task is key to the performance of the netcentric environment as a netforce and network. For the execution of this task we have introduced in the NFRM the concept of a Netforce Management Cell (the NFMC). The NFMC is a S node and is responsible for setting up, managing and controlling the netforce architecture (see Figure 18). In Figure 18 the hexagon symbol represents a S node.

To identify the areas of operation of the Netforce Management Cell of Figure 18 we used a simple but very effective diagram method of identifying and drafting operational functions.

The horizontal time axis is the operational timeline divided into a pre-operational, an operational and a post-operational area, while the vertical axis reflects four organisational levels of hierarchy: political, strategic, operational and tactical. This diagram allows to specify the 'working area' of a function or service with respect to a hierarchical level and the operational timeframe.
The NFMC can be implemented in different ways. Although for the highest level a single NFMC is most likely the best solution, for the underlying level it is more probable to chose for a distributed implementation where redundancy is being built into the organisation. Part of the distribution consideration can be geographical separation of controlled areas or hierarchical considerations. A whole range of topics need to be addressed (coalition as well as national) to ensure an optimized netforce architecture for an operation.

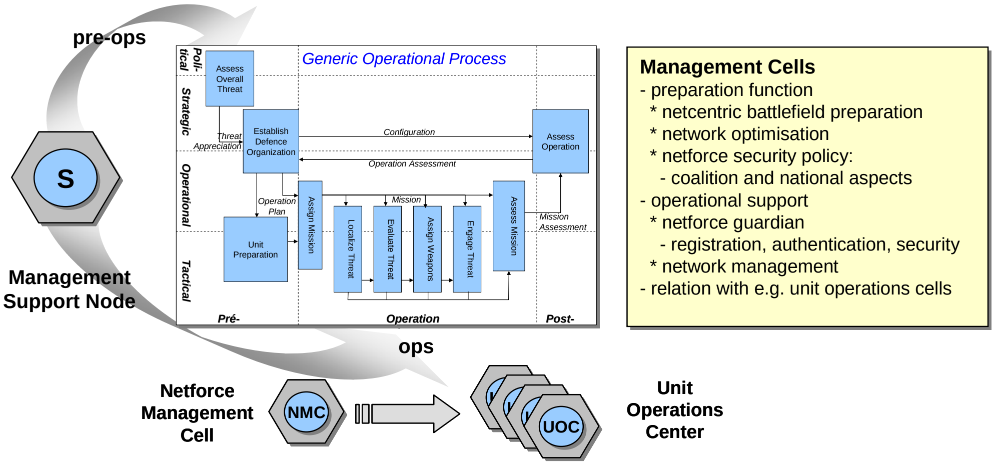


Figure 18 The Netforce Management Cell

Major Preparation Tasks of the NFMC comprise:

- preparation of the netforce structure database (the NFSdb, see section 5.5.1);
- maintaining the integrity of the architecture and composition of the netforce: this comprises the overview of the participating nodes and their interactions/relations and their composition;
- netcentric battlefield preparation: all the functions that harmonize common data sets, the use and the availability of them;
- establishing netforce and network security policy.

Major Operational Support Tasks of the NFMC are:

- acting like a netforce guardian, with respect to integrity maintenance;
- enforcing and maintaining security policy;
- network management.

5.3 Network Services

In Table 3 we mentioned several examples of network services. These were the 'standard' communication services, network optimisation and security management. We will not go into detail with respect to the 'standard' communication services since they are outside the scope of this paper. Also for security we refer to related remarks on security in this paper and to a lot of other existing work on network security.

With respect to network optimisation we only mention that I-I and I-D interactions, which optimize the information provision for D nodes are a major guiding mechanism for network optimisation. The QoS mechanism of the Com nodes enables a negotiation mechanism to be developed that optimizes part of the network for optimal information throughput to specific D nodes.

5.4 Netforce Grids and Architecture

In the preceding sections we discussed the typical netforce functions and services that are based upon the netforce principles. In this section we will show how these netforce concepts map on architectural approaches that are commonly used in the discussions about netcentric architectures.

A common concept is that of *'grids'*. Often the concept of sensor and weapon grids are used, without actually specifying what is meant by them. In reality those grids do not always exist as real grids: that is, all collectors are not connected together in one grid, nor are all effectors. Nevertheless, the 'grid' concept is frequently encountered and used in architectural descriptions. It has more a logical meaning than a real physical one. We will adopt the grid concept for its logical meaning here.

In Figure 19 we have shown the grid structure we derive in our NFRM. We have a logical placement of four operational oriented grids. The decider grid uses the information from the information grid that is provided by the collector grid to direct the effector grid. All grids are connected to the network which is the supporting grid. Also shown are the so-called conceptual world types that are applicable for each grid level. We distinguish between the real world (physical domain), the perceived world (information domain) and the interpreted world (cognitive domain) (see for instance [13] for a more elaborate description). We can derive from the grid structure in a very straight forward way an architectural model that is shown in the right hand part of Figure 19. This is the Netforce Architectural Model NFAM. In the NFAM we see four operational oriented layers and two support layers. The vertical service layer contains the network services discussed earlier. Information oriented services, like email, messaging, chat, VTC, are contained in the Information services layer. We see that the structure of the NFAM follows directly from the netforce principles.

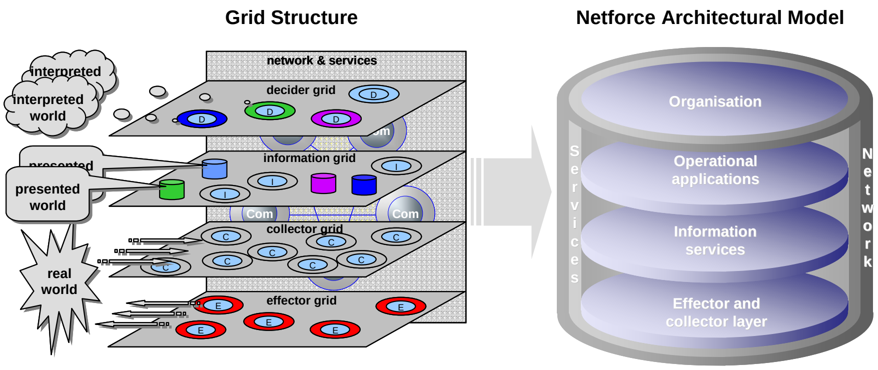


Figure 19 Netforce Grids and Architecture

The NFAM differs slightly from most other architectural models in that the service and network layers are vertical here in stead of horizontal. We felt the need to emphasise that the services and network are used on all horizontal layers and have chosen to depict them like vertical layers.

The NFAM can be related to other currently developed reference frameworks and models. Important ones to consider are the GIG Architecture, the GIG ES, DoD Netcentric Data Strategy, the Netcentric Operations and Warfare Ref Mod, [14]. All efforts to position the netforce functions and services need to be consistent with existing and emerging major, de facto initiatives, frameworks and models. With respect to the GIG architecture the NFAM only deals with the top four layers of the GIG.

5.5 The Four Generic Databases in the Netforce

Adopting the process point of view on NEC (conform to what we did in section 2) we can make the following analysis concerning the *generic types of information* that are required for NEC. The netforce environment that performs NEC can be regarded as a multi-process environment (multiple nodes interacting with each other). These processes work together in a co-ordinated way to accomplish a common goal. Because of its multi-process nature *and* the required co-ordination between these processes to accomplish the common goal, *four generic types of information* are required. (Note that this is true for any multi-process environment where processes work together to achieve a common goal).

The four *generic types of information* are:

1. Information about the available resources in the netforce: this is netforce information about the nodes and their capabilities. One may call this is a kind of self awareness of the netforce about itself.
2. Information about the operational situation. This is situational awareness information on the real world on all hierarchical levels and results in (Shared) Situational Awareness.
3. Information about the intentions and the operational plans. This information is needed in order to direct the actions within the multiple node environment.
4. Information about the actual actions (effects) already taken to achieve the intentions and operational plans. This information is used to take into account existing actions, to determine successive actions (e.g. for synchronisation, force multiplication and deconfliction).

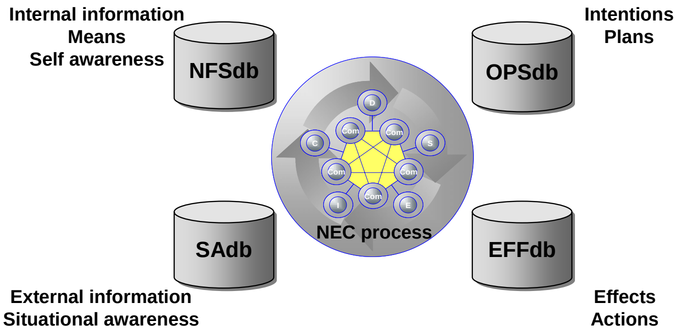


Figure 20 The Four Generic Netforce Databases

We have mapped these four generic types of information onto four generic netforce databases, as is shown in Figure 20. Actually, these generic types of information are *information sets* and we do *not* place constraints to the actual implementation of these sets in the netforce. It can be done by using a database or by a different mechanism. These *information sets* in the netforce will usually be of a distributed nature because of the many nodes involved and the likely segmentation of them (e.g. on strategic, operational or tactical levels, but also segmentation according to land, air, and sea entities). To simplify the discussion we take the logical point of view and regard these information sets as a database, regardless whether they are distributed or not and whether they are implemented in other ways than a database.

According to that reasoning we arrive at the following databases:

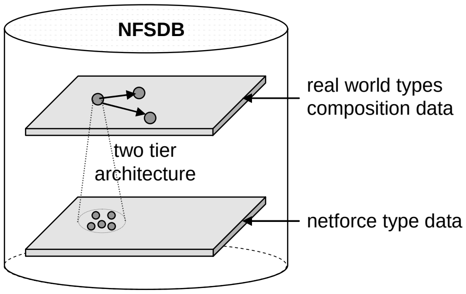
- the NFSdb, the netforce structure database which was already mentioned several times and which we will discuss in a little more detail in the next section.
- the OPSdb: the operational database, which contains the operational intentions and planning about the operation at the three SOT levels. This OPSdb will in reality be an

aggregation of several other databases at each of the SOT levels. The information of the OPSdb together with that of the NFSdb (for providing the means) and the SAdb (for providing the situational awareness) is used to fulfil the information demands of D nodes to perform their decision making.

- the SAdb: the situation awareness database, which is an abstraction and simplification of the various situational awareness databases found on all SOT levels. Examples are a JCOP, a RMP, RAP, RGP, SIAP. Also Intel data is to be stored in the SAdb. The SAdb information is used in several GF&GS.
- the EFFdb: the effects database, which contains information on the effects resulting from the decided actions. It is the information of the OPSdb and the EFFdb which are used in synchronisation processes with respect to planning and execution of actions.

5.5.1 The Netforce Structure Database NFSdb

One of the relatively new concepts we derived is the netforce structure database NFSdb. For our purposes in this paper the NFSdb is a two tier database. The upper layer is equivalent with ‘normal’ data schemes we encounter in current operational databases. Here we have objects like a tank, a battalion, a frigate, a fighter squadron or jet, etc. This upper layer can therefore be equivalent with already existing databases. The second layer is the netforce layer where we have the netforce node representation of the entities of the upper layer. This lower layer contains the node information including the QoS data of the nodes.



Netforce Structure Data Base NFSdb
- meta data db with two tier architecture
- top level: common current data schemes of real life object
- lower level: mapping through node structure specification on netforce components
- QoS data on lower tier
- allows use of current data schemes
- distributed nature, data replication mechanisms

Figure 21 The Netforce Structure Database NFSdb

Creating a two tier database allows us to use at the high level the normal well-known data schemes we are familiar with, and on the lower level the netforce entities and their data needed for the netcentric environment to be maintained and operated properly. For managing and controlling the netcentric environment this netforce information is provided to functions and services. How this is done is a matter of designing the netcentric environment. In the netforce concept the NFSdb will be maintained by the NFMC discussed in the previous section. It will be most likely that the NFSdb will be a segmented and distributed database, with segments containing the data of specific parts of the netcentric environment. Segmentation makes the total NFSdb more manageable, but will require adequate data synchronisation mechanisms.

6 Netforce Warfare Area Modelling

6.1 Transition to the Warfare Domain

In the preceding sections of this paper we have described a stepwise derivation and definition of the netforce principles that are the elementary building concepts for NEC.
These netforce principles were:

- Netforce Node Concept, including Node Types and Node Properties
- Netforce Node Interface & Architecture Concept
- Composite Nodes

- Logon/logoff/status Protocol
- Node Ownership, Access control
- Basic Netforce Node Interactions
- The Netforce Function and Service Concept
- The Netforce Generic Inter-node Functions and Services
- The Netforce and Network Management Services
- The Netforce Architecture Model
- The Four Generic Netforce Databases

This set of netforce principles all describe and define the elementary building blocks or concepts that make up the total netcentric environment. They are all formulated independently from the application of these concepts in specific operational settings. Although we do not claim the current set of netforce principles to be complete or conclusive, we will in the remainder of this paper now make the transition to the warfare domain and demonstrate how an operational domain can be modelled using these netforce principles. Because of length constraints of this paper we will only model the highest level. The domain can be any warfare area, like air defence or mine detection or an amphibious operation, a crisis response operation, peace keeping operation, etc.

6.2 The Generic Netforce Warfare Model

In deriving a high level generic netforce description of a warfare area or of an operation in general, we took the approach of using the netforce GF&GS and combining them in one overall process view. The GF&GS themselves are warfare area or operation independent. The model that results from them gives an insight in the overall structure of a warfare area. It is also useable as a starting point for simulating several processes that take place in the netforce environment, like nodes entering and leaving the netforce environment (processes like registration, logging on and logging off), the creation of shared awareness on the SOT levels and the exchange of information between them, the creation of AIS and AMG, the synchronisation of decision making and synchronisation of actions, etc.

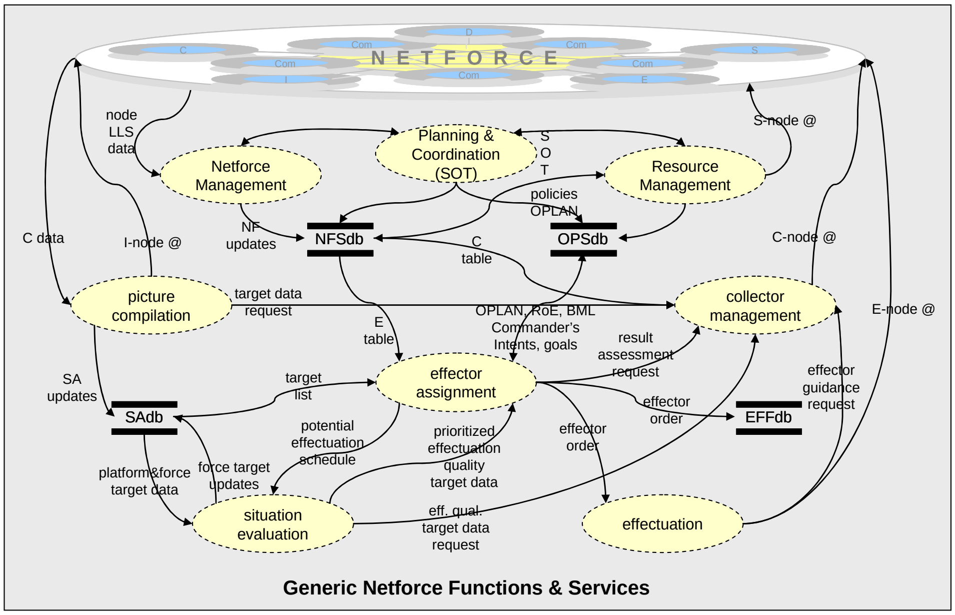


Figure 22 The Generic Netforce Warfare Model

The result of this modelling exercise is given in Figure 22. In Figure 22 we see the symbolic representation of the netforce environment as the ellipse in the top of the figure, the eight netforce GF&GS and the four generic netforce databases. Each of the eight GF&GS we identified earlier are combined in the model to create the overall process of a warfare function. In the generic model we can follow logical paths of information flows between the high level functions for all kind of processes in the netcentric environment. It should be realized that in this generic model we have 'folded together' the strategic, the operational and the tactical dimensions to reduce the complexity of the diagram. The model also does not give timing or sequential information. When we are going to consider the timing aspects in relation to the processes shown of the generic model and take into account the three SOT levels we need to combine the generic model of Figure 22 with the diagram as shown in section 5.2.1 and Figure 18.

6.3 Using the Generic Netforce Warfare Model

The generic netforce warfare model is the result of a stepwise derivation process where the generic structure of a warfare area is modelled in terms of functions, data flows and generic data stores. It is in a way a template, giving the overall structure of every warfare area. As such, it helps to understand the structure, or generic functional architecture, of a warfare area.

The next step in using this generic netforce warfare model is to distinguish the different SOT levels, differentiate the GF&GS at these levels in actual operational processes and specify the resulting GF&GS on each of the SOT levels. And also to take time aspects into account as we already mentioned earlier. We also refer to the end of the discussion of the GF&GS (see the end of section 5.1). A more extensive discussion on the use of the generic netforce warfare model to derive operational and system architectures is beyond the scope of this paper. We will address that issue in subsequent articles.

The Generic Netforce Warfare Model is currently used for several follow-on activities and studies:

- as a starting point of modelling specific warfare areas: current initiatives include missile defence [15], joint fire support [16], information operations;
- as one of the high level starting points in the design of a netcentric modelling and simulation environment in which specific netcentric processes can be studied;
- to further detail a netcentric description of the GF&GS [15,17].

7 Conclusions

In this paper we have presented a set of netcentric principles, called the netforce principles, which can be regarded as a foundation for understanding and modelling NEC. We have shown how they can be derived and formulated in a stepwise process, starting with a single axiom, the *Network-Node Paradigm*. Following the identification of the elementary nodes and their properties, we discussed single node concepts resulting from the node properties, followed by multi-node concepts like functions and services. It is interesting to note that a number of not often encountered concepts could be derived from this stepwise approach: the notion of the I nodes, the agile information force, the generic netforce databases. We also saw the netforce interfacing mechanism allowing legacy systems to be integrated into the netforce encapsulation.

The current status of the NFRM can be described as follows: it gives a basic understanding of the most elementary building blocks in the netcentric environment and it offers several placeholders for more advanced concepts based upon these elementary building blocks. We realize that these more advanced topics need to be described in much more detail but is outside the scope of this paper. Some of this work is addressed in the next section.

7.1 Future Work

The development of the NFRM is still far from complete. A substantial effort is required for a more formal derivation and description of the netforce principles and the assessment of the complete NFRM itself. Part of these activities are currently carried out in several national projects and initiatives, but also in international ones. We mention the BMC4I Working Group of the multi-national MTMD (Maritime Theater Missile Defence Forum) [15], the European MPEC (Multi-platform Engagement Capability) Working Group [17]. Currently the NFRM has also been introduced to the NATO NNEC initiative and the NATO ACT program. A majority of future activities deal with the development of guidelines of how to apply netforce principles in netcentric systems design and in formulating netcentric CONOPS (Concepts of Operations).

Current activities we have identified are:

Areas of activity

- formalisation of the Netforce Principles, e.g. in UML for M&S application
- formalisation of the C2 process, in functional as well as in QoS terms
- treatment of the creation and handling of AIS and AMG
- inter-node GF&GS design and formalisation of GF&GS principles
- derivation of operational and systems architectures from the generic warfare model
- definition of information processing and provision mechanisms
- QoS in the netcentric environment
- mapping of the NFRM on existing models and initiatives, like the GIG (Global Information Grid) [14], the NAF (NATO Architecture Framework) [18] or DoDAF (DoD Architecture Framework) [19]
- application of the Netforce Principles to the civil domain

This list is not complete but gives a fair indication of the areas and amount of work that needs to be carried out. Initiatives from others to carry out joint work in these directions are welcome.

8 References

[1] Network Centric Warfare, D.S. Alberts, J.J. Garstka, F.P. Stein, CCRP Publication

[2] Network Enabled Capability, JSP 777 Edn 1, Publication of the UK MoD

[3] NNEC Foundation Document, document from the IS-NNEC IPT, 1 December 2004

[4] MTMD Open Architecture WG, the following documents apply:
a. Captain Thomas J. Strei, USN. “Open Architecture Functional Architecture Definition Document,” Program Executive Office for Integrated Warfare Systems, 2004.
b. Captain Thomas J. Strei, USN. “Open Architecture Computing Environment Design Guidance,” Program Executive Office for Integrated Warfare Systems, 2004.
c. Captain Thomas J. Strei, USN. “Open Architecture Computing Environment Technologies and Standards,” Program Executive Office for Integrated Warfare Systems, 2004.

[5] OMG (Object Management Group), C4I Domain Task Group, e.g. work on Open Architecture Radar Interface Standards

[6] Single Integrated Air Picture (SIAP) System Engineering Task Force, instituted in October 2000 by the Under Secretary of Defence

[7] Agile Mission Group, netcentric concept introduced in NEC, see ref [2]

[8] Battle Management Language (BML), M.R.H. Hieb, A. Tolk, W.P. Sudnikovich, J.M. Pullen, The MSIAC’s M&S Journal Online, http://www.msiac.dmso.mil/journal/tolk_1_61.html

[9] MIP-Message Exchange Mechanism, Multilateral Interoperability Program MIP-baseline1:2003, and ATCCIS Replication Mechanism (ARM), NATO WP14-3_Ed5.0_20020318.pdf. See www.mip-site.org

[10] Swarming on the Battlefield: Past, Present and Future, S.A. Edwards, Publication of the RAND Corporation, ISBN 0-8330-2779-4, 2000

[11] Quality of Service: for network QoS see http://www.cisco.com/univercd/cc/td/doc/

cisintwk/ito_doc/qos.htm

[12] Position Paper on Network Enabled Capability Security, NATO RTO/IST Task Group on Network Enabled Capability Security, 15 October 2004

[13] A Framework for Analysis and Decision Processes in Teams, H.E. Keus, Proceedings CCRP Symposium 2002, June 2002, Monterey, CA, USA

[14] Global Information Grid, see DoD Memorandum CIO, 9 May 2003

[15] Technical Plan Of Work for the MTMD BMC4I Architecture Definition Project, version 5.1, 07 July 2004, internal document of the MTMD BMC4I WG

[16] SENECA co-operative project between NL MoD, TNO, Thales Netherlands

[17] European Multi Platform Engagement Capability (MPEC) Working Group, France, Germany, Italy, The Netherlands

[18] NATO C3 Systems Architecture Framework (NAF), Version 2, (AC/322-D(2004)0041, August 2004

[19] DoD Architecture Framework, version 1.0, 30 August 2003, document of the DoD Architecture Framework Working Group (AFWG),

Acknowledgement

The author wishes to thank the many reviewers in the TNO organisation that have helped to substantially improve this work. To mention anyone specific would not do credit to the work of the others.

List of Abbreviations

AIS	agile information source
AMG	agile mission group
BML	battle management language
C	collector
CEC	co-operative engagement capability
CM	collector management
Com	communicator
D	decider
E	effector
EA	evaluation assessment
Eff	effector management
Effdb	effects database
I	information provider
F&S	functions and services
GIG	global information grid
GF	generic function
GS	generic service
NCO	netcentric operations
NCom	network communications
NCW	netcentric warfare
NEC	network enabled capability
NInt	node interface
NF	netforce
NFAM	netforce architecture model
NFMC	netforce management cell
NFRM	netforce reference model
NFSdb	netforce structure database
NM	netforce management
NNEC	NATO NEC
NP	netforce principles
NSpec	node specification
OPSdb	operational database
PC	picture compilation
PLC	planning & co-ordination
QoS	quality of service
RM	resource management
S	supporter
SA	situation awareness
SAdb	SA database
SE	situation evaluation
SoS	system of systems
SOT	strategic, operational, tactical
TEWA	threat evaluation and weapon assignment