Allied Data Publication 34

(ADatP-34(E))

NATO Interoperability Standards and Profiles

Volume 5

Design Rules

27 April 2011

C3 CCSC NATO Open Systems Working Group

Table of Contents

1. NISP Design Rules 1
1.1. Introduction 1
1.2. Summary 1
1.3. Introduction 1
1.4. General 2
1.4.1. Target Group 2
1.4.2. Definitions, Abbreviations and Acronyms 2
1.4.3. References 3
1.5. Background 3
1.6. Design rules summary 4
1.6.1. Introduction to design rules 4
1.6.2. Benefits from using design rules 5
1.6.3. Consequences of using design rules 5
1.7. Design rules in a NATO NEC federated environment 5
1.7.1. Problems or opportunity description 5
1.7.2. Solution 6
1.7.3. Consequences 10
1.8. Reference architecture - National design rules 11
1.8.1. The Swedish Design rules contributions 11
1.8.2. Nation x 14
2. International Military Interoperability for information exchange in the NNEC context 15
2.1. General 15
2.1.1. Unique Identity 15
2.1.2. Target Group 15
2.1.3. Definitions and abbreviations 15
2.2. Design Rule 17
2.2.1. Context 18
2.2.2. Problem 21
2.2.3. Solution 24
2.2.4. Rejected solutions 41
2.3. Motivation 41
2.4. Consequences from the solutions 42
2.5. Examples 43
2.6. Meta data 44
2.6.1. Keywords 44
2.6.2. Associated design rules 44

This page is intentionally left blank

List of Figures

1.1. Design rule model 8
1.2. Releationship between NISP objects Profiles, standards and Designrules 11
2.1. Simplified NNEC Technical Services framework with design rule scope 18
2.2. Federation Overview 20
2.3. Services and the information aspect 31
2.4. Informationzones in the federation 33
2.5. Technology Overview 41
2.6. Evolving C3 Requirements and Technology Trends for NNEC 42
2.7. Service Interoperability Points and their relationship to the Overarching Architecture 44

This page is intentionally left blank

1. NISP DESIGN RULES

1.1. INTRODUCTION

001. This agreed document was developed by the NATO Open Systems Working Group (NOSWG) under the authority of the NATO Consultation, Command and Control Board (NC3B). It was noted by the NATO C3 Board (AC/322-N(2011)0021-REV2-AS1 Dated 26 Apr 2011) making the Volume 2 standards and profiles mandatory for use in NATO common funded systems, and made available to the general public as a replacement for ADatP-34(D).

1.2. SUMMARY

002. This guideline document describes a concept and model for how knowledge of proven solutions can be documented and packaged in order to form a shared basis for supporting the development and the implementation of NNEC based systems for NATO.

1.3. INTRODUCTION

003. This document introduces the concept of design rules by describing what design rules are and how they shall be applied in a NATO Network Enabled Capabilities context.

004. Design rules are about reusing knowledge of proven solutions for reoccurring problems. Reuse of solutions that give NNEC-specific characteristics is particularly important. These solutions should solve frequent and/or difficult problems, promote important system characteristics and/or improve the quality of the resulting product in a cost effective way.

005. A design rule consists mainly of the following three parts:

- Context; describes under what circumstances the design rule is valid
- Problem/Opportunity; is a description of the problem it solves or the opportunity it exploits.
- Solution; is a description how the problem/opportunity shall/should be resolved in the given context

006. Design rules can give solutions on all levels, but it is anticipated that the produced design rules mainly takes care of the higher system levels (relating to the breakdown patterns in a system design) in order to avoid a cumbersome number of rules. If possible design rules shall be based on standards and/or NISP/NAF and will preferably be associated with as concept (generic concept of design).

007. The introduction of design rules in the NISP will also need to be integrated with other design related artefacts and frameworks within NATO such as the NATO Architectural Framework (NAF).

1.4. GENERAL

1.4.1. Target Group

1.4.2. Definitions, Abbreviations and Acronyms

Acronym	Explanation	Reference	Definition
DR	Design Rule	NOSWG	A standardized, reusable solution to a design problem in a specific context within a problem space that provides value to the user. Note: There are four (4) types of design rules: a. A development method that supports the life cycle perspective; b. A defined structure that supports descriptions of complex relations; c. A detailed description of suggested technical solutions; d. A proven and reusable solution for a generic problem.
DRP	Design Rule Package	NOSWG	A specific set of design rules that make up a solution package within a defined problem area.
SIOP	service interoperability point	EAPC(AC/322)D(2006)0002-REV1	A reference point within an architecture where one or more service interfaces are physically or logically instantiated to allow systems delivering the same service using different protocols to interoperate. Note: A service interoperability point serves as the focal point for service interoperability between interconnected systems, and may be logically located at any level within the components, and its detailed technical specification is contained within a service interface profile.
SIP	service interface profile	EAPC(AC/322)D(2006)0002-REV1	A set of attributes that specifies the characteristics of a service interface between in-

Acronym	Explanation	Reference	Definition
			teroperable systems in the Networking and Information Infrastructure. Note: A service interface profile is identified at a service interoperability point in an architecture system view.

1.4.3. References

Referenced documents

[1] C. Alexander et al. 1997 A Pattern Language, Oxford University Press, New York,

[2] E. Gamma, R. Helm, J. Vlissides 1995. Design Patterns: Elements of Reusable Object-Oriented Software. Reading, MA: Addison-Wesley

[3] F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad and M. Stal. 1996. Pattern-Oriented Software Architecture, A System of Patterns. New York: John Wiley and Sons

[4] Designrules, in the commercial world. David B. Kim Clark

1.5. BACKGROUND

008. Packaging knowledge into something reusable is nothing new in the software engineering field of science. Almost ten years ago a book was published that made a huge impact on how software engineers look upon packaging and sharing knowledge of proven solutions. The Design Pattern-book gave the engineers a tool not only on how to describe, formalize, package and distribute their knowledge and experience but also a tool on how to discuss different possible solution alternatives to a specific problem. It enables efficiency in both the communication and the implementation of software design, based upon a common vocabulary and reference.

009. The design pattern concept described in this book was not an original idea but the adaptation of the ideas from a building architect, Dr Christopher Alexander, who wrote a book on patterns found when categorizing floor plans, buildings, neighbourhoods, town, cities, etc. In that book Alexander writes:

010. "Each pattern is a three-part rule, which expresses a relation between a certain context, a problem, and a solution."

011. This is the central thing about being able to package our knowledge and experience. It is not enough to describe a solution. To make a solution useful you also have to state what problem the solution solves or what opportunity that the solution makes possible as well as the context in which the problem/opportunity - solution pair is valid. For instance, the optimal solution to the

problem on how to enter and exit a building will be very different in the context of a building situated in Stockholm or somewhere in the arctic.

012. The design patterns from the Design Pattern-book are the type of patterns that have become most widely known. These patterns solve problems or makes opportunities possible at a analysis or design level of abstraction. However, this is not the only level of abstraction covered by patterns. 1996 an important piece of work regarding patterns was published dealing with patterns on an architectural level of abstraction. This book identified patterns for system architecture at a higher level than the original design patterns. The patterns relate to the macro-design of system components such as operating systems or network stacks.

013. After this, patterns of higher and higher level of abstraction have been published, sometimes, but not very often, also on lower levels. A specific level of interest to us is the system level-of abstraction. System-level patterns identify and describe the overall structure and interactions that can occur between components of a system. Furthermore, Enterprise-level patterns are possible, showing how to efficiently organise ones enterprise and what type of services to offer to its clients.

014. Consequently, mechanisms similar to the design rules described in this guideline have been used in different contexts and at different levels of abstraction. In many cases they have been quite popular and proven practical. Thus, it can be assumed that the design rule concept can be an efficient means to provide reuse of knowledge within the future development of the NNEC.

1.6. DESIGN RULES SUMMARY

1.6.1. Introduction to design rules

015. Design rules are about reusing knowledge of proven solutions for reoccurring problems. Reuse of solutions that give NNEC-specific characteristics is particularly important. These solutions should solve frequent and/or difficult problems, promote important system characteristics and/or improve the quality of the resulting product in a cost effective way.

016. Design rules consist mainly of the following three parts:

- Context; describes under what circumstances the design rule is valid
- Problem/Opportunity; is a description of the problem it solves or the opportunity it exploits.
- Solution; is a description how the problem/opportunity shall/should be resolved in the given context

017. Design rules can give solutions on all levels, but it is anticipated that the produced design rules mainly takes care of the higher system levels (relating to the breakdown patterns in a system design) in order to avoid a cumbersome number of rules. If possible design rules shall be based on standards and/or NISP/NAF and will preferably be associated with as concept (generic concept of design).

018. A design rule package is a mechanism for packaging of design rules (by reference) within a certain domain or for a specific kind of system. The dependencies between design rules that are part of a design rule package shall be defined and minimized.

1.6.2. Benefits from using design rules

019. In today's knowledge oriented organizations it is very important to make sure that the knowledge of people is preserved in the organization even if the people change positions or leave the company. Design rules are important tools to be able to aid the process of managing this knowledge since they force documentation of knowledge in a structured way.

020. The use of design rules to document and package proven solutions is expected to speed up development, and reduce cost and risk, by reusing knowledge on how to solve recurring problems and by providing verified solutions to those problems.

021. Moreover, the use of design rules provide the means to coordinate development of different federated systems in order to make them network enabled and facilitate the evolvement of combined capabilities. Another important aspect is also that design rules aid organisations in creating a common understanding of the problems and challenges they are facing.

1.6.3. Consequences of using design rules

022. In order for design rules to have effect in an organization there must be a framework which describes what design rules are and how they shall be used, i.e. this document. Design rules will also affect the way solutions are described and must be an integral part of the architecture description framework.

023. Another important thing to remember is that design rules will affect the way we work, thus putting new requirements on the processes and people within our organization.

1.7. DESIGN RULES IN A NATO NEC FEDERATED ENVIRONMENT

024. This guideline document describes a concept and model for how knowledge of proven solutions in the form of design rules can be documented and packaged in order to form a shared basis for the future development of NNEC based systems for NATO.

025. The processes in which design rules are identified, produced and used are not described within this guideline.

1.7.1. Problems or opportunity description

026. In the development of large systems of systems or federated systems for the future needs of the NATO there are several problems to be solved as well as opportunities to exploit. The

problems range from what methods to use for requirements capture and design to how to solve detailed technical matters.

027. In order to be able to establish a set of building blocks that can be used to meet the needs of the future NNEC, design regulations are absolutely essential if the building blocks shall be possible to be used together and combined in different ways, from a technical as well as from a business point of view.

028. Design regulations in this context are the descriptive or normative regulation work necessary for NATO nations to be able to implement, configure and use systems in a federated environment. This includes not only technical and business design, but also the ability to manage and maintain these regulations to be able to provide the NATO nations with flexible component based systems.

029. Moreover, there is a strong incentive to endorse reuse of proven solutions or implementations and thus get a more cost-effective solution. The overall quality is also expected to benefit from this kind of reuse.

030. In this document we will focus on the model for design rules, and the patterns for setting up the SIOP and SIP:s between federations, this in order to be able to exchange information services between parties.

031. Design rules patterns and knowledge for supporting NATO Nations in designing NNEC compliant components and services can also be retrieved from different Nations repositories as reference architectures, Sweden Design rules (releasable to NATO) will be included as one of the Partner nations reference architecture as recommended and proven patterns in order to achieve NNEC interoperability.

1.7.2. Solution

1.7.2.1. Design rules in the NNEC context

032. Design rules are about reusing knowledge of proven solutions. In the context of NNEC we are especially interested in reuse of solutions that provide typical NNEC characteristics. In addition to this, the use of design rules aim at making the development of NNEC more cost-effective and improve the quality in the resulting products.

033. As mentioned before, a design rule is in the most general description a three-part rule, which expresses a relation between a certain context, a problem or an opportunity and a solution.

034. Different design rules may be in conflict with each other, e.g. in that the solution of one design rule can be incompatible with the solution of the other.

035. Moreover, design rules can be singular or aggregates meaning that it either is an atomic rule or an aggregate of rules that together constitute the rule. The aggregate may include rules on

how to combine the possibly conflicting aggregated rules in order to generate a rule according to the current priorities.

036. Design rules may be implemented for solutions on different levels. There may be design rules for specific technical design problems or rules, how to handle a major business opportunities. It is however anticipated that the majority of design rules valid for an NNEC-system will be focused on the higher levels.

037. Design rules can be used in order to meet functional as well as non-functional needs of the system of interest. It should be clear from all design rules which problem or opportunity it is supposed to solve.

1.7.2.2. General guidance for using design rules

038. The prime prerequisites for implementing a design rule are:

- The use of the design rule shall make the resulting design "NNEC-compliant", i.e. the design rules shall provide essential NNEC-characteristics such as flexibility, interoperability, security and usability
- A design rule shall provide a solution to frequently shown problems, to enable reuse of solutions or implementations and thus get a more cost-effective solution.
- A design rule shall provide a solution to difficult problems, or explore an opportunity, i.e. be a part of the corporate or federated memory
- A design rule shall improve the quality of the resulting product relative a product solution not using the design rule.

039. At least one of the mentioned prerequisites should be fulfilled. There may of course be other valid prerequisites, which will be assessed and used to initiate the design of a design rule.

040. Design rules shall consist of either atomic rules or aggregates of rules that together shall constitute the rule. The aggregate may include rules on how to combine the possibly conflicting rules in order to generate a rule according to the priorities.

041. An atomic design rule must not contain solutions for more than one subject area, e.g. mixing of business and technical subjects shall be avoided. Detailed technical rules shall in the same way be separated from rules of information or logical nature.

042. Design rules shall where applicable be based on concepts and rules in an extended NATO Architecture Framework.

043. A design rule shall not be of too low granularity or too trivial in order to avoid an explosion in the number produced of design rules. To achieve the approved mandatory validity, a design rule shall specify the way to solve the problem it is intended for. Rules that can be expressed in single sentences are collected in general sections in the design rule solution part.

044. Great efforts shall be made to ensure that the design rule is maintainable. This is primarily achieved by limiting the problem area that the design rule is intended for. More complex problems or opportunities shall be supported by aggregates of rules.

1.7.2.3. Design rule model

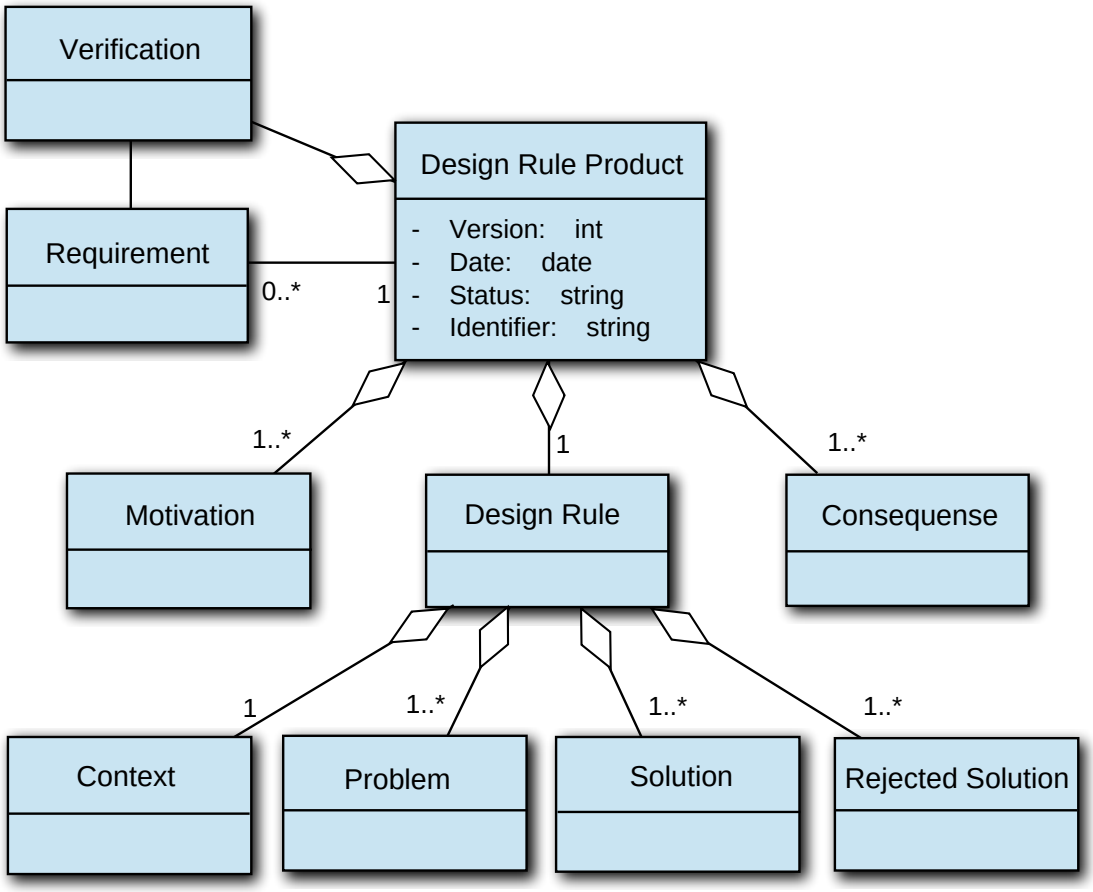

Figure 1.1. Design rule model

045. The design rule product consists of:

- The basic design rule which, as already described, is a three part rule consisting of context, problem and solution. This shall also be complemented with one or more rejected solutions, i.e. solutions which shall not be used.

- An analysis and motivation why the solution fits the problem in the given context. This needs to be linked to direct business benefits such as cost savings or increased efficacy in operations.

- A description of the consequences from the proposed solution which is used to create an understanding at what cost the solution comes. This could include financial impacts, but also how people, processes or technology needs to be adjusted in order to achieve the solution. When describing the consequences from a design rule solution the impact on (at least) the following areas should always be considered:
  - Security
  - Interoperability
  - Cost
  - Usability
  - Flexibility and
  - Procedures
- Verification information which explains how the application of the rule can be verified.

046. A template for design rules, including guidelines, is defined in a separate document.

047. A design rule product is like Standards in the NISP related to near, mid and far term. A design rule can also exist in different versions with different status. The status of the design rule indicates which state of development the design rule is in.

- Candidates
- Approved
- Disposed

048. The solution described in a design rule may refer to other design rules to form an aggregate design rule. This may be the case for instance in a design rule describing a configuration to use in a specific context or for a specific type of system. If so, the validity of the referenced design rule within the current context shall be stated.

049. Each design rule is configured in one, and only one, Design Rule Package.

050. The status of a design rule indicates in which state of development it is.

051. Validity of a design rule is only used when referring as e.g. to form aggregates. The validity labels that can be used are defined in the table below.

Validity	**Description**
Mandatory	The rule shall be treated as a norm and is mandatory to use.
Optional	The rule gives good design principles and is recommended for use.

Validity	Description
Candidate	The rule is planned for future use in this context. The design rule exist but is not appropriate to use due to reasons like cost, compatibility etc.

Table 1.1. Rule validities

052. The lifecycle for a design rule must be coordinated with profiles and standards in the manner, following the NOSWG NISP model

1.7.2.4. Packaging of Rules (Rule Package)

053. Design rules are configured in packages named DRP, Design Rule Package. A DRP may also configure other DRPs, thus creating a hierarchy of packages. A design rule or DRP belongs to one, and only one, DRP.

054. DRPs are defined so that each DRP-structure covers rules that are specific to one particular domain defined for a specific subject area of norms.

055. Dependencies between DRPs shall be defined, and the dependencies shall be minimized. Circular dependencies must not exist. The visibility of design rules configured by a DRP may in addition be limited to the DRP only; default is however that only the DRP exposes the external visibility for a design rule.

056. No design rule shall be part of more than one DRP, if necessary cross-references between DRPs according to the rules for dependencies between DRPs shall be used. Common design rules must for this reason be allocated to higher levels in a DRP hierarchy.

1.7.3. Consequences

057. If the design rule concept is going to be successfully implemented, it is important to understand how they impact the other frameworks and processes used in design. These frameworks and processes also have to be adjusted so it becomes clear as to what is documented where and when.

1.7.3.1. Standards with the use of design rules

058. Standards is often about WHAT but not always about HOW. A vast number of standards are applicable for NNEC, what are applied where, how and together with what, does not always mean that complex system will work. In order to support profiling development when using NISP, Designrules is adopted by NATO as a complementary set of tools for :

- Helping to choose the right standard
- How to apply the standard on a specific problem
- Understanding the relations between different standards

- Applicability in different domains
- Helping with best practice and good patters in order to speed up the development of a profile.

1.7.3.2. Profiling with the use of NAF and Standards and Designrules in the NISP

059. The relations between the NISP and NAF objects in focus. The following picture shows the relations between the NISP objects Profile, Standards and Designrules. For more information about Profile guidance document.

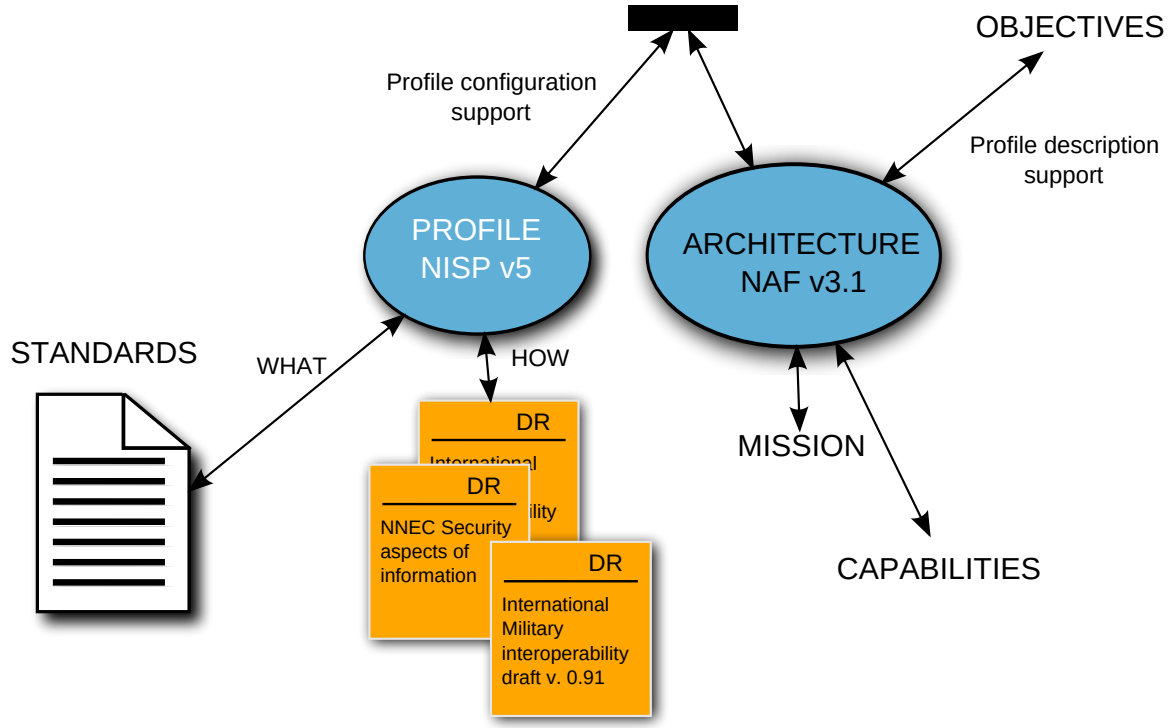

Figure 1.2. Releationship between NISP objects Profiles, standards and Designrules

1.8. REFERENCE ARCHITECTURE - NATIONAL DESIGN RULES

1.8.1. The Swedish Design rules contributions

FMLS Architecture Framework Designrules

LT9O P05-0486 Executive Summary 1.0

Leif Nyberg, JV Network Based Defence, Framework Service Description LT1K P04-0320 Version 7.0 December 2006.

LT1K P05-0074 Overarching Architecture 4.0

LT1K P05-0075 Systems Engineering Vision FMLS 2010 5.0

LT1K P05-0026 - SOA for NBD Principles 3.0

LT1K P05-0507 Architecture Description Framework 2.0

LT1K P06-0025 Integrated Dictionary for FMLS 2010 Technical Systems rev 1.0

FMLS Generic Designrules

LT1K P04-0438 Definition of service Service Registry 3.0

LT1K P05-0235 Definition of service User Registry 2.0

LT1K P05-0446 NERE metadata specs for tech and softw syst 2.0

LT1K P06-0036 SD Provide Report 2.0

LT1K P06-0039 SD Access COP Information 2.0

LT1K P06-0061 Definition of Service SW and Data Distribution 1.0

LT1K P06-0064 Definition of Service Configuration 1.0

LT1K P06-0102 Definition of Service GetRevocation 1.0

LT1K P06-0269 Definition of Service TimeStamp 1.0

LT1K P06-0272 Definition of Service ComBroker 1.0

LT1K P06-0298 D3C 1.0

LT1K P05-0034 Infrastructure Overview 3.0

LT1K P05-0236 Definition of service Organization Registry 2.0

LT1K P05-0557 Design Target Architecture NERE 2.0

LT1K P06-0037 SD Process intelligence 2.0

LT1K P06-0059 Definition of Service Policy 1.0

LT1K P06-0062 Definition of Service Action 1.0

LT1K P06-0091 COPS Information model 1.0

LT1K P06-0134 Definition of Service DNS 1.0

LT1K P06-0270 Definition of Service AccessControl 1.0

LT1K P06-0274 Definition of API data validation 1.0

LT1K P05-0035 Communication Infrastructure Overview 4.0

LT1K P05-0443 NCES Reference Architecture 2.0

LT1K P06-0035 SD Provide Streaming Data 2.0

LT1K P06-0038 SD Support COPS 2.0

LT1K P06-0060 Definition of Service Log 1.0

LT1K P06-0063 Definition of Service Monitoring 1.0

LT1K P06-0095 NCES Management Information and Data models 1.0

LT1K P06-0145 Design Overview 1.0

LT1K P06-0271 Definition of Service NereRegistryAdmin 1.0

LT1K P06-0279 Definition of Service Network Time synchronization 1.0

FMLS Technical Designrules

LT1K P05-0217 - DR Data Incest Prevention 2.0

LT1K P06-0049 DR Risk management 2.0

LT1K P06-0106 Design Rule Mobility 2.0

LT1K P06-0350 DRP Flexibility 1.0

LT1K P05-0547 - DRP Common Operational Picture 2.0

LT1K P06-0050 DR Flexibility 2.0

LT1K P06-0108 DR security aspects of information 1.0

LT1K P06-0351 DRP Interoperability 1.0

LT1K P06-0008 Design Rule Legacy Integration 1.0

LT1K P06-0051 DR Interoperability 2.0

LT1K P06-0321 DR Scalability 1.0

LT1K P06-0352 DRP Security 1.0

1.8.2. Nation x ...

2. INTERNATIONAL MILITARY INTEROPERABILITY FOR INFORMATION EXCHANGE IN THE NNEC CONTEXT

Summary

060. This design rule describes how military organisations can develop and implement the ability to exchange information and services with military organizations from other nations to become interoperable. It touches on, but does not fully address the problems related to organizational structures and behaviour when multiple organisations collaborate in a federative manor in a mission.

2.1. GENERAL

2.1.1. Unique Identity

061. [An identifier that uniquely identifies the design rule. (Product ID)]

2.1.2. Target Group

062. This design rule targets any military organization that plan or foresee that it will participate in a mission where exchange of information and services with other military organizations is vital.

063. Within these organizations, the intended users are requirement analysts, architects and high-level designers of NNEC compliant systems.

064. This document defines patterns for enabling information exchange between parties in federations, and is to be used by architects designing SIOPs and SIPs according to NISP and the NATO C3 System Architecture Framework [6].

2.1.3. Definitions and abbreviations

CIA	Confidentiality, Integrity and Availability. Aspects which are to be considered when performing security analysis.
COI	Community Of Interest.
Design rule	A standardized, reusable solution to a design problem in a specific context within a problem space that provides value to the user.
ESB	Enterprise Service Bus. An ESB refers to a software architecture construct, implemented by technologies found in a category of middleware infrastructure products usually based on Web services standards that provides foundational services for more complex service-oriented architectures.
IEAT	A concept for Information Exchange Architecture and Technology developed within the frame of Multinational Experiment 5 with Sweden as lead nation.

IEG	Information Exchange Gateway. A technical system which is used to protect information assets. IEG are described in the IEG concept [10].
IEM	An Information Exchange Model (IEM) is a specification of the information which is exchanged between operational nodes. IEMs are used when deciding which information objects are to be exchanged in service interactions.
IER	Information Exchange Requirement, a specification of the required information exchanged between operational nodes which are described in an architecture.
IES	Information Exchange Service, a part of an IEG.
Information Zone	Information Zones is a concept identified and defined [11] to achieve confidentiality with high assurance, for a gathering of information within a defined perimeter, and interactions to its surrounding with a number of services and nodes inside the zone.
IPS	Information Protection Service, a part of an IEG.
NAF	NATO Architectural Framework.
NEC	Network Enabled Capabilities.
NNEC	NATO Network Enabled Capabilities.
NISP	NATO Interoperability Standards and Profiles [8].
NPS	Node Protection Service, a part of an IEG.
Operation	An operation where actors from multiple national system is tasked in a federation of system.
Service	In this context a technical mechanism which allows access to one or more capabilities in order to enable service interaction.
SIOP	Service Interoperability Point. A reference point within an architecture where one or more service interfaces are physically or logically instantiated to allow systems delivering the same service using different protocols to interoperate [6].
SIP	Service Interoperability Profile. A set of attributes that specifies the characteristics of a service interface between interoperable systems in the Networking and Information Infrastructure. A SIP is identified at a SIOP in an architecture system view [6].
SOA	Service Oriented Architecture. An architectural style which aims at a loose coupling of services with operating systems, programming languages and other technologies which underlie applications.

Bibliography

Steering documents

[1] Design Rule Framework, See NATO NISP DR guidance document

References

[2] DR Interoperability Sweden proposal, P06-0051 rev 3.0

[3] IEAT Concept, MNE-5 initiative

[4] Design Rule Flexibility, Sweden P06-0050 (NATO doc ?)

[5] Design Rule Security aspects of information, Sweden P06-0108 (NATO doc ?)

[6] NATO C3 System Architecture Framework, EAPC(AC/322)D(2006)0002-REV1

[7] Federated Governance of Information Sharing Within the Extended Enterprise, AFEI Information Sharing Working Group, Nov 17 2007

[8] NISP Volume 1, Version 3

[9] NATO Architecture Framework (NAF), Version 3. AC/322-D(2007)0048

[10] Guidance Document on the Implementation of Gateways for Information Exchange between NATO and External CIS Communities, AC/322(SC/4)N(2007)0007

[11] Swedish FMLS Security Architecture Overview, http://www.fmv.se/upload/Bilder%20och%20dokument/Vad%20gor%20FMV/Uppdrag/LedsystT/Overgripande%20FMLS-dokument/Generiska%20designdokument/LT1K%20P04-0385%20Security%20Architecture%20Overview%205.0.pdf , 33442/2006 Version 5.0, May 4 2007

[12] NISP Volume 3, Version 3

[13] TACOMS: TACOMS Post 2000 Profile, STANAG 4637

2.2. DESIGN RULE

065. This design rule is developed for use in NATO Interoperability Standards & Profiles (NISP) version 4. It is based on experiences from the Swedish Network Based Defence initiative where it extends the design rule for Interoperability [2] and the IEAT concept developed within the frame of Multinational Experiment 5[3]. The design rule also considers the NATO Information Exchange Gateway (IEG) concept[10].

066. The design rule is applicable for collaborative federations in the coming 2-6 years which means that it covers both existing systems which won't be replaced as well as new systems which are developed and implemented during this time period.

067. The technical scope for the design rule is the highlighted areas of Figure 2.1. The design rule does not describe how to achieve interoperability on the Transport/Network level. Furthermore, it does not cover interoperability on the Community of Interest level. However, when

design rules for these levels are created, this design rule will be used as the basis for enabling information exchange via services.

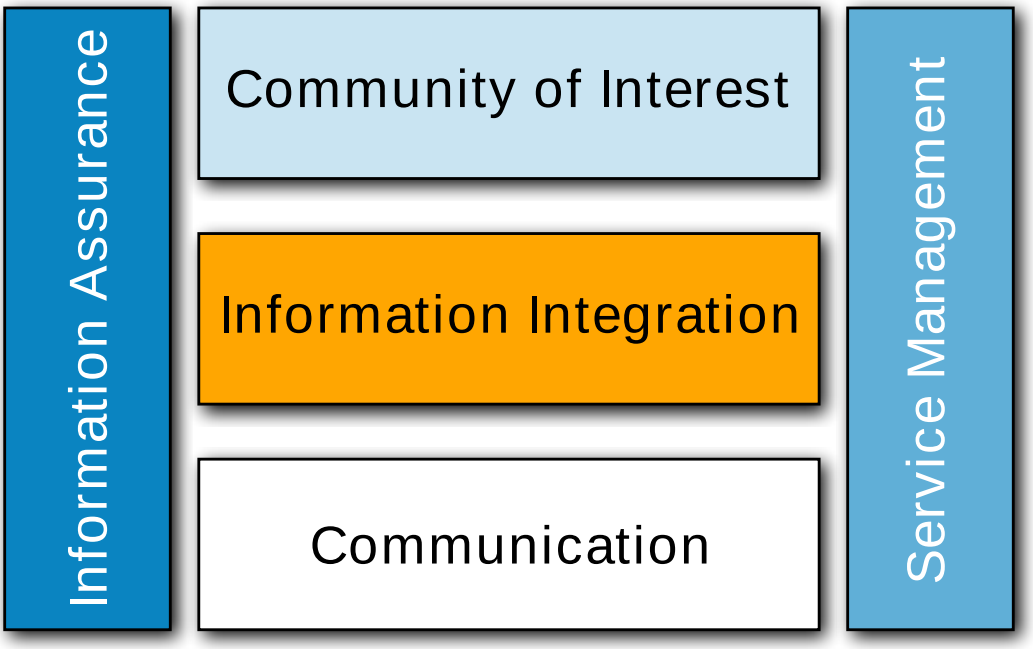

Figure 2.1. Simplified NNEC Technical Services framework with design rule scope

2.2.1. Context

2.2.1.1. Introduction

068. The design rule should be used when there is a need for several different military actors to cooperate in a federative manor in order to solve a common mission. The key capabilities that this design rule will help enable are:

- Collaborative planning between multiple actors in a federation
- Collaborative synchronization of execution between multiple actors in a federation
- Collaborative assessment between multiple actors in a federation

069. The design rule does not address the operational activities needed to achieve the above capabilities, nor does it address the Community Of Interest (COI) technical services which supports these activities. Instead the design rule describes a set of principles, technologies and activities needed to create a technical platform which enables information exchange between the actors and can act as a foundation for the COI specific technical services when these are to be developed and deployed.

070. Since the design rule captures knowledge from previous experiences in this area it can save time and money for the involved actors. If the design rule is applied when defining the profile for such a mission, less time will be spent on getting to agreement on which services and underpinning technologies shall be used in the mission.

071. Many of the activities and technologies described in this design rule can also be applied when exchanging information and services with other actors than military organizations. However, there are specific aspects of collaborating with this type of organizations which are not covered by this design rule.

072. A suitable definition of interoperability in this design rule context (i.e. technical context) is: The ability of technical systems and/or organizations using technical systems to operate together by making (necessary) data & information and/or services produced by one system or organization available to the others, in an agreed format.

2.2.1.2. The International Military Federation

073. There are many challenges that have to be overcome in order to make collaborative work and knowledge sharing among the actors in an operation successful. In Section 2.2.3 of this design rule mainly addresses the technical aspects of the establishment of federation in which collaborating actors can exchange information. However, organizational, process and legislation aspects must be covered to some extent since all of these needs to be harmonized in order to make the collaboration effective. Therefore, a number of non-technical issues are described in Section 2.2.2.

074. The federation, depicted in Figure 2.2, is where the collaborating actors provide services which the other actors can consume. To create a federation, the actors need to create a federation agreement which defines the rules of the federation, such as which data formats, information classifications should be used. Rules regarding information ownership and service levels (including quality of service) are also included in the federation agreement.

075. Collaboration in multilateral operations has previously been based on bi-lateral agreements between all participants, but in order to achieve the speed and flexibility needed today, there is a need to establish a baseline federation agreement which can be used as a starting point when creating new missions.

076. Actors which participate in the federation connect networks and systems within their responsibility (i.e. domain) to other actors in order to be able to exchange information. To protect the internal information and control which information is being exchanged one or more Information Exchange Gateways (IEG) are stood up between the federation and the actors' network. In the IEG, one or more service interfaces are physically instantiated. This is referred to as a Service Interoperability Point (SIOP) according to the NATO C3 System Architecture Framework [6].

077. Within an actor's domain there can be one or more networks where information is stored. The decision which internal networks shall be connected is taken by each actor (Federation

member) independently of the other actors. In Figure 2.2 two example networks are depicted, one federation network which holds information only relevant to the federation and one which is the actors' internal network. In this case, the IEG handles information exchange between these two networks as well as information exchange with other actors IEGs.

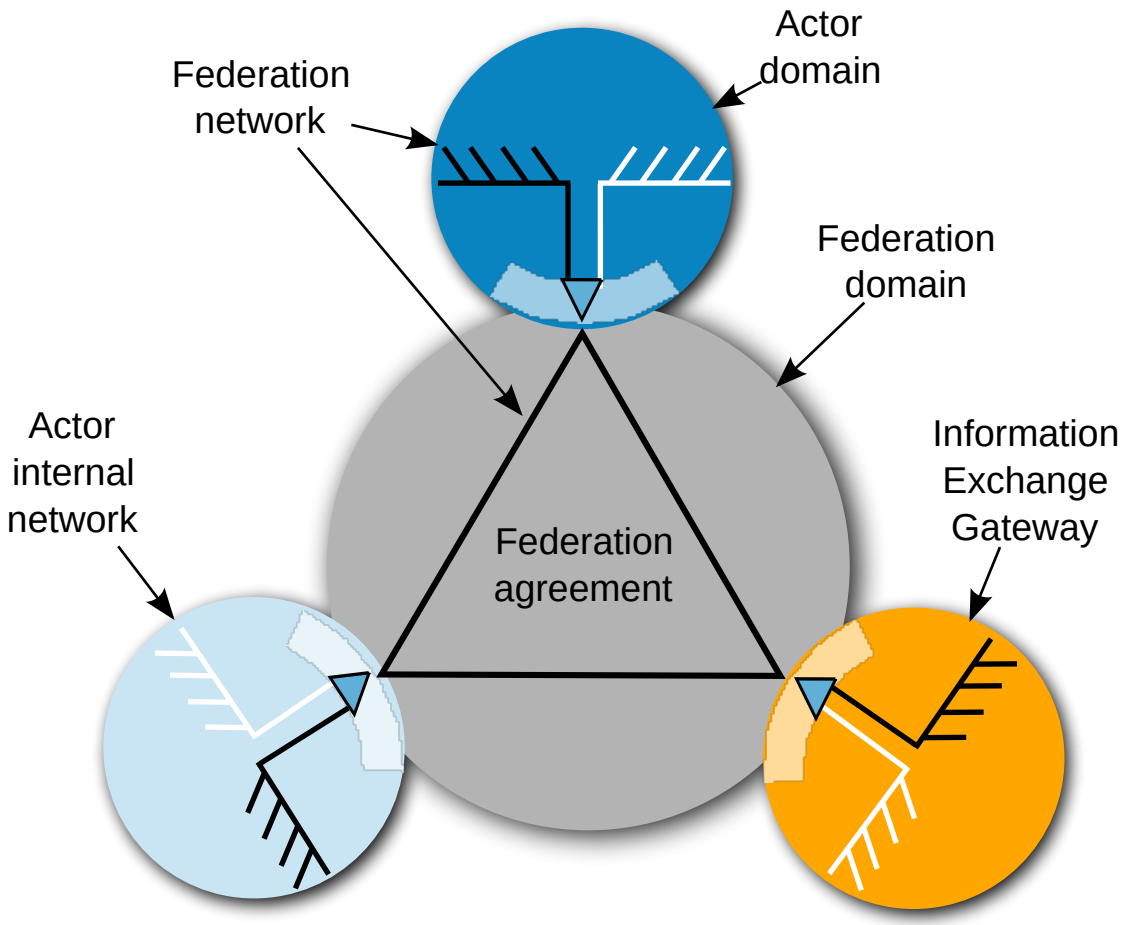

Figure 2.2. Federation Overview

078. The remainder of the design rule describes the challenges the actors face and how they can cooperate in order to create a federation to exchange information in a secure manor.

2.2.1.3. Related design rule areas

079. Interoperability is closely linked to the following other design rule areas:

080. **Flexibility**: The requirements on interoperability will change over time. Also, in some situations, very limited time will be available for making the necessary modifications of the system in order to fulfil the new requirements. This means that the organization, security and technical systems need to be very flexible with respect to configuration and modifiability in

order to be able to adapt to changing and extended interoperability requirements. For more information, refer to [4].

081. **Information security**: With interoperability follows information security risks that must be handled. The connection of external systems must be done in such a way that the information security of each nation or organisation is not compromised. However information security mechanisms cannot be allowed to be static. In each specific case the need to protect information must be balanced against the possible consequences from not sharing the information. The three aspects of security; confidentiality integrity and availability, must all be considered.

2.2.2. Problem

082. There are several challenges to the effort of creating a federation for collaboration between military partners, both related to technology, but also related to how organizations, humans and legislation systems work.

083. This chapter summarizes the basic requirements for the federation and identifies the challenges which must be overcome in order to establish the federation. The issues identified for these challenges are given an answer to in Section 2.2.3.

Basic requirements for information exchange

084. The intent of this section is to identify a few of the most elementary (information exchange) requirements which are set on all international military federations. This is not a complete list, but these requirements acts as a driver for identifying the basic set of technologies needed in a federation.

[IER 1] People from the different organisational actors SHALL be able to communicate with each other using voice or text communication.

[IER 2] It SHALL be possible to discover and retrieve information (i.e. search) provided to the federation by different actors.

Challenges based on international agreements and regulations

085. Information and services exchange between nations and organisations (e.g. unclassified, restricted, secret and top secret classification) is based on government agreement between nations and organisations. Qualified information and services exchange can only take place if such agreement exists. To achieve this agreement is a lengthy process that often takes many months to finalize. It has also been proven complicated to negotiate and sign such an agreement between more than two nations and organisations at a time (multilateral). Nations are willing to share more information and services with some parties and less with others. This creates complicated situations during multilateral operations.

[Issue_1] How can a common, agreed description for analyzing and describing international military interoperability be created?

Challenges based on national law, national integrity and regulations

086. Differing laws, rules and regulations together with different cultures regarding information sharing are likely to impact willingness to share information and slow down process of getting agreements on what to share.

087. Parties participating in a multilateral operation are likely to have different requirements and priorities which will imply different scope and granularity of information exchange for each party. The parties will be required to protect their national integrity while sharing information with the other parties. By this, it is likely that the parties wish to get access to more information and services than they are willing to provide themselves. It is also so that the parties will need to limit the possibilities for others to control how and what information is provided.

[Issue_2] How can the impact of national laws and regulations in coming to agreement of what information to share be minimized in order to support the requirements of flexibility and ability to change?

[Issue_3] How can parties participating in a multilateral operation protect their national integrity by using mechanisms to protect internal information and be able to control what information is released to others?

[Issue_4] How can the parties in a multilateral operation jointly come to agreement of what information shall be exchanged, how it shall be exchanged and how it shall be handled by receiving parties?

Challenges based on interpretation of information content

088. Semantic differences, i.e. differences in languages and the meaning of words and expressions, are likely to be an issue when exchanging information. If the collaborating parties cannot understand the information being communicated, the information will not be of any use and the trust of accessible information will be challenged. There is a need for the parties to eventually meet in a combined opinion, a common and agreed set of descriptions in order to reach wanted effects.

089. In order to solve the semantic challenge there is a need to understand the content of information and services exchanged between different systems/actors to be able to come to an agreement of the meaning of the information. However, the increasing requirements of the ability to rapidly change directions of the flow of information, as well as the actual content, means that the work with defining models and requirements for information exchange must be done continuously and during the whole lifecycle of an operation.

[Issue_5] How can the parties in a multilateral operation agree on what information shall be exchanged?

[Issue_6] How can differences in semantics and information models be handled in order to minimize the risk of the parties not understanding each other?

[Issue_7] How can it be ensured that the work with understanding others semantics and information models is done in all stages of the development lifecycle?

Challenges based on technical issues

090. Architecture and technical implementations of information systems will be different in most of the cases. The complete technical system will probably not be homogenous, rather a federation of heterogeneous systems and therefore hard to govern and manage.

091. Agreeing on standards, formats and mechanisms for information exchange is a critical success factor, however the sovereignty of the parties will increase the complexity of this task since there is no governing organ that can make the decisions.

092. A common understanding and agreement on the architecture and design for the federation is vital in order to succeed with agreeing on how information shall be exchanged. A major challenge in this perspective is that the maturity of using architecture and design as governing tools is likely to vary greatly among collaborating parties, thus slowing down the agreement process.

093. Since each actor has huge amounts of data of various kinds within their internal networks there is a need to have the means to organize and prioritize what to share. Also, when information has been shared within the federation, there must be mechanisms to be able to verify the authenticity, track usage of and prevent that the information is used by actors which are not meant to use it.

[Issue_8] Which architecture can enable governance and structure to mechanisms for information exchange between heterogeneous systems?

[Issue_9] Which standards, formats and mechanisms for information exchange should be used?

[Issue_10] What does a common architecture description framework for multilateral operations contain?

[Issue_11] What mechanisms shall be used in order to control what information to make available to partners in an international military operation?

[Issue_12] What mechanisms can be used to maintain information security and system safety, e.g. weapon safety, when external systems are connected to a nation's internal network?

Challenges based on culture, lack of trust and organizational issues

094. Even if we have solved "challenges based on international agreements and regulations" we will still most likely hesitate to share information since the organizational culture does not foster incentives to share information[7]. This is understandable, but not very efficient from an operational perspective. We have to overcome these limitations and see the goal of the operations as more important than the individual organizations ego.

095. Today's military organizations are experienced and usually organized around various stovepipe principles. This is a convenient, straight forward way of defining requirements, responsibilities and timetables for implementing new and enhanced systems. Operations were information is expected to be exchanged between both organizations and technical systems will set new requirements on the procurement process, working methods and the organizations working those issues.

[Issue_13] Data are not generally created to support enterprise needs. There are typically technical and political boundaries that inhibit this. To "line" applications development organizations, enterprise-level requirements for data are typically viewed as "external", as their direct customers, and typically the sponsor of the application, is not rewarded for serving the greater good, but for locally optimizing the performance of their organization[7].

2.2.3. Solution

2.2.3.1. Architecture for interoperability

096. The most important instrument in resolving the issue of creating a description for analyzing and describing international military interoperability as described in [Issue_1] is to create an architecture. This design rule outlines an architecture which provides the means to create a foundation for the federation in which information exchange among parties can take place.

097. The architecture is described by:

- Governing aspects (design principles and rules) used to explain and develop architectural principles and structures in important areas of the architecture.
- Common terminology & definitions.
- Structure. How systems, aspects and terminology/definitions are organized and grouped.
- Systems in terms of mission and/or technical systems.
- Services which describe how systems interact.

098. It is absolutely vital that the architecture addresses both operational and technical aspects so that there is a clear description of what purpose the technical implementation has [Principle_4].

2.2.3.1.1. Service Oriented Architecture

099. The Architecture outlined in this Design rule is Service Oriented [Principle_5]. The aim of this is to achieve a loose coupling of services with underlying systems, whether it is mission or technical systems. So, instead of describing interaction directly between systems, the systems use services to interact with each other. By specifying a contract for information exchange, a service definition [Principle_6], the inside of a system can be replaced or modified without hav-

ing to change other systems which interacts with it. Thereby the issue of enabling information exchange between heterogeneous systems [Issue_8] is resolved.

100. Services used or provided by technical systems should as far as possible be expressed in a common way and contain formal descriptions suitable for IT processing.

101. The Service description shall contain:

- The allowed service protocols (process) to be used for information exchange.
- The interfaces (or message types) that are used to exchange information between a service consumer and a service producer.
- The definition of the data types that are used in the interfaces (messages) and therefore are in the information exchange model.
- The properties that consumers can use to distinguish between different implementations of a service.

102. To enable systems to find and connect to each other, information about services shall be published and accessible for the collaborating parties' IT systems.

2.2.3.1.2. Architecture description framework

103. In order for all parties to obtain a common "language" on how to describe their systems and the services they bring to the federation this design rule also covers an architecture description framework. The architecture description framework does not describe the architecture itself, but rather guides how the architecture shall be structured and what it should describe.

104. The current valid description framework within NATO is the NATO Architectural Framework (NAF) version 3[9] which provide the rules, guidance, and product descriptions for developing, presenting and communicating architectures which includes both operational aspects as well as technical aspects [Principle_4].

105. In the Framework, there are seven major perspectives (i.e., views) that logically combine to describe the architecture of an enterprise. These are the NATO All View (NAV), NATO Capability View (NCV), NATO Programme View (NPV), NATO Operational View (NOV), NATO Systems View (NSV), NATO Service-Oriented View (NSOV) and NATO Technical View (NTV). Each of the seven views depicts certain architecture attributes. Some attributes bridge several views and provide integrity, coherence, and consistency to architecture descriptions.

106. To support the creation of views and make sure they are consistent, NAF v3 defines a metamodel. The NATO Architecture Framework Metamodel (NMM) defines the relationships between the different components of the framework. It defines the architectural objects and components that are permitted in NAF v3 views and their relationships with each other.

107. There are certain views which are more important when designing architectures for multinational operations where interoperability is in focus [Issue_10]:

108. **NATO All-Views (NAV)** which capture aspects which overarch all other views. These views set the scope and context of the architecture, such as goals and vision, scenario and environmental conditions as well as time.

109. **NATO Capability View (NCV)** which explain what capabilities are needed in order to fulfil the strategic intent for the mission. Specifically, capabilities related to interaction between actors are important to identify in these views. If produced correctly, these views can already say a lot of which services are needed to fulfil the business needs. In particular, the NCV-2, Capability Taxonomy and NCV-7, Capability to Services Mapping views are important.

110. **NATO Operational View (NOV)** which is a description of the tasks and activities, operational elements, and information exchanges required to accomplish NATO missions. To design for interoperability all of these views do not have to be complete, but it is important to know which operational nodes exist and how they interact (NOV-2). Also, the information model defined in the NOV-7 view is important, especially for such information for which there are no or unclear standards to rely on. When going into more details of the architecture, the requirements on information exchange (NOV-3) are necessary to understand.

111. Currently, the operational views in NAF does not fully support modelling of services. The authors of this design rule recommends that future versions of NAF are complemented with the capabilities of using services to describe interaction between operational nodes instead of needlines.

112. **NATO Service-Oriented View (NSOV)** focuses strictly on identifying and describing services. The view also supports the description of service taxonomies, service orchestrations and a mapping of services to operational activities. The service description (NSOV-2) is a key component of a Service Oriented Architecture [Principle_6]. It is used to detach the functionality provided by a system (or services provided by an organizational unit) from the actual system. A service description includes information on how to interact with the service, what requirements a system must fulfil if it implements the service and what information model the services uses. Within NSOV-2 a SIOP can be depicted as a higher-level service interface. The detailed technical specification of a SIOP is contained within a Service Interoperability Profile (SIP). SIPs are addressed in NTV-1 Technical Standards Profile.

113. In the **NATO Systems View (NSV)**, the NSV-1 view is the most important since it describes how the different systems interact to fulfil the operational needs. The system descriptions should be kept on a black-box level, i.e. it is not relevant to describe the internals of the systems.

2.2.3.2. Key Principles

Sovereignty of collaborating parties

114. The sovereignty of the collaborating parties is fundamental; organizational right to use organic information systems and working methodology with various support tools shall in all

situations be respected. The decision to publish information to the federation is the responsibility, and right, of each actor. Information content and possible restrictions will always be any actor's sovereign decision.

[Principle_1] Each collaborating party decides which information to publish into the federation.

View on information

115. Information shall be regarded as an operations wide asset and not be exclusive to any single operational area or function, with exceptions for agreed confidentiality. Collaborating parties should avoid over-classification of information. Information should be provided as a published service.

[Principle_2] Information published into the arena is available to all parties, if no restrictions have been agreed.

Agreements for Information Exchange

116. Agreements to facilitate Information Exchange shall exist for the operation and between the collaborating parties. The agreements includes which information is required to be exchanged, models for how exchanged information shall be structured, how information can be translated between models and the format of the exchanged information.

[Principle_3] Requirements, models, translations and format for information exchange in the arena are regulated by agreements.

Architecture

117. Establishment of a consistent and understandable architecture should be supported by a common terminology and a common architecture description framework. In order to ensure that the technical architecture fully supports the operational needs, there is a need for a joint architecture.

[Principle_4] The operational and technical aspects of the architecture are described using a common description framework.

118. The architecture of the federation must support exchange of information between many heterogeneous systems in order to fit all actors' needs. A Service Oriented Architecture (SOA) achieves this by separating information exchange capabilities from business logic and system specific implementations.

[Principle_5] The technical architecture for information exchange follows the tenets of the Service Oriented Architecture concept.

119. OASIS (organization) defines Service as "a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description."

[Principle_6] Technical services for information exchange are specified in a service description.

Technology

120. Open and accepted international standards, both civilian and military should be used. Bespoke and proprietary standards shall only be considered when it delivers significant higher value.

[Principle_7] Technical services for information exchange uses open standards whenever possible.

Security

121. To achieve information exchange in a secure way using services, a set of principles which guides the use of security functions is needed:

[Principle_8] Service consumers and service providers use a common methods for authentication and authorization of users and services.

[Principle_9] There is a common method to obtain integrity by which a service consumer can check that the data sent from another part is not changed by a third part.

[Principle_10] There is a common method to guarantee the confidentiality of the information exchanged. This means that it is possible to prevent outsiders from getting access to the information that is exchanged.

122. It is important to remember that these principles only apply between the borders of the actors in the federation, not end-to-end between users. The reason for this is that it is very hard and cost driving to govern how security mechanisms shall be implemented within an actor.

2.2.3.3. The information aspect

123. In order to meet operational needs for information exchange and to build a federation, supported by technical systems serving as operational nodes, a number of areas must be addressed:

- Information Exchange Requirement specifications
- Information Exchange Models within collaboration areas and their relation to international standards, domain Community Of Interest (COI) models, semantic structures etc
- Translation specifications and translation mechanisms
- Specification of information exchange mechanisms in the federation e.g. common data management services, mediation services and bridges to external systems

124. Documenting the above according to [Principle_3] address issues [Issue_1], [Issue_2], [Issue_4], [Issue_5], [Issue_6] and [Issue_9] by creating agreements of what information is to be exchanged, how to interpret the information and which mechanisms are utilised to enable the information exchange.

125. This chapter covers the definition aspect of information, technologies which implement these definitions, like for example mediation, are covered in Section 2.2.3.

2.2.3.3.1. Information Exchange Requirements

126. An Information Exchange Requirement (IER) is a specification of the required information exchanged between operational nodes. IERs are identified in the business modelling process and specify the elements of the user information used in support of a particular activity. The specification is done according to the NOV-3 view of NAF[9].

2.2.3.3.2. Information Exchange Models

127. An Information Exchange Model (IEM) is a specification of the information which are exchanged between operational nodes. IEMs are used when deciding which information objects are to be exchanged in service interactions. The specification is done according to the NOV-7 view of NAF[9].

128. An IEM is constructed top-down based on model elements from other existing Information Models e.g. standards as well as bottom-up based on information requirements specifications from Operational Concepts and Requirements Implications (OCRI)[8].

129. When designing Information Exchange Models several different approaches exist:

- Model based, e.g. JC3IEDM, ISO19100 series
- Ontology based e.g. Semantic web
- Message based e.g. ADatP-3

130. Given the timeframe for this design rule, a model based approach is the best approach considering what the technology can handle and results from ongoing modelling work. The ontology based approach can be adopted at a later stage when the technology and methods are more mature while the message based approach is to be avoided if possible since it cannot handle the complexity of integrated models.

2.2.3.3.3. Translations

131. There may be a large number of translations between two information models. Each translation is based on thorough analysis and is documented in a translation specification together with estimates of information loss.

132. There are different approaches to making translations between the models:

- Manual model mapping, that is when two models are compared and decision are made at element level on how to map and/or translate to the other models. This is often the case when the models to compare are documented according to different standards regarding ontological metadata notation, modelling style etc.

- Rule based model mapping that is when two models are compared and mapped to each other based on formalized rules. Automated translation has the potential to be applied in runtime, thus increasing flexibility in information exchange.

133. Technologies which perform automated translation between information models is not yet available to any greater extent. Therefore, the translation technologies described in Section 2.2.3.5.6 focuses on supporting translation rules which are based on manual model mappings.

2.2.3.3.4. Information Exchange Objects

134. An information object is a set of data elements that are contained and treated as one unit. The content structure may vary in complexity from the simplest form with a number of data elements and an identifier to complex data structures and large quantities of data elements. Examples of information objects are documents, messages and data sets such as geographical data sets.

135. Information objects are created, processed, stored and moved/exchanged via services. An information exchange object is a standardised view, or an excerpt from, an information exchange model which from a technical point of view is suitable to exchange as a coherent set. Thus information exchange objects is a subset of all information objects which are meant to be exchanged via services.

2.2.3.3.5. Services and the information aspect

136. In a Service Oriented Architecture [Principle_5], information objects are created, processed, stored and moved/exchanged via services. Therefore it is important to understand the architectural relationship between services and information. I.e. how are services and information specified in order to enable the implementation of a service oriented architecture.

137. As depicted in Figure 2.3, a service has operations. They are used for specification of how a consumer can interact with the service, for example create, read, update, delete. An operation requires one or more information objects to be exchanged between the consumer and provider, for example a message or a document. These exchange objects are excerpts from an information exchange model.

Figure 2.3. Services and the information aspect

138. Translations are use to describe how information exchange models relate to each other and can also be used by mechanisms to automatically translate exchange objects from different information models. Information exchange requirements are set on service operations and exchange objects, i.e. what functionality shall the service provide and what information shall it handle.

2.2.3.4. The security aspect

139. When determining appropriate security solutions for a federation it is of outmost importance to analyse the information which needs to be assured. This is important in order to avoid a "too secure" solution, thus introducing higher costs and more difficult procedures than needed. The flexibility which is introduced by the NNEC concept requires a constant analysis of the need for information confidentiality, integrity and availability (CIA). Also, time needs to be considered in these analyses, i.e. how long does the information need to be protected.

140. This design rule does not cover how to perform CIA analyses, but it is certain that there is a need to be able to handle different levels of security in the federation. A set of scenarios has been defined in the IEG concept[10] which are used in this design rule to handle difference in security levels.

The Information Exchange Gateway Concept

141. Information Exchange Gateways (IEGs) are used to protect information assets of the participants in the federation. Since each participant provides an IEG to protect their assets there is a need to standardise the services and the architecture of IEGs in order to enable sharing of IEG components between the participants and use of commercially available technology. The NATO IEG concept[10] describes that each IEG has three major services:

142. "The first is the Node Protection Service (NPS). The NPS provides protection to the infrastructure; its purpose is to protect the physical assets of the "node" or nation being protected by the IEG."

143. "The second major component/service is the Information Protection Service (IPS). NATO and each nation are responsible for protecting the flow of information out of its area (node or network). The mechanisms used to protect the information flow must satisfy the organization (nation or NATO) that the IEG is protecting."

144. "The third major component/service is the Information Exchange Service (IES). The IEG must facilitate the flow of information between the protected node/network and the external organizations that are authorized (by the Information Protection Service)."

145. Together these services provide the solution to issues [Issue_3], [Issue_11] and [Issue_12]. More details on the implementation of IEGs can be found in Section 2.2.3.5.7.

Information zones

146. Information Zones is a concept identified and defined to achieve confidentiality with high assurance, for a gathering of information within a defined perimeter, and interactions to its surrounding with a number of services and nodes inside the zone. The concept gives the advantage to separate assurance on security mechanisms to meet external and internal threats.

147. In a federative approach such as the one described in this design rule, each federation participant (actor) is to be considered as (at least) one information zone. The reason for this is that there is a clear responsibility for information and information management within each actor. At the border of the information zones there are Information Exchange Gateways (IEG) which protects the information within the zone and allows controlled sharing of information between information zones. See Figure 2.4.

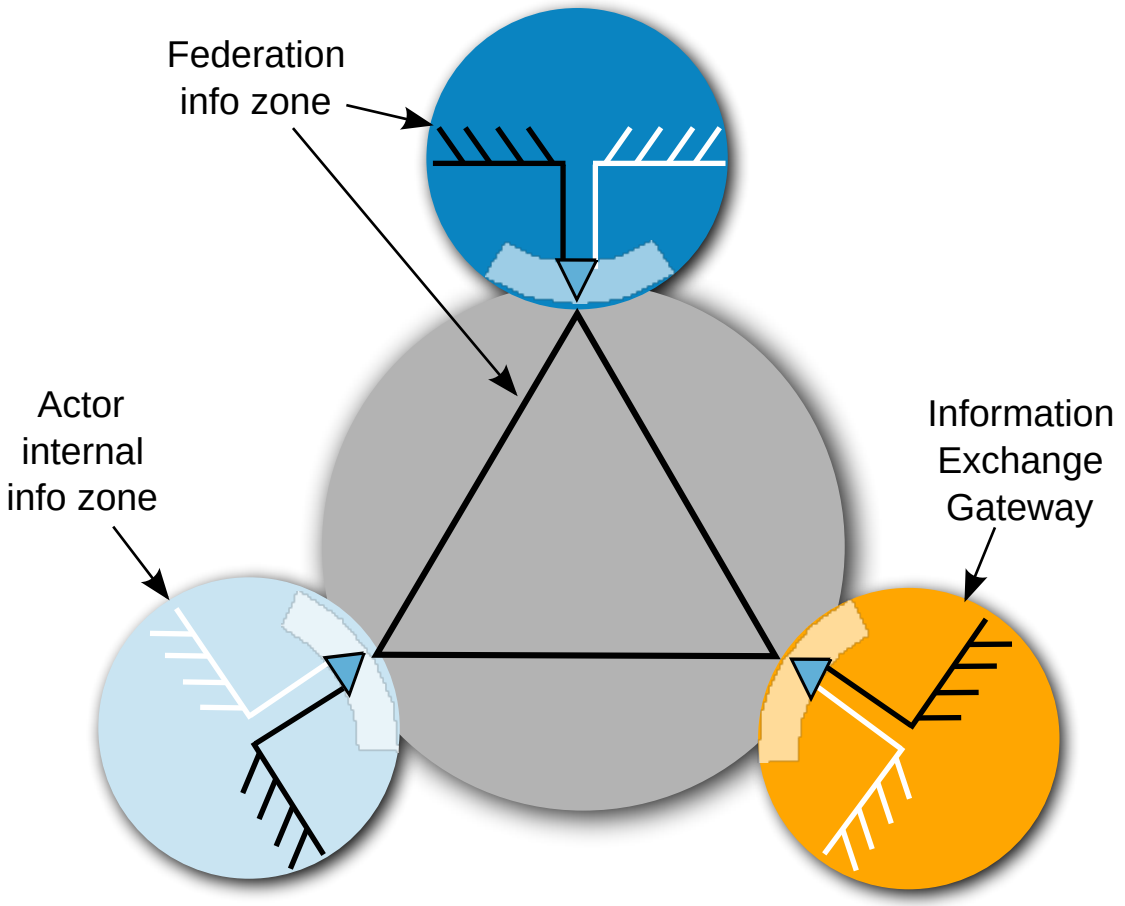

Figure 2.4. Informationzones in the federation

148. The information classification level in each zone will differ and therefore the information assurance level needs to be adjusted accordingly. I.e. the more sensitive information within a zone, the more protection and dissemination control is needed.

149. By basing the security on information zones with boundary protection and controlled information flow and access to the zone, it is made easier to achieve high assurance since only a few mechanisms, i.e. the IEG, needs to be inspected/evaluated to meet the security requirement.

150. In the federation there may be several information zones depending on the classification of exchanged information. However, the number of information zones should be kept to a minimum in order to avoid unnecessary costs and complexity for implementation and maintenance of the federation.

2.2.3.5. Technology and profiles

151. As mentioned in Section 2.2.1.2, there is "a need to establish a baseline federation agreement which can be used as a starting point when creating new missions". The technology de-

scribed in this chapter supports the creation of such an agreement by addressing [Issue_9] > "Which standards, formats and mechanisms for information exchange should be used?"

152. In other terms, the standards, formats and mechanisms defined in this chapter shall serve as the baseline for an international military federation.

153. There are two basic user requirements defined in Section 2.2.2 which acts as drivers for the technology defined in this chapter. These requirements are:

[IER 1] People from the different organisational actors SHALL be able to communicate with each other using voice or text communication.

[IER 2] It SHALL be possible to discover and retrieve information (i.e. search) provided to the federation by different actors.

154. To be able to fulfil these requirements, a set of technical capabilities are needed. First of all, there must be network (IP) connectivity between the actors in the federation; however this is not covered by this design rule. Once network connectivity is established, the technical systems of the actors need to be able to publish and find the services which are to be used. Of course, all communication in the federation network must be secured by relevant security mechanisms.

155. In order to fulfil [IER 1], users first need to be able to find each other and once they have done that they can start collaborating.

156. To fulfil [IER 2] the Information Discovery Services are used to find relevant information. To retrieve the information, Messaging Services can be used. In some cases the information models used by the different actors does not match and then the Translation Services are used to translate the content.

157. Lastly, it is important for the actors in the federation to know the status of the services in the federation, especially if there are mission critical services which are provided by other actors.

158. The following chapters describe the above in more detail giving advice how to implement the technologies needed to provide these services.

2.2.3.5.1. Discovery services

Service Discovery Services

159. The Service registry enables the technical systems to discover each other. The service registry is a vital part needed for enabling the loose coupling between systems since it provides functionality for the systems to find each other , with such registry the relationships between the systems does not need to be hard coded into the systems. This means that it will be easy to add or remove participants and services from the federation.

160. The Service registry SHALL be implemented using UDDI v3 according to NISP[12]. In order to achieve high availability and allow each participant to be able to publish services, the

Service registry shall be implemented using a replication pattern. I.e. the service registry is replicated between all participants in the federation.

161. The Service registry SHALL include the following information (metadata):

Service provider

- Unique id, Name, Description

Service type

- Unique id, Name, Description, Version

Service instance

- Unique id, Name, Description,Service interfaces (bindings e.g. WSDL) and applicable security mechanisms, Endpoint (e.g. URL), Owner - both service provider and human user owning the service, Security Classification - UNCLASS, RESTRICTED etc

Information Discovery Services

162. Each actor in a federation holds information which might be relevant to other actors. Therefore it is of outmost importance that there are mechanisms to discover information across actors. These mechanisms have to include the capability for an actor to decide which information shall be available to others according to [Principle_1] and [Principle_2].

163. There are mainly two ways of making the information discovery happen. One is to copy information between actors and let each actor make the information searchable, but this is not very efficient since it requires a lot of bandwidth and makes it hard to keep track of which information has been copied.

164. The other way of enabling information discovery is to use a federated search pattern where each actor provides a search interface to its information. This is much more efficient from a data distribution point of view, but requires that all actors come to agreement on the search interface. There are initiatives ongoing to standardise the ability to perform federated search, the most prominent one is the OpenSearch initiative[1]. Even though OpenSearch is not a formal standard it is well on its way to be adopted by many of the major tool vendors.

165. In either case, the actors in the federation must implement search engines which can index information (if the have any) and search clients which can access the search engines. A search client is in most cases an ordinary web browser, but can also be a more complex application if there are specific needs.

2.2.3.5.2. Repository Services

Metadata Registry Services

[1] http://www.opensearch.org/

166. A metadata registry is a database which contains information about information which is useful for enabling information discovery. For example, search engines create metadata registries when they index content. But there are also other applications for metadata registries, like when an actor has sensitive information which needs to be able to be discovered. Say that there is a database which contains classified analyses of some sort. The analyses are of very good quality and can be of use to many, but it is impossible to publish them to everyone in the federation. So in order to make other actors aware that the analysis exists, unclassified analysis metadata, like what the analysis looks at and who has done it, can be published in a metadata repository. Now the other actors can discover that there is an analysis and contact the author to get approval for getting the contents.

167. To be able to store the metadata, the NATO Discovery Metadata Specification (NDMS) SHALL be used. This specification is based on the international standard ISO 15836 the Dublin Core (DC) Metadata Element Set.

2.2.3.5.3. Directory Services

Enterprise Directory Services

168. Sharing information about users is key to a federation since it enables people to find each other. The user directory holds information which enables authentication of users by certificates and public keys, authorization of users by roles and discovery of users by contact information which enables collaboration.

169. Each actor in the network shall provide information about the users that represents them. However, it is preferable if the federation has one point of access to all user directories. Therefore, the implementation of user directories in a federation shall follow the federated database pattern. This means that each actor provides their own database, but one actor provides a single entry point to all databases.

170. For the user registry LDAP shall be used according to NISP[12]. Products which can provide the single entry point to multiple LDAP databases are often referred to as Virtual LDAPs.

2.2.3.5.4. Collaboration Services

Audio based conference service

171. For voice communications standards SHALL be applied as according to TACOMS[13]. Streaming voice and video communication cannot be handled by the IEGs, TACOMS describes how to implement this functionality without the use of IEGs.

2.2.3.5.5. Messaging Services

Server-to-server e-mail messaging service

172. E-mail has become one of the most important applications for any business or organization of today. The main challenge for using e-mail in a federation is to be able to control that no classified information is embedded or attached to e-mails going out from an actor and protecting the actors from malicious software, such as viruses. This means that the IEG needs to be able to scan and filter incoming and outgoing messages.

173. Extra care needs to be taken for outgoing information where confidential information can be hidden in document history and inside images. Therefore, only text-based attachments (like OpenDocument Format or Office Open XML, see NISP[12]) without inserted code or images shall be allowed through the IEG.

174. It is also vital to have a manual inspection capability in the IEG to be able to assess the degree of confidentiality of the e-mail messages leaving an actor.

175. As described by NISP[12], SMTP according to RFC 2821 and others SHALL be used for e-mail. To secure communication between SMTP agents, TLS according to RFC 3207, SHOULD be used.

Instant messaging service

176. For instant messaging XMPP (IETF RFC3920:2004 -3923:2004) SHALL be used according to NISP[12]. XMPP is an XML based publish/subscribe protocol which is used by most of the dominant tool vendors. Using XML enables possibility for inspection and control of messages in IEGs which is very important in a federation.

177. There is one important aspect of XMPP which is not covered by the current standard specification; there is no security tagging options available which is needed when messages shall be passed between information zones with different security classifications. So if this is required a custom extension to XMPP needs to be defined.

178. Another thing which must be considered in a federation is routing of messages. Currently there are no XMPP servers which support routing of XMPP messages. This consequence of not being able to route messages is that the IEG has to be implemented as a transparent proxy, i.e. the systems on the outside of the IEG need to know about the systems on the inside. Even though the IEG can be used for inspection and filtering of messages in this case; it is not always a preferred solution from a security perspective. So, if the security requirements say that the IEG needs to act as a non-transparent proxy, the XMPP server needs to be modified to be able to act as an XMPP server and be able to route messages between XMPP domains.

Message passing service

179. In order to achieve an efficient exchange of information between the actors in a federation there is a need to be able to route and distribute messages. This type of capability is often included in the Enterprise Service Bus (ESB) concept.

180. An ESB refers to a software architecture construct, implemented by technologies found in a category of middleware infrastructure products usually based on Web services standards that provides foundational services for more complex service-oriented architectures.

181. An ESB generally provides an abstraction layer on top of an implementation of an Enterprise Messaging System which allows integration architects to exploit the value of messaging without writing code.

182. The ESB shall enable endpoints to interact in their native interaction modes through the bus. It shall support a variety of endpoint protocols and interaction styles. These interaction patterns are the least which shall be supported:

- Request/response: Handles request/response-style interactions between endpoints. The ESB is based on a messaging model, so a request/response interaction is handled by two related one-way message flows -- one for the request and one for the response.

- Request/multi-response: A variant of the above, where more than one response can be sent. Is often referred to as a subscription pattern.

- Event propagation: Events may be anonymously distributed to an ESB-managed list of interested parties. Services may be able to add themselves to the list.

183. When passing messages in the above patterns, the ESB SHALL be able to perform the following:

- Route: Changes the route of a message, selecting among service providers that support the requester's intent. Selection criteria can include message content and context, as well as the targets' capabilities.

- Distribute: Distributes the message to a set of interested parties and is usually driven by the subscribers' interest profiles.

184. The ESB SHALL be able to handle the following formats and protocols:

- SOAP over HTTP for Web Services

- JMS for Java messages

- XMPP for Instant messaging and XML based Publish subscribe messaging

185. When implementing the ESB concept in federations there are some things which must be considered. First, the products which realize the messaging and mediation capabilities needs to be the same everywhere since there are very small chances of realizing integration between two different products due to a lack of standardization. This means that the federation agreement must include which product to use.

186. Secondly, the management of rules for transformation of messages needs to be considered. ESB and messaging products are often built for central management of transformation rules, thus enabling a better control over the messaging capabilities in an enterprise. However, this can be problematic in a federative approach since all actors need to agree on the transformation rules or appoint one actor which has the authority to manage these.

2.2.3.5.6. Mediation Services

Translation Services

187. Translation is about manipulating messages in-flight between a service provider and a consumer (requests or events). This means that messages dispatched by a requester are transformed into messages understood by a slightly incompatible provider selected from a set of potential endpoints.

188. Translation services are often considered being a part of the ESB concept.

189. The patterns which translation products SHALL be able to handle are:

- **Protocol switch**: Enables service requesters to dispatch their messages using a variety of interaction protocols or APIs, such as SOAP/HTTP and JMS. Transcodes requests into the targeted service provider's format. Can be applied at the requester or the provider end of an interaction, at both ends, or anywhere in between.

- **Transform**: Translates the message payload (content) from the requester's schema to the provider's schema. This may include enveloping, de-enveloping, or encryption.

- **Enrich**: Augments the message payload by adding information from external data sources, such as customization parameters defined by the mediation, or from database queries.

- **Correlate**: Derives complex events from message or event streams. Includes rules for pattern identification and rules that react to pattern discovery, for example, by generating a complex event derived from content of the triggering event stream.

190. Also see Section 2.2.3.5.5 for details in ESB implementation.

2.2.3.5.7. Information Assurance Services

191. As a minimum baseline for IEGs in a federation, the following shall be implemented in order to fulfil [Principle_8], [Principle_9] and [Principle_10]:

192. The IEGs shall include a Information Protection Service (IPS). This shall provide the following services:

- Authentication to verify the identity of users and systems sending/receiving data

- Authorization to verify rights for users and systems to send/receive data

- Content encryption/decryption capabilities to assure confidentiality and integrity of the data

- Information dissemination control to be able to control which data is passed through the IEG.

193. To be able to inspect the data flowing through the IEG, the data must be unencrypted. The IEG can send and receive encrypted data, but encrypted data must be decrypted by the IEG before it can be inspected and decrypted again for further transport.

194. The Information Exchange Service (IES) which the IEG shall be able to handle is described in the other technology sections of Section 2.2.3.5.

195. The requirements for Node Protection Service (NPS) is not determined by this design rule, however some type of node protection is always needed. Since this design rule does not cover the communication layer, there is a need to create a design rule which describes this.

2.2.3.5.8. Service Management Services

196. Service management can be divided into managing, where the technical systems and services are being controlled, and monitoring where information regarding the status of the technical systems and services are shared.

197. In a federation, the participants may be able to managed systems and services provided by other participants, but this is unlikely due to information responsibility of organizations. I.e. a participant which is responsible for the information within its information zone will not let another actor have administrative privileges to the system where this information resides.

198. However, sharing monitoring information between the participants is essential if the Service Level Agreements (SLAs) shall be fulfilled. These SLAs are included in the agreements for information exchange as specified by [Principle_3].

199. Monitoring information is to be provided using the Simple Network Management Protocol version 3 (SNMP v3) standard according to NISP[12]. Using a non-XML based format for monitoring, like SNMP, will require a special filtering engine in the IEG IPS (see chapter Section 2.2.3.5.7).

200. It is important to set the monitoring scope properly when implementing the monitoring solution in order to avoid dissemination of to much information into the federation. Therefore, monitoring information SHALL only be provided regarding the services which are provided by an actor. Important metrics to provide monitoring information about are:

- Availability of services, both past, current and future (planned outages)
- Performance in the form of response times and throughput
- Capacity, like for example maximum number of users or used storage space

2.2.3.6. Summary

201. To summarize, Figure 2.5 depicts all the technologies mentioned in the chapters above. Together these technologies provide the foundation for secure information exchange in a multilateral collaboration federation in the NNEC context.

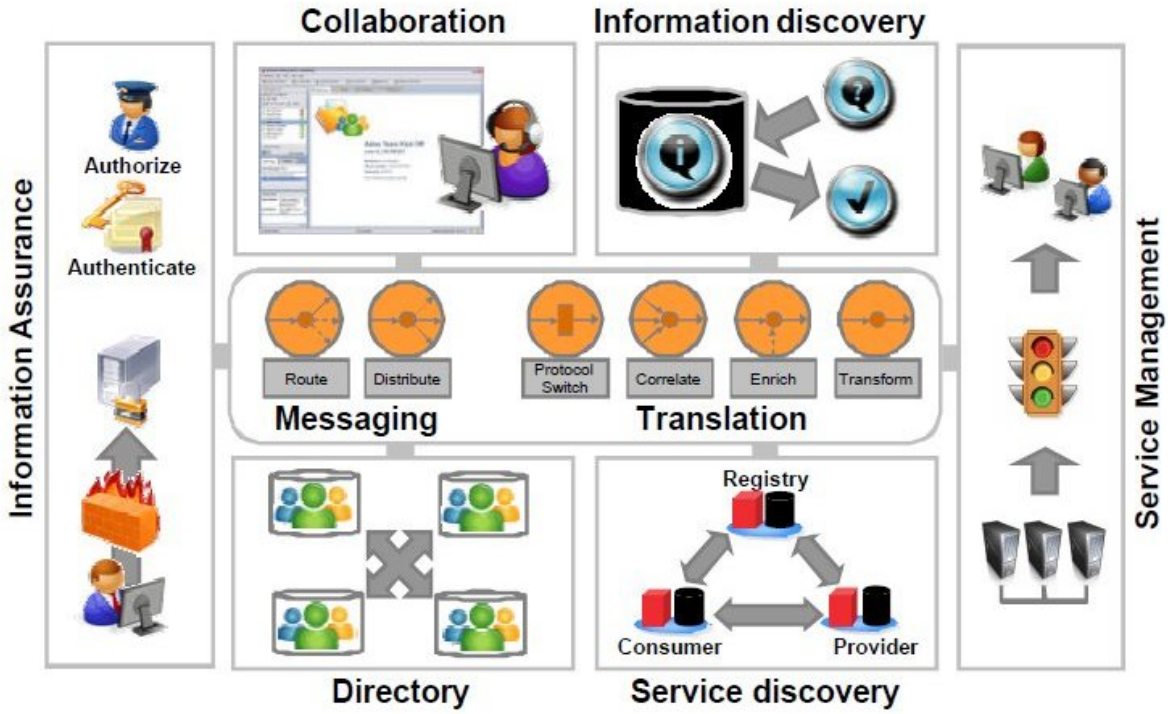

Figure 2.5. Technology Overview

2.2.4. Rejected solutions

2.3. MOTIVATION

202. The NATO Network Enabled Capability (NNEC) Feasibility Study[2] highlights that "at their meeting in November 2002, the NATO C3 Board (NC3B) agreed that there was a need to develop a NATO concept to adapt national initiatives such as the U.S. Network Centric Warfare (NCW) and the U.K. Network Enabled Capability (NEC) to the NATO context. This NATO concept is referred to as NNEC. The NNEC must provide for the timely exchange of secure information, utilising communication networks which are seamlessly interconnected, interoperable and robust, and which will support the timely collection, fusion, analysis and sharing of information".

203. One of the key milestones along the route towards realising the NNEC strategy has been set out in the NATO Networked Consultation, Command and Control Interoperability Policy[3] refers.

204. In particular, the policy states that "It is the intent of NATO that measures shall be put into effect by the Organisation and by individual nations to ensure that information sharing requirements are met securely and expeditiously. This intent requires that appropriate interoperability

[2]EAPC(AC/322)N(2005)0007
[3]AC/322-D(2008)0041 (INV) dated 30 October 20008

solutions and procedures to match IOR over time shall be identified/developed with the nations and documented by the NC3B."

205. This design rule satisfies the above requirement of the NATO Networked C3 Interoperability Policy by identifying the high level design rules required for exchange of information services.

206. Information services are the primary mechanism for information interchange in a NATO environment. This is highlighted in the NATO Networked C3 interoperability policy: "This policy identifies NATO's intent for NNC3 interoperability, and identifies the principles and responsibilities for ensuring the development and effective use of systems to provide interoperable services supporting the sharing of information across the physical, information and human domains".

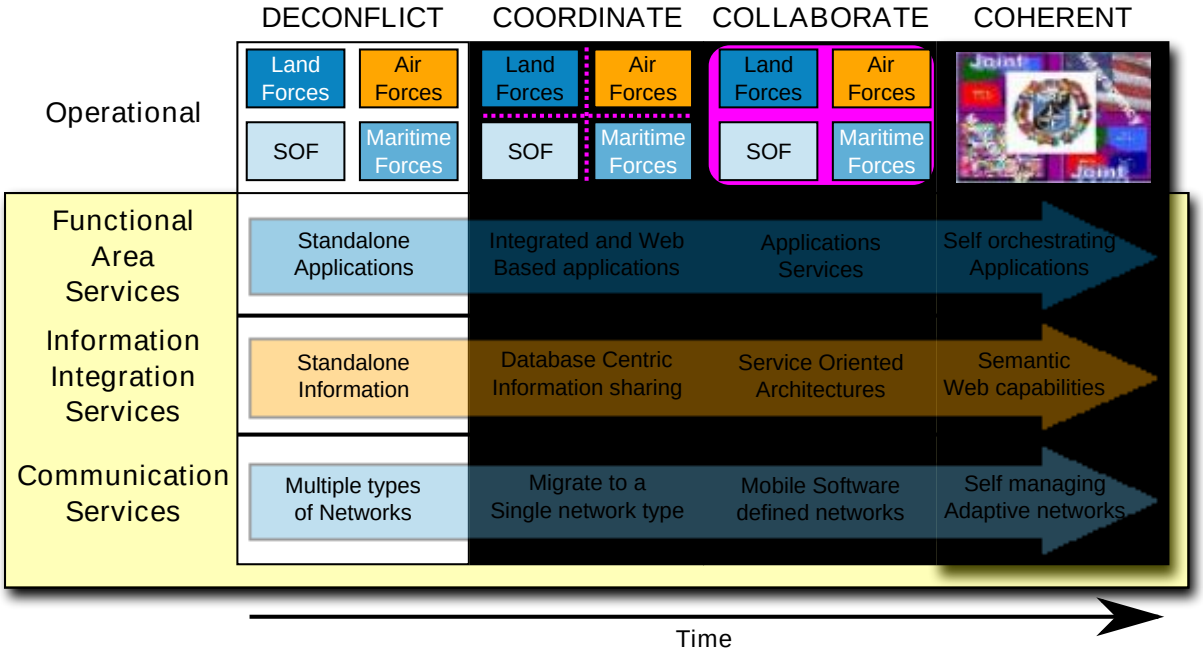

Figure 2.6. Evolving C3 Requirements and Technology Trends for NNEC

2.4. CONSEQUENCES FROM THE SOLUTIONS

207. SOA offers a mechanism for achieving the agility required for NNEC. Whereas the current stove-piped way of doing business is rigid and difficult to adapt because business functions and the supporting IT are so tightly coupled, an SOA exploits newly available software components and web standards that can be reconfigured easily and quickly. SOA translates capabilities, processes and functions into services which can be invoked by a user through an interface. This requires the services to be available and the user to know the "what, how, how much and when" of accessing them. How the services work is of no consequence to the user but is important to designers and architects. The underlying principles are not new, but the web services and related technology to bring it to life are; reinforced by their wide acceptance.

208. The predominant precept is that SOA is business driven. This puts designated defence Process Owners in the driving seat because they place requirements for service provision. If SOA is to be successful it means that they must truly understand what drives the capability they are entrusted to deliver so that they are in a position to inform/drive how it can be delivered to users in the most effective and efficient manner possible. New technology enables much looser coupling between business processes and the IT systems which support them and so overcome one of the key drivers of cost in most IT deployments - tight coupling i.e. changes in one area requiring a cascade of other required changes in order to work; with familiar cost, time and performance penalties. To support this, a high level governance structure is essential to enforce data and quality of service standards which enable reuse of services.

209. There are many benefits to SOA. They include access to previously unavailable information, the design of reusable services, the ability to make up new services from existing ones, the ability for businesses to make changes without costly IT expenditure, and so on. Moreover, the issues subtending from the use of legacy systems and the requirement to leverage as much value for money as possible from their continued use, becomes much less difficult by adopting a service perspective. For those who embrace SOA and see it through, the prospect of a working NNEC becomes realisable for the first time.

210. SOA is already here and any new major system provided by any one of the leading industry vendors is likely to have an SOA capability embedded in it. However, it should be noted that the federated model of SOA described in this design rule is still an emerging concept which will take time to reach maturity.

2.5. EXAMPLES

211. The diagram below shows the concept of federated SOA using a simplified model with participants of Organisation A and Organisation B. Organisations are required to build SOA enterprise scale systems that conform to the NATO Overarching Architecture. The organisations' SOA are connected in a federated manner providing maximum scalability and interoperability.

212. The actual physical connection between the SOAs is at the communications layer. The point of interconnection is called the Service interoperability point (SIOP). The standards used to connect at the SIOP are documented in a Service interoperability profile or SIP.

213. There are also logical connections at the Core Services layer and COI Services layers. These connections also have associated SIPs.

214. An example of the Core Services SIOP is currently being investigated and demonstrated by UK MOD.[4]

215. There is also a logical connection at the COI Services layer. The ability to share COI services is where the main benefit is realised as these are the business services used to undertake missions. Using the guidelines outlined in this design rule, organisations can interoperate by

[4]Federated ESB Interoperabilty Specification - version dated 1 April 2008.

sharing COI services to perform business tasks. For example the UK MOD SOA pilot project has demonstrated a "logistics demand service" which follows a business process to fulfil a request for a store item or spare part.

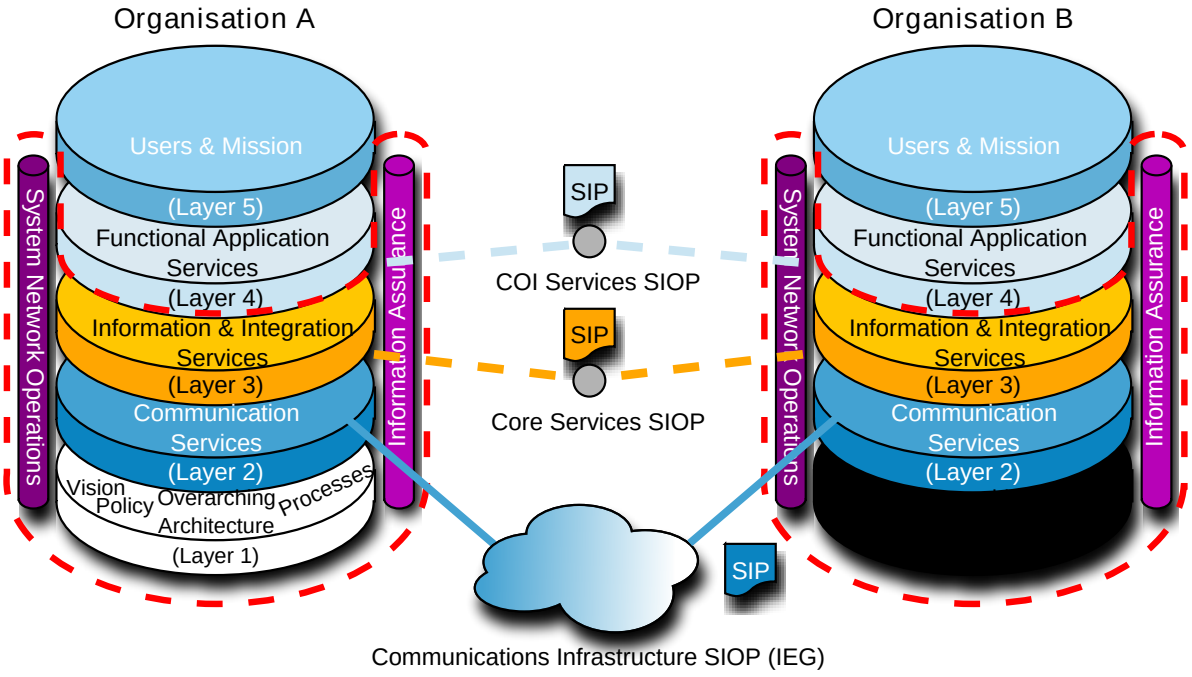

Figure 2.7. Service Interoperability Points and their relationship to the Overarching Architecture

2.6. META DATA

2.6.1. Keywords

216. Interoperability, partner, national, international, external, interface,

2.6.2. Associated design rules

Assoc. #	DR ID	DR Product Name & Solution Reference	Release	Validity
1.				
2.				