FFI-rapport 2013/01729

Architecture for the Norwegian defence information infrastructure (INI) – remarks on the C3 Classification Taxonomy

Trude Hafsøe Bloebaum, Jo Erskine Hannay,
Ole-Erik Hedenstad, Svein Haavik
and Frode Lillevold

FFI Forsvarets forskningsinstitutt

FFI-rapport 2013/01729

Architecture for the Norwegian defence information infrastructure (INI) – remarks on the C3 Classification Taxonomy

Trude Hafsøe Bloebaum, Jo Erskine Hannay, Ole-Erik Hedenstad, Svein Haavik and Frode Lillevold

Norwegian Defence Research Establishment (FFI)

14 June 2013

FFI-rapport 2013/01729

1176

P: ISBN 978-82-464-2294-7
E: ISBN 978-82-464-2295-4

Keywords

Arkitektur

Informasjonsinfrastruktur

Interoperabilitet

Approved by

Rolf Rasmussen	Project Manager
Anders Eggen	Director

English summary

The Norwegian Defence Research Establishment (FFI) has during the past decade conducted research on architectural topics related to the Norwegian Defence Information Infrastructure (INI). Recently, these activities have focused on service orientation; in line with strategic decisions in NATO. At the same time, the impact on the INI from these activities has been modest. Therefore, the Norwegian Armed Forces Architecture Advisory Board and the Norwegian Armed Forces Logistics Organization is now initiating a collaboration with FFI on central aspects of architecture development.

The Information Management Division at FFI has identified a need for active use of architectural descriptions as a common reference for many ongoing activities. In particular, there is a need for a common understanding and description of the INI architecture. FFI's strategic decision to continue focusing on Network Based Defence (NbF) puts renewed emphasis on this issue. The department has decided to put together a working group, consisting of members from a number of relevant projects, to investigate this issue. The group will initially consist of resources from the service-oriented architecture (SOA), modeling and simulation, land domain, communications and information security research communities.

This working group, "Architecture for INI", has been given the following tasks:

- The long term goal is to create an architectural description of INI
- The short term goal is to test an approach to architectural descriptions based on the NATO C3 Classification Taxonomy and existing INI reference models. Using this approach, the group will try to describe elements relevant to the group's expertise
- The results of the work done by the group will be documented in a report
- The architectural descriptions generated by the group can be used as a template when considering what to implement in the upcoming INI laboratory at FFI
- Relevant research communities at FFI will be involved when the need arises
- The group is encouraged to clarify the relationship between the C3 Taxonomy and the NATO Architecture Framework

The working group has, through its work on the C3 Classification Taxonomy, identified the strengths and weaknesses of the C3 Taxonomy. The process of developing and refining the taxonomy is still on-going. This means that there are variations in the maturity and level of detail provided by the taxonomy based on which part of it one studies. The high level structure and descriptions are fairly stable and mature. In addition, the overall structure of the taxonomy is compatible with a service-oriented approach.

Two significant challenges to using the C3 Taxonomy arises when considering the C3 Taxonomy's description of the communication layer and its handling of cross-layer issues such as information assurance and service management and control.

Sammendrag

FFI har de siste 10 år hatt aktiviteter på arkitekturarbeid i forbindelse med Forsvarets Informasjonsinfrastruktur (INI). I den senere tid har disse aktivitetene vært fokusert rundt tjenesteorientering, noe som er i tråd med de strategiske beslutningene som er tatt i NATO. Aktiviteten innen arkitektur har vært lav de siste årene, men forventes å øke i forbindelse med en revitalisering av Forsvarets Arkitekturråd. I tillegg har Cyberforsvaret og FLO/IKT invitert FFI til et samarbeid om sentrale deler av arkitekturutviklingen.

Avdeling Ledelsessystemer ser behovet for aktiv bruk av arkitekturbeskrivelser som noe som forener mange av våre prosjekter. Særlig har det vært pekt på et behov for å ha en felles oppfatning/beskrivelse av en arkitektur for INI. Dette er også et aktuelt behov sett i lys av instituttets satsning på Nettverksbasert Forsvar (NbF) som et strategisk område fremover. Avdelingen ønsker å bruke representanter fra relevante prosjektmiljøer til å gjøre en innsats for dette på deler av sin arbeidstid. I første omgang involveres ressurser innen tjenesteorientert arkitektur (SOA), modellering og simulering, land-domenet, kommunikasjon og IT sikkerhet.

Den 21.1.2013 ble det derfor gitt et mandat til en arbeidsgruppe “Arkitektur for INI” som følger:

- Det langsiktige målet er en beskrivelse av en arkitektur for INI
- Det kortsiktige målet er å prøve ut en fremgangsmåte basert på C3 Classification Taxonomy og de referansemodellene av INI som finnes, og søke å beskrive inn de elementene som pekes på fra våre fagmiljøer
- Resultatet fra gruppen skal dokumenteres i en rapport som inkluderer en anbefaling til videre arbeider.
- Arkitekturbeskrivelsene kan med fordel stå modell for det som skal implementeres i vår kommende INI-lab
- Relevante fagmiljøer på FFI involveres etter behov
- Gruppen utfordres til å etablere et avklart forhold til bruk av NATO Architecture Framework. Innholdet i beskrivelsene er viktigst.

Gruppen har, gjennom sitt arbeid med taksonomien, dannet seg et bilde av taksonomiens sterke og svake sider. Ettersom prosessen med å utvikle C3 Classification Taxonomy fremdeles pågår varierer modenheten og detaljnivået kraftig mellom de ulike delene av taksonomien. På høyt nivå er strukturen og innholdet forholdsvis stabilt og modent. Det kan også nevnes at taksonomiens overordnede struktur er kompatibel med en tjenesteorientert tilnærming.

De to største utfordringene når det gjelder bruk av C3 Classification Taxonomy er relatert til taksonomiens beskrivelser av kommunikasjonslaget og dens håndtering av krysslagfunksjonalitet, slik som informasjonssikkerhet og tjenestehåndtering.

Contents

1 Introduction

The Norwegian Defence Research Establishment (FFI) has over the past decade conducted research on architectural topics related to the Norwegian Defence Information Infrastructure (INI). Recently, these activities have focused on service orientation; in line with strategic decisions in NATO. At the same time, the impact on the INI from these activities has been modest. Therefore, the Norwegian Armed Forces Architecture Advisory Board and the Norwegian Armed Forces Logistics Organization is now initiating a collaboration with FFI on central aspects of architecture development.

From a research perspective, the Information Management division at FFI sees the need for an explicit use of architecture methodology and models to unifying many of FFI's ongoing projects. To reflect the vision of networked-enabled defense (NbF), it would be benficial to integrate projects and results in a mirror version of the INI which demonstrates the feasibility of a service-oriented information infrastructure supporting NbF. Such an "experimental INI" will then be a first working service-oriented information infrastructure, from which the constructors of the INI may gather results and guiding principles.

A prestudy was initiated at FFI in January 2013 with the purpose of mapping the ground for addressing the strategic initiatives above. The prestudy involved a small subset of FFI's research portfolio which, nevertheless, was expected to bring into play essential issues for architectural work for INI. The involved domains were communications, core enterprise services, land applications, modeling and simulation applications and information assurance. The first two domains (communications and core enterprise services) are generic technical enablers for the user-facing applications (land applications, modeling and simulation applications), while information assurance is a cross-cutting concern over all domains in an information infrastructure. The idea is to do initial deliberations and exemplify with this modest set of domains, and to extend the study with further domains when the path forward has been clarified.

The main contribution of this prestudy is an assessment of the feasibility of applying the C3 Classification Taxonomy as basis for architecture descriptions of the INI. This assessment is done based on current research that is on-going at FFI, since these represent functionality that is likely to be found in a furture INI. The assessment covers the feasibility of using the taxonomy to describe both future and ”as is” architectures.

The report is structured as follows: In Chapter 2 we introduce the C3 Classification Taxonomy along with terms, concepts and initiatives that are relevant for information infrastructures and their architectures. We give an assessment of the technical areas covered by the C3 Taxonomy and also the feasibility of applying the C3 Taxonomy in Chapter 3. Further, in Chapter 4 we give two examples of using the taxonomy. The way forward is given in Chapter 5.

2 Information Infrastructures and their Architectures

An information system is, by the Encyclopedia Britannica, defined as "an integrated set of components for collecting, storing, and processing data and for delivering information, knowledge, and digital products." This fairly broad definition of an information system includes software and hardware components, as well as telecommunication resources, security mechanisms, and human resources and processes. In our discussion we will use a somewhat narrower definition of the term *information system* to refer to application software that collect, store and process information, and the communication resources needed to access the communication systems.

An *information infrastructure* is, in our discussion, a system of interoperating information systems, the communication systems that connect them, the security systems that protect them, and the related service management systems. Usually, individual systems are designed with the intent that their constituent parts *interoperate*; i.e., work together and communicate with each other to fulfill the system's goals. When assembling systems into a system of systems; i.e., an *information infrastructure*, it is not obvious that the systems will interoperate well—or at all—without considerable effort. This is because individual systems are often not designed to interoperate with other systems; and in particular, not designed to interoperate with a range of systems that may not be known at the time of design (design time). The idea of service orientation is that systems can be designed to interoperate with other, perhaps future systems.

In addition to the terms information system and information infrastructure, we also use the term 'architecture", which is a structural description at some suitable level of abstraction of a (planned) concrete working system. We will also use the term "architecture framework" to denote a framework for developing architectures. We will later introduce the terms "overarching architecture", "reference architecture" and "target architecture".

An *architecture* of a system is, according to ISO/IEC 42010:20071:

> The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution.

Thus, an architecture provides plans or blueprints for the system, as we indicated above. But there should also be a methodology for constructing an architecture and for maintaining it. Such a methodology is what we here refer to as an *architecture framework*. In addition, we hold that there should exist a methodology for constructing a working information system from an architecture; see Figure 2.1. An architecture framework is a specification of what an architecture should be, preferably with a methodology for constructing a concrete architecture according to the framework. In turn, an architecture should preferably come with a methodology for constructing a working system (e.g., an information system) according to the architecture.

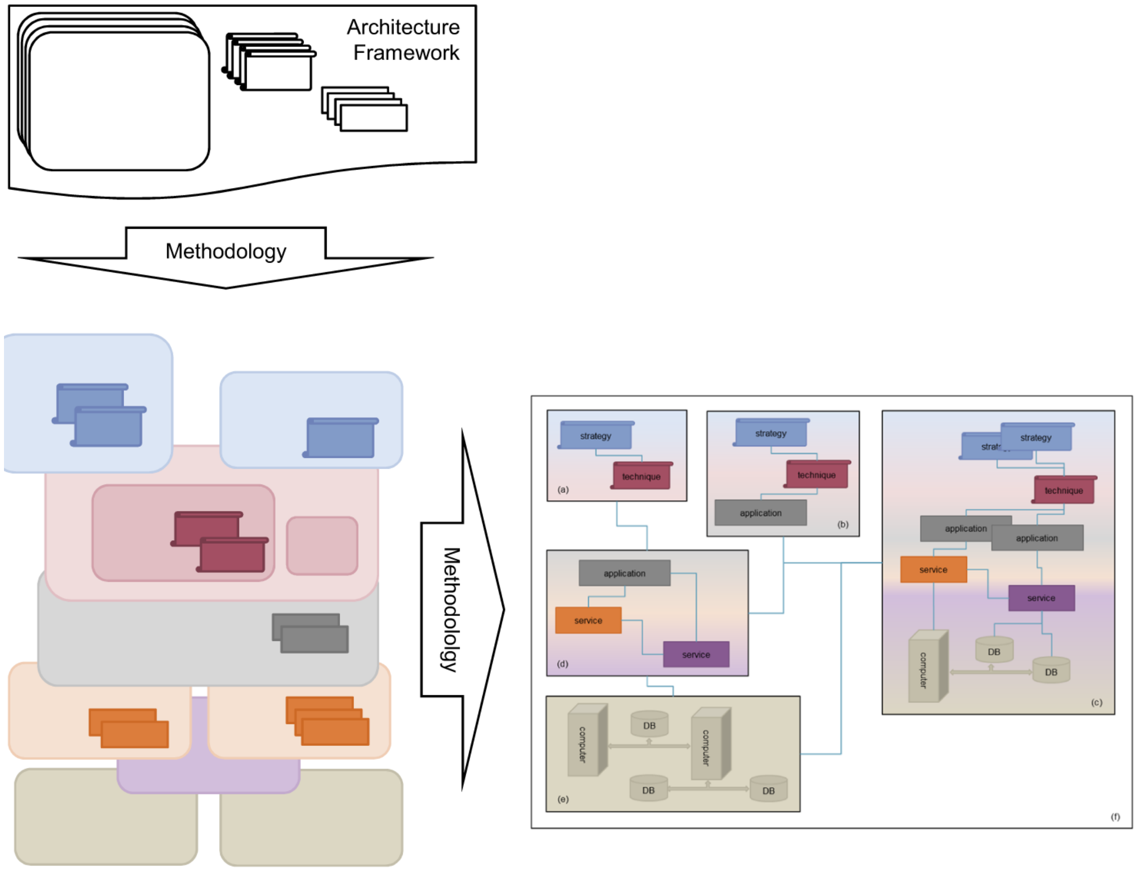


Figure 2.1 Methodologies are used to transform between an architecture framework, an architecture and an actual system, shown here as a complex system-of-systems.

2.1 Service-Oriented Architecture

Service-Oriented Architecture (SOA) is an architecture designed specifically for building distributed systems that have a high degree of support for interoperability with other information systems. There are many definitions of SOA, but the most commonly used is the following definition, which is a part of the SOA Reference Model from the standardization organization OASIS [23]:

> SOA is a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations.

This definition highlights one of the key principles behind SOAs, namely the fact that distributed capabilities need to be accessible via a uniform method. These distributed capabilities, also known as services, are all accessed using the same data formats, message types, protocols and standards. In addition to the uniform and standardized interfaces in the above definition, there exists a set of SOA principles that capture the key properties a service-oriented system should be based upon [8].

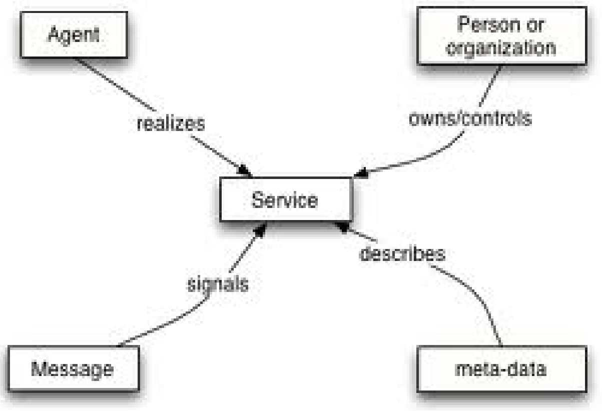


Figure 2.2 The service*, and how it relates to other SOA concepts, from [30].*

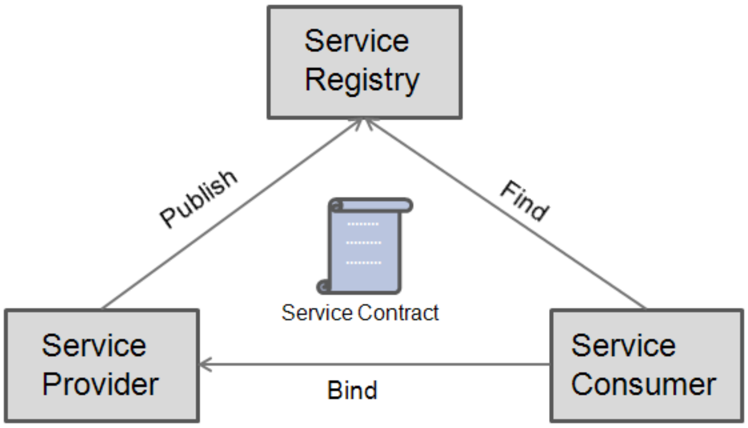


Figure 2.3 The SOA Triangle, which shows the relationship between the main SOA entities.

The key concept in a SOA is that of a service, which can be seen as a capability made available through a predefined interface. Figure 2.2 shows a simplified view of the properties of a service [30]. The agent that implements the service, often called the *service provider* is responsible for providing the metadata that describes the service. This description, known as the service contract or service description, is made available through the use of a discovery service. This service functions as a directory of services, and allows potential *service consumers* to find out which services that are available, and how to use them. Figure 2.3 shows the three main entities within SOA and their relationships to each other.

NATO has, for a number of years, focused on SOA as the key enabler for interoperability in future NATO coalition networks. This is because the focus on standardization within SOA makes it possible to achieve interoperability throughout the coalition, while at the same time supporting the need for autonomy of national systems. Building a federation-of-systems, where each system remain autonomous, relies on the fact that the interfaces between systems are clearly defined if interoperability is to be achieved. The high level of standardization, and the focus on interface descriptions, means that SOA is well suited to build such federated systems.

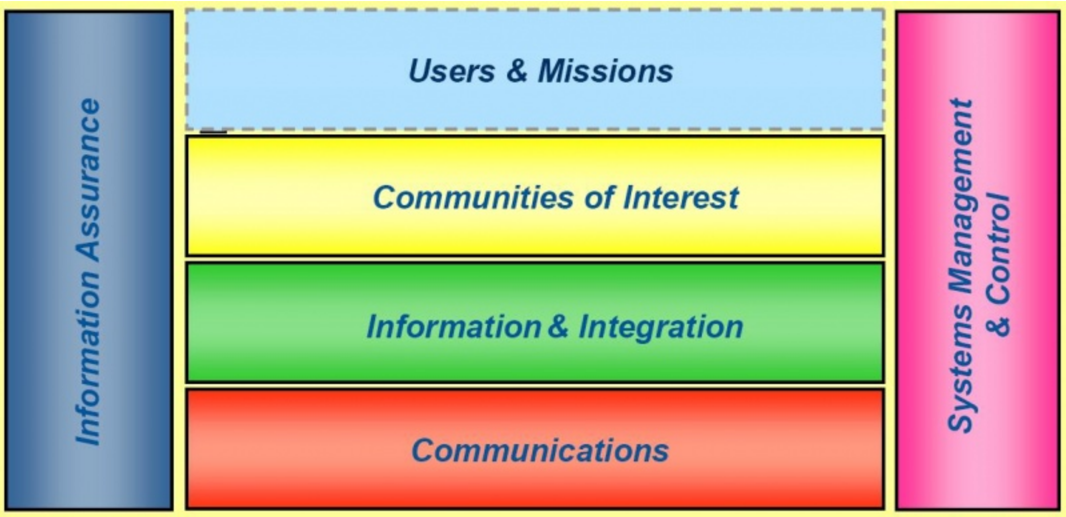


Figure 2.4 A high level view of the NNEC architecture.

The decision to base future NATO Network Enabled Capability (NNEC) systems and networks on SOA, in particular SOA implemented using Web services technology, is well founded within NATO. The NNEC Feasibility Study[1] (FS) pointed to SOA as a key building block for interoperability between nations as early as in 2005. Further work within NATO, in particular from the Core Enterprise Services Working Group (CESWG), further supports this decision.

Figure 2.4 shows the high level architectural view of the NATO Information Infrastructure (NII), as defined by the NNEC FS. Here, the NNEC architecture is broken down into six areas. Two of the areas, Users & Missions and Communities of Interest (COI), relate to the activities, services and system capabilities needed to fulfill operational needs. The remaining four areas, made up of two horizontal and two vertical groups, describe the NII, and thus cover the functionality that must be supported in a federated information infrastructure. After this high level architecture was defined, NATO has continued the work on defining how the NII should be implemented. One example of such work is the SOA Baseline [4], which divides the functionality of the Information & Integration level into Core Services, and recommends standards for how these services should be implemented in NATO.

2.2 Architecture for the Norwegian Armed Forces Information Infrastructure

Figure 2.5 shows a sketch of an architecture for the Norwegian Armed Forces Information Infrastructure (INI) [29], which closely resembles the NNEC architecture shown in Figure 2.4. The INI architecture is layered into decision support services (yellow) and core services (light blue) with a communication infrastructure (gray). The decision support services are divided into Specific functional services and Generic functional services. Information security and service management flank the figure as cross-cutting concerns.

The present sketch of an architecture is very high level and simply indicates what types of applications

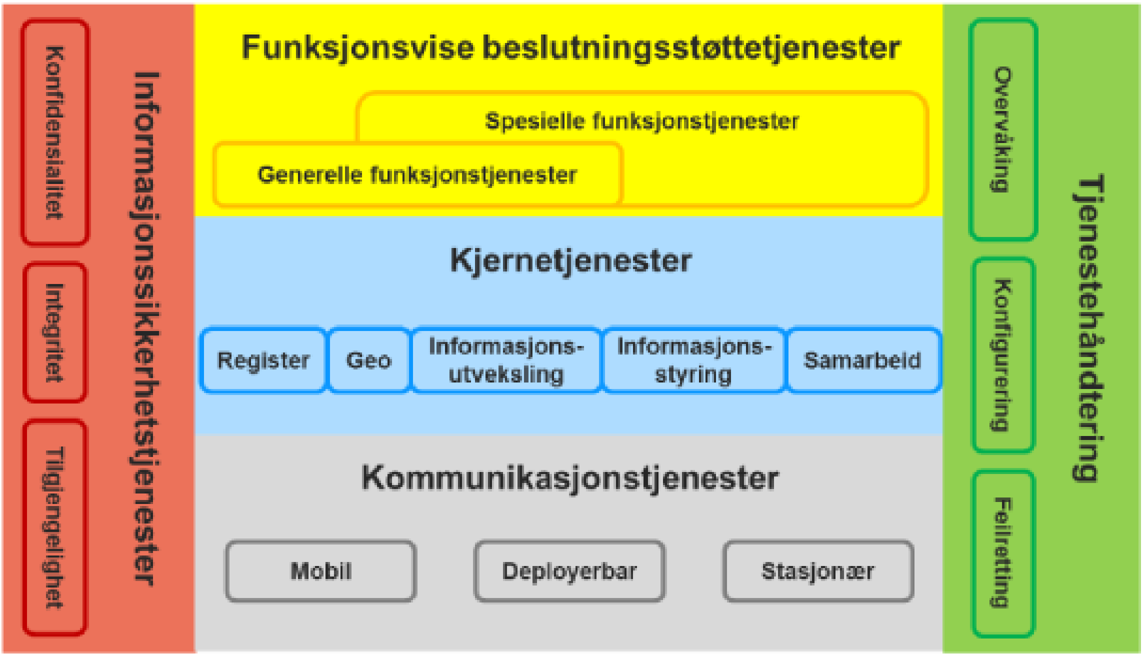


Figure 2.5 Architectural sketch for the Norwegian Armed Forces Information Infrastructure (INI) [29]

and services should be included in the information infrastructure and at which level of end-user versus technical orientation they should be considered. To populate the categories (boxes) with applications and services is a step toward developing an information infrastructure from the architecture. The architecture lacks explicit and official population of working software, although the category names indicate where several such pieces of software belong.

In the latest IT strategy document from the Norwegian Chief of Defence [24], the following has been decided in relation to the development of an architecture for INI:

- Architecture descriptions follow the NATO Architecture Framework (NAF) [21]
- Architecture development follow The Open Group Architecture Framework (TOGAF) [14]
- The INI is to be developed in pace with NATO's Networked-Enabled Capability (NNEC) program and is to be harmonized with NATO's Networking and Information Infrastructure (NII) and the C3 Classification Taxonomy

Together, NAF and TOGAF provide guidelines for implementing a methodology for constructing architecture models and descriptions. One has to provide the concrete methods for requirements elicitation, entity modeling, etc, but with that in place one has an architecture framework; i.e., a methodology for constructing an architecture of the INI, in line with our remarks above. The third point entails an explicit focus on NATO's information infrastructure architecture, to which we will now turn.

2.3 The C3 Taxonomy

The C3 Classification Taxonomy (C3 Taxonomy for short) is an categorization of the functionality that is expected to be found in NATO's information infrastructure NII. More precisely, it is a sorting of capability concepts relevant to producing enterprise computer system support for Consultation, Command and Control (C3) in NATO; see Figure 2.6 and Figure 2.7 (more detailed view). It explicitly includes, in the same picture, the operational context (the *Operational Context* frame in Figure 2.6) and the computing context (the *Communication and Information Systems (CIS) Capabilities* frame in Figure 2.6). The C3 Taxonomy is not an architeture in itself, but it can potentially be used as a starting point for making an architectural description of NII and INI. The following summarizes the motivation for the C3 Taxonomy:

> "The C3 Classification Taxonomy provides a tool to synchronize all capability activities for Consultation, Command and Control (C3) in the NATO Alliance by connecting the Strategic Concept and Political Guidance through the NATO Defence Planning Process (NDPP) to traditional Communications and Information Systems (CIS) architecture and design constructs [...] Throughout the years, many communities have developed and contributed components to the overall CIS capability of the Alliance but sadly, most groups did their work in splendid isolation. Today we are confronted with a patch-quilt of systems, applications, vocabularies and taxonomies and simple English words such as service or capability have become highly ambiguous. As a result of extreme stove-piping, NATO now faces a very complex fabric of capabilities that are not interoperable and attempts to solve these problems are often hampered by lack of mutual understanding caused by confusing vocabularies" [2].

The guiding of technology by an explicit focus on operational context is very much in line with the motivation behind SOA. The focus on enterprise-driven service definition shifts the definition of an organization's enterprise processes back to where they belong, in the organization's strategy domain, and away from the IT-department.

As can be seen from Figure 2.6, the taxonomy has an *Operational Context* at the top, layered into *Missions and Operations* which are supported by *Operational Capabilities*; the latter being foundational, generic operational modules on which missions and operations may be built. Below the operational context are the *Communication and Information Systems (CIS) Capabilities*, which are the information technology support for the operational context. The CIS capabilities presents themselves to the end user in the form of *User Applications* geared toward specific domains (air, land, maritime, joint, etc.) and communities of interest (modeling and simulation, environment, missile defense, etc.); see Figure 2.7. Below this layer are various layers of *Technical Services*, which may be used to develop and implement the user-facing capabilities. The Technical Services are layered in a manner reminiscent to the structure of the Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models, both of which have more domain-dependent IT functionality at the top and increasingly generic and technical functionality,

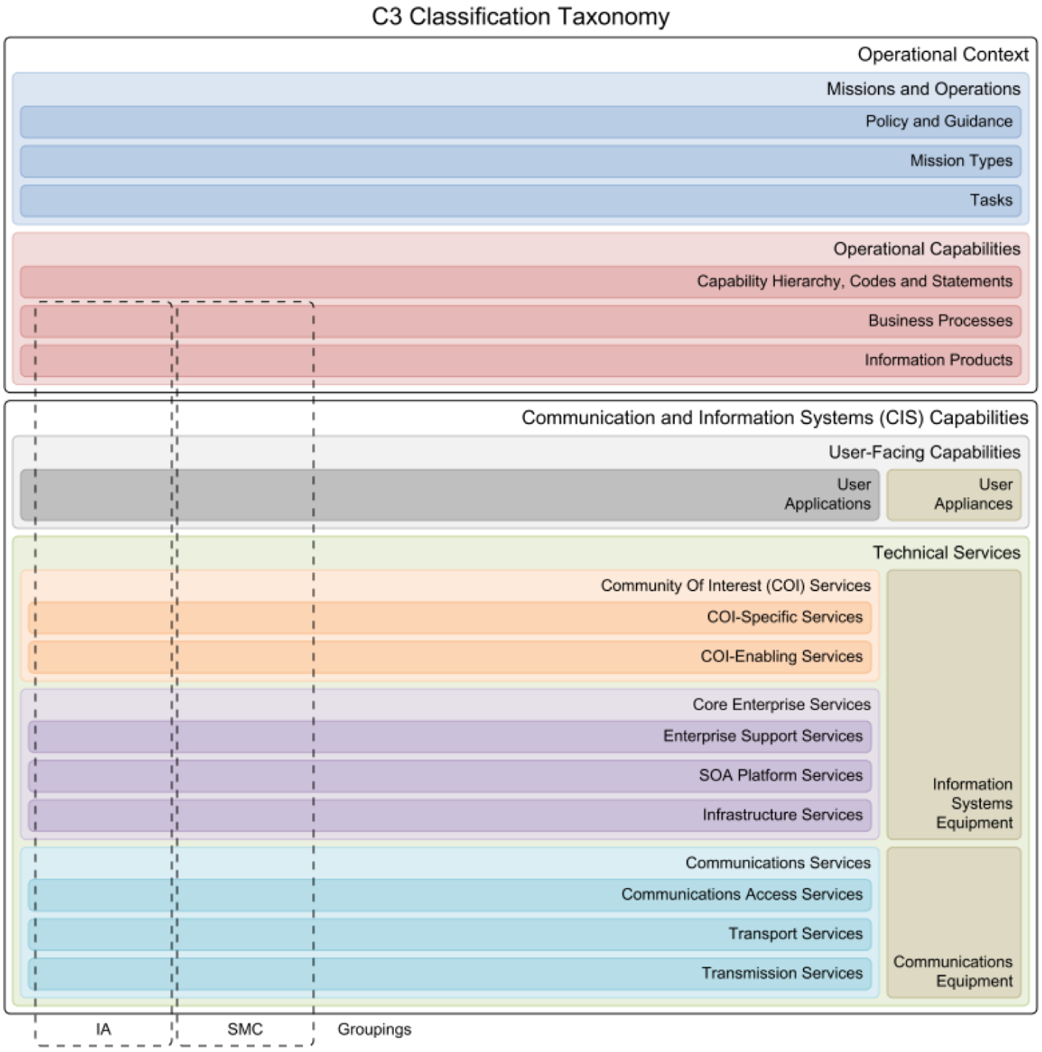


Figure 2.6 C3 Classification Taxonomy [20]—Main categories

including hardware, lower down. Thus, the upper layers of the C3 Taxonomy's Technical Services consist of the *Community of Interest (COI) Services* geared toward realizing User Applications.

At the *User-Facing Capabilities* layer, software is denoted *applications*. Software and hardware at the Technical Services layers are denoted *services*. However, services and applications should both fulfill requirements of interoperability and loose coupling. We will return to this below.

Two cross-cutting concerns are defined in the taxonomy (IA and SMC Groupings in Figure 2.6). The *Information Assurance (IA)* concern "provides a collection of measures to protect information processed, stored or transmitted in communication, information or other electronic systems in respect to confidentiality, integrity, availability, non-repudiation and authentication" [2]. The *Service Management and Control (SMC)* concern "provides a collection of capabilities to coherently manage components in a federated service-enabled information technology infrastructure. SMC tools enable service providers to provide the desired quality of service as specified by the customer" [2].

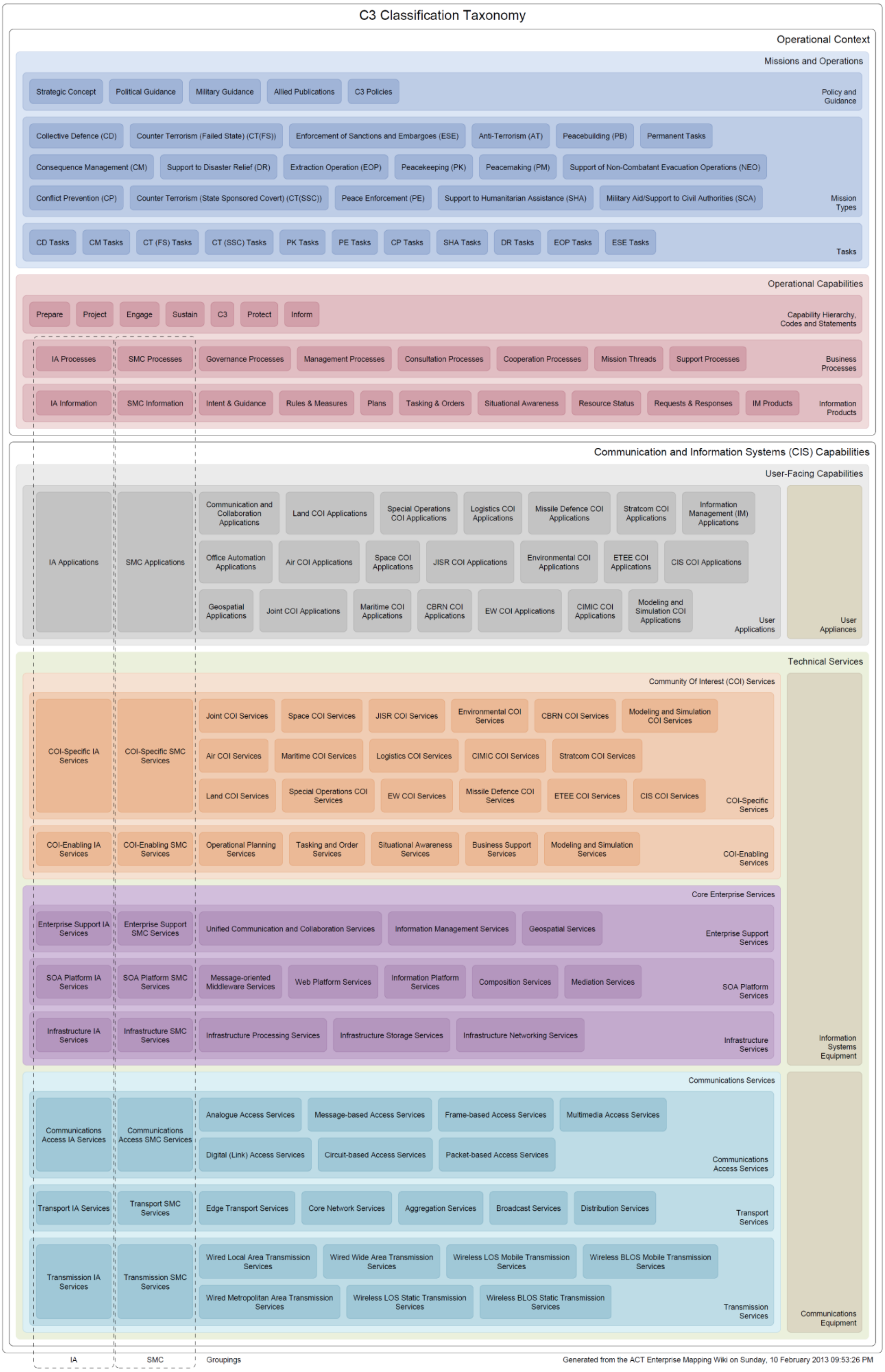

C3 Classification Taxonomy
Operational Context
Missions and Operations
Strategic Concept
Political Guidance
Military Guidance
Allied Publications
C3 Policies
Policy and Guidance
Collective Defence (CD)
Counter Terrorism (Failed State) (CT(FS))
Enforcement of Sanctions and Embargoes (ESE)
Anti-Terrorism (AT)
Peacebuilding (PB)
Permanent Tasks
Consequence Management (CM)
Support to Disaster Relief (DR)
Extraction Operation (EOP)
Peacekeeping (PK)
Peacemaking (PM)
Support of Non-Combatant Evacuation Operations (NEO)
Conflict Prevention (CP)
Counter Terrorism (State Sponsored Covert) (CT(SSC))
Peace Enforcement (PE)
Support to Humanitarian Assistance (SHA)
Military Aid/Support to Civil Authorities (SCA)
Mission Types
CD Tasks
CM Tasks
CT (FS) Tasks
CT (SSC) Tasks
PK Tasks
PE Tasks
CP Tasks
SHA Tasks
DR Tasks
EOP Tasks
ESE Tasks
Tasks
Operational Capabilities
Prepare
Project
Engage
Sustain
C3
Protect
Inform
Capability Hierarchy, Codes and Statements
IA Processes
SMC Processes
Governance Processes
Management Processes
Consultation Processes
Cooperation Processes
Mission Threads
Support Processes
Business Processes
IA Information
SMC Information
Intent & Guidance
Rules & Measures
Plans
Tasking & Orders
Situational Awareness
Resource Status
Requests & Responses
IM Products
Information Products
Communication and Information Systems (CIS) Capabilities
User-Facing Capabilities
IA Applications
SMC Applications
Communication and Collaboration Applications
Land COI Applications
Special Operations COI Applications
Logistics COI Applications
Missile Defence COI Applications
Stratcom COI Applications
Information Management (IM) Applications
Office Automation Applications
Air COI Applications
Space COI Applications
JISR COI Applications
Environmental COI Applications
ETEE COI Applications
CIS COI Applications
Geospatial Applications
Joint COI Applications
Maritime COI Applications
CBRN COI Applications
EW COI Applications
CIMIC COI Applications
Modeling and Simulation COI Applications
User Applications
User Appliances
Technical Services
Community Of Interest (COI) Services
COI-Specific IA Services
COI-Specific SMC Services
Joint COI Services
Space COI Services
JISR COI Services
Environmental COI Services
CBRN COI Services
Modeling and Simulation COI Services
Air COI Services
Maritime COI Services
Logistics COI Services
CIMIC COI Services
Stratcom COI Services
Land COI Services
Special Operations COI Services
EW COI Services
Missile Defence COI Services
ETEE COI Services
CIS COI Services
COI-Specific Services
COI-Enabling IA Services
COI-Enabling SMC Services
Operational Planning Services
Tasking and Order Services
Situational Awareness Services
Business Support Services
Modeling and Simulation Services
COI-Enabling Services
Core Enterprise Services
Enterprise Support IA Services
Enterprise Support SMC Services
Unified Communication and Collaboration Services
Information Management Services
Geospatial Services
Enterprise Support Services
SOA Platform IA Services
SOA Platform SMC Services
Message-oriented Middleware Services
Web Platform Services
Information Platform Services
Composition Services
Mediation Services
SOA Platform Services
Infrastructure IA Services
Infrastructure SMC Services
Infrastructure Processing Services
Infrastructure Storage Services
Infrastructure Networking Services
Infrastructure Services
Information Systems Equipment
Communications Services
Communications Access IA Services
Communications Access SMC Services
Analogue Access Services
Message-based Access Services
Frame-based Access Services
Multimedia Access Services
Digital (Link) Access Services
Circuit-based Access Services
Packet-based Access Services
Communications Access Services
Transport IA Services
Transport SMC Services
Edge Transport Services
Core Network Services
Aggregation Services
Broadcast Services
Distribution Services
Transport Services
Transmission IA Services
Transmission SMC Services
Wired Local Area Transmission Services
Wired Wide Area Transmission Services
Wireless LOS Mobile Transmission Services
Wireless BLOS Mobile Transmission Services
Wired Metropolitan Area Transmission Services
Wireless LOS Static Transmission Services
Wireless BLOS Static Transmission Services
Transmission Services
Communications Equipment
IA
SMC
Groupings
Generated from the ACT Enterprise Mapping Wiki on Sunday, 10 February 2013 09:53:26 PM

Figure 2.7 C3 Classification Taxonomy [20]

The C3 Taxonomy is maintained via the NATO Allied Command Transformation (ACT) Technology for Information, Decision and Execution superiority (TIDE) Enterprise Mapping (EM) portal on Tidepedia (a NATO Wikipedia analog). Through EM, the taxonomy functions as a semantic Wiki on which authorized persons may summarize current knowledge, develop a common understanding of concepts and ultimately populate the taxonomy with working systems (human, software and hardware). The wiki has a structure which allows one to record requirements, dependencies, and other documentation for the artifacts entered into the taxonomy. Thus, even though the taxonomy at present is rudimentary, it has a potential to embody both an information infrastructure itself, as well as its architecture.

2.4 Methodology for Developing the INI and its Architecture

The lack of progress on developing both an architectural description of INI and the INI itself is likely the result of many factors. One important factor is limitations in the amount of resources that has been available for this work. However, another important obstacle is the lack of a leveraged practitioner-oriented methodology for engaging in development work on the INI. The strategic decisions to use NAF, TOGAF and the more detailed C3 Taxonomy with its wiki interface are improvements in this respect. However, to reach a stage of actual development, one needs further concretization of methodology, and usable guidelines for using the methodology.

One objective of this prestudy was to establish a consolidated view on the use of NAF and TOGAF toward the C3 Taxonomy. A conclusion along these lines must be the result of concerted efforts on aligning NAF, TOGAF and the C3 Taxonomy followed by empirical evidence as to the usability and efficiency of NAF and TOGAF in conjunction with the C3 Taxonomy according to agreed criteria. The set timespan for the pre-study was too short to undertake this work. Time was also insufficient to plan such efforts, so we thus limit ourselves to summarizing NAF and TOGAF and relevant work on integrating the two.

2.4.1 NAF and TOGAF

The NATO Architecture Framework (NAF) [21] provides a range of guidelines on how to describe and document an architecture. It suggests organizing development and results in views:

NAV	NATO All View
NCA	NATO Capability View
NOV	NATO Operational View
NSOV	NATO Service-Oriented View
NSV	NATO Systems View
NTV	NATO Technical View
NPV	NATO Programme View

In addition to the views listed here, version 3.0 of NAF also includes two taxonomies, namely the NSOV-1 Service Taxonomy Subview and the NCV-2 Capability Taxonomy Subview.

To frame this, NATO includes defintions of four *architecture types* in its NATO Architecture Framework Metamodel (NMM). The *overarching architecture* should look 10–15 years into the future and is an enterprise-wide description of the future situation with limited detail. It should answer the questions of *what* the enterprise is doing, and *why*. A *reference architecture* covers a span of a few years and is a more focused description of the construction with full detail to guide program execution. Such an architecture should answer *how* the enterprise functions. It can focus on a specific subject area or span the full enterprise. A range of *target architectures* are then derived from a reference architecture. They are at a detail sufficient for solutions development; i.e. to direct the acquisition and integration of components to achieve a desired capability. They cover technical aspects and answer *with what* the capabilities of the enterprise are realized. Finally, a *baseline architecture* describes the technical aspects of the fielded “as is” state of the NATO C3 enterprise.

The Open Group Architecture Framework (TOGAF) is proposed as an architecture development methodology for the INI. TOGAF comes with an Architecture Development Method (ADM) which “provides a tested and repeatable process for developing architectures. The ADM includes establishing an architecture framework, developing architecture content, transitioning, and governing the realization of architectures. All of these activities are carried out within an iterative cycle of continuous architecture definition and realization that allows organizations to transform their enterprises in a controlled manner in response to business goals and opportunities” [14]. Phases within the ADM are as follows:

Preliminary Phase: Preparation activities required to create an Architecture Capability including customization of TOGAF and definition of Architecture Principles.

Phase A: Initial phase of an architecture development cycle. It includes defining the scope of the architecture development initiative, identifying the stakeholders, creating the *Architecture Vision*, and obtaining approval to proceed with the architecture development.

Phase B: Development of a *Business Architecture* to support the agreed Architecture Vision.

Phase C: Development of *Information Systems Architectures* to support the Architecture Vision.

Phase D: Development of the *Technology Architecture* to support the agreed Architecture Vision.

Phase E: Initial implementation planning and the identification of delivery vehicles; i.e., *Opportunities & Solutions* for the architecture defined in the previous phases.

Phase F: How to move from the Baseline to the Target Architectures by finalizing a detailed *Implementation and Migration Plan*.

Phase G: Gives *Implementation Governance* for architectural oversight of the implementation.

Phase H: Gives *Architecture Change Management* to establish procedures for managing change to the new architecture.

Requirements Management: Examines the process of managing architecture requirements throughout the ADM.

There is an explicit emphasis on iteration within and between phases, which puts TOGAF in line with current best practices.

There have been efforts to align TOGAF and NAF; e.g., [13, 5]. Conclusions are that TOGAF and NAF align well at top-levels, but that sub-levels require more work; especially when using NAF implementations in the Unified Modeling Language (UML). One important point is that simplification should be strived for [13]:

> TOGAF proposes an elaborate methodology and a simple content framework, while NAF contains a simple methodology and an elaborate content framework. The two approaches are thus complementary. Ideas for simplifying the rather complex methodology of TOGAF or the content framework of NAF, can be derived from the simpler solutions chosen by the other standard. So far, this has mainly resulted in a simpler metamodel in our work, while the architecture development methodology to a greater extent has been adapted in order to fit with the local organizational practices and procedures. The work has also resulted in a number of change requests for NAF, put forward to NATO.

Clearly, both NAF and TOGAF have useful aspects for developing the architecture for INI, as well as laying the grounds for developing the INI itself from that architecture. However, similar work as that mentioned above needs to be undertaken on aligning TOGAF, NAF and the C3 Taxonomy.

3 Assessing the C3 Taxonomy

The C3 Taxonomy has the same high level structure as the NNEC Reference Model shown in Figure 2.4, and it can be seen as a further refinement of the concepts behind the already existing SOA efforts within NATO. The C3 Taxonomy has retained the focus on having a set of Core Enterprise Services as a common enabler for interoperability between NATO and the nations, but seeks to become a common reference for all activities within C3. Having such a common reference would help guide the development of systems towards becoming a part of a larger federation-of-systems rather than isolated stovepipe systems.

The information infrastructure of the Norwegian Armed Forces is undergoing the same transition from specialized systems that have limited interaction with each other towards a more connected INI for the future. As a basis for this report, we have investigated the C3 Taxonomy, and applied it to selected areas of the INI-related research at FFI. These INI-related activities represent functionality that is likely to become part of a future INI, and these activities are thus well suited as a test case for evaluating how well the C3 Taxonomy fits with how we expect the INI to develop in the years to come.

In this section we discuss our assessment of the different technical areas covered by the C3 Taxonomy, before we present our view on the feasibility of using the C3 Taxonomy as a basis for the architecture of the future INI. We also briefly discuss the application of the C3 Taxonomy to the current “as is” INI, and address the alignment of the C3 Taxonomy with NAF and TOGAF in sections 3.6 and 3.7, respectively.

3.1 The C3 Taxonomy and SOA

When assessing the C3 Taxonomy for use a common reference for SOA-based information infrastructures, the first step is to evaluate how well the C3 Taxonomy fits with the ideals and principles of service-orientation as a concept. SOA builds on a number of principles which together describe how a service-oriented system should be constructed [8], and the structure and principles behind the C3 Taxonomy fits well with this service-oriented approach.

In particular, the layered design of the C3 Taxonomy fits well with the SOA principle of *service reusability*. This principle means that common functionality should be identified and made available as a stand-alone service, so that this stand-alone service can be reused whenever the common functionality is needed. The C3 Taxonomy has a layered approach which follows this principle. As an example of this, consider the COI Services group of the C3 Taxonomy, where functionality common to multiple COIs has been placed in a separate subgroup, the COI-Enabling Services. In addition, the more detailed descriptions of the taxonomy groups, found in EM, identify relationships and dependencies between groups, which show how higher level services utilizes lower level services that provide access to this common functionality. Constructing complex services by combining other, simpler services in new ways is another key principle of SOAs, known as *service composability*.

Another important aspect of SOA is the relationship between the business and the service. One of the driving principles behind service-oriented design is that it is the business processes of an enterprise that should decide how one divides technical capabilities and resources into services. Once these business processes have been identified, the technical capabilities that support these processes can then gradually be refined down to reusable services. One should start with first defining the high level functionality, and then breaking this down into increasingly more detailed services and service description. The EM approach taken by the C3 Taxonomy supports this business centered approach well, as the EM provides different levels of abstraction in its groupings. This means that one can use the different layers of detail within the EM to describe different aspects of the architecture.

In conclusion, the C3 Taxonomy fits well with the ideals and principles of service-orientation as it supports different levels of detail in its service descriptions. In addition, the high level groupings seem well chosen when taking the principles of service reuse and composition into account.

3.2 Core Enterprise Services

The Core Enterprise Services group provides the common technical functionality that is needed in order to access IT capabilities and resources. The goal is that these services are generic and domain independent, and can thus be reused no matter which physical hardware and underlying communications technology a specific domain uses. The Core Enterprise Services are divided into three subgroups, namely Infrastructure Services, SOA Platform Services and Enterprise Support Services. This division appears reasonable, as the three groups form logical layers where the services found within a higher layer logically builds on functionality found in the grouping below it.

3.2.1 Infrastructure Services

The Infrastructure Services is the group that forms the logical lowest layer of the Core Enterprise Services, and contains functionality that bridges the gap between the Core Enterprise Services and the Communication Services groupings. In addition, this group provides services that give access to software resources that are required in order to host services, such as storage, computing and high-level networking capabilities.

Infrastructure Services are subdivided into five groups, two of which constitute the overlap with the IA and SMC categories. The other three categories provide access to shared physical or virtual infrastructure resources such as computation, storage and network.

3.2.2 SOA Platform Services

The SOA Platform Services cover the basic functionality that is needed in order to build and support a service-oriented system. The services within this group can be seen as common building blocks which one can reuse in order to build a service-oriented system in an efficient and flexible way, while at the same time retaining interoperability. The SOA Platform Services thus become a key factor in achieving interoperability between NATO and the nations, and it is important that the services defined here are compatible with the SOA standardization and profiling efforts already taking place in NATO.

The NATO efforts on defining the Core Enterprise Services needed to build the NII has so far been documented in in the CES Framework [3] and more recently in the SOA Baseline[4]. In this work, key functionality has been identified and designated as Core Enterprise Services. Considerable effort has been put into defining these services, and also into giving recommendations as to how these services should be realized in the NII and between nations. Of the core services identified, not all are expected to become available at the same time, and the descriptions available for the different core services vary in maturity. These descriptions have however become a baseline for which core services one can expect to be available in the NII, and it is thus important that the C3 Taxonomy is compatible with the already existing core services specifications. Figure 3.1 shows the Core Enterprise Services as defined by the CES Framework, many of which can be refound in the SOA Platform Services group.

The SOA Platform Services are further divided into subgroups as shown in Figure 3.2. The two first categories, SOA Platform IA Services and SOA Platform SMC Services are categories that overlap with the two vertical groupings in the C3 Taxonomy. These will be discussed as a part of the general discussion on IA and SMC below. Note that the service discovery, which provides an essential functionality in any service-oriented system, is classified as a SMC component in the C3 Taxonomy, and will thus be discussed later.

The Message-oriented Middleware Services (MMS) provide the functionality needed to exchange messages between the message producer and the message receiver, independent of data format, content and transport mechanism. This group of services provides a number of different message

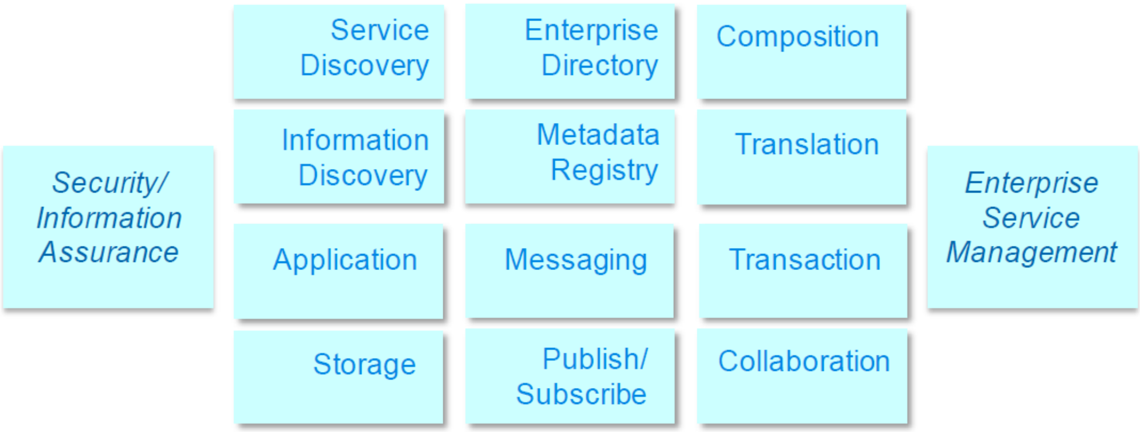


Figure 3.1 The Core Enterprise Services according to the CES Framework, from [3].

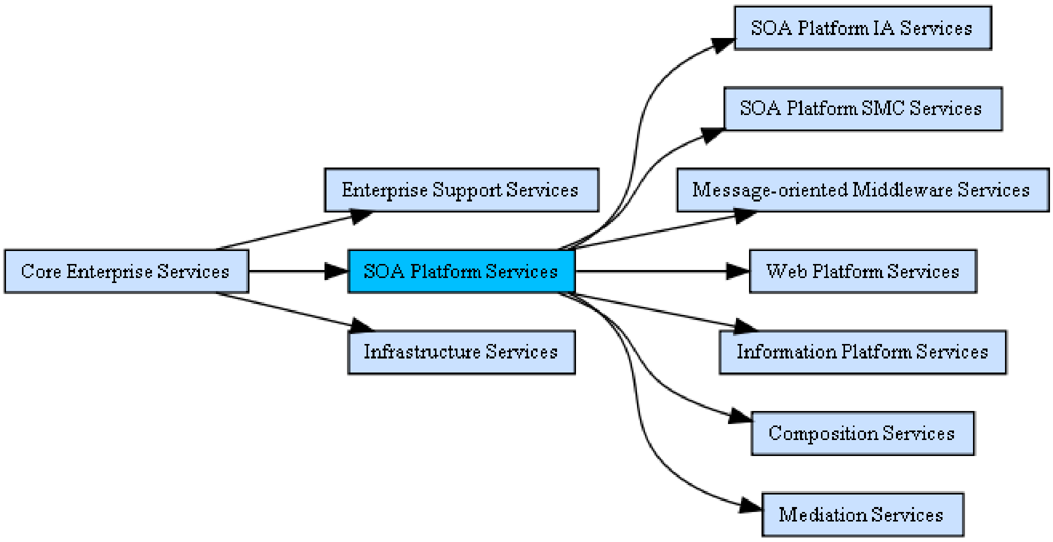


Figure 3.2 Decomposition of SOA Platform Services, from the C3 Taxonomy Enterprise Mapping.

exchange patters, such as request/response and publish/subscribe, and different message delivery modes. When compared to the CES Framework definitions of core services, the MMS group of the C3 Taxonomy cover multiple core services. Both the Messaging and Publish/Subscribe core services are found here, in addition to other value-adding services such as caching, proxying and message queuing support. Grouping these CES Framework core services together in this manner is reasonable, as they provide similar functionality to their users.

The Web Platform Service provides functionality that can be used to support the deployment of SOA services onto a Web based platform, and provide access to the services through that platform. Such a web hosting service, provided by for instance an application server or a enterprise service bus, is a capability that should be available within the enterprise. The Web Hosting Service provides not only hosting services, but also caching and other support services for Web content. Solutions and products providing this capability often provide other functionality bundled together, and there will thus be an overlap between the service offered by a Web Hosting Service and a service provided for instance through a SMC or IA component.

The Information Platform Services group includes services that deal with finding information, transforming information, and provisioning and maintenance of information. It provides functionality covering several CES Framework core services, namely Information Discovery and Metadata Registry. In addition the Information Platform Services include an Information Access Service, which is a generic mechanism for providing easy access to information content exiting in for instance legacy databases and systems. Service wrappers, which are light-weight services providing access to legacy systems by implementing a service interface to a non-service enabled system, fall into this category.

Composition is both a CES Framework core service, and a C3 Taxonomy subgroup of its own. These services deal with building composite services from simpler services, and then combining the data from those services so that a single combined result can be returned to the user. There are two main approaches to service composition, choreography and orchestration, and the C3 Taxonomy have subgroupings for both approaches. In addition, the Composition Services group covers Transaction handling, which is defined as a separate CES Framework core service. This joining of core service is sensible, as the functionality they support are closely related to each other. Note that the currently existing standards for service composition, which the C3 Taxonomy points to, are designed for use in static compositions. As technology matures, and dynamic composition becomes viable, it might be beneficial to expand this part of the Core Services group in order to reflect the difference in capabilities between static and dynamic composition services.

Mediation Services are services that provide functionality such as data format translation, data fusion and protocol adaptations. These services act as intermediaries that enable communication between two parties that are technically incompatible. This subgroup of the C3 Taxonomy directly corresponds to the CES Framework core service of the same name, and provides that same critical functionality. The C3 Taxonomy divides the Mediation Service into two subgroups, one for data format conversion and one for protocol conversion, which cover the most basic types of mediation. In the long term it might be sensible to add further subgroups to this category as the need arises.

3.2.3 Enterprise Support Services

The Enterprise Support Services are service that are independent of a given COI, and that need to be available throughout the enterprise. Enterprise Support Services are enablers used by other services and users across the whole enterprise, acting as "building blocks" for developing more sophisticated COI services and applications.

Enterprise Support Services have an IA subgroup and a SMC subgroup, which overlap in functionality with the IA and SMC vertical categories in the C3 Taxonomy. The remaining subgroups cover functionality related to information management and collaboration, in addition to a dedicated subgroup for Geospacial Services. The CES Framework core services Collaboration and Enterprise Directory are covered by the Enterprise Support Services group.

3.2.4 Core Enterprise Services Summary

The Core Enterprise Services Grouping of the C3 Taxonomy corresponds well with already ongoing SOA efforts, both when it comes to international standardization and with respect to the experimentation and profiling work done within NATO. The different subgroupings under Core Enterprise Services vary in the amount of detail that is given, but there is a close correlation between the level of detail provided in the C3 Taxonomy and the maturity of the technical standards available. In areas where the standards are mature the C3 Taxonomy's EM provides links to standards and NATO developed profiles, while in other areas no specific technology has been chosen.

3.3 Communications Services

The C3 Classification Taxonomy decomposes the Communications Services into three subgroups as seen in Figure 3.3.

This decomposition may seem reasonable at a first glance, but after closer scrutiny it seems to have some deficiencies. First, the definition of transmission services is limited to only cover the physical layer (PHY) as defined in the OSI Reference Model, or optionally only parts of the PHY. This seems to create a gap between transmission services and the other two categories that are users of the transmission services.

One alternative could be to omit transmission services as a separate category and let transport services include all aspects of transmission. Then, communications access services would always have to rely on the transport services.

Another preferred alternative could be to replace Transport and Transmission by two new categories called e.g. Network and Link services. Network services would offer end-to-end communications services while Link services would offer services between directly connected communication nodes/elements. Link services would cover both the Link and Physical layers of the OSI Reference model.

The difference between Communications Access and Transport services is also a bit hard to understand. The user/application will only see the Communications Access Services. The Transport Services are only visible within the network.

As a general comment to the Taxonomy, we disagree on the way it is described and have problems understanding many of the elements. Even though, we have tried to see how INI could fit into this model and have also tried to populate it my making a mapping between the C3 Taxonomy and relevant research activity at FFI.

3.3.1 Communication Access Services

The C3 Classification Taxonomy describes a large number of subcategories of Communications Access Services, see Figure 3.4. Most of these services describe existing communications infrastructures. As our task is to describe the INI of the future, we are left with a small subset.

The following is an assessment of the different subcategories with regard to INI, based on existing plans and knowledge:

- Message-based access services should not be kept as a communications service, but should reside as an application or a higher-layer service and use another communications service.
- Analogue access services, transported as digitized voice or data using a voice coder, are still in some use today. Such services will be phased out of INI.
- Circuit-based access services (e.g. ISDN) are extensively used in INI for telephony, but will also be phased out in the future. These services are being replaced by VoIP and e.g. SIP signaling.
- Frame-based access services are not found in INI today, but may become relevant in the future. There are no existing plans today for such services, but transport of Ethernet frames may be introduced.
- Digital (Link) access services offering asynchronous or synchronous data transfer were extensively used for data prior to the introduction of packet-switching. These services will be almost phased out within a few years. INI should not support such services. Any user requiring such services should rely on a gateway towards e.g. packet-based access services.
- Packet-based access services are definitely most relevant for INI. Most applications and higher layer services have or will quickly migrate to rely on IPv4 and/or IPv6 as the preferred communications services. IPv6 will replace IPv4 in INI in a few years. We do not consider Virtual Private Network (VPN) as a communications service to be offered by INI.
- Multimedia access services such as VTC should not be categorized as communications services. Such services should reside within applications or higher layer services.

An important aspect of the communications access services is the ability to signal and handle QoS requirements. This is not well described by the Taxonomy.

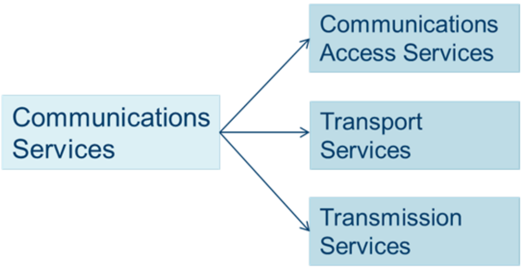


Figure 3.3 Decomposition of Communications Services.

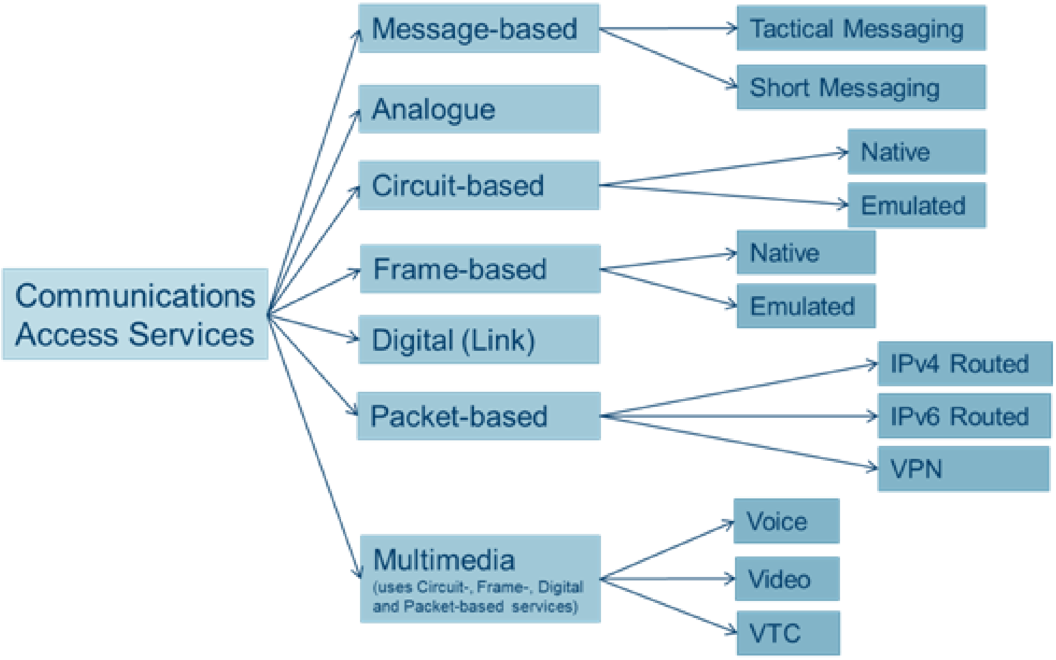


Figure 3.4 Decomposition of Communications Access Services.

3.3.2 Transport Services

The C3 Classification Taxonomy defines transport services to provide connectivity to the communications access services. Transport services interact with the transmission services, constituting the physical layer of the transport. Despite our disagreement, we have evaluated the Taxonomy decomposition with regard to INI for the defined subcategories as seen in Figure 3.5.

- The difference between Edge and Core is described in Protected Core Networking (PCN) terms as the edge is considered to be the entry point into the Protected Core (interface PCN2). PCN defines another interface (PCN1) between segments within the core. We have problems understanding the need to distinguish between the two subcategories, especially when also keeping Access services facing the users.
- Aggregation services should not be considered as a separate service category.
- Broadcast services are used in some existing maritime systems, but should not be offered in the future INI.
- We do understand the definition and need to define Distribution services as a separate category.

Edge Transport Services

The edge transport services provide the delivery or exchange of traffic flows over different Transmission Services. In PCN terms these services are provided between two entry points into the Protected Core.

- IP-based transport services will be the dominant category in future INI.
- Frame-based transport is not found in INI today, but is a candidate for new services in the future
- TDM-based transport services (e.g. ISDN) are extensively used today in INI, for telephony. They will be phased out in the future sometime after the phase-out of Circuit Switching as a Core Network Service.
- Link Emulation provides emulation of synchronous serial data streams (e.g. V.35 and RS449). These are not relevant services for INI.

Core Network Services

Core Network Services are services offered within the core of the PCN or WAN. They shall, when implemented at the edge of WAN/PCN, include Edge Transport Services

- Packet Routing Services are the most dominant group of services for INI.
- Frame Switching Services based of Carrier Ethernet may become relevant for INI in the future, while ATM and MPLS are less relevant technologies.
- Circuit Switching Services will be phased out from INI as they have already been for most commercial telecommunications service providers. ISDN as an edge or access service may survive for a limited time even after CS is phased out as a core service.

3.3.3 Transmission Services

The C3 Classification Taxonomy defines transmission services to be limited to (parts of) the physical layer of the OSI Reference model. The reason for describing this separate from transport services is probably due to the described fact that transmission services can be offered directly to Access Services or user appliances (not via transport services). This is probably related to traditional military communications, but less relevant for a modern networked communication system like INI. As already mentioned, we find this subcategory hard to understand and would prefer a different decomposition. However, we have tried to evaluate the different subcategories of transmission services.

Transmission services are split into two groups, wired and wireless. While the wired is further decomposed based on its area of coverage (Local Area Network(LAN), Metropolitan Area Network (MAN) and Wide Area Network(WAN)), the wireless is split in Line of Sight (LOS)/Beyond Line of Sight (BLOS) and Static/Mobile. This decomposition is shown in Figure 3.6. Further, all the four wireless categories are further decomposed into two sub-categories: Narrowband and Wideband.

Three examples illustrate some possible deficiencies of the C3 Taxonomy breakdown of Transmission Services:

- Combat Net Radio (CNR) is categorized as a Static Wireless LOS service, while one of the important aspects of CNR is to handle mobility. Also, a modern CNR offers much more than just physical transmission, e.g. routing.
- A VHF CNR, a Wireless LAN (WLAN) or a cellular service end up in the same category (Static Wireless LOS) as a Radio Relay. The technical differences between these systems are huge.
- CNRs at HF frequencies[1] or satellite radio are in a separate category (Wireless BLOS) from VHF CNRs.

The difference between static and mobile services is probably more relevant to e.g. routing and switching, which are not considered to be part of the transmission services. It is not obvious that this part of the C3 Classification Taxonomy is as adequate for INI as some other parts of the Communications Services.

3.3.4 Conclusion

The decomposition of communications services, first into access and transport services, and additionally transport into edge and core services, seems to introduce an unnecessary complexity. A model decomposing communications into access, network (end-to-end) and link services is assessed as a better description.

The transmission services are defined to cover the physical layer functionality of the OSI reference

[1] Actually, an HF radio will end up in four different categories, depending on whether it communicates via ground wave (LOS) or sky wave (BLOS) and whether all nodes are static or some are mobile.

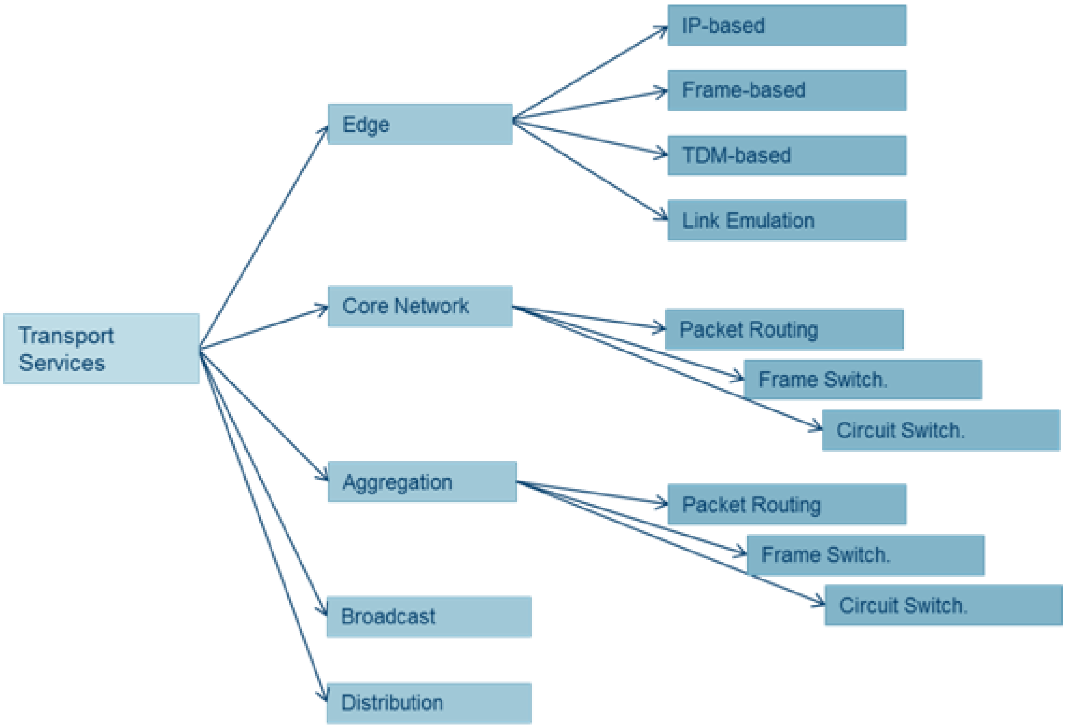


Figure 3.5 Decomposition of Transport Services.

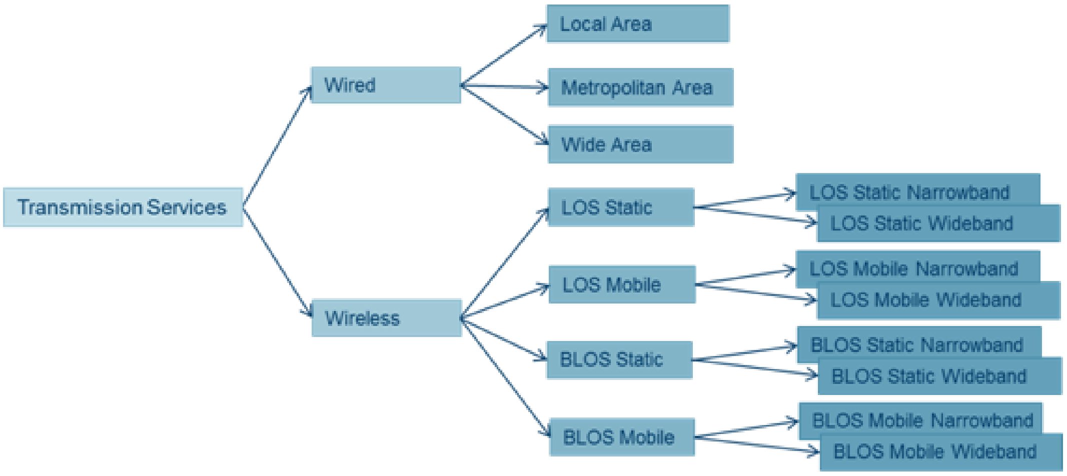


Figure 3.6 Decomposition of Transmission Services.

model, while the transport services focus on the networking aspects. Actually, it is mentioned that modulation and coding, which are very important aspects in wireless systems, are not always considered part of the transmission services but rather part of the transport services. Also, the Link layer of the OSI Reference model is required for the communications services, but is not described anywhere. This lack of clear distinction between transport and transmission is a deficiency of the taxonomy. As already mentioned, there should be a distinction between link and network services, where network services are concerned with end-to-end communication over multiple links.

Several of the access sub-categories (message, analogue and digital) are not relevant to INI as they describe past or present technologies which are not likely to be a part the future INI. In addition, circuit-based access will be phased out from INI within a few years and multimedia should not be a separate communications service.

Some of the transport sub-categories (aggregation, broadcast and distribution) are either overlay over communications services or describe attributes to other services. For edge and core sub-categories of transport, link emulation is not relevant to INI and TDM/circuit switching will be phased out prior to the equivalent access service.

The taxonomy does not yet give a sufficient description of some important aspects related to service quality and availability. Such aspects are only assessed by the communications Service Management and Control (SMC) as separate services. In future systems, negotiation between the service user and the service provider is important in order to adapt applications to available service qualities.

The existing decomposition of the C3 Classification Taxonomy does not give a good classification of our work with communications at FFI. We focus on different technologies and distinguish between wired and wireless systems, and between network layer and lower layers for wireless communications but not between access and transport. Several of our research topics will be found in a number of services defined in the taxonomy.

3.4 Information Assurance

IA is a vertical group in the C3 Classification Taxonomy that provides a collection of measures to help ensure confidentiality, integrity, availability, non-repudiation and authentication of information processed, stored or transmitted in an electronic system. It should be seen as a logical grouping of critical components and not as a class itself.

User applications and COI-Specific Services are divided in two main groups: Cyber Defence and Cyber Security. The distinction is not entirely sharp, but it seems like Cyber Security contains applications that helps to manage protection of systems and resources in a classical and static security setting, while Cyber Defence is aiding the dynamical handling of concrete incidents and attacks.

There is in general very little information available for the different terms in the taxonomy, and most of them could be considered placeholders with a couple of lines of general descriptive text. The exceptions are mainly the SOA Platform Services where references to documents and/or standards usually are given. The taxonomy mentions a relatively broad range of terms, and most IA-related activities will fit into a one or more of them.

The way security and IA is treated in the taxonomy and similar models may give the impression that system security can be isolated to a few critical components. However, in many cases implementation details of non-IA services could weaken the overall security of the system, especially at the lower layers. The IA services and applications in the taxonomy should be seen as tools and building blocks needed to improve the overall security of a system.

Different terms in the taxonomy have very different levels of detail and technological maturity. There are for example a strong focus on guards and labeling and release mechanisms. While such mechanisms no doubt will give a much needed functionality, there are still challenges concerning how to implement the functionally in a secure way, especially if high assurance is needed. The dangers by making a taxonomy too detailed in these areas are that one could give the impression that technology is more mature than it is.

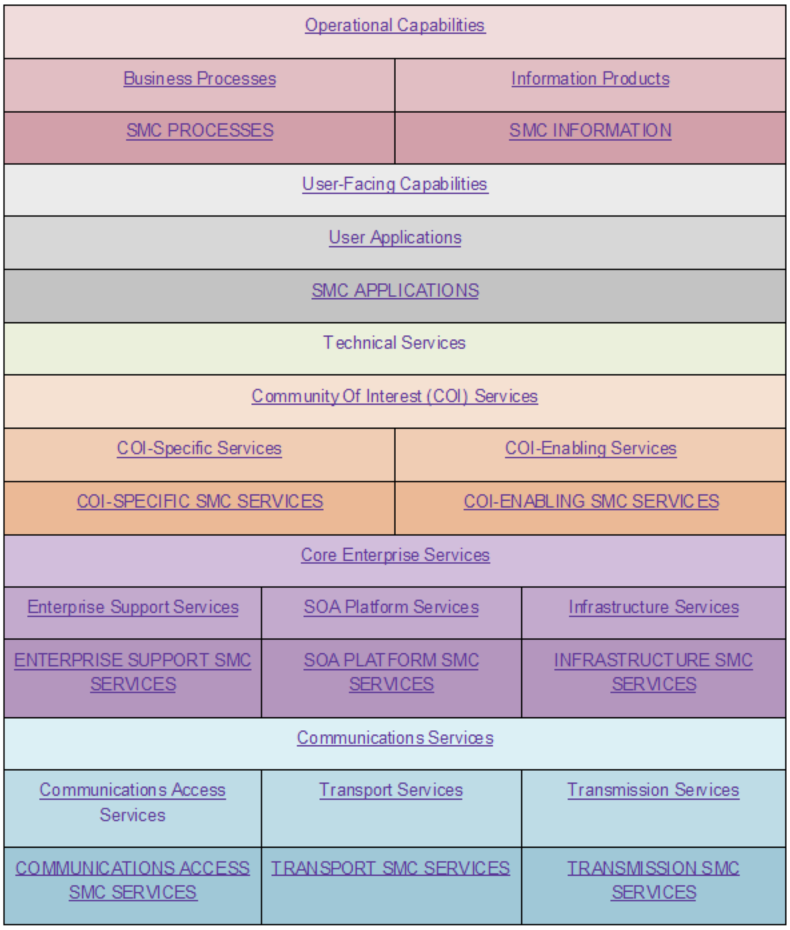
To summarize, for IA the taxonomy is mostly a collection of names for services and applications that presently are not very well defined. Some categories are very broad and maturity of concepts varies, and we have some concerns about how well IA and security fits a service oriented setting. The taxonomy seems to cover most ongoing activities, and it tries to standardize terminology. It remains to see if the organization of concepts is useful for IA.

3.5 Service Management and Control

Service Management and Control (SMC) is, in the same manner as IA, a vertical group in the C3 Taxonomy. It is a logical grouping of functionality related to the management of components in a federated service-oriented information infrastructure. The functionality represented by the SMC group will in practice be implemented within the services found on the horizontal groupings in the C3 Taxonomy, and most of these horizontal groups have subgroupings related to SMC already defined. Figure 3.7 shows where within the Technical Services elements of the C3 Taxonomy the SMC functionality is located. It is noted in the EM wiki that there is an overlap between the vertical SMC group and the sub-groups of Core Enterprise Services in this area, and that the functionality should be considered to exist in both groupings. In addition, there is a tight connection between IA and SMC, as both of these categories seek to control the information flow within the infrastructure, and to ensure that the information flow that takes place does so in accordance with current policies and business and legal rules.

3.5.1 Core Enterprise Services SMC

Within the Core Enterprise Services Grouping, there is a SMC element in each of the three subgroupings, and each of these SMC groups are subdivided again. In most areas the information available is not very detailed, and the services that exist should be viewed as placeholders for more detailed descriptions that will become available as the technology within this area matures.



Operational Capabilities

Business Processes | Information Products

SMC PROCESSES | SMC INFORMATION

User-Facing Capabilities

User Applications

SMC APPLICATIONS

Technical Services

Community Of Interest (COI) Services

COI-Specific Services | COI-Enabling Services

COI-SPECIFIC SMC SERVICES | COI-ENABLING SMC SERVICES

Core Enterprise Services

Enterprise Support Services | SOA Platform Services | Infrastructure Services

ENTERPRISE SUPPORT SMC SERVICES | SOA PLATFORM SMC SERVICES | INFRASTRUCTURE SMC SERVICES

Communications Services

Communications Access Services | Transport Services | Transmission Services

COMMUNICATIONS ACCESS SMC SERVICES | TRANSPORT SMC SERVICES | TRANSMISSION SMC SERVICES

Figure 3.7 Location of SMC groups within the horizontal groups of the C3 Taxonomy, from the EM.

At the Enterprise Support Services level SMC functionality is closely linked to IA functionality, as there is a focus on both identity and attribute management and on guard services. In addition to these IA linked services the Enterprise Support SMC also includes application storage and database management services.

The SOA Platform Services SMC group is a suite of services that will handle the life cycle management of services, including ensuring that services are running and are accessible and that they are operating and performing as they should. Below we will discuss some of the services found within the Core Enterprise Service SMC group.

The Service Discovery Service, which covers the ability to discover available services, is located within the SOA Platform Service SMC group. Having this capability as a subgroup of SMC can be debated, but it is not an unreasonable placement of this functionality. The Service Discovery Services subgroup provides access to the metadata about services, and this metadata is central in order to be able to efficiently manage services. Note that current standards for service descriptions and for service discovery only support certain types of metadata, namely the syntactical interface description of services. Further standardization and profiling is needed to ensure that service descriptions are detailed enough to support more advanced SMC functionality.

SOA Monitoring Services are responsible for monitoring the performance of both single services and whole processes, as an input to other SMC functions. The C3 Taxonomy's EM identifies the functional requirements of this service, but gives little detail as to how these requirements are to be fulfilled. This is as expected, as this area of SOA research is less mature than for instance the Service Discovery Service.

As previously mentioned, a key principle in SOA is that the information exchange within the infrastructure should be based on policies, which control information flow, access to resources and compliance with business and legal rules. The SOA Plaform Services SMC group contains a Policy Enforcement Service, which is responsible for ensuring that the current policies are adhered to by service and service users. This functionality is closely linked to the IA group, where similar mechanisms exist in order to enforce security policies and rules.

3.6 Applying the C3 Taxonomy to the current INI

So far we have focused on the C3 Taxonomy and its application to the INI of the future. However, the C3 Taxonomy may also be used for describing the ”as is” architecture of INI. Such an architecture will probably use a small subset of the service categories of the taxonomy. Existing information systems are typically self-contained with respect to functionality, as they are not structured according to a three-layer architecture consisting of the presentation layer, logical layer and data layer. Such self-contained systems are categorized as applications according to the C3 Taxonomy. If the C3 Taxonomy is applied to the information systems that make up the current INI, almost all systems will be placed within the User-Facing Capabilities group, as User Applications. Few (if any) current systems will fit into categories such as the COI Services and Core Enterprise Services groups.

User applications, and indeed everything else in the INI, should undergo timely refactoring so as to factor out common functionality which is then pushed downward in the architecture according to level of generality. The aim is that non-generic software and hardware become thin clients to more generic services in underlying layers. However, all else being equal, the total amount of functionality in the INI should remain constant and not depend on whether software or hardware is service-oriented. Another way of saying this is that the INI itself should evolve to become service-oriented without its functionality changing due to service-orientation.

3.7 Aligning the C3 Taxonomy with NAF and TOGAF

As previously mentioned, NAF defines several architecture types, which all describe architectures at different levels of detail and with different focus. The overarching architecture covers the future view of the entire enterprise, and has limited detail, the reference architecture is more detailed and is intended to be used to guide program execution, the target architectures guide solutions development, and the baseline architecture describes the “as is” state of the enterprise.

When using the C3 Taxonomy together with NAF, it is important to consider the different architecture types and how they differ in focus and level of detail. The C3 Taxonomy is intended to become a replacement for the current NNEC Overarching Architecture, but the usability of the C3 Taxonomy is not nessecarily limited to this specific architecture type. It should be possible to use the C3 Taxonomy as a common reference for all these architecture types, by varying the degree of detail that is used in the descriptions. For instance, when describing an overarching architecture, one can opt to only use the less detailed groupings of the C3 Taxonomy in order to keep the descriptions at a high level of abstraction. However, when describing a target architecture, the full level of detail relevant to that architecture can be utilized. As previously mentioned, the C3 Taxonomy is still undergoing further development and refinement, which means that creating detailed descriptions based on the C3 Taxonomy is challenging. This means that the current state of the C3 Taxonomy is best suited for higher level architectural descriptions such as overarching and reference architectures, but its ability to also be used for more detailed architectural descriptions is improving as it matures.

When it comes to the views defined by NAF, the layering of the NAF is not fully compatible with the C3 Taxonomy, as there is no obvious direct mapping for all views. The Capability View and the Operational View map roughly to the Operational Capabilities layers of the C3 taxonomy, while the Service-Oriented View and System View map roughly to the User Applications, COI Services and Core Enterprise Services layers. However, aspects of the Systems View and Technical View are more aligned to traditional systems development, as they are intended to be used to define the applications that generate the services described in the Service-Oriented View.

Additionally, the two taxonomies defined in NAF version 3.0, namely the NSOV-1 Service Taxonomy Subview and the NCV-2 Capability Taxonomy Subview, are defined, but not included into the newest release of NAF. If one is to base the architecture of the future INI on the combination of NAF, TOGAF and the C3 Taxonomy, it is vital to ensure that these NAF taxonomies are compatible with the C3 Taxonomy.

3.8 Feasibility of Applying the C3 Taxonomy

When assessing how feasible it is to use the C3 Taxonomy as a basis for an architecture for INI, there are a number of factors one needs to take into consideration. Note that this evaluation is based on work that is currently taking place at FFI, and that this evaluation thus must be considered an evaluation of the C3 Taxonomy as applied to the INI of the future, rather than with respect to the currently existing information infrastructure within the Norwegian Armed Forces.

There are a number of questions that need to be answered before one can conclude if the C3 Taxonomy is suitable as a starting point for describing the future INI, such as:

1. Does the C3 Taxonomy support the same basic principles as the architectural approach that has been chosen for INI?
2. How well does the C3 Taxonomy fit with the technology that we expect the future INI to consist of?
3. Is the C3 Taxonomy compatible with other architectural descriptions of relevant technologies?

In addition, there are other factors such as the maturity of the C3 Taxonomy that should be taken into consideration. The development of the C3 Taxonomy is a fairly new effort, and it is still on-going. Much of the technology that it covers is also immature, and this is reflected in the large variations in level of detail within the EM which describes the C3 Taxonomy. The higher levels of detail, as shown in the C3 Taxonomy poster in Figure 2.7, are stable and fairly well defined, while the lower levels of detail are subject to frequent alterations and additions.

The division of the COI Service category into COI-enabling and COI-specific services seems reasonable, because the COI-enabling services provide building blocks that can be used by more than one community of interest. For example, a COI-enabling Situational Awareness service may provide the basic software modules that can be used in various COI-specific situational awareness services. When it comes to the lower levels of detail of the COI Service category we sometimes find it hard to understand the rationale for a category. However, this is not a major objection as the development of the taxonomy is still on-going.

Seen from a SOA perspective, the C3 Taxonomy is structured is such a way that is it compatible with the basic principles of service-orientation. The division of functionality into logical layers, where the services on one layer utilize the capabilities offered at other layers match well with the goal of making services that are reusable and combinable. Furthermore, having the functionality covered by the C3 Taxonomy divided into services in a hierarchical manner means that it is easy to find a service description with the correct level of abstraction for different usages.

At the Core Enterprise Service level, there is a close match between the functionality that one can expect to see in a future INI and the functionality covered by the C3 Taxonomy. In addition, the manner in which core functionality is broken down into services in the C3 Taxonomy seems reasonable. The C3 Taxonomy layers the core functionality, and also combines central functionality into groups based on common traits.

With respect to the Communication Services layer, the division into subgroups seems unnecessary complex, and not in line with other descriptions of communications services. There is for instance a lack of a clear distinction between transport and transmission, and the description of important aspects related to service quality and availability is lacking. The communication services research at FFI focuses on different technologies than the ones described in the C3 Taxonomy, and also categorize these technologies based on other factors than those found in the C3 Taxonomy.

The two vertical groups of the C3 Taxonomy, IA and SMC, are both logical groupings of functionality that is likely to be implemented as a part of the horizontal groups they intersect with rather than as separate entities. In general, the level of detail in the description of these groups is very broad, and it is not immediately clear how these vertical groups will fit into the larger C3 Taxonomy. The C3 Taxonomy covers many on-going efforts, but further specification is required in order to determine if the organization of concepts is in line with the future development of INI.

4 C3 Taxonomy usage examples

In the previous section we have discussed our experiences with the C3 Taxonomy's descriptions of the technical capabilities in the Communication Services, Core Enterprise Services, Information Assurance and Service Management & Control groups. We have noted that INI's architecture, as depicted in Figure 2.5, can be mapped onto the C3 Taxonomy. The overall structure of the latest version is almost exactly that of the C3 Taxonomy, including crosscutting concerns corresponding to IA (red) and SMC (green). This correspondence is why it is meaningful to relate to the C3 Taxonomy when developing the INI.

The C3 Taxonomy has been populated with a substantial number of artifacts in some of the categories directly related to specific defense branches. There have been no comparable efforts toward populating the INI architecture. In line with our introductory remarks, a stepping stone has been laid if one is able to populate the C3 Taxonomy sensibly with systems associated with FFI's research portfolio. In the following, we report on our efforts toward doing this with regards to two examples from INI-related work at FFI.

4.1 Land Community of Interest

In this section we identify services that are relevant for land forces. The *Land COI Services* category constitutes situational awareness, operational planning and tasking/order services for command and control of land forces. Examples of such services are given in Figure 4.1. In addition we have identified some other tentative categories that are relevant for the land domain. These are the *JISR*[2] *COI Services*, *Artillery COI Services*, *Air Defence COI Services*, *Engineer COI Services*, *Medical Service COI Services* and *Logistics COI Services*. So far these tentative categories have not been populated with services. At a later stage, also the *COI-Enabling Services* layer should be populated with relevant services.

[2] JISR stands for Joint Intelligence, Surveillance and Reconnaissance

In the following, we describe the tentative services of the Land COI Services category. For the services providing access to information, we also identify the service type.

Situational Awareness Services

- **Situation Picture Service**: The service provides a Recognized Ground Picture for a military unit (e.g. brigade). The service is provided (owned) by the unit's headquarter. Type of service: publish/subscribe.
- **"Current" Picture Service**: The service provides a situation picture at a lower tactical level, e.g. battalion. Type of service: publish/subscribe.
- **Shared database service**: The service provides access to stored information, e.g. pictures, observations and sensor data. An information element can be from a single source, it can be aggregated information (can be merged from more sensors), or analyzed information. The service is provided (owned) by a unit (e.g. intelligence unit) that has stored information it will share. Type of service: pull type of service.
- **Position Service**: The service provides information on the position of units within an area. Type of service: publish/subscribe.
- **Alert/Warning Service**: The service provides information on various events that is important to share with others within an area. The events can be Chemical, Biological, Radiological and Nuclear (CBRN) threats, Improvised Explosive Devices (IED) threats, snipers or other. Type of service: publish/subscribe.
- **Operational and Logistics Status Service**: This service provides operational and logistics status for all blue forces, both combat and support forces. Relevant parameters for reporting are for example ammunition reserves, fuel reserves and combat condition (resting, ready, tasked, etc.). Type of service: publish/subscribe.
- **Observation Service**: The service provides information (position and classification) on observed objects. The observed objects are typically enemy or neutral forces. Type of service: publish/subscribe.
- **Current Plans Service**: The service provides access to various plans that units needs in their planning process. Type of service: pull type of service.

Planning Services

These are services for assessing courses of action, developing plans and coordination of plans. It includes services for coordination of plans towards the sea and air domains, joint level and international cooperation partners. Special services adjusted to the needs of support forces (e.g. artillery, intelligence, air defense, military police, engineer, logistics) are also provided.

Tasking/Order Services

These are services for preparing orders (also fragmentary orders), reporting and coordination. It includes services for coordination towards the sea and air domains, joint level and international partners. Special services adjusted to the needs of support forces are also provided.

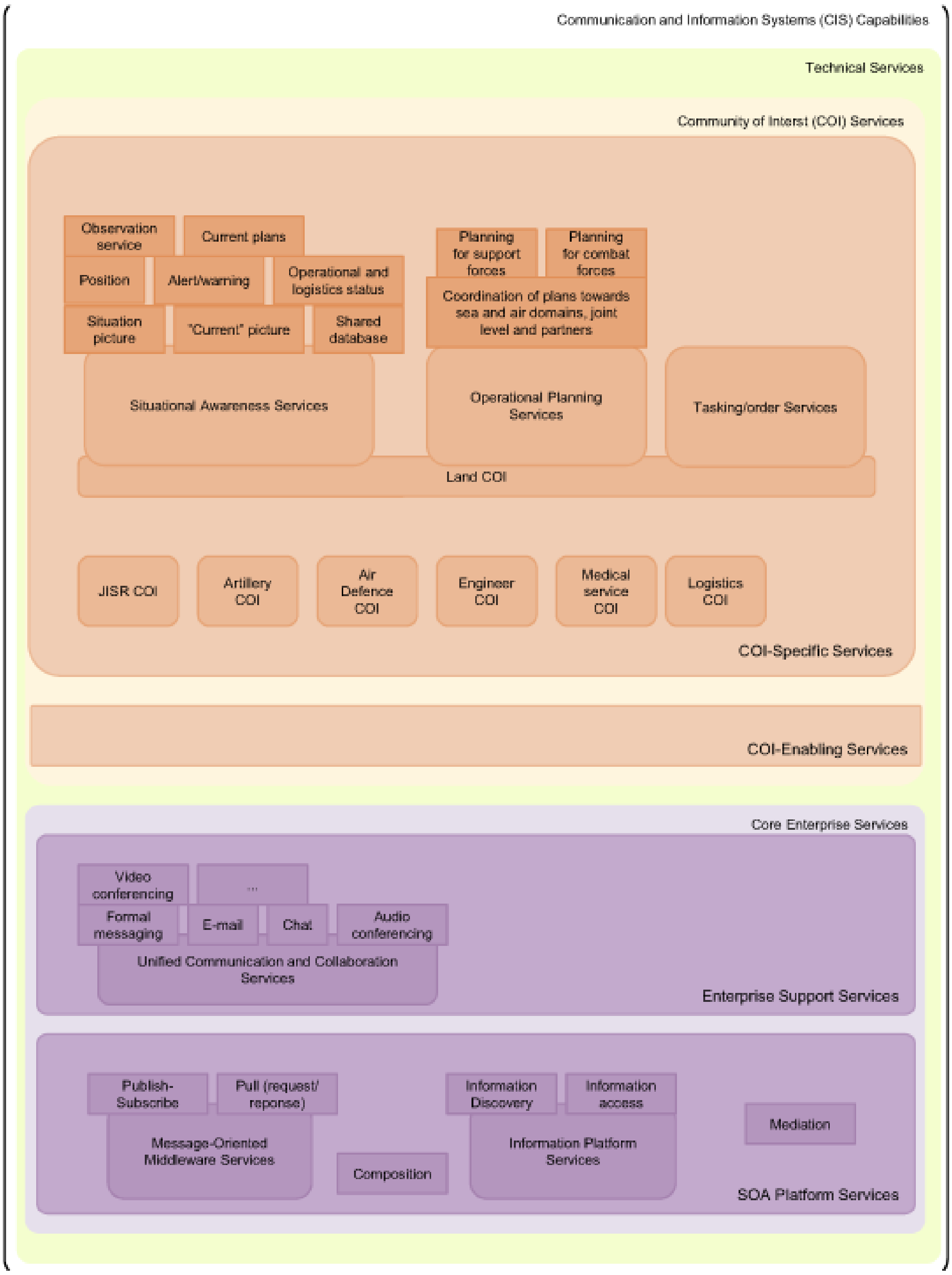


Figure 4.1 Tentative population of some services relevant for land forces.

4.2 Modeling and Simulation Community of Interest

In modeling and simulation, interoperability and loose coupling have been in focus for some time. The High Level Architecture (HLA) is a design, development, and runtime standard for distributed simulation software systems [25, 15] which enables viable principles toward loose coupling and interoperability. In HLA, the main simulation software modules that make up a simulation system are called *federates*. Federates may be combined to form a *federation*, coordinated by a runtime infrastructure (RTI); see Figure 4.2. Federates communicate with the RTI by means of APIs for Java or C++. In the most recent version, HLA Evolved, there is, in addition, a Web service API which allows one to package federates as Web services within the federation [18, 16, 19]. HLA prescribes a publish/subscribe protocol: federates publish object attributes, and federates may subscribe to updates of published attributes. The RTI coordinates these messages and is also capable of synchronizing events according to advanced time-management schemes [9]. Federates may also query the RTI on-the-spot for updates.

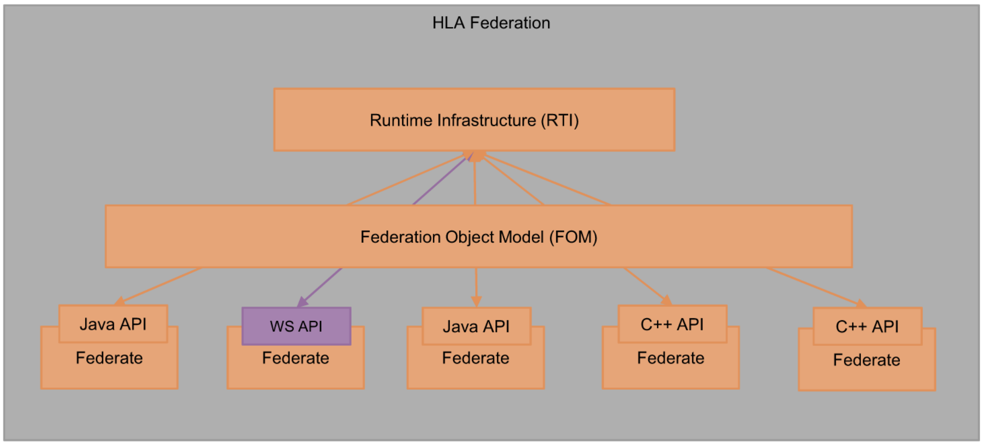


Figure 4.2 High-Level Architecture (HLA).

In SOA terminology, the RTI in HLA federations functions as a state management deferral mechanism, since state management has been delegated away from the federates and to the RTI [8]. The RTI could be seen as a utility service; i.e., middleware that intentionally violates the SOA ideal of statelessness in order that other services may enjoy their level of statelessness and state processing deferral [8].

We have tentatively placed modeling and simulation-relevant artifacts in categories in the current state of the C3 Taxonomy as illustrated in Figure 4.3. Note that we here place software, including machine-readable documents, in the taxonomy. In our proposal, standards are not first-class citizens of the taxonomy unless they actually play the role of use cases (a use case being a requirements specification and production element). On the other hand, standards are relevant as necessary references and complementary requirements specifications attached to the software. The EM wiki's structure gives ample opportunity to record such "second-class citizens" in the C3 Taxonomy. We have also added two categories which we comment on below.

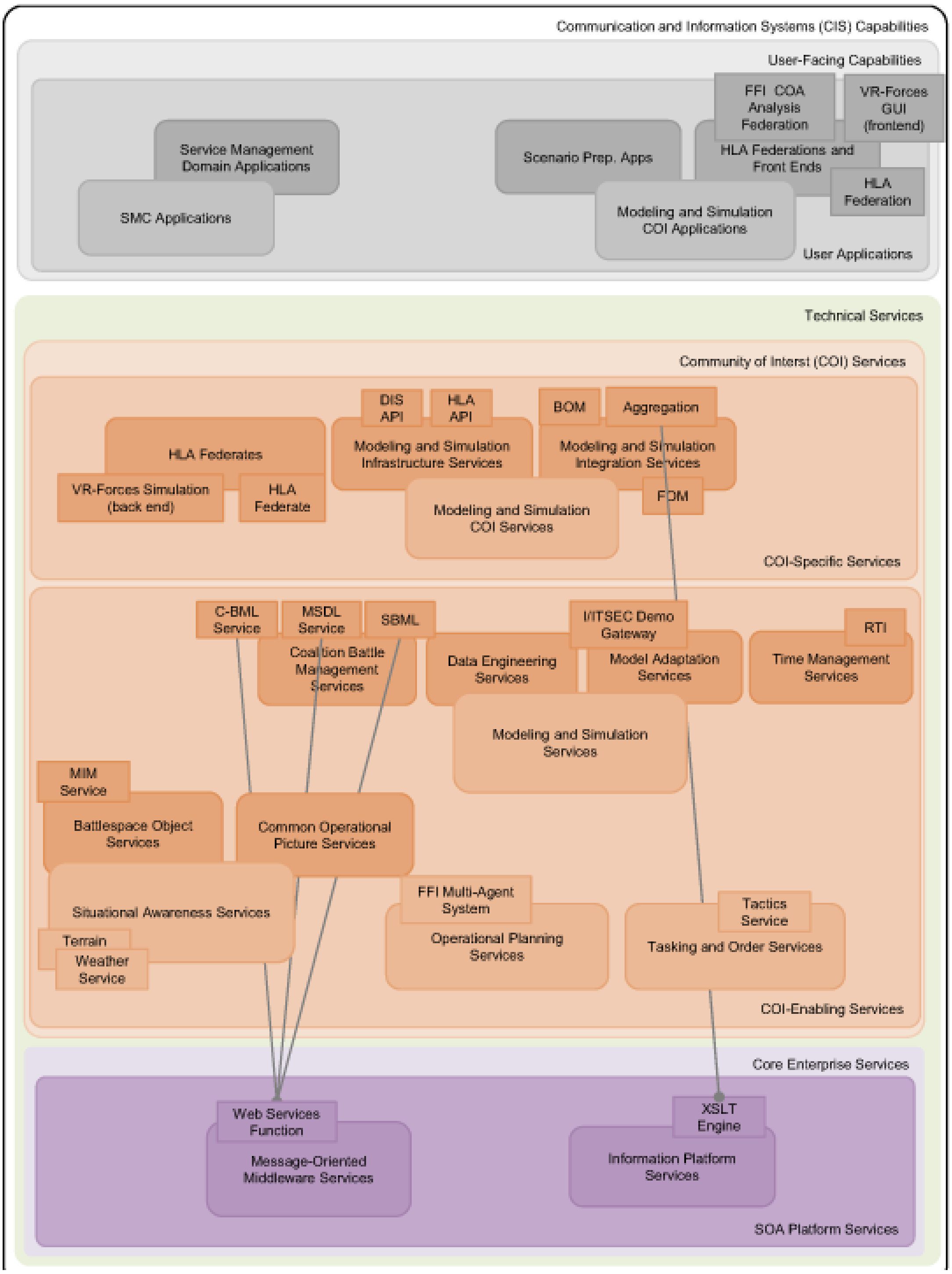

Communication and Information Systems (CIS) Capabilities
User-Facing Capabilities
FFI COA Analysis Federation
VR-Forces GUI (frontend)
Service Management Domain Applications
SMC Applications
Scenario Prep. Apps
HLA Federations and Front Ends
HLA Federation
Modeling and Simulation COI Applications
User Applications
Technical Services
Community of Interst (COI) Services
DIS API
HLA API
BOM
Aggregation
HLA Federates
Modeling and Simulation Infrastructure Services
Modeling and Simulation Integration Services
VR-Forces Simulation (back end)
HLA Federate
FOM
Modeling and Simulation COI Services
COI-Specific Services
C-BML Service
MSDL Service
SBML
I/ITSEC Demo Gateway
RTI
Coalition Battle Management Services
Data Engineering Services
Model Adaptation Services
Time Management Services
Modeling and Simulation Services
MIM Service
Battlespace Object Services
Common Operational Picture Services
Situational Awareness Services
Terrain
Weather Service
FFI Multi-Agent System
Operational Planning Services
Tactics Service
Tasking and Order Services
COI-Enabling Services
Core Enterprise Services
Web Services Function
Message-Oriented Middleware Services
XSLT Engine
Information Platform Services
SOA Platform Services

Figure 4.3 Tentative population of some modeling and simulation-related software in the C3 Taxonomy

User Applications

Modeling and simulation artifacts will need to exist at different layers of the C3 Taxonomy, here we have identified potential User Applications, which will rely on functionality provided by the lower layers.

HLA Federations and Front Ends: This category is suggested by us and is not in the C3 Taxonomy at present.

VR-Forces GUI (front end): VR-Forces (MÄK Labs) is a framework and set of tools for developing simulation systems according to HLA. A VR-Forces front end is, in some sense, a thin simulation system client using services provided by a VR-Forces Simulation back end and other federates in a HLA federation. The front end participates in the federation as a federate, but its role is user-facing.

FFI Course of Action (COA) Analysis Federation: FFI has developed a *multi-agent framework*, where a multi-agent system receives Coalition Battle Management Language (C-BML) orders (see below) from a Command & Control (C2) system and executes the orders by generating appropriate entity command movements in a simulation engine. A battle order originating from a C2 system is a general instruction which has to be executed according to knowledge about terrain, enemy position, weather etc. The multi-agent system operates as a federate in an HLA federation. Communication between the C2 system and the HLA federation goes via a JC3IEDM database (see below) and uses C-BML/MSDL (see below) over WebSockets.

HLA Federation: This represents any HLA federation regardless of commercial frameworks such as VR-Forces. The degree to which a federation may be considered a service in the SOA sense is a topic for discussion; see [12].

COI Services

The majority of modeling and simulation artifacts will be found at the COI Services level, where there is a COI-specific Services category already dedicated to this type of functionality. Below we suggest a mapping of modeling and simualtion functionality into both the COI-specific Services and COI-Enabling Services subgroups.

HLA Federates: This category is suggested by us and is not in the C3 Taxonomy at present.

VR-Forces Simulation (back end): This represents simulation federates which provide services to a VR-Forces front ends.

HLA Federate: This represents any HLA federate regardless of commercial frameworks such as VR-Forces. The sense in which a federate may be considered a service in the SOA sense is a topic for discussion; see [12].

DIS API: This represents the concrete functionality provided by implementations of the DIS standard.

HLA API: This represents the concrete functionality provided by implementations of the HLA standard.

BOM: This represents concrete Base Object Models (BOMs) which function as machine-readable (XML-based) specifications of interaction patterns and entities in HLA simulation. It has been argued that BOMs could function as service interface descriptors [28, 11], and it is relevant to provide these through services (if not as services themselves).

FOM: In HLA, the objects and interactions that are shared (i.e., whose attributes are published and subscribed) among federates in a federation are declared in a (XML-based) Federation Object Model (FOM), which is input to the RTI. Concrete FOMs may be reused, and it is relevant to provide these as services.

Aggregation: There are guidelines on how to aggregate BOMs in order to aggregate entities in a simulation. SimVentions Inc. has developed a BOM Aggregation Framework (BAF) with a BOM Aggregation Support Server (BASS) which provides simple aggregation/deaggregation functionality as run-time services into a HLA federation.

C-BML Service, **MSDL Service**, **SBML**: C-BML is a formalized language under standardization to provide a common language between C2 systems, simulation systems and also autonomous systems [22]. The Military Scenario Definition Language (MSDL) SISO-STD-007-2008 [27] is a standard for describing scenarios; e.g., for initializing simulation systems. Services which provides functionality for handling C-BML and MSDL are relevant. For example, a Scripted BML (SBML) server coordinated the joint MSDL initialization as well as the exchange of C-BML battle orders in a demo (in which FFI participated) at the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC) involving several C2 and simulation systems and [26].

MIM Service: The Multilateral Interoperability Program (MIP) has developed the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) STANAG 5525, which sets out to specify the minimum set of data that needs to be exchanged in coalition or multinational operations. Software systems that operate and communicate in terms of JC3IEDM data structures therefore gain a certain level of interoperability since they, at least, operate in terms of the same data structure. The next generation of the JC3IEDM—the MIP Information Model (MIM)— is currently under release and is UML based. Services for handling MIM data are relevant. For example, a JC3IEDM database was used in the above-mentioned demo for storing scenario and position data, and a gateway for interchanging JC3IEDM data and C-BML and MSDL was used.

I/ITSEC Demo Gateway: The above-mentioned demo used gateways or wrappers to service-enable traditional (stove-piped) systems. These gateways, or the common functionality in them, could be offered as services. For more ideas on this topic, see [7, 6].

RTI: This is the Runtime Infrastructure of HLA. Concrete implementations of the RTI could be offered as middleware services. We have placed it in **Time Management Services**, but it should be relocated to a more appropriate category, since the RTI also fulfills several other functions.

FFI Multi-Agent System: The multi-agent system mentioned above in the **FFI Course of Action (COA) Analysis Federation** uses context-based reasoning [10] to compute appropriate entity movements in the simulation according to contextual data available in the simulation. It is relevant to service-enable the multi-agent system in the sense of offering varying battle order-execution strategies; e.g., in terms of reasoning algorithms (context-based reasoning, decision trees, neural nets, etc.), in terms of environment data to be considered (terrain, weather, season, mode of aggressiveness, etc.) and in terms of operational tactics.

Terrain Service, **Weather Service**, **Tactics Service**: These services are relevant for simulations for increased realism and for the ability to readily and rapidly alter scenarios for planning, training and rehearsal, see[12].

Core Enterprise Services

The modeling and simlulation artifacts on the COI Service level will require support from components the the Core Enterprise Services level. We have identified two such requirements, in the form of support for Web services technology and XSLT, as described below.

Web Service Function: This represents functionality according to the Web Service standard. Several of the above services use Web Service functionality.

XSLT Engine: XML parsing and translation is needed to aggregate BOMs. It is also possible to translate a BOM aggregate to a FOM [17, 11]. This can be done with a Extensible Stylesheet Language Transformation (XSLT). In theory, one may therefore use BOMs as simulation service interface specifications, and when combining services, the aggregated BOMs can be automatically translated to the appropriate FOM necessary for the resulting federation to run. With modular FOMs, one can also extend the federation at runtime. In this manner, the declaration for shared state (the FOM) can be constructed during orchestration time using loosely coupled simulation components.

To summarize, modeling and simulation architecture and systems have several properties promoted by SOA. There are still issues which need to be dealt with before simulation federations and/or federates (in HLA) can be viewed as services in the SOA sense [12]. Some of these issues are inherent to modeling and simulation technology. We postulate that the C3 Taxonomy will prove useful for structuring existing solutions and for structuring further work. At present, there are few sub-categories for the M&S COI, and more could easily be gained through concerted efforts.

5 The Way Forward

Describing the architecture of INI is a complex and challenging task, and there are many open questions and issues related to this task. One important requirement for success is that sufficient resources, from both research communities and from domain experts, are dedicated to the task. In addition, a methodology for development of the architectural descriptions is required. As the latest IT strategy document from the Norwegian Chief of Defence points to NAF, TOGAF, and the C3 Taxonomy, these form a natural starting point, but a better understanding of how, and if, these can be successfully combined is needed. Furthermore, TOGAF is clearly well suited for developing architectures for information systems. However, further research is required to determine to what extent TOGAF is suited and useful for developing architectures for other INI components types (communication, security, and management systems).

Another question related to the methodology for developing the INI architecture is whether the development of the INI architecture and the development of the INI components themselves (e.g. a procurement project for a given information system) should be considered to be two separate, but connected, processes, or if they should both be integrated into the same development process. One one side, the stakeholders responsible for these two processes are likely to be different: the stakeholders responsible for planning the INI (Cyberforsvaret) should provide architecture products, such as the overarching architecture and reference architecture for INI, that will guide the various systems development projects. System development, however, is the responsibility of procurement projects. On the other hand, there is a mutual dependency between these processes, and utilizing a whole product methodology based on current best practices within agile development might be advantageous. Further work is needed to investigate this topic.

In addition, if the architectural descriptions are to be based on the C3 Taxonomy, the shortcomings of the taxonomy need to be addressed. The communication services description needs to be brought in line with how the communication systems of the future INI are likely to develop, something that might require developing an alternative breakdown of the communication services group. Furthermore, clarification is needed on how the cross-layer groups are to be handled, and how the functionality represented by these groups are to be integrated into the functionality found in the horizontal groups. Finally, it is important to remember that using the C3 Taxonomy to guide system development is not, on its own, sufficient to ensure compatibility between systems. Further technical specifications, such as the SOA Baseline documentation, are needed to ensure that independently developed systems are able to interoperate.

And finally, it is vital that the stakeholders responsible for the development of INI devote sufficient resources to develop architectural descriptions of INI. In order to ensure that all procurement projects are well coordinated, and are working together towards a common information infrastructure, this should be done outside the procurement process, for instance in a separate project with focus on the INI architecture.

References

[1] M. Booth, T. Buckman, J. Busch, B. Caplan, B. Christiansen, R. van Engelshoven, K. Eckstein, G. Hallingstad, T. Halmai, P. Howland, V. Rodriguez-Herola, D. Kallgren, S. Onganer, R. Porta, C. Shawcross, P. Szczucki, and K. Veum. Nato network enabled capability feasibility study vii version 2.0. Technical report, NC3A, 2005.

[2] C4ISR Technology & Human Factors (THF) Branch, Allied Command Transformation (ACT). The C3 Classification Taxonomy. Technical report, 2012. Document generated from the ACT Enterprise Mapping Wiki on November 2012.

[3] Consultation, Command and Control Board (C3B). Core Enterprise Services Framework. NATO Unclassified releasable to EAPC/PFP, 26 May 2009.

[4] Consultation, Command and Control Board (C3B). CORE ENTERPRISE SERVICES STANDARDS RECOMMENDATIONS: THE SOA BASELINE PROFILE VERSION 1.7. Enclosure 1 to AC/322-N(2011)0205, NATO Unclassified releasable to EAPC/PFP, 11 November 2011.

[5] F. Dandashi, R. Siegers, J. Jones, and T. Blevins. The Open Group Architecture Framework (TOGAF) and the US Department of Defense Architecture Framework (DoDAF). White paper W061, The Open Group, 2006.

[6] D. L. Drake, I. X. Martins, R. A. Roca, and F. Carr. Live-Virtual-Constructive Service-Oriented Architecture. Service-Oriented Architecture application to Live-Virtual-Constructive simulation: Approach, benefits, and barriers. Technical Report NSAD-R-2011-025, National Security Analysis Department, The Johns Hopkins University, Applied Physics Laboratory, 2011.

[7] D. L. Drake and K. L. Morse. Use of SOA for distributed simulation: A way forward. In *Proc. 2012 Spring Simulation Interoperability Workshop (SIW)*. Simulation Interoperability Standards Organization (SISO), 2012.

[8] Thomas Erl. *SOA Principles of Service Design (The Prentice Hall Service-Oriented Computing Series from Thomas Erl)*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2007.

[9] R. M. Fujimoto. *Parallel and Distributed Simulation Systems*. Wiley-Interscience, 2000.

[10] A. J. Gonzalez, B. S. Stensrud, and G. Barret. Formalizing context-based reasoning: A modeling paradigm for representing tactical human behavior. *Int'l J. Intelligent Systems*, 23:822–847, 2008.

[11] P. Gustavson, T. Chase, L. Root, and K. Crosson. Moving towards a Service-Oriented Architecture (SOA) for distributed component simulation environments. In *Proc. 2005 Spring Simulation Interoperability Workshop (SIW)*. Simulation Interoperability Standards Organization (SISO), 2005.

[12] J. E. Hannay, K. Bråthen, and O. M. Mevassvik. Simulation architectures and service-oriented defence information infrastructures - preliminary findings. Technical Report FFI-rapport 2013/01674, Norwegian Defence Research Establishment (FFI), 2013.

[13] H. D. Jørgensen, T. Liland, and S. Skogvold. Aligning TOGAF and NAF—experiences from the Norwegian Armed Forces. In P. Johannesson, J. Krogstie, and A. Opdahl, editors, *The Practice of Enterprise Modeling*, volume 92 of *Lecture Notes in Business Information Processing*, pages 131–146. Springer, 2011.

[14] A. Josey. TOGAF Version 9.1 Enterprise Edition—an introduction. `http://pubs.opengroup.org/architecture/togaf9-doc/arch/`, 2011. Accessed January 2013.

[15] F. Kuhl, R. Weatherly, and J. Dahmann. *Creating Computer Simulations—An Introduction to the High Level Architecture*. Prentice Hall PTR, 1999.

[16] B. Möller and C. Dahlin. A first look at the HLA Evolved Web Service API. In *Proc. 2006 European Simulation Interoperability Workshop (SIW)*. Simulation Interoperability Standards Organization (SISO), 2006.

[17] B. Möller, P. Gustavson, R. Lutz, and B. Löfstrand. Making your BOMs and FOM modules play together. In *Proc. 2007 Fall Simulation Interoperability Workshop (SIW)*. Simulation Interoperability Standards Organization (SISO), 2007.

[18] B. Möller and S. Löf. A management overview of the HLA Evolved Web Service API. In *Proc. 2006 Fall Simulation Interoperability Workshop (SIW)*. Simulation Interoperability Standards Organization (SISO), 2006.

[19] B. Möller, K. L. Morse, M. Lightner, R. Little, and R. Lutz. HLA Evolved—a summary of major technical improvements. In *Proc. 2008 Fall Simulation Interoperability Workshop (SIW)*. Simulation Interoperability Standards Organization (SISO), 2008.

[20] NATO Communications and Information Agency (NCIA). The C3 Classification Taxonomy. `http://www.ncia.nato.int/ourwork/Pages/Coherence/C3-Classification-Taxonomy.aspx`, 2011. Accessed August 2012.

[21] NATO Consultation, Command and Control Board. NATO Architecture Framework Version 3. `http://www.nhqc3s.nato.int/ARCHITECTURE/_docs/NAF_v3/ANNEX1.pdf`, 2007. Accessed January 2013.

[22] NATO Research and Technology Organisation. Coalition Battle Management Language (C-BML). Technical Report RTO-TR-MSG-048, 2012.

[23] OASIS. Reference model for service oriented architecture 1.0. https://www.oasis-open.org/committees/soa-rm/, October 2006.

[24] Norwegian Ministry of Defence. Forsvarets ikt-strategi, 2013.

[25] M. D. Petty and P. Gustavson. Combat modeling with the High Level Architecture and Base Object Models. In A. Tolk, editor, *Engineering Principles of Combat Modeling and Distributed Simulation*, chapter 19, pages 413–448. Wiley, 2012.

[26] J. M. Pullen, D. Corner, A. Brook, R. Wittman, O. M. Mevassvik, and A. Alstad. MSDL and C-BML working together for NATO MSG-085. In *Proc. 2012 Spring Simulation Interoperability Workshop (SIW)*. Simulation Interoperability Standards Organization (SISO), 2012.

[27] Simulation Interoperability Standards Organization (SISO). Standard for: Military Scenario Definition Language (MSDL). `http://www.sisostds.org/DigitalLibrary.aspx?Command=Core_Download&EntryId=30830`, 2008. Accessed August 2012.

[28] B. Sisson, P. Gustavson, and K. Crosson. Adding aggregate services to the mix: An SOA implementation use case. In *Proc. 2006 Spring Simulation Interoperability Workshop (SIW)*. Simulation Interoperability Standards Organization (SISO), 2006.

[29] E. Winjum, O. I. Bentstuen, A. Eggen, K. Lund, R. H. MacDonald, N. A. Nordbotten, R. Rasmussen, B. Reitan, and J. E. Voldhaug. Forslag til innretting av perspektivplan materiell (PPM) for programområde NbF-systemer. Technical Report FFI-rapport 2012/02075, Norwegian Defence Research Establishment (FFI), 2012.

[30] World Wide Web Consortium (W3C). Web Services Architecture. http://www.w3.org/TR/ws-arch/, February 2004.