The NL C4ISR Architecture for Groundbased Operations: Evolutionairy development of Network Enabled Capabilities

Author: ltcol Msc. Dirk Jan Blaas
Co-author: Theo Derksen Msc.

RNLA C2 Support Centre

Addres: Nieuwe Kazernelaan 10
PO box 9012
6710 HC Ede

c2sc.ba@rnla.mindef.nl

ABSTRACT

The Royal Netherlands Army RNLA has over the last years developed an Architecture that is governing all design and development activities in the C2 Support Centre, where new systems are built to deliver Situation Awareness throughout the chain of command in the Dutch Army.

The scope of the NL C4ISR Architecture for Groundbased Operations covers the complete set of information systems and ICT infrastructure systems that are to be used in all operations that the RNLA is performing, spanning from support in national crises to peace supporting operations including peace enforcing scenario's (OOTW).

Driving vision behind the architecture is the NCW/NCO concept. The Netherlands Defence policy shows a huge commitment in building Network Enabled Capabilities, not only for the Dutch Defence organisation but also as a contribution to NATO- and other coalition operations.

The architecture relates to NATO Technical Architectures but is much more detailed and scoped so that it can really give guidelines and constrains to projects where functionalities are built and prepared for implementation.

The architecture approach in the Netherlands is unique in that it is developed evolutionary and that in parallel projects are realising, also in an evolutionary way, fieldable systems that deliver required functionalities. The credo that the C2SC uses is:

'Design a little, Build a little, Test a little, Field a little, and Learn a lot !'.

The evolutionary approach enables the RNLA to adapt to changes in the Defence organisation and tasking, it enables new technology to be incorporated in systems at the proper moment, and it enables a step-by-step method to discover the exact requirements of end-users as well as a possibility for step-by-step adaptation to new technology and new doctrines.

The success of this approach is not only recognised by end-users of systems within the RNLA but also by the United States NCW community, that has recently awarded the Netherlands for the TITAAN project as the best NCW-programme within a coalition nation.

1.0 INTRODUCTION

The Royal Netherlands Army RNLA has over the last years developed an Architecture that is governing all design and development activities in the C2 Support Centre, where new systems are built to deliver Situation Awareness throughout the chain of command in the Dutch Army.

The scope of the NL C4ISR Architecture for Groundbased Operations covers the complete set of information systems and ICT infrastructure systems that are to be used in all operations that the RNLA is performing, spanning from support in national crises to peace supporting operations including peace enforcing scenario's (OOTW).

Driving vision behind the architecture is the NCW/NCO concept. The Netherlands Defence policy shows a huge commitment in building Network Enabled Capabilities, not only for the Dutch Defence organisation but also as a contribution to NATO- and other coalition operations.

Following the NCO concept, **mission effectiveness** in all kinds of operations can be significantly enhanced by achieving **information superiority** that enables the level of **shared awareness** needed for **adequate decisionmaking** (both in terms of the quality of decisions and in de speed of decisionmaking). Adequate decisionmaking in its turn leads to **speed of command** that enables commanders to mentally 'outmanoeuvre' the adversary commanders.

The C2 Support Centre, responsible to provide the systems to support command and control for all commanders in the groundbased environment, is building enablers for NCO. That means that an enabling network of networks is realized throughout the tactical and operational levels of command and that the information system of systems is realised that enables the unrestricted information sharing that is envisioned in the NCO concept.

For all of that to become reality the RNLA has adopted an architectural approach known as **'design & development under architecture'**. Following this approach all design and development of information- and infrastructure-systems are governed by an overarching C4ISR Architecture. In the architecture an architecture framework is introduced that puts all the systems needed for achieving information superiority for commanders into perspective, thus enabling optimal inherent interoperability between the respective systems. The optimum is reached by maximizing information-integration and infrastructure-integration.

The architecture approach in the Netherlands is unique in that it is developed **evolutionary** and that in parallel projects are realising, **also in an evolutionary way**, fieldable systems that deliver required functionalities. The credo that the C2SC uses is:

'Design a little, Build a little, Test a little, Field a little, and Learn a lot !'.

The evolutionary approach enables the RNLA to adapt to changes in the Defence organisation and tasking, it enables new technology to be incorporated in systems at the proper moment, and it enables a step-by-step method to discover the exact requirements of end-users as well as a possibility for step-by-step adaptation to new technology and new doctrines.

This paper describes an overview of the C4ISR Architecture.

2.0 REQUIREMENTS FOR A NCO-ENABLING ARCHITECTURE

2.1 Richness of the architecture

To reach its full potential NCO must deeply rooted and integrated in the Operational processes. As such new technologies cannot simply be applied to current infrastructure, systems and organisations / business processes. For this reason, an **overall architecture** is needed in which these domains (operations, informationsystems, infrastructuresystems) are dealt with in relation to each other. Therefore the architecture will follow a layered structure. For the architecture to serve as a tool for mastering the complexity of the system of systems there must be a limitation to the number of layers the architecture is split up into. As a rule of thumb we will allow three layers that can be sublayered on more detailed abstraction levels.

2.2 The role of industry standards and COTS products

The architecture framework must be set up in such a way that third parties can realise parts of it. This is the only way to speed up the development and make use of the lead that commercial organisations have in the ICT field. For this one needs one's own overall architecture to steer the developments, to outsource parts of it, to incorporate new technologies and so on. Also from the point of view of the architecture framework the experiences and developments of these organisations can be examined, and an assessment of their applicability can be made. In this way commercial off-the-shelf (COTS) products can be judged and made use of.
If COTS products are used, concentration on the following is necessary:

- the integration of components / technologies,
- applicability in respect of the Operational processes and
- usage in the operational field.

The development of the components is not the core business of the RNLA; moreover, the RNLA cannot compete with the rapid developments of new technologies outside the organisation. Another reason is that in a network centric approach one has to collaborate with others. This means that standards are extremely important. Consequently, one has to use the industry standards to make this possible. An additional advantage is that the industry standards provide sufficient expertise and trained manpower. One cannot set one's own standard in this age of changes and rapid evolutions. Don't rule the waves, but sail the waves.

2.3 The role of the Common Operational Picture

The network infrastructure technology at present makes networking possible at the Operational and Tactical level. The power of NCW is derived from the effective linking or networking of knowledgeable entities that are geographically or hierarchically dispersed. The networking of knowledgeable entities enables them to share information and collaborate to develop shared awareness, as well as to collaborate with one another to achieve a degree of self-synchronisation and to increase the speed of command.

One of the basic concepts in this regard is the Common Operational Picture (COP). In this context, 'operational' depicts the military operation and in that respect the COP is not only valid for the operational levels of command but also at the tactical levels. 'Picture' is meant metaphorically as well as literally. The former implies that all actors have the same information with respect to the operations (if permitted). The latter means that information is presented in a (geo-)graphical mode. In the COP it is possible to present all relevant information (positions of units, vehicles, movements, etc) of a battlefield on a map tailored for the commander in terms of his area of interest.

2.4 Generic and Flexible

The network centric concept is inherent flexible. In network centric operations one is capable of acting rather than reacting and of dictating the time, place, purpose, scope, intensity and location of operations. This concept makes it possible to achieve awareness, speed of command and responsiveness not only in battle operations but also in other operations, such as peacesupport operations and operations in support of (national) crisis-response. The NCO concept itself is applicable in all those situations. This requires the systems and infrastructure to be very generic, enabling the same solution to be applied in all situations; the difference is only a matter of information and usage.

The potency of a network centric solution is extremely high, and can also be applied in civil organisations, for instance the fire brigade, police, transport organisations, health services, etc.

A network environment makes it possible to couple with a diversity of sensors and other systems and take advantage of the direct use of the information they deliver. This will also increase efficiency and limit the errors that occur in the case of intermediate (manual) chains. This demands higher requirements with respect to the interfaces / couplings. The consequences to be dealt with in respect of using different networks and systems are coupling of different physical transport media and different data communication protocols onto different systems. The NCO enabling architecture should thus support Joint collaboration, interconnecting the different NCO solutions of the services to create one logical informationdomain.

Combined operations will put the members of the alliance in close cooperation. Some standardisation and mutual agreements already exist to facilitate possible future combined operations. Although many areas of standardisation have been formalised, there are many other areas in which standardisation does not exist. These agreements and standards have to be worked out and fine-tuned. The most difficult part is to bring about agreement in respect of information definition at Operational level. Thus information modelling and the standard for exchanging information are the basis for all. For exchanging information MIP C2IEDM is used as a basis.

Coalition operations involve more than one nation and usually tend to be the result of a temporary combination of national forces brought together for a specific purpose. In a coalition situation, agreements on doctrine, principles, and operating techniques will probably be only partially developed, if they exist at all. Forces may have to work out procedures for coalition operations under the pressure of imminent conflict or even while operations are ongoing. This requires an extremely generic and flexible solution, which must be an intrinsic property of the C4ISR overall architecture.

2.5 Information security

The interaction with all kind of partners and civil organisations in specific scenarios needs an open infostructure but classified information needs to be properly safeguarded as well. This means that the architecture must provide guidelines and solutions to fulfill both requirements. Not always are technological solutions available or permitted. That could lead to uncomfortable solutions for the present, like for instance man-in-the-loop-interfaces. However the architecture should point out the path to travel towards multi-level security solutions in the future.

3.0 OVERVIEW OF THE RNLA C4ISR ARCHITECTURE

In this part of the paper a high level overview of the architecture is given. For the purpose of this paper it is impossible to describe the architecture in more detail, although it could be interesting to study it in more detail to understand the full impact of the architecture on the projectdevelopment as it takes place in the RNLA C2 Support Centre.

3.1 C2, C3, C3I, C4I, C4I2, C4ISR, C4ISTAR…..

In the rest of the paper, for reasons of readability, the RNLA C4ISR Architecture will be abbreviated as C3IA, baring in mind that Intelligence, Surveillance and Reconnaissance are part of the scope of the architecture bud are regarded as directly in support of C2 and therefore absorbed within the scope of C2. Consultation at the level of operational and tactical commanders is also considered to be part of the scope of C2.

3.2 Architecture Framework

3.2.1 The overall framework

In the following picture the overall C3IA framework is given.

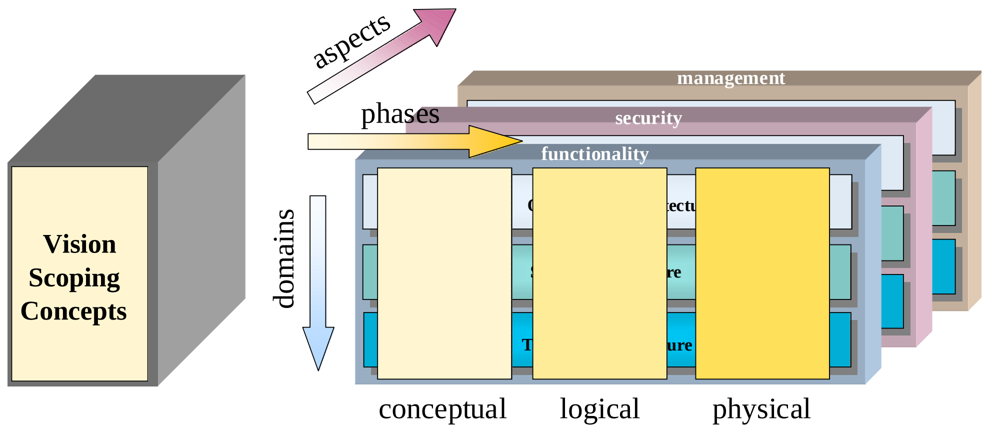

Figure 1 : Overall C3I Architectureframework

A description of the framework is given in the following paragraphs.

3.2.2 Vision, Scoping and Concepts

The vision and scoping stage is aimed at the definition of the boundaries of the overall architecture and for determining what the main concept will be for the operations within that scope. Besides the business drivers, concepts and goals, the vision and scoping definition also contains the drivers, concepts and goals for the systems and technical infrastructure implementation. Based on this vision and scope (main concept) the basic concepts of the architecture, the architecture framework, can be determined. The architecture framework will be used to design the architecture for functionality, security and management.

The **leading vision** behind the C3IA is, as can be expected, the NCO concept.

Second vision that the RNLA has adopted is the concept of evolutionairy development.
The credo that the C2SC uses is:

'Design a little, Build a little, Test a little, Field a little, and Learn a lot !'.

The evolutionary approach enables the RNLA to adapt to changes in the Defence organisation and tasking, it enables new technology to be incorporated in systems at the proper moment, and it enables a step-by-step method to discover the exact requirements of end-users as well as a possibility for step-by-step adaptation to new technology and new doctrines.

Not only the functional systems are developed evolutionary but also the C3IA itself must be. It is impossible to set up and implement a complete architecture in advance, before the various implementation projects gain in-depth experience. People have to learn step-by-step and grow in synch with the development and changes. Otherwise such a huge change will not work. The next picture illustrates the evolutionary change of the architecture in relationship to the use of it and the feedback to it, so that both will grow in maturity.

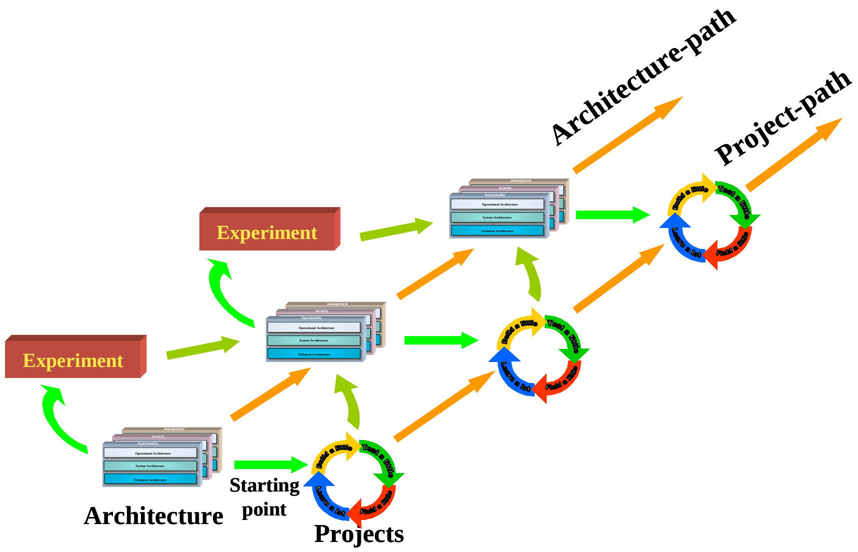

Figure 2 : Evolutionary development of the C3IA

The sum of these evolutionary architectures is the C3I Architecture; this will therefore evolve gradually. The most important issue at this level is the steering of the overall coherent development of the architectures for the different domains and aspects. This requires good architecture management, including a release planning of the architectures. The migration of the existing applications and systems must also be involved in the release planning.
In each step, many projects implement part of the overall architecture. All the results must have an added value to the architecture and to each other. The sum of these results must be planned and delivered to the end-users as a release. Thus the successive steps will deliver successive releases of the architecture. Each release will be used in projects. The use of each release of the architecture must be evaluated and fed back to the program responsible for the development of the C3I Architecture. Based on the evaluation the C3IA could be adjusted and changed, but even the planned parts of the architecture still have to be developed. The evolutionary development of the architecture will be managed and controlled by the applicability of the architecture in projects for the development of business processes, systems and technical infrastructure.

A **third vision** that is leading the developments of C3I systems is that de-facto standards should be adopted as much as possible. Sometimes a NATO-standard is a de-facto standard in this respect but for a lot of functions to be developed there are no NATO-standards available or following the NATO-standard would lead to excessive costs (due to tailored industry-solutions). In these cases an industry de-facto standard can be adopted to build the required function, and if necessary an interface to the NATO-standard will be provided.
Related to this, the development of C3I systems within the RNLA is done by making maximum use of COTS or MOTS components, wherever they are available and affordable, on the condition that they can be fitted in with the other components of the system and that they (can be adapted/enhanced to) deliver the required functionalities.

The **scope** of the C3IA is first of all the support of the command & control process at all levels of command for groundbased units, either within the RNLA but also outside like the Royal Marines. The technical infrastructure will however support **all** information services for the deployed (mobile) operations of groundbased units. This would include support for logistics informationsystems etc.

Basic **concepts** for the C3IA are:

C3I Generic Processes
In all C3I Systems, information is gathered, processed, presented and distributed. In most C2 systems information must be presented on a geographical map.
The various C3I projects are all based on this very general description. This supports the idea of defining a generic informationservices-framework and a generic ICT infrastructure for all C2 systems, which can be applied as the common C3I infostructure. Such an infostructure should comply with the C3I architecture. Applications should then fit into this architecture.

Zero-latency concept
A zero-latency concept is a concept that exploits the immediate exchange of information across geographical, technical and organisational boundaries to achieve business benefit. Latency is the time it takes for a system to respond to input. The modern enterprise can be viewed as a kind of a complex system. Divisions, departments and even groups in external business partners are treated as co-operating subsystems, regardless of where they are located.
Zero-latency is practically not achievable. It is a goal to aim for. The purpose of this concept is to support near real time Command & Control. That the COP for any commander should not lag behind for more than a few seconds.

Zero-Dependency concept
In a multi-tier client-server solution all the tiers have to be operative to enable any part of the functionality. This creates an all-or-nothing situation and graceful degradation is not possible. As much functionality as possible should be available when a server is disconnected. For the core C2-system (COP) the use of the client-server concept should be avoided anyhow, or serverfunctions should be replicated to avoid single points of failure.

Zero-maintenance concept
Because military operations depend more and more on ICT, instant and total function loss can have devastating effects. Furthermore, future C3I systems will be used by units that have no large ICT maintenance organisation. These problems have to be dealt with wherever possible. If avoidance is not possible, the consequences have to be minimised.
Systems can be designed to accommodate the zero-maintenance concept. This means that maintenance is not necessary and even impossible. In the event of a failure, the system is either self-healing or the failing unit is replaced, after which automatic reconfiguration takes place as much as possible (plug and play).

Actor Based Security Concept

Based on the guidelines from the security regulations, the Zero-Maintenance Concept and the Zero-Dependency Concept of the C3I Architecture, the security concept for the C3I architecture has to define a conceptual solution that can be implemented in an operational situation.

The actor is the initiator of activities; therefore the related security level of this actor has to be coupled to a person, a role or function element. Combined they will create and activate the necessary security levels.

On the basis of the above-mentioned overall concepts, the following characteristics of the architecture framework can now be described.

The architecture must be:

- a layered structure
- service oriented
- component based

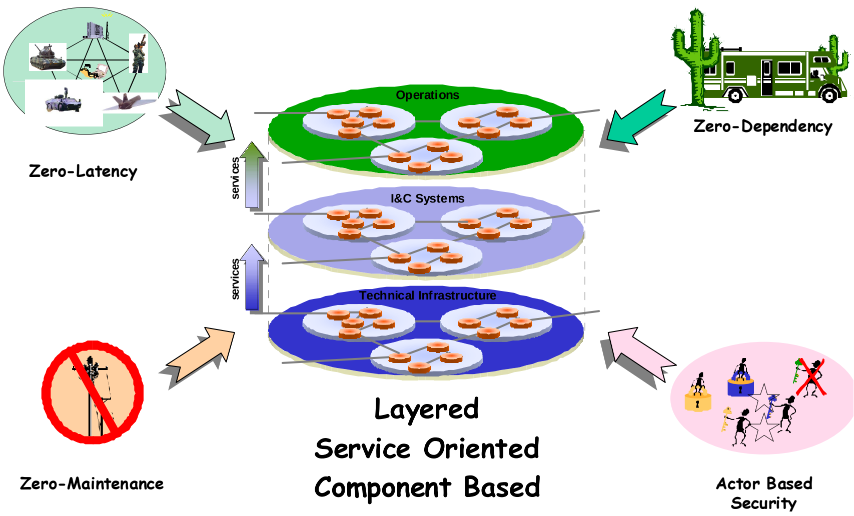

Figure 3 : Basic characteristics

3.2.3 Architecture Domains

The architecture is split up into three domains as a result of requirements in para 2.1: the Operational Architecture (OA), the System Architecture (SA) and the Technical Architecture (TA). Figure 1 shows an overview of the architecture domains.

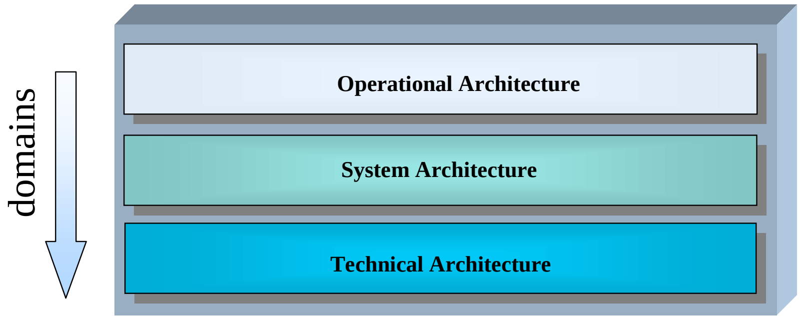

Figure 4 : Architecture Domains

Short description of the architecture domains:

The Operational Architecture (OA) helps to give an understanding of the operational environment (the operational scenarios, processes and organisation) for which ICT systems will developed to support the operational (command and control) processes.

Understanding of the operational processes is a prerequisite for the design and development of flexible solutions in the sense of information and communication systems. The Operational Architecture describes the operational processes, their relationships, process threads that will be triggered by Operational events and the description of the process by operational services.

The System Architecture (SA) describes the architecture of the Information Systems and the Communication Systems that are used to support the Operational processes. The System Architecture describes the resultant systems environment of the C3IA program. It describes which applications and communication systems will be present, how they will interact and where the Operational services will be implemented. Identified applications can be existing legacy applications, can be part of a newly installed (ERP) package or can be newly built within or outside the C3IA program.

The Systems Architecture describes the architecture of the individual systems by means of components that deliver services to support operational services for specific operational processes.

The Technical Architecture (TA) defines the infrastructure (middleware, hardware, network, transmissions media, protocols etc.) required to run systems. The other domains mainly trigger the development and change, not only by the functionality but also by the characteristics of those domains. Characteristics include performance requirements, volume figures, frequencies, actuality of information, method of use of functionality and resources, etc. The development and implementation of the technical infrastructure take these characteristics as a major input.

Although they are separate architecture domains, the three have strong relationships and for the different aspects of functionality, security and management, they together form the architecture for C3IA.

3.2.4 Architecture Phases

For each domain of the C3I architecture the three phases listed below will be followed:

Conceptual - this phase will describe the concepts, strategy, requirements and environmental constraints of the concerning track. In other words the conceptual phase will describe **what** is needed at the respective domain layers.

Logical - this phase will describe the mechanisms, design and structures at a logical level. In other words the logical phase will describe **how** the desired functions will be realised.

Physical - this phase will identify the mapping of the logical design in the physical environment of the products, components and interfaces that will be implemented, whether they are COTS/MOTS or internally developed. In other words the physical phase will describe the actual **implementation** of the desired functions.

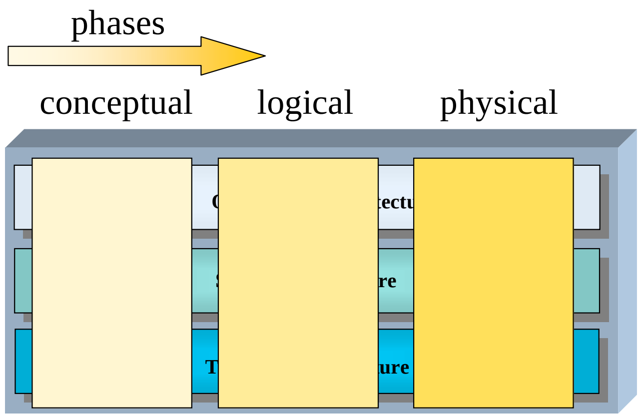

Figure 5 : Architecture Phases

3.2.5 Architecture Aspects or Subjects

The subjects of the architecture to be described can cover a variety of aspects that are of interest. The most important aspects are Functionality, Security and Management.

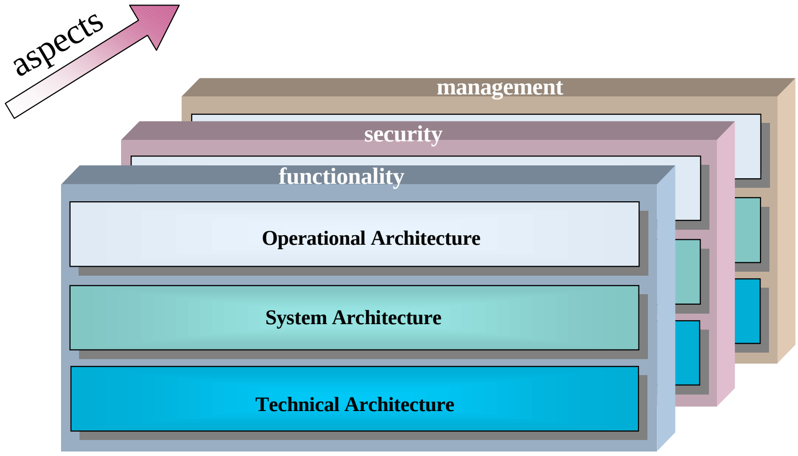

Figure 6 : Architecture Aspects

The most important architecture is the one that describes the core functionality of a business. This functionality deals with the vision, mission and goals of the organisation. The **Functionality Architecture** is therefore the primary architecture and the others are supporting architectures for other aspects.

The Security Architecture describes the security that must be taken into account for the formulated functionality. The architecture of the other aspects follows the same structure and also covers the same three domains, i.e. Operational, System and Technical (infrastructure). For example, the Security at the System Architecture level describes the security with respect to the Systems (Information systems and communication systems) in the Functionality Architecture.

The Management Architecture describes the management aspect that is needed for the control and changes of the implemented functionality, as well as the implemented security.

It also encompasses the management of the ICT operations, the control, administration and management of the objects which will be taken into operation and which are liable to change. This aspect also covers the administration and maintenance of the results of the Business Process Modelling activities.

3.2.6 Relationships between the architectures

Within each domain the specific architecture is, and will be further developed in relation to the others. For each domain there are the conceptual, logical and physical (implementation) phases. Not only within a specific domain must this be consistent, but also between the separate architecture domains and aspects.

The interdependencies between the domains and the phases allows a certain level of parallelism when developing these architectures, because it is impossible to develop the architectures for the total C3IA scope in full depth in a short period and in all of these domains. It is important to develop the architectures in sync in respect of the planning for releases (milestones) of the C3IA-realisationprogram.

The mapping of the architectures with regard to their contents and the planning of the evolution of the architectures is the essence of the overall program of C3IA. (See the chapter on the subject of the Evolutionary approach of the architecture).

In an ideal situation the Operations request the information and communication systems needed, as well as the technical infrastructure this requires. The development and change can also be triggered by technology changes, for example the changes that have occurred as a result of the development of hand-held devices or the Internet. Coming from the ICT-domain, within the C3IA this can be seen as a **technology push**, coming from the Operational domain it is a **business pull** for realisation

3.2.7 Positioning of projects and systems

With regard to the responsibility and the program planning of the architecture development it is important to restrict the scope of a project to an architecture sub-domain layer. The relations or impacts with the other layers (and vice versa) must be tuned to the overall architecture and other projects.

The C3I Architecture makes it possible to position the different projects in the overall architecture and to make clear which parts of it are conditional and for which parts it will offer services. These are the interfaces with which it has to link up, both with respect to content and organisationally.

In the following picture several development projects are mapped in the architecture framework.

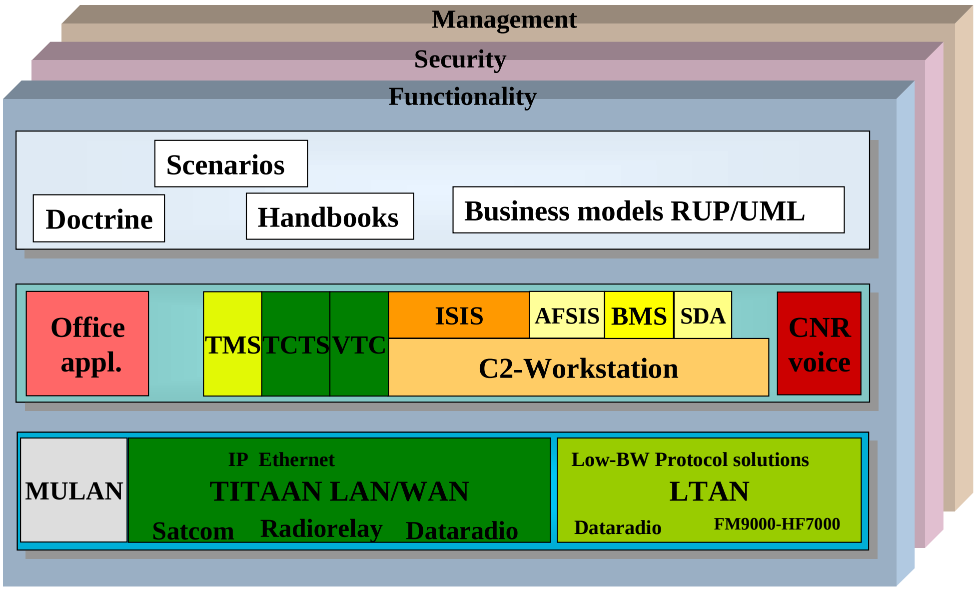

Figure 7 : Mapping of development projects

3.3 Architecture Documentation structure

As said before, for the purpose of this paper it is impossible to describe the architecture in more detail. To provide some insight in the level of detail that is in the C3I Architecture at present, the following picture shows the architecture document structure.

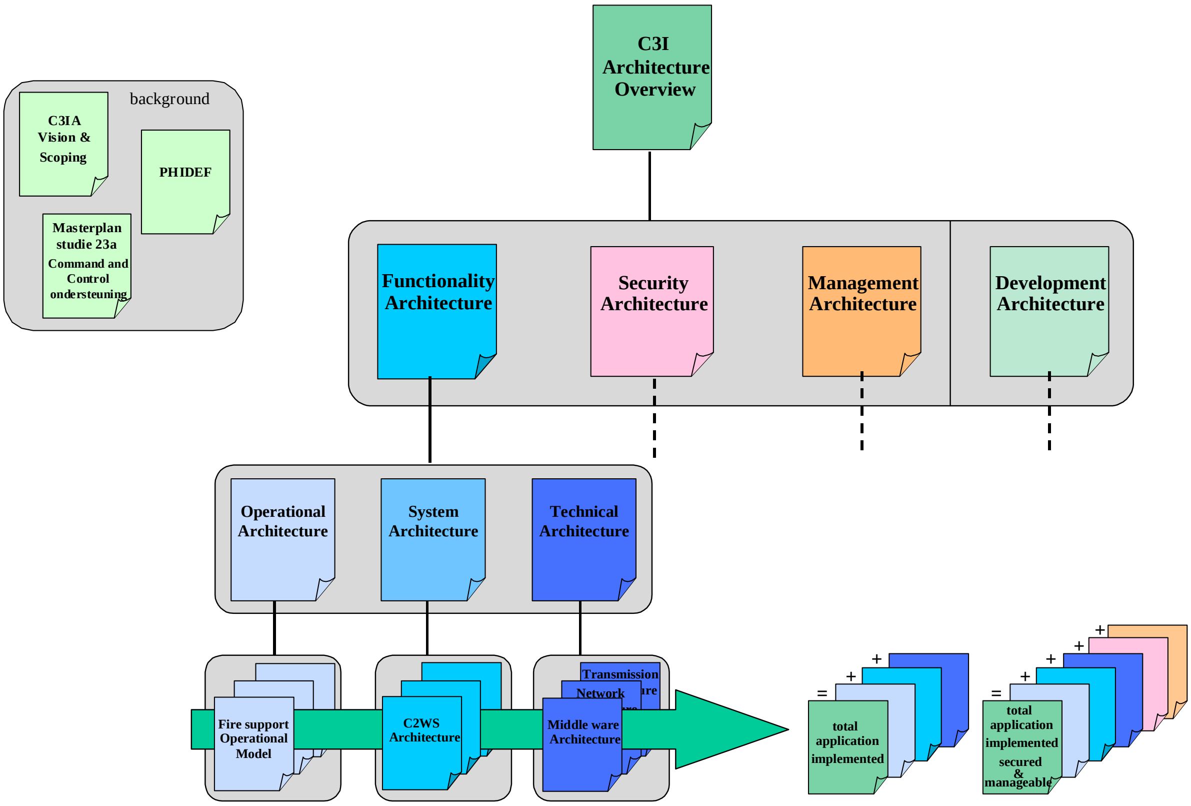

Figure 8 : Architecture document structure

The C3IA is organised into one major document "C3IA Architecture overview", followed by additional documents for each architecture aspect (Functionality, Security and Management). In turn, each aspect is worked out in three documents, one for each sub domain (Operational, System and Technical infrastructure, here only shown for Functionality).

For each sub domain several areas (mostly realised by different projects) can be identified and form a set for each sub domain. For instance for the sub domain System Architecture for the aspect of Functionality we recognise ISIS and the C2 Framework (C2WS in figure 8), or for the Technical Architecture e.g. the Network architecture and the Transmission architecture.

In accordance with the document organisation there are four levels of description (overview, aspects, sub domain, application/area). Each level deals with another feature of the architecture, and each level moving downwards provides more detail.

If the right areas/modules are assembled at the lowest level for a specific application / use, this gives that view from that standpoint. This could be a specific application for a user with all the functionality over all the sub domains possible, extended with the security and management aspects for that specific application (this is shown in the bottom right corner of the figure).

4.0 EXPERIENCES WITH DESIGN & DEVELOPMENT UNDER ARCHITECTURE

4.1 Organisation of architecture development

In the past four years the C3I Architecture has been developed step-by-step into its present release, where the description of the architecture parts (domains, phases en aspects) is now mature enough to serve as a guideline for all developments within the RNLA within the scope of the architecture. This could not have been accomplished without a team of architects, each an expert on his part of the architecture. Together they form the Global Architecture Team within the C2SC.
Experience has shown that for developing the Operational architecture, army officers with recent experience on C2 at several commanding levels are best suited for the job. For the System, the Technical and the Management architectures hired personnel from ICT-consultancy firms have proven to be the best fit. Only they can meet up to the high standard of (technical) knowledge and skills that are needed for the development of these architectures. For the Security architecture a mix of militairy and civil specialists is the best solution, because expert knowledge of (militairy and government) security regulations is needed as well as expert knowledge of state of the art technical security solutions.
Because of the required mix of militairy and civil expertise the architecture development is best performed under direct responsibility of the RNLA (C2SC). In the early stage (2000) an attempt to outsource has proven to be unsuccessful.

4.2 Usefulness

During these past few years the C3IA has proven to be very useful in two respective directions: upwards and downwards. Downwards as a tool for the managementteam of the C2SC to govern the running developmentprojects, as well as for drawing the roadmap for future developments. During the grow to maturity of the architecture there have been occasions that there were no sufficient guidelines for running projects which led to the projects developing their own guidelines. In some instances these were not in line with architecture guidelines that were developed later. That has led to rework in these cases. However the evolutionary approach that is followed within the RNLA offers sufficient opportunity-windows to correct these issues. As an example the development of the Dutch ISIS (Integrated Staff Information System) has started up on a client-server concept solution. This has led to a well-appreciated implementation of desired functions for commanders of units. During the architecture-development it has become clear that there were problems to be expected on scalability of ISIS, and the ISIS server posed too much of a vulnerability as a single point of failure. Further more the end-users (commanders and staffmembers) have a strong desire to be able to work on their ISIS workstation during the build-up and breakdown phases of the CIS-infrastructure when a commandpost is relocated. This has led to a complete new system-concept, based on a thick-client / peer-to-peer technology that is now implemented in the newest version of the ISIS system.

The usefulness in the upward direction has been proven during the development of the NL Defence Information Architecture (DIA), for which the C3IA has been used as a startingpoint. The NL DIA has adapted a framework very similar to the C3IA framework. This serves the purpose to connect architectures from the services and defence-level to each other, thereby enabling joint interconnectivity of informationdomains and the governance of central (defence) informationsystems projects.