



AGENCY TECHNICAL DIRECTIVE 00.01.02

NATO C4ISR System Design Principles

Effective date: 1 October 2011

Revision No: Original

Issued by: David Burton, Chief Technology Officer

Approved by: Georges D'hollander, General Manager

AGENCY TECHNICAL DIRECTIVE

NATO C4ISR System Design Principles

1. PURPOSE

The purpose of this document is to establish – based on existing NATO Policies and directives – a minimum set of system design principles that current capabilities should strive to evolve to, and new developments must comply with to facilitate the seamless sharing of information and services within the Alliance Consultation, Command and Control (C3) and Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) system environment to meet the Alliance's requirements.

2. APPLICABILITY

This Technical Directive is applicable throughout the NATO C3 Agency.

3. REFERENCES

- A) C-M(2007)0118, NATO Information Management Policy, dated 11 Dec 2007
- B) C-M(2010)0063, NATO Policy for standardization, dated 22 Jun 2010
- C) AC/322-D(2005)0053-REV2, NNEC Data Strategy, dated 14 Sep 2009
- D) EAPC(AC/322-SC/1)N(2008)0015-REV2
EAPC(AC/322-SC/1-WG/1)N(2008)0011-REV2, NATO Networked C3 Interoperability Policy, dated 22 Aug 2008
- E) NSA/0725-C3/5524, STANAG 5524 C3 (Edition 1), dated 14 Jul 2005
- F) NSA/0641(2007)5525, STANAG 5525 (Edition 1), dated 26 Jun 2007
- G) NSA/1120(2007)C3/5500, STANAG 5500 (Edition 6), dated 7 Dec 2007

4. POLICY

4.1 Scope

Within this document the term "NATO C4ISR System" is used to embrace all Information Systems and Services¹ developed or acquired by NATO civil or military bodies to support Alliance's missions, in particular enabling an efficient assessment of the situation, planning and execution at all levels.

4.2 Audience

NATO Civil and Military Bodies are already responsible for applying NATO Policies and Directives to all relevant aspects of their Programme of Work, this includes central planning, system integration, design and systems engineering for NATO C4ISR systems and installations. The NATO C4ISR System Design Principles are intended for all stakeholders – especially project and program managers – involved in Alliance C4ISR Capability Development.

5. PROCEDURES AND PROCESSES

5.1 Design Principles

A design principle is a generalized, accepted common practice in association with a common objective. When it comes to building solutions, a design principle represents a highly

¹ This does specifically address systems and services that fall into the following classes of the C3 Classification Taxonomy depicted in Fig. 1: User Applications, COI-Specific Services, COI-Enabling Services and Core Enterprise Services.

recommended guideline for shaping solution logic in a certain way and with certain goals in mind. Design principles are not necessarily right or wrong but are a reflection of the fundamentals that guide decision making in NATO C4ISR system development.

The fundamentals of information² and data management to be applied by NATO Nations and NATO civil and military bodies are established in the NATO Information Management Policy (Ref A). NATO Network Enabled Capability (NNEC) is the Alliance's way for federating various components of the wider C3 and C4ISR environment, which could be best characterized as a peer-to-peer federation with limited central control³. The NNEC Data Strategy (Ref C) identifies the goals for data sharing in this environment. The effectiveness and efficiency of such a federated environment is highly dependent on the level of interoperability of all its constituent parts.

Interoperability⁴ of information and C4ISR systems employed by NATO essentially rests upon two pillars: standardization (Ref B) and the enterprise architecture based planning approach. Interoperability is not an end in itself but is a key enabler and an important capability multiplier. The NATO Networked C3 Interoperability Policy (Ref D) mandates the definition of appropriate architectures and the selection of and adherence to appropriate military and open industrial interoperability standards.

The objectives of the NATO C4ISR Design Principles are:

- a) to support the achievement of information superiority within an information sharing networked environment; and
- b) to support the effective and efficient use of information resources in the conduct of the NATO mission.

The following 10 C4ISR System Design Principles have been derived based on the fundamentals laid down in NATO Policy:

5.1.1 Information Sharing

Responsibility-to-share is an obligation to make information and services available, discoverable and accessible. Information and services must be structured for global deployment in various nations and support multi-language and multi platforms. Users and applications must be enabled to discover the existence of information and services through catalogues, registries, and other search and other discovery mechanisms. Information (raw data, and processed) and services are to be advertised or "made visible" by providing metadata, which describes the asset and make it discoverable. Metadata shall be extracted or provided by applications automatically whenever possible (e.g. using business rules) and validated against appropriate standards in order to guarantee data consistency and quality. Data developed due to business rules or other algorithms should be checked to ensure that it is in compliance with those rules/algorithms. Security-related metadata will be provided to facilitate access to information protected under the security principle of 'need-to-know'.

² Information is any communications or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual forms.

³ See also "NATO Network Enabled Capability Feasibility Study (NNEC FS)" Version 2 dated October 2005.

⁴ Interoperability is the ability to act together coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objectives.

5.1.2 Information Ownership and Custodianship

Communities of Interest (COI) shall identify authoritative sources for information and services within their domain. To avoid duplication, all information will be sourced from dedicated repositories, managed and maintained by the responsible COI. Capability Developers shall assist COIs in resolving potentially conflicting sources and, where appropriate, coordinate with the NATO-wide governance body to identify authoritative source(s).

Duplication of information shall be avoided and authoritative sources are to be designed so that information can be reused by as many COIs as possible. Electronic information systems are only as good as the data they process; therefore the acquisition of critical data (sources) for a system must be part of the overall capability development process; in case of system replacements data migration must be planned.

Developers need to ensure that authorized users and applications have immediate access to data posted to the network with minimum processing, exploitation, and dissemination delays. Users and applications shall “tag” data assets with metadata (data about data) that enables intelligent, efficient access and management of data.

5.1.3 Information Assurance

Designing any solution for the Alliance C4ISR enterprise need to take potential attacks of aggressors into account; therefore a predictive analysis of potential threats and risk must be part of the solution design process from the outset. Planners must have a precise understanding of active and emerging threats so that they can design solutions in anticipation to oppose cyber-attacks against computers and networks.

Systems must be designed to protect information that they store, process or transmit with respect to confidentiality⁵ (“need-to-know”) and integrity⁶, as well as to guarantee the availability⁷ of the information. Depending on the specific use cases systems must also be enabled to prove the integrity and origin of information and provide accountability of service use and information access by maintaining internal records. Instead of application specific mechanisms, core authentication services shall be used.

A particular challenge within the Alliance context is the ability to exchange information across different security domains. Observing the “responsibility-to-share” obligation, systems must be designed at the outset to allow for automated sharing of information by labelling data at the object and where appropriate at the attribute level with standard security metadata.

5.1.4 Re-use and Federation

In designing solutions pursuing a “one-size-fits-all” strategy based on a single vendor, a single hardware platform or a homogeneous software family must be avoided. However, the (re-) use of recognized design patterns shall be maximised. The flexible deployment of systems through acceptance of heterogeneous and scalable solutions, using the Internet and its principles as a model is the preferred approach as it facilitates the ‘ability-to-federate’ capabilities. When designing solutions, developers shall take different mission requirements

⁵ confidentiality – assurance that the information is accessible only to those who are authorised to have access.

⁶ integrity – a guarantee of the exactness and completeness of the information, and the methods for processing it.

⁷ availability – assurance that the users have access when they require it.

from all relevant scenarios as defined by NATO's Defence Planning Process (NDPP) into account in order to avoid "over-optimising" a system for a particular mission.

Alliance C4ISR solutions shall be designed so that re-usable functionality is being made available as services. If life cycle costs and functionality merit an enterprise wide usage those services shall be designed so that they can be scaled up and deployed as enterprise services by NATO or NATO nations. Autonomy and loose coupling promotes the independent design and evolution of a service's logic and implementation, enabling re-usability and positioning of services as enterprise resources. Reducing the degree of coupling fosters interoperability by making individual services and components less dependent on others and therefore more open for invocation by different consumers.

With a federated environment management of change is a very complex task. From a C4ISR Systems design perspective, systems must be designed so that they are backwards or downward compatible and that a new system or technology is able to fully take the place of an older system or version of the same product, by inter-operating with systems that were designed for the older system. Backward compatibility is a relationship between components and systems, rather than being an attribute of just one of them. A new system or service must be designed to provide all of the functionality of its predecessor. In practice backwards compatibility cannot be maintained forever, software and service interfaces and exchange formats must be maintained for at least a period of 24 months before they can be deprecated and support can be dropped in later releases.

Solution developers shall also share the knowledge behind the design of new software solutions developed under NATO funding. With access to NATO Community Developed (NCoDe) software and specifications underpinning software design, developers across the enterprise either within NATO bodies, NATO nations or national defence industries can create new and innovative solutions to meet operational requirements utilising existing knowledge and solution patterns. Using open source software, products developed collectively by the NATO Community and open industry standards as the baseline to underpin technology solutions increases the interoperability of systems, proliferation of systems and improves delivery of services to the wider NATO enterprise and – if and when required – to non-NATO entities as well.

5.1.5 Architecture Approach

In general, development of enterprise C4ISR capabilities results from the identification of a need for such capabilities through the NATO Defence Planning Process (NDPP) or as a result of a capability gap analysis for current operations. In a complex, dynamic and loosely coupled environment like the NATO C4ISR Enterprise, centralised long-term planning approaches have limitations. Therefore all architectural and acquisition activities should apply an evolutionary approach where in parallel to the on-going planning activities projects are realising field able systems that deliver required functionalities. In order to succeed, projects shall work incrementally starting small and targeted, expanding over time.

All design activities are to be conducted within an architectural approach to provide coherence (Ref D). The engineering or acquisition of solutions must utilise target architectures that are to be aligned with the applicable Reference Architectures (RA) and with the overarching C4ISR enterprise architecture as an integral part of the system design process. To achieve interoperability at the enterprise level, reference architectures must specify their interface

requirements as detailed as possible by developing reference designs⁸ where comprehensive interface specifications are to be defined between key modules within RAs and between other Architectures.

Architectural information and products shall be centrally managed to enable coherence checks, alignment of pan-enterprise business process, training needs analysis, optimisation of infrastructure usage and support arrangements etc.

The overarching architecture defines and maintains taxonomies and ontologies like the NNEC services framework that are to be used for linking activities in different C3 communities (e.g. defence planning, standardization, acquisition, operation and support). NATO C4ISR solutions must be designed in accordance with the C3 Classification Taxonomy (see Fig. 1).

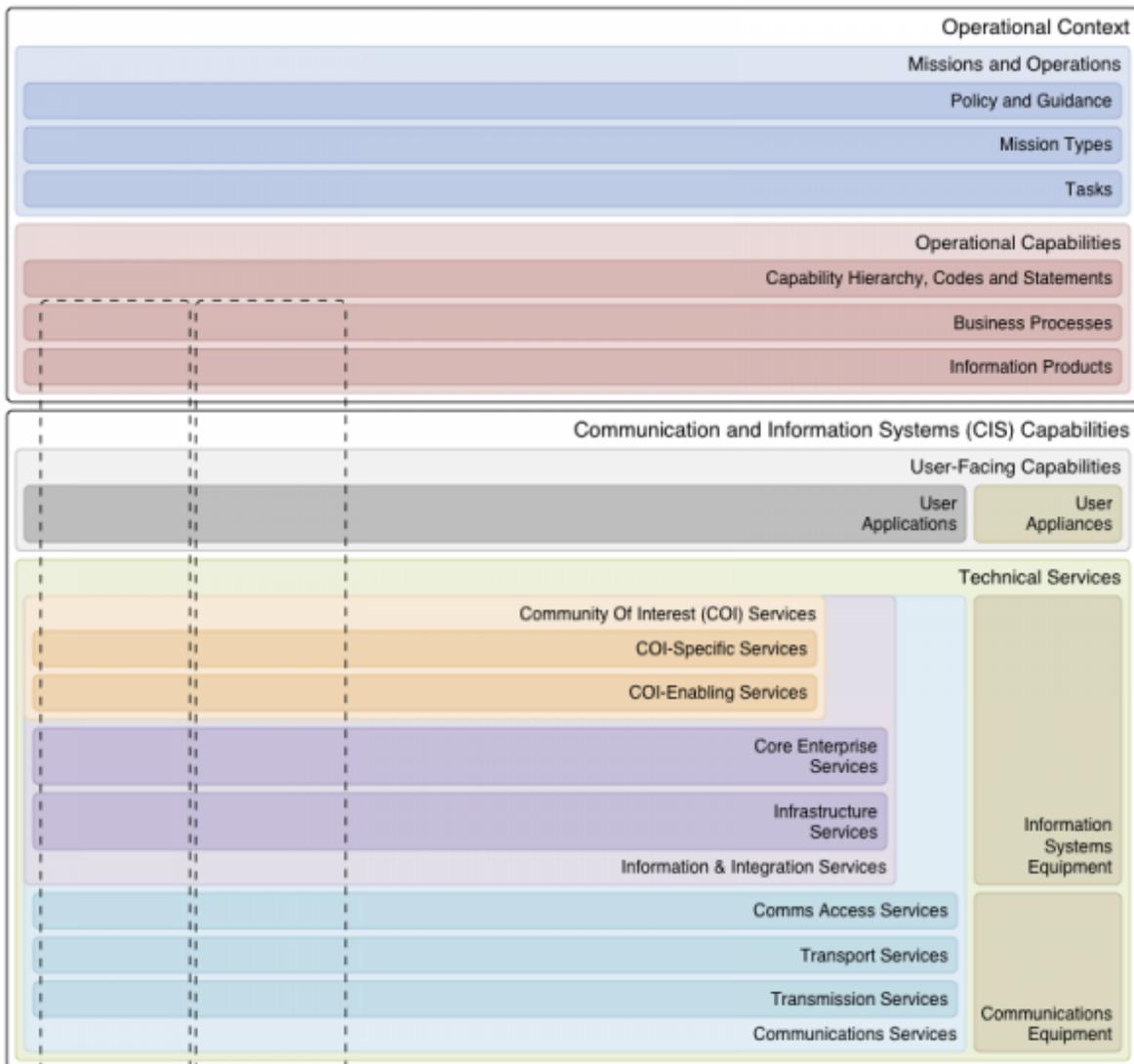


Fig. 1: C3 Classification Taxonomy

⁸ The term “reference design” is not defined within the current NATO Architecture Framework. A reference design is a technical reference architecture amended by detailed interface specifications and an associated Interoperability Standards Profile.

The C3 Classification Taxonomy is part of the overarching Service Oriented Architecture (SOA) approach. The taxonomy is a typical hierarchical model consisting of nine layers (User Applications, User Appliances, COI-Specific Services, COI-Enabling Services, Core Enterprise Services, Infrastructure Services, Communication Access Services, Transport Services, and Transmission Services) organized into four broad categories (User interface or presentation services, Community of Interest Services encapsulating functional and business logic, Information & Integration Services, and Communications Services). Each layer may talk to a layer adjacent to it (e.g., a User Application may call a COI-specific service via the communication module of the User Appliance which could be a workstation or a mobile device).

5.1.6 User Focus

Development of new enterprise C4ISR capabilities takes time; the specificity of requirements increases over time and the more specific requirements become the rate of change increases. The process of requirements engineering can be divided into discrete steps usually preceded by a feasibility assessment and stakeholder analysis. There are various approaches for conducting requirements engineering. Typical steps are requirements elicitation, requirements analysis and negotiation, requirements specification, system modelling, requirements validation. Capability Developers shall follow a standard or industry best practice approach like IEEE 830-1998 which describes the specification of software requirements.

Requirements need to be maintained and managed throughout the complete life-cycle of a capability. To avoid scope creep, requirements must be documented in formal requirements baselines, and any requirements change need to be dealt with through the appropriate change request process.

Next to current operational requirements, capability developers must take into account emerging requirements and associated targets developed through NATO's Defence Planning Process (NDPP). Any work required to further develop the NDPP requirements to the appropriate level of detail must be based on the same assumptions and operational context (mission types, generic planning situations and case studies) as defined in the NDPP and must be traceable to the Level of Ambition stipulated by NATO Defence and Foreign Ministers. NDPP requirements shall be incorporated into the overarching architecture.

The operational environment generally equates to echelons ranging from the strategic level (including NATO HQ) down to the tactical level. Software components must meet the needs of their operational environment(s) while maintaining alignment with overall goals and priorities. Solution designers must document and understand not only functional and technical requirements but also the operational environment, business processes, different military functions and associated decision making processes and of the user communities they are supporting.

Solution developers must understand business processes within the C4ISR enterprise in order to design solutions that can adapt to changing operational requirements and conditions by modifying flows between business services. SOA is based on the notion of being able to initiate dynamic collaboration across constituents. SOA therefore requires that the component parts of how a business operates are being designed and delivered as re-usable or isolated services without over-specifying particular business contexts and addressing the typical needs of the military environment.

In order to prevent information overload, solutions developers must use their understanding of business process to identify typical user roles and associated information needs so that information can be made available to the right person, at the right time in the right format.

User interface capabilities or applications must be defined as simply as possible, focusing on typical roles and processes; by reducing complexity, training can become shorter and more role focused. Not all activities in a workflow must be automated; solution designers shall perform holistic cost-benefit analyses across technical and human boundaries often resulting in more flexible and cost effective solutions.

5.1.7 Information Standards

All information representations must be semantically aligned with the corporate core data exchange model, e.g. for non-real-time data exchange the Joint C3 Information Exchange Data Model (see Ref F) domain values shall act the starting point. If information requirements cannot be reflected in the core data exchange model or by other already endorsed Information Exchange Specifications (IES), COI specific extensions may be developed and existing COI specific data models and IES shall be harmonised with the corporate core data exchange model. Users and applications can understand and interpret the data, both structurally and semantically, and readily determine how the data may be used for their specific needs. COI shall develop representations such as taxonomies or ontologies that reflect the communities' understanding of their data that can be shared with other communities to facilitate a common interpretation. However, within a loosely coupled SOA environment the preferred data exchange mechanism is message oriented, therefore any system design must also consider the Concept of NATO Message TextFormatting System (CONFORMETS) (Ref G) in addition to Ref F⁹.

All data exchange activities shall adhere to published network-enabled interoperability standards, including information and data standards and exchange mechanisms where applicable. Metadata must be made available to allow, in part, mediation or translation of data between interfaces, where no data exchange standard exists. Data assets are typically provided in a common structure such as eXtensible Markup Language (XML). Mediation and translation are to be the exception not the rule.

5.1.8 Technical Standards

Solution designs that depend on particular commercial products or vendors are to be avoided. Where no applicable open civil standard exists or if there are compelling reasons that did require the development of a dedicated NATO standard, the NATO standard is to be used. Suitable open civil and military standards for each NNEC service area are listed in NATO Interoperability Standards and Profiles (Ref E).

When designers are faced with situations where multiple competing standards exist, the decision on which standard to use must not be made locally. It needs to be deferred to the overall Design Authority for the NATO C4ISR Enterprise. For larger projects and programs (e.g. Bi-SC AIS, Afghanistan Mission Network (AMN)), dedicated standards profiles are to be developed and maintained throughout the system life-cycle.

5.1.9 Communication and Infrastructure Environment

In a military enterprise, service-based capabilities must be designed taking communications constraints into account. Each echelon is characterized by the availability and robustness of

⁹ Within the NC3B there is a long term effort to harmonise STANAGs 5500 and 5523.

the network (connectivity, bandwidth, latency, reliability and predictability). Depending on the echelon and mission criticality, capabilities must be designed to cope with situations of disconnected, intermittent and limited communications. C4ISR capabilities must be capable of autonomous operation in the event of unavailability of reach-back communications and/or services for a period of up to 24 hours¹⁰.

Being cognisant of networking and infrastructure constraints also means that solution developers must explicitly assess and calculate expected networking and infrastructure requirements for their solutions. These requirements must be documented and made available to the Enterprise Architects in order to inform or generate projects improving the lower layers of the NNEC Services Stack.

Enabling flexibility for the deployment of C4ISR capabilities requires the abstraction from a physical infrastructure. C4ISR server side capabilities must be designed to be hosted on a standard environment consisting of a virtual machine, a guest Operating System, Commercial Off-The-Shelf (COTS) and/or NATO Off-The-Shelf (NOTS) software, such as an application server or database, and COI enabling services provided in a static or deployed configuration. Access to information should be controlled through a single point of authentication infrastructure.

5.1.10 Verification and Validation

In addition to functional requirements compliance and to standards or policies conformance solution developers must define a set of criterion to assess specific characteristics that qualify a system or a service. Those measures of attributes (MoAs) could specify a number of quality factors such as: interoperability, reliability, efficiency, supportability, agility, measurability, utility and last but not least usability.

Measures of effectiveness¹¹, measures of performance¹² and associated test cases are to be specified during the requirement analysis and design phase and must be made available at the beginning of the system/service acquisition or development so that it can be ensured that all requirements are testable. Applications requiring critical response time should be thoroughly tested for performance under realistic conditions e.g. testing C4ISR capabilities with large (test) data volumes in realistic networking and infrastructure environments.

Selecting and implementing standards as defined by STANAG 5524 (Ref E) is not sufficient to ensure interoperability, due to the ambiguity of civil and NATO standards and the lack of common agreement as to the usage of optional components. Projects shall plan to establish sufficiently detailed design parameters associated with each required profile and plan appropriate interoperability verification capabilities and activities to ensure that it can actually deliver the expected level of interoperability.

¹⁰ Scenarios for autonomous operation include:

- Complete loss of reach back for a complete theatre of operations;
- Isolation of single Command and Control (C2) elements;
- Isolation of users attached to tactical or liaison nodes.

¹¹ Measures of effectiveness (MoEs) consist in a set of criterion used to assess the physical configuration of a system, or any change to its condition, configuration, behaviour, or capability to reach a certain state, to achieve a task, to accomplish a mission or to produce an effect. MoEs measure the degree to which a system or a service can be used according to prescribed concepts of operations, under specified standards and conditions.

¹² Measures of performance (MoPs) consist in a set of criterion to evaluate the varying levels of task achievements, mission accomplishment or effect production. MoPs measure the degree to which a system or a service can deliver predefined objectives, under specified standards and conditions.

Reliability requirements address the system itself, test and assessment requirements, and associated tasks and documentation. Reliability requirements are to be included in the appropriate system/subsystem requirements specifications, test plans, and contract statements. Reliability testing throughout the development process will discover potential problems with the design as early as possible. The most common reliability program tasks are documented in reliability program standards, such as MIL-STD-785 and IEEE 1332.

Utility (or 'fit for purpose') and usability (or 'fit for use') become the final arbiter of quality; therefore in addition to more technical related verification activities, project managers must plan for utility and usability tests from an end user and from a wider business process perspective. Utility testing will de-risk the acquisition/engineering phase, by verifying the implementation of NNEC guiding principles, and should be driven by architects. Usability testing need to take knowledge about human computer interfaces and wider human factors issues into account. Without passing the user acceptance test at the end of the development process all other activities are useless, therefore users should be engaged throughout the system definition and design stages, to ensure that the systems meet their needs and expectations.

6. SUMMARY

Managers responsible for NATO C4ISR systems development shall use the NATO C4ISR Systems Design Principles laid out in this document to develop more detailed implementation directives and training programs for their staffs. Individuals involved in NATO C4ISR systems acquisition and development shall use these principles to direct their activities.

Staff responsible for providing coherence and quality control to the NATO C4ISR systems development and acquisition process shall use these NATO C4ISR Systems Design Principles to verify that implementation projects and programs adhere to them.

This framework is neither exhaustive nor fixed in concrete and will have to evolve as NATO's transformation progresses. Gaps and overlaps identified during on-going capability development activities are to be documented and provided as change requests to NC3A CTO.