

# **Allied Data Publication 34**

## **(ADatP-34(H))**

### **NATO Interoperability Standards and Profiles**

**Volume 4**

### **Design Rules**

**22 August 2014**

**C3B Interoperability Profiles Capability Team**



## Table of Contents

1. NISP Design Rules .....	1
1.1. Summary .....	1
1.2. Introduction .....	1
1.3. General .....	1
1.3.1. Target Group .....	1
1.3.2. Definitions, Abbreviations and Acronyms .....	2
1.3.3. References .....	3
1.4. Background .....	3
1.5. Design rules summary .....	4
1.5.1. Introduction to design rules .....	4
1.5.2. Benefits from using design rules .....	5
1.5.3. Consequences of using design rules .....	5
1.6. Design rules in a NATO NEC federated environment .....	5
1.6.1. Problems or opportunity description .....	5
1.6.2. Solution .....	6
1.6.3. Consequences .....	10
1.7. Reference architecture - National design rules .....	11
1.7.1. The Swedish Design rules contributions .....	11
1.7.2. 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
A. STANAG Transformation Framework .....	45
A.1. Introduction .....	45
A.1.1. Background .....	45
A.1.2. Scope .....	46
A.1.3. Abbreviations and Definitions .....	46
A.2. Executive Summary .....	47
A.3. Recommendations .....	48

A.4. Document Information .....	49
A.4.1. Document Revision Information .....	49
A.4.2. Document Survey .....	49
A.5. Analysis .....	52
A.5.1. Context .....	53
A.5.2. Problem areas and opportunities .....	54
A.5.3. Solution Introduction .....	56
A.5.4. STF Layers and Definition .....	58
A.5.5. STF Design Rules & Methodology .....	73
A.5.6. Consequences .....	112
A.5.7. Limitations .....	120
A.5.8. Deviations .....	120
A.5.9. Examples .....	120
A.6. Relations to other products .....	121
A.6.1. Dependencies .....	121
A.6.2. Impacts .....	121
A.6.3. Interferences .....	123
A.6.4. Replacement .....	123
A.6.5. Change Request (CR)/Improvements .....	123
A.7. V&V (Verification and Validation) .....	123
A.7.1. Verification and Validation of STF .....	123
A.7.2. STF V&V Case Studies .....	126
A.7.3. V&V in the Asset Tracking COI .....	127
A.7.4. V&V in the Friendly Force Tracking (FFT) COI .....	129
A.7.5. V&V in the JISR COI .....	132
A.7.6. V&V in the TDL COI .....	137
A.7.7. V&V for other information exchanges and COIs .....	146
A.8. Methods .....	146
A.9. Tools .....	147
A.10. Outstanding questions .....	147
A.11. Miscellaneous .....	147
A.12. Future Plans .....	147

## List of Figures

1.1. Design rule model .....	8
1.2. Relationship between NISP objects Profiles, standards and Design rules .....	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. Information zones 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
A.1. Requirement for Data, Information and Services (derived from NNEC Data Strategy) .....	53
A.2. Layers of the STANAG Transformation Framework .....	59
A.3. SatCom, Radio, Newspaper, Internet communication bearer .....	61
A.4. Britain's first Official Post Card, the first commercial telephone switchboard .....	63
A.5. Data Element Dictionary .....	64
A.6. Message Structure .....	66
A.7. Implicit and explicit parts of a dialogue .....	67
A.8. Past, Current and future security mechanisms .....	69
A.9. Human Association between different information .....	72
A.10. STF - Holistic Process .....	74
A.11. Data Element Dictionary Logical Model .....	80
A.12. Data Element Dictionary .....	81
A.13. Structure for Data Element Dictionary XML Schema .....	84
A.14. Example of Data Element Dictionary XML instance for Link 16 .....	85
A.15. Structure for BaselineInfo XML Schema .....	86
A.16. Structure for Security XML Schema .....	87
A.17. Structure for Data Element XML Schema .....	89
A.18. Example of DataElement XML instance for Link 16 .....	92
A.19. Example of DataElement XML instance for ADatP-3 .....	93
A.20. Structure for Enum XML Schema .....	94
A.21. Structure for CodingSwitch XML Schema .....	96
A.22. Message Structure Logical Model .....	102
A.23. Message Structure with adapters .....	103
A.24. Root level MessageStructure XML Schema Definition .....	105
A.25. Word XML Schema .....	106
A.26. Word within the Generic Message Structure XML Schema Definition .....	107
A.27. Example of Word XML instance for Link 16 .....	108
A.28. Example of Message and 2 Words XML instance for OTH Gold .....	109
A.29. StructureSwitch XML Schema Definition .....	110
A.30. Bit-based Message Structure XML Schema .....	111
A.31. STF V&V Process Overview .....	124

A.32. xTDL Framework ..... 139

## **1. NISP DESIGN RULES**

### **1.1. SUMMARY**

001. 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.

### **1.2. INTRODUCTION**

002. 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.

003. 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.

004. 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

005. 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).

006. 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).

### **1.3. GENERAL**

#### **1.3.1. Target Group**

007. This subject will be described in a future revision of the volume.

### 1.3.2. Definitions, Abbreviations and Acronyms

<b>Acronym</b>	<b>Explanation</b>	<b>Reference</b>	<b>Definition</b>
DR	Design Rule	IP CaT	<p>A standardized, reusable solution to a design problem in a specific context within a problem space that provides value to the user.</p> <p>Note: There are four (4) types of design rules:</p> <ul style="list-style-type: none"> <li>a. A development method that supports the life cycle perspective;</li> <li>b. A defined structure that supports descriptions of complex relations;</li> <li>c. A detailed description of suggested technical solutions;</li> <li>d. A proven and reusable solution for a generic problem.</li> </ul>
DRP	Design Rule Package	IP CaT	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	<p>A focal 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.</p> <p>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.</p>
SIP	service interface profile	EAPC(AC/322)D(2006)0002-REV1	A document that specifies the characteristics of a service interface between interoperable systems in the Networking and Information Infrastructure.



Acronym	Explanation	Reference	Definition
			Note: A service interface profile is identified at a service interoperability point in an architecture system view.

### **1.3.3. 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] Design rules, in the commercial world. David B. Kim Clark

### **1.4. 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 organize 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.

## **1.5. DESIGN RULES SUMMARY**

### **1.5.1. 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.

### **1.5.2. 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 organizations in creating a common understanding of the problems and challenges they are facing.

### **1.5.3. 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.

## **1.6. 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.

### **1.6.1. 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.

## **1.6.2. Solution**

### **1.6.2.1. 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.

### **1.6.2.2. 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.

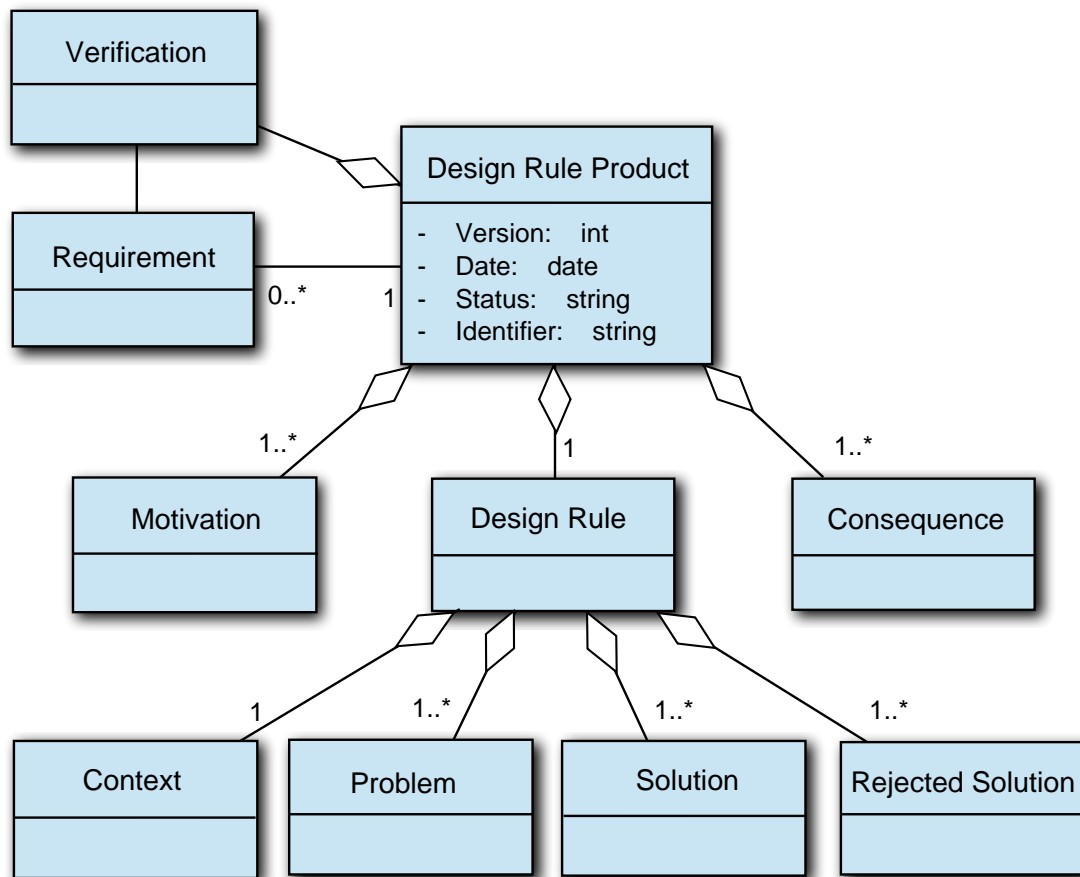
041. An atomic design rule must not contain solutions for more than one subject area, e.g. mixing of business and technical subjects shall be avoided. Detailed technical rules shall in the same way be separated from rules of information or logical nature.

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.

### 1.6.2.3. 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.

**Table 1.1. Rule validities**

<b>Validity</b>	<b>Description</b>
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.

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

#### **1.6.2.4. 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.

### **1.6.3. 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.

#### **1.6.3.1. 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, Design rules is adopted by NATO as a complementary set of tools for :

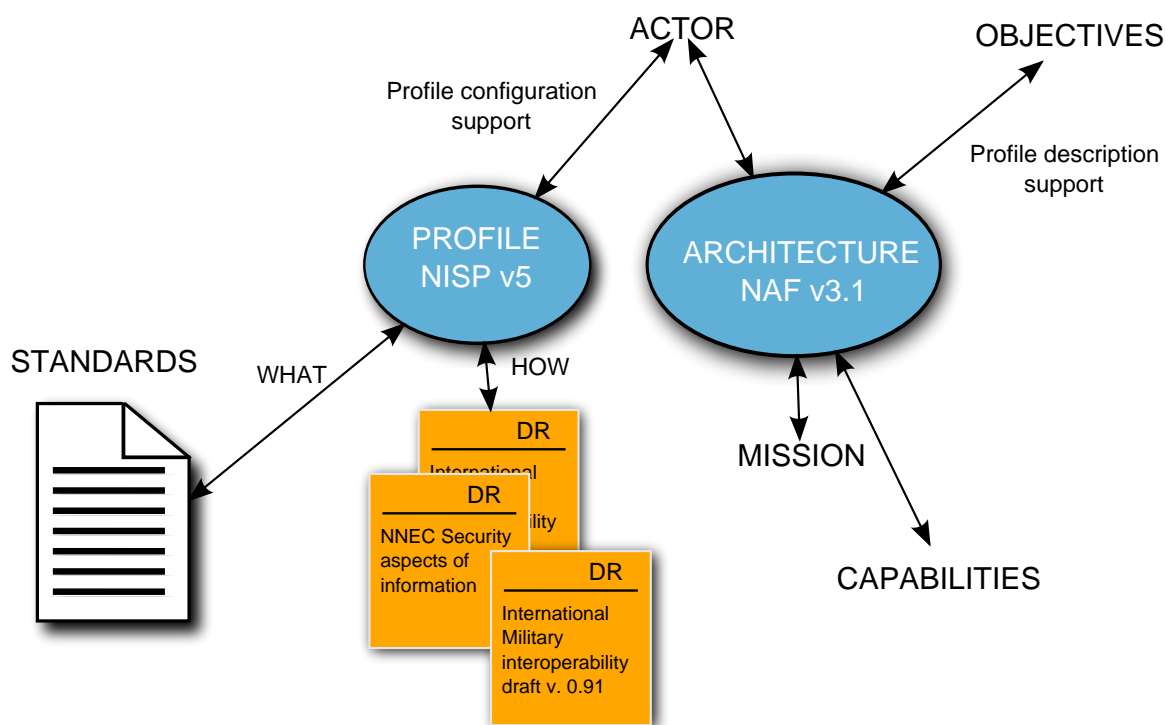
- Helping to choose the right standard
- How to apply the standard on a specific problem
- Understanding the relations between different standards
- Applicability in different domains



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

### 1.6.3.2. Profiling with the use of NAF and Standards and Design rules 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 Design rules. For more information about Profile guidance document.



**Figure 1.2. Relationship between NISP objects Profiles, standards and Design rules**

## 1.7. REFERENCE ARCHITECTURE - NATIONAL DESIGN RULES

### 1.7.1. The Swedish Design rules contributions

**FMLS Architecture Framework Design rules**

LT90 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 Design rules**

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 Design rules**

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

### **1.7.2. Nation x ...**

060. This subject will be described in a future revision of the volume.

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

### **Summary**

061. This design rule describes how military organizations 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 organizations collaborate in a federative manor in a mission.

### **2.1. GENERAL**

#### **2.1.1. Unique Identity**

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

#### **2.1.2. Target Group**

063. 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.

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

065. 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

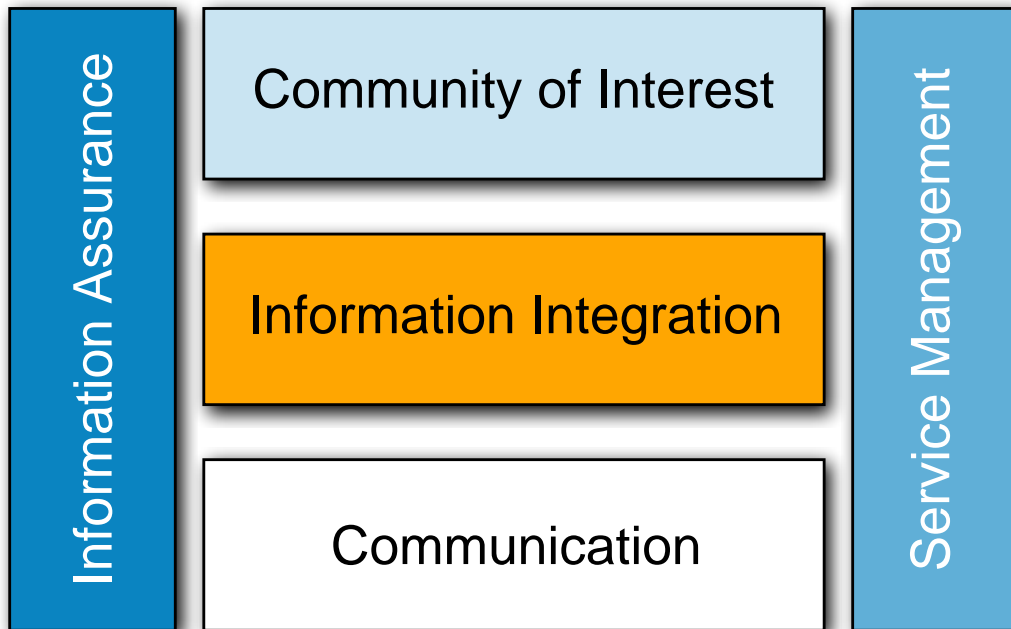
## **2.2. DESIGN RULE**

066. 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].

067. 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.

068. 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**

069. 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

070. 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.

071. 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.

072. 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.

073. 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**

074. 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.

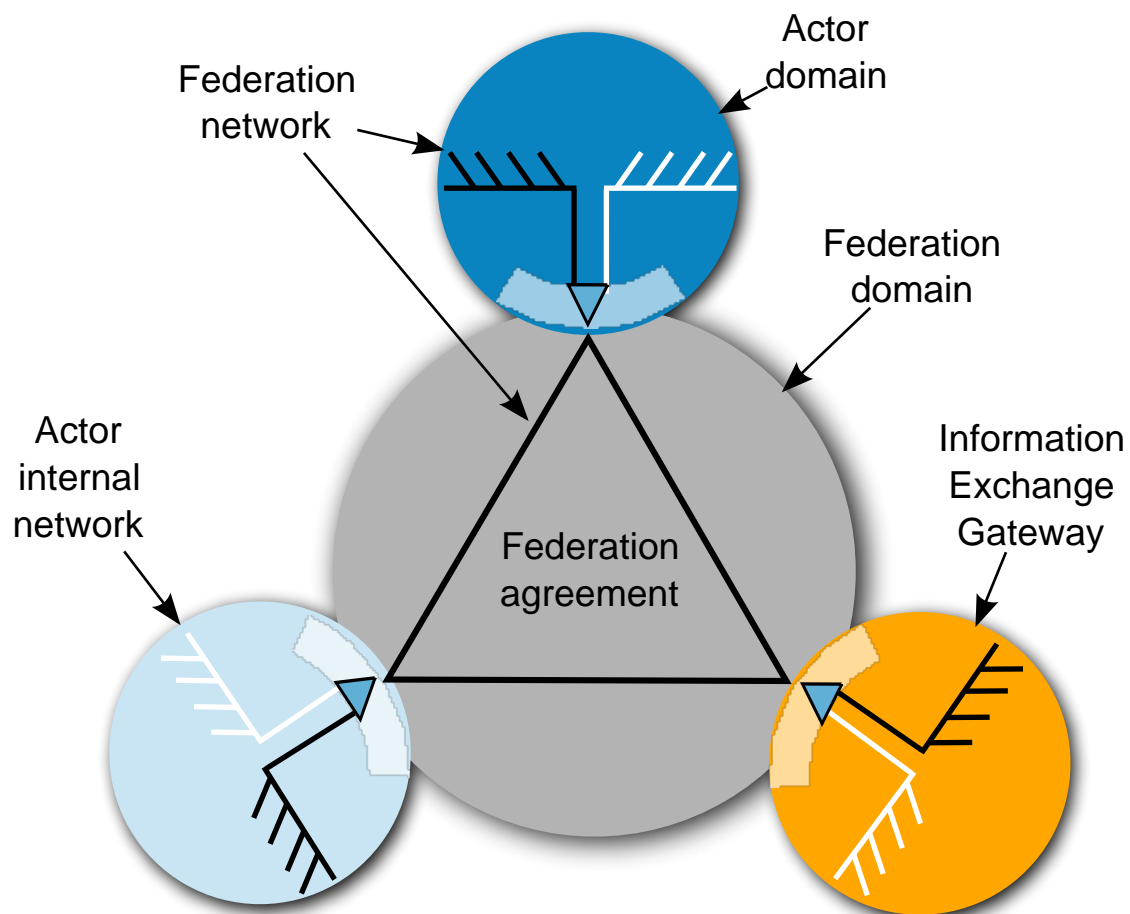
075. The federation, depicted in Figure 2.2, is where the collaborating actors provide services which the other actors can consume. To create a federation, the actors need to create a federation agreement which defines the rules of the federation, such as which data formats, information classifications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

076. 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.

077. 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].

078. 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**

079. 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**

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

081. **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 fulfill 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].

082. **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 organization 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**

083. 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.

084. 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**

085. 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 organizational 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**

086. Information and services exchange between nations and organizations (e.g. unclassified, restricted, secret and top secret classification) is based on government agreement between nations and organizations. 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 organizations 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**

087. 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.

088. 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**

089. 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.

090. 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**

091. 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.

092. 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.

093. 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.

094. 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**

095. 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.

096. 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 where 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**

097. 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 that provides the means to create a foundation for the federation in which information exchange among parties can take place.

098. 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.

099. 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**

100. 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 having to change other systems which interacts with it. Thereby the issue of enabling information exchange between heterogeneous systems [Issue\_8] is resolved.

101. 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.

102. 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.

103. 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**

104. 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.

105. 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].

106. 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.

107. 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.

108. There are certain views which are more important when designing architectures for multinational operations where interoperability is in focus [Issue\_10]:

109. **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.

110. **NATO Capability View (NCV)** which explain what capabilities are needed in order to fulfill 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 fulfill the business needs. In particular, the NCV-2, Capability Taxonomy and NCV-7, Capability to Services Mapping views are important.

111. **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.

112. 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.

113. **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 fulfill 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.

114. In the **NATO Systems View (NSV)**, the NSV-1 view is the most important since it describes how the different systems interact to fulfill 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**

115. 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**

116. 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**

117. 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**

118. 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.

119. 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.

120. 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**

121. 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**

122. 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.

123. 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**

124. 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

125. 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 utilized to enable the information exchange.

126. 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**

127. 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**

128. 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].

129. 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].

130. 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

131. 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**

132. 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.

133. 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.

134. 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 that are based on manual model mappings.

### **2.2.3.3.4. Information Exchange Objects**

135. 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.

136. Information objects are created, processed, stored and moved/exchanged via services. An information exchange object is a standardized 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**

137. 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.

138. 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**

139. Translations are used 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

140. When determining appropriate security solutions for a federation it is of outmost importance to analyse the information that 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.

141. 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**

142. 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 standardize 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:

143. "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."

144. "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."

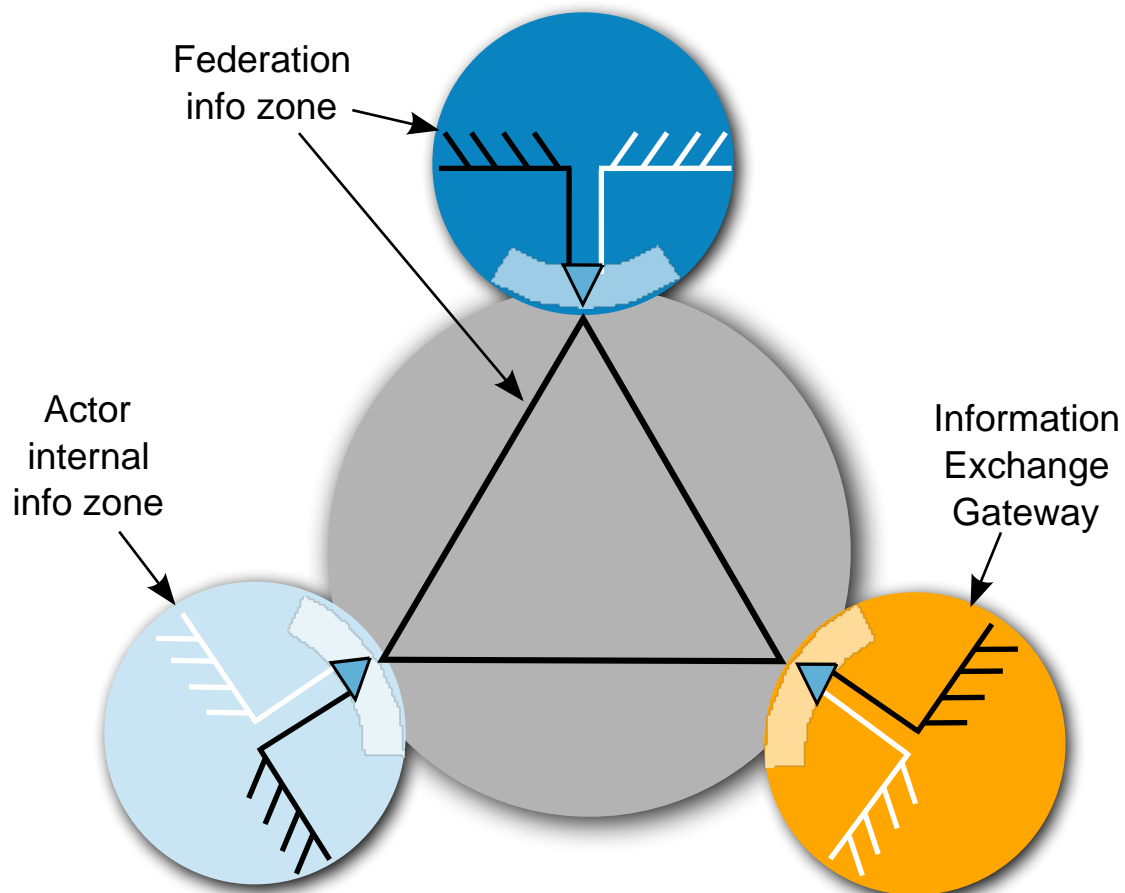
145. "The third major component/service is the Information Exchange Service (IES). The IEG must facilitate the flow of information between the protected node/network and the external organizations that are authorized (by the Information Protection Service)."

146. 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**

147. 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.

148. 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. Information zones in the federation**

149. 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.

150. 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.

151. 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**

152. 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

described 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?"

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

154. 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 organizational 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.

155. To be able to fulfill 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.

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

157. To fulfill [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.

158. 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.

159. 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**

160. 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.

161. 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.

162. 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**

163. 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].

164. 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.

165. 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 standardize the ability to perform federated search, the most prominent one is the OpenSearch initiative<sup>1</sup>. Even though OpenSearch is not a formal standard it is well on its way to be adopted by many of the major tool vendors.

166. In either case, the actors in the federation must implement search engines which can index information (if they 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**

---

<sup>1</sup><http://www.opensearch.org/>

167. A metadata registry is a database that contains information about information that 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 that 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.

168. 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**

169. 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.

170. 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.

171. 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**

172. 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**

173. 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.

174. 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.

175. 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.

176. 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**

177. 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.

178. There is one important aspect of XMPP that is not covered by the current standard specification; there is no security tagging options available that 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.

179. 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**

180. 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.

181. 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.

182. 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.

183. 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.

184. 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.

185. 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

186. 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.

187. 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

188. 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.

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

190. 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.

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

### 2.2.3.5.7. Information Assurance Services

192. As a minimum baseline for IEGs in a federation, the following shall be implemented in order to fulfill [Principle\_8], [Principle\_9] and [Principle\_10]:

193. 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.

194. 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.

195. 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.

196. 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**

197. 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.

198. 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.

199. 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].

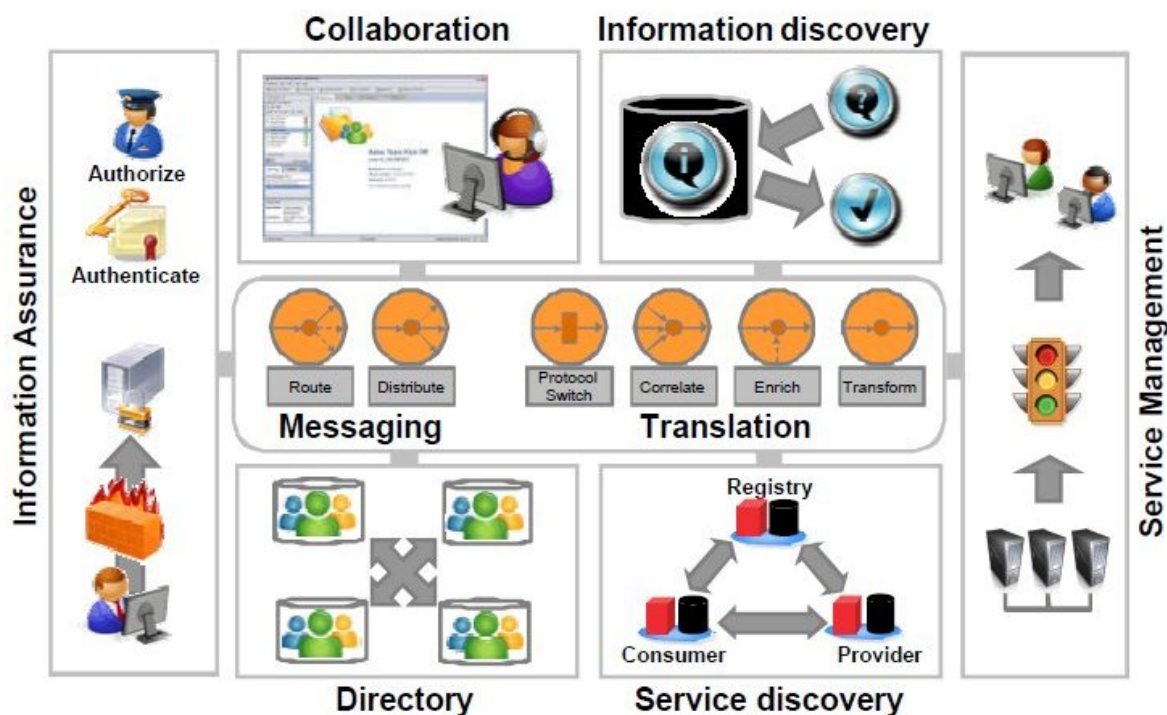
200. Monitoring information is to be provided using the Simple Network Management Protocol version 3 (SNMP v3) standard according to NISP[12]. Using a non-XML based format for monitoring, like SNMP, will require a special filtering engine in the IEG IPS (see chapter Section 2.2.3.5.7).

201. 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**

202. 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**

203. This subject will be described in a future revision of the volume.

**2.3. MOTIVATION**

204. The NATO Network Enabled Capability (NNEC) Feasibility Study<sup>2</sup> highlights that "at their meeting in November 2002, the NATO C3 Board (C3B) 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, utilizing communication networks which are seamlessly interconnected, interoperable and robust, and which will support the timely collection, fusion, analysis and sharing of information".

205. 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<sup>3</sup> refers.

206. In particular, the policy states "It is the intent of NATO that measures shall be put into effect by the Organization and by individual nations to ensure that information sharing requirements

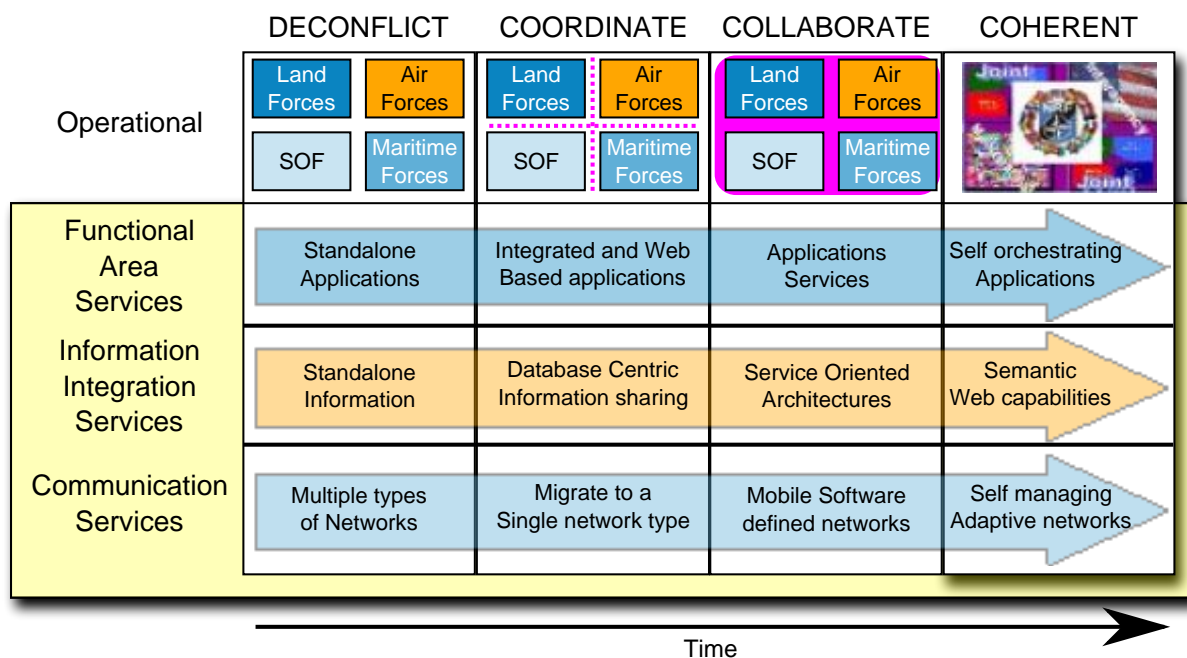
<sup>2</sup>EAPC(AC/322)N(2005)0007

<sup>3</sup>AC/322-D(2008)0041 (INV) dated 30 October 2008

are met securely and expeditiously. This intent requires that appropriate interoperability solutions and procedures to match IOR over time shall be identified/developed with the nations and documented by the C3B."

207. 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.

208. 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**

209. 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.

210. 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.

211. 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.

212. 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**

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

214. 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.

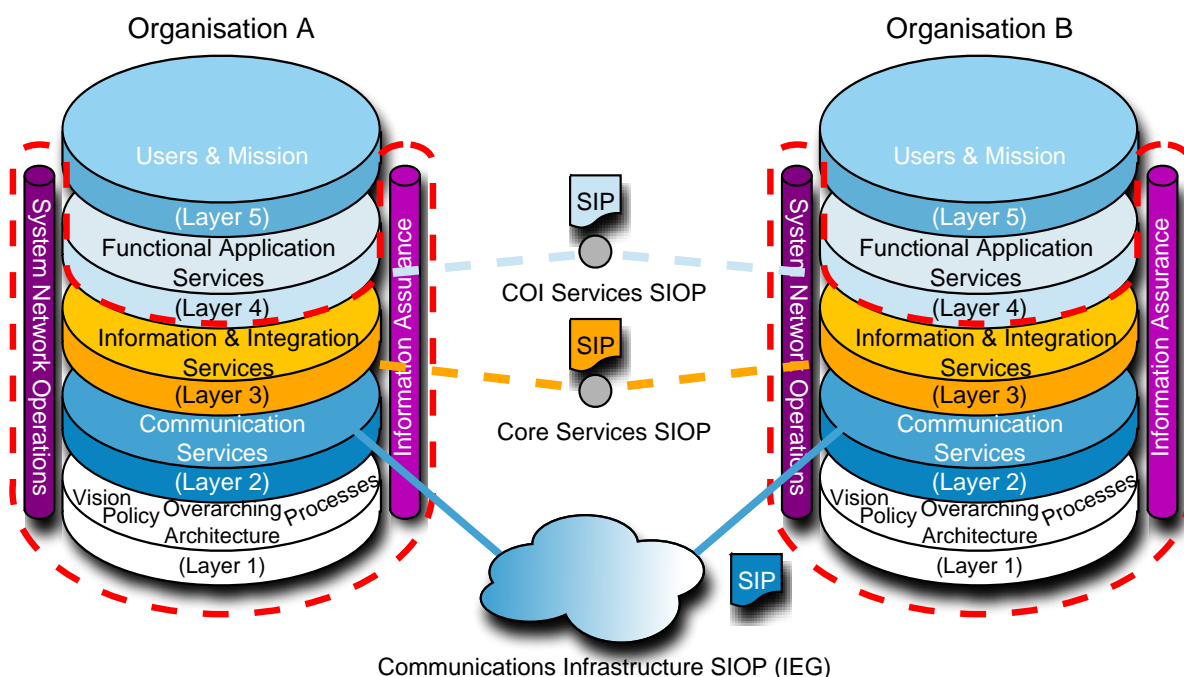
215. There are also logical connections at the Core Services layer and COI Services layers. These connections also have associated SIPs.

216. An example of the Core Services SIOP is currently being investigated and demonstrated by UK MOD.<sup>4</sup>

---

<sup>4</sup>Federated ESB Interoperability Specification - version dated 1 April 2008.

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

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

### 2.6.2. Associated design rules

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

## **A. STANAG TRANSFORMATION FRAMEWORK**

219. This annex describes the STANAG Transformation Framework (STF) included in the NISP.

**Table A.1. Article Metadata**

Project name:	Interoperability & Standardization (ACT Sponsor: Troy Turner)
Topic:	STANAG Transformation Framework (STF)
Area of Validity:	Common framework and methodology to transform textual STANAGs into XML
Original Author:	Dario Cadamuro
Original Author:	Jelle van Zeijl
Original Author:	Mimi Nguyen
Maintained by:	NCI Agency CapDev
Version:	v1.0

### **A.1. INTRODUCTION**

#### **A.1.1. Background**

220. NATO captures the definition of processes, procedures, terms, and conditions for common military or technical procedures or equipment between member countries using a Standardization Agreement (STANAGs).

221. The NATO Standardization Agency (NSA) and Consultation, Command and Control Board (C3B) with Capability Panels (CaPs) and Capability Teams (CaTs) develop and maintain STANAGs under configuration management within NATO.

222. STANAGs form the basis for enabling technical interoperability between a wide variety of Communication and Information Systems (CIS). In particular, information exchange STANAGs are used to standardize the protocols and data formats which regulate the information exchange between various CISs. Within the NATO APP-15 such types of STANAGs are called Information Exchange Specifications (IES). In this document, STANAG shall be read as a STANAG related to an IES within NATO.

223. STANAGs constantly evolve in line with the evolution of NATO roles and derived requirements. The evolution implies the enhancement, modification and reduction of their contents. NATO has identified several gaps and areas for improvement within the current STANAGs that require action to ensure current and continual interoperability among forces and to enable the information sharing in a seamless infrastructure.

224. As NATO and Nations are evolving to achieve the vision of the NATO Network-Enabled Capability (NNEC) , it has been realized and agreed that the NNEC data strategy goals involve making data Visible, Accessible, Understandable and Interoperable. In order to support these goals, traditional text-based information exchange STANAGs need to evolve into an unambiguous, machine-interpretable format, such as the extensible mark-up language (XML).

225. A common framework and methodology to transform textual STANAGs into XML have been developed and are presented here as the STANAG Transformation Framework (STF) set of design rules.

226. With the application of the STF, NATO and Nations are provided a mechanism to start tackling the data strategy vision and facilitating the improvement of current and future STANAG development efforts.

### **A.1.2. Scope**

227. The scope of the analysis is to introduce a common framework, the STF, and associated design rules and methodology to transform textual STANAGs into XML to support the NNEC data strategy goals to make data Visible, Accessible, Understandable and Interoperable in an NNEC, service-oriented architecture (SOA) based, environment.

228. The STF set of design rules also aims to assist in the development of current and future STANAGs within NATO. The STF, design rules and methodology are applicable to all information exchange STANAGs related to technical interoperability between systems and services.

229. Although it may be applicable to all types of information exchanges, it does not aim to regulate the development of standards used outside of NATO.

230. The STF is not intended to be used for transforming STANAGs that are unrelated to information exchange (e.g. STANAG 2832 - Restrictions for the Transport of Military Equipment by Rail on European Railways).

### **A.1.3. Abbreviations and Definitions**

231. In this section abbreviations and concepts used in the analysis report are listed.

**Table A.2. Abbreviations**

APP	Allied Procedural Publication
AST	Asset Tracking
C3B	Consultation, Command and Control Board
CaP	Capability Panel
CaT	Capability Team

CIS	Communication and Information System
COI	Community of Interest
FFT	Friendly Force Tracking
IES	Information Exchange Specification
NATO	North Atlantic Treaty Organisation
NMRR	NATO Metadata Registry & Repository
NNEC	NATO Network Enabled Capability
NSA	NATO Standardization Agency
SOA	Service-oriented architecture
STANAG	NATO Standardization Agreement
STF	STANAG Transformation Framework
TDL	Tactical Data Link
V&V	Verification & Validation
XML	Extensible Mark-up Language

## **A.2. EXECUTIVE SUMMARY**

232. STANAGs regulate the information exchange between systems and services and form the basis for technical interoperability. These STANAGs are under configuration management within NATO and are evolving in line with the evolution of NATO roles and derived requirements.

233. Gaps in current STANAGs related to this evolution and areas for improvement of the STANAGs have been identified. These include lack of support for NNEC Data Strategy requirements, a lack in the ability to verify and validate (V&V) the quality of the STANAG content and implementation, and the need for resource optimization required for the management and maintenance of the STANAGs. The STANAG Transformation Framework (STF) set of design rules is based on a proven solution to the identified problems related to the contents, the quality and the resources required for the management of the STANAG that are regulating the information exchange within NATO.

234. The STF set of design rules provides a methodology to apply STF in order to transform traditional human-readable textual representation of the STANAGs into equivalent machine-readable representations to support NNEC goals of making data Visible, Accessible, Understandable and Interoperable.

235. The STF has been successfully applied to various STANAGs related to and tested within different Communities of Interest (COIs). In particular, STF design rules have been applied to the Tactical Data Link (TDL), the Asset Tracking (AST), Joint Intelligence, Surveillance and Reconnaissance (JISR) and the Friendly Force Tracking (FFT) communities within NATO.

236. Viewed from a common perspective, the STF design rules have been shown to address problems that occur over and over again within different contexts. This has demonstrated its usefulness, applicability, reliability and trustworthiness as a means to develop and transform STANAGs that regulate the information exchange within NATO. Also as organisations and nations convert STANAGs to XML to meet their own systems requirements, the STF sets out the design rules to enable this process, thus providing standardization and ensuring interoperability of our systems.

237. The NATO Standardization Agency (NSA) and Consultation, Command and Control Board (C3B) with Capability Panels (CaPs) and Capability Teams (CaTs) develop and maintain STANAGs under configuration management within NATO. As these bodies develop or maintain STANAGs, it is highly recommended that they apply the STF as needed based on the context of the problem they are trying to solve.

### **A.3. RECOMMENDATIONS**

238. The identified recommendations based upon the findings of the analysis are listed below:

- NATO and Nations to mandate the usage of the STF set of design rules to develop new information exchange STANAGs and to transform existing STANAGs into equivalent machine-readable and machine-interpretable representations to support the NNEC Data Strategy goals.

239. In order to make this feasible, the following is the recommended Way Ahead:

- Develop a roadmap and development plan detailing the sequencing and prioritisation of activities related to the transformation of existing STANAGs.
- Develop a NATO stakeholder plan to define which bodies within NATO shall apply the STF set of design rules.
- Establish a NATO Metadata Registry and Repository that is configuration managed, to store the STF set of XML artefacts as well as the XML artefacts produced by applying the STF.
- Establish the STF namespace to maintain the XML artefacts that are part of the STF set of design rules under configuration management and shareable within NATO.

There is a need to continue active and constructive interaction between NATO, Nations and Industry, leading towards the definition of a roadmap for the transformation and maturity of information exchange STANAGs. As the NSA and C3B develop or maintain STANAGs, it is highly recommended that they apply the STF.

## **A.4. DOCUMENT INFORMATION**

### **A.4.1. Document Revision Information**

**Table A.3. Document Revision Information**

<b>Date</b>	<b>Issue</b>	<b>Description</b>	<b>Author</b>
2012/05/31	First version	STANAG Transformation Framework (STF) Design Rules. Analysis report	NCI Agency

### **A.4.2. Document Survey**

#### **A.4.2.1. Enclosures**

240. The enclosed documents listed in the table below form the STF Set of XML artefacts and are provided here for the reader's reference. The authoritative versions of these STF XML artefacts are available electronically via the interim NATO Metadata Registry & Repository (NMRR) within the STF Namespace.

**Table A.4. Enclosures**

<b>Document ID</b>	<b>Date of publication</b>	<b>Issue number / version</b>
STF-common.xsd	31 August 2012	1.0
STF-security.xsd	31 August 2012	1.0
DataElementDictionary-Base.xsd	31 August 2012	1.0
DataElementDictionary-Codelists.xsd	31 August 2012	1.0
DataElementDictionary-Bit-Based.xsd	31 August 2012	1.0
DataElementDictionary-Text-Based.xsd	31 August 2012	1.0
MessageStructure-Base.xsd	31 August 2012	1.0
MessageStructure-Codelists.xsd	31 August 2012	1.0
MessageStructure-BitBased.xsd	31 August 2012	1.0
MessageStructure-TextBased.xsd	31 August 2012	1.0

### A.4.2.2. Government Documents

**Table A.5. Government documents**

Document ID	Date of publication	Issue number / version
TBD		

### A.4.2.3. References

**Table A.6. References**

Document ID	Date of publication	Issue number / version
[APP15] NATO Consultation, Command and Control Board (NC3B) Information Services Sub-Committee (ISSC), ANNEX 1 to EAPC(AC/322-SC/5)N(2009)0001, APP-15 (Allied Procedural Publication) NATO Information Exchange Requirement Specification Process, (NATO/EAPC Unclassified)	November 2008	Original
[NNEC-FS] NATO Network Enabled Capability Feasibility Study (NNEC FS)	October 2005	2.0
[NNEC-DS] NATO Network Enabled Capability (NNEC) Data Strategy	January 2005	1.1
[RTO-IST-088] RTO-LS-IST-088 - Interoperability Enhancement via Standards Transformation	November 2009	
[MP-IST-01] Street, M.D, "Software Defined Radio to Enable NNEC: Technical Challenges and Opportunities for NATO", MP-IST-01, pp 7 (NATO Unclassified)	April 2008	
[W3C-XML] Extensible Markup Language (XML) 1.0, W3C Recommendation <a href="http://www.w3.org/TR/2008/REC-xml-20081126">http://www.w3.org/TR/2008/REC-xml-20081126</a>	26 November 2008	Fifth Edition
[ISO/OSI] International Organization for Standardization and International Electrotechnical Commission (ISO/IEC 7498-1:1994(E), "Information technology " Open Systems Interconnection " Basic Reference model: The Basic Model"	November 1994	
[W3C-SWA] World Wide Web Consortium (on-line), "W3C Semantic Web Activity", at <a href="http://www.w3.org/2001/sw/">http://www.w3.org/2001/sw/</a>	17-09-2009, viewed 2 Octo-	



Document ID	Date of publication	Issue number / version
	ber 2009	
[ISO/IEC11179] International Organization for Standardization and International Electrotechnical Commission (ISO/IEC 11179-1:2004, "Information technology - Metadata registries (MDR)")	2004	Edition 2
[BiSC-C2] Bi-SC Secure C2 Data Strategy v1.0 (BI-SC Secure C2 Data Strategy (3805/SPTCIS/CFOISM/2010/82-270734))	27 July 2010	1.0
[NAC-INFOSEC] AC/322-WP(2004)0006(INV), "INFOSEC Technical and Implementation Guidance for Electronic labeling of NATO Information", North Atlantic Council, Brussels, Belgium (NATO Unclassified)	2 Febru- ary 2004	Work- ing pa- per
[RTO-XML-2008] RTO RTG-031/IST-068-2008 "XML In Cross-Domain Security Solutions: XML Security labeling proposal, 2008", NATO Research and Technology Organization, Paris, FR, (NATO Unclassified))	Novem- ber 2008	
[RTO-XML-2009] RTO RTG-031/IST-068-2009, "XML Confidentiality Label Syntax - A Proposal for a NATO Specification", NATO Research and Technology Organization, A. Eggen, R. Haakseth, Norwegian Defence Research Establishment (NFFI), A. Thümmel (NC3A) (NATO Unclassified)	April 15, 2009	Draft Version 0.3, Not pub- lished
[xTDL] EAPC(AC322-SC5-WG1)N(2009)0008 - xTDL Framework Document Original Distribution	May 2009	Original
[NC3A-TN-1391] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1391, "Tactical Information Sharing, Improved Sharing via Standards Development and Validation", D. Cadamuro, J. van Zeijl, R. van Klaveren, N. Kol, A.C. Dinc, L. Fallani, M. van Nierop, M. van Schouwen, NC3A, The Hague, Netherlands (NATO Unclassified)		Draft
[NC3A-TN-1311] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1311, "Administrative NATO Metadata Registry and Repository (NMRR) User Requirements", D. Cadamuro, N. Kol, NC3A, The Hague, Netherlands, (NATO Unclassified)	Decem- ber 2008	
[NC3A-TN-1312] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1312, "Administrative NATO Metadata Registry and Repository (NMRR) Functional Requirements", D. Cadamuro, N. Kol, NC3A, The Hague, Netherlands (NATO Unclassified)	Decem- ber 2008	
[NC3A-TN-1313] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1313, "Administrative NATO Metadata Registry and Repository (NMRR) Architecture and Design", D. Cadamuro, N. Kol, NC3A, The Hague, Netherlands (NATO Unclassified)	Decem- ber 2008	

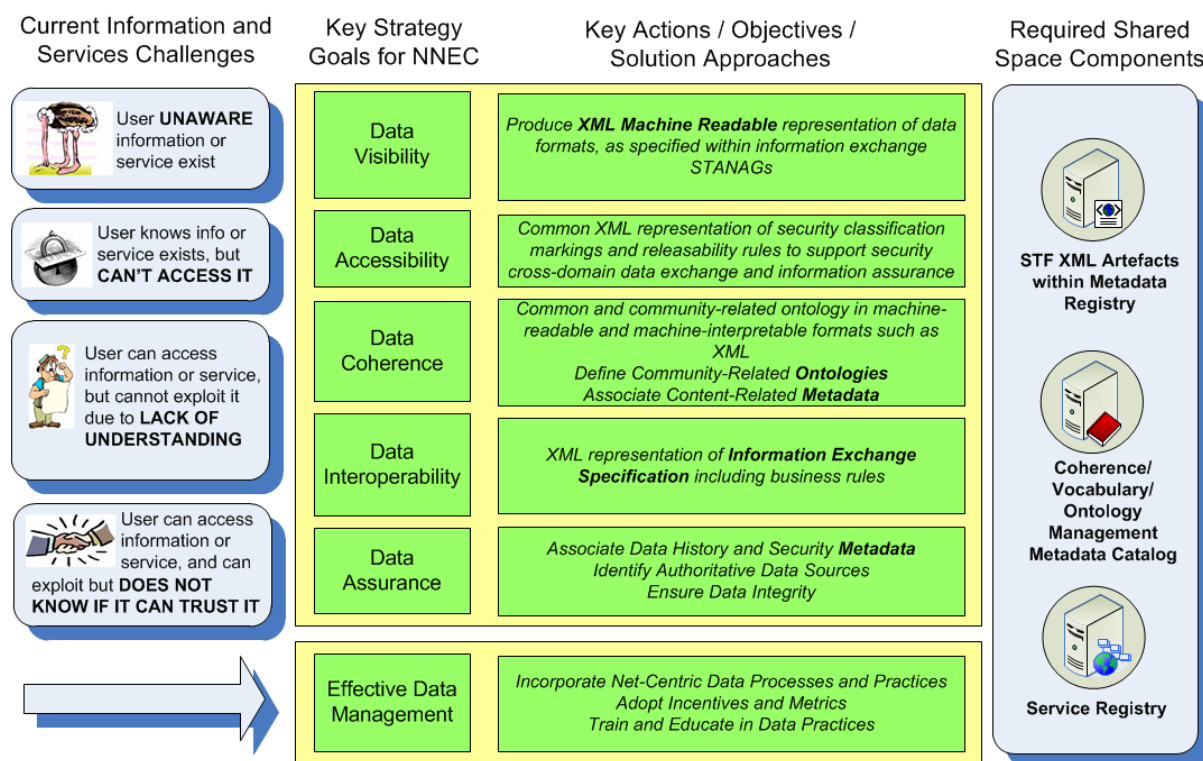
<b>Document ID</b>	<b>Date of publication</b>	<b>Issue number / version</b>
[NC3A-TN-1367] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1367, "Operational NATO Metadata Registry and Repository (NMRR) System Requirements Specification (SRS)", D. Cadamuro, N. Kol, R. van der Lingen, M. van Schouwen, H. van Woudenberg, NC3A, The Hague, Netherlands (NATO Unclassified).		Draft
[NC3A-TN-1368] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1368, "Operational NATO Metadata Registry and Repository (NMRR) Feasibility Overview", D. Cadamuro, N. Kol, R. van der Lingen, M. van Schouwen, H. van Woudenberg, NC3A, The Hague, Netherlands (NATO Unclassified)	December 2008	
[NC3A-TN-1369] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1369, "Operational NATO Metadata Registry and Repository (NMRR) Interface Control Document", D. Cadamuro, N. Kol, R. van der Lingen, M. van Schouwen, H. van Woudenberg, NC3A, The Hague, Netherlands (NATO Unclassified)	December 2008	
[RTO-EN-IST-088] RTO-EN-IST-088, "NATO Metadata Registry and Repository: Core Service for XML", D. Cadamuro, N. Kol and R. van Klaveren (NATO Unclassified)	October 2009	
[NC3A-TN-1254] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1254, "Standardization and the Power of Metadata", D. Cadamuro, N. Kol, NC3A, The Hague, Netherlands (NATO Unclassified)	December 2008	
[NC3A-NU/CCS/ADP/2008/331] NATO Consultation, Command and Control Agency CD-ROM NU/CCS/ADP/2008/331, "Link-16 ALTBMD-MRS Interoperability Matrix for Command and Control/Battle Management/Communications Ballistic Missile Defence Systems (BMDS) Interface Control Document (ICD)", D. Cadamuro, NC3A, The Hague, Netherlands (NATO Confidential)	April 2008	Version 1.0
[BiSC-DLMS] AC322-N0638 - Bi-Strategic Commands Data Link Migration Strategy (Bi-SC DLMS)	11 December 2000	Original

## **A.5. ANALYSIS**

241. In this chapter, the STF set of design rules is introduced by first providing the context and the problem it is addressing. Following, the solution and derived consequences are described. Finally, the limitations, the deviations and examples are presented.

### A.5.1. Context

242. As NATO and Nations are evolving to achieve the vision of the NATO Network-Enabled Capability (NNEC), there are four basic challenges which have to be addressed in order to achieve the NNEC requirements that "data, information and services be visible, accessible, understandable and trusted across the networked environment for all authorized users, whether anticipated or unanticipated." Each of these challenges build on top of each other - as one challenge is solved, the next becomes relevant as the new challenge to be addressed.



**Figure A.1. Requirement for Data, Information and Services (derived from NNEC Data Strategy)**

243. As depicted in Figure A.1, these challenges are addressed by six key strategy goals, known as the NNEC Data Strategy goals, of making data Visible, Accessible, Coherent, Interoperable, and Assured, and their related actions/solution approaches. These solution approaches deal with data and information exchanges across a networked environment, and in particular a Service Oriented Architecture (SOA) environment, and thus require standardization of the protocols and data formats to ensure interoperability within the NATO context. As stated in Section A.1.1, these standardizations are captured by NATO as information exchange STANAGs.

## **A.5.2. Problem areas and opportunities**

244. Essentially, NATO has identified several gaps and areas for improvement within the current STANAGs that require action to ensure an appropriate interoperability among forces and to enable the information sharing in a seamless infrastructure.

245. In general, the identified problems are related to the following areas:

- Lack of ability to efficiently and accurately perform Verification and Validation (V&V) on the quality of the contents and implementations of the STANAGs.
- Limited resources available for the management and maintenance of the STANAGs.
- Lack of support to address specific needs to support the NNEC Data Strategy goals.
- No agreed or standardized approach to the conversion of STANAGS to XML (design rules, methodology).

246. In particular, STANAGs have to be matured in the following aspects, based on the NNEC requirements and their identified gaps:

- Security matters related both to information exchange security within the same security domain and cross security domains.
- Operational cross-domain addressing harmonization of the information being exchanged across-COIs.
- Open/common architecture framework to describe the enterprise and the common/core services.
- Service Oriented Architecture enabling seamless sharing of information.
- Supporting object uniqueness and coherent object identification within a particular COI and among other COIs.

247. The above mentioned areas are further described in the following sections.

### **A.5.2.1. Lack of automated support for V&V of STANAG content & implementation quality**

248. Current STANAGs are text-based documents often composed of many pages (e.g. STANAG 5516 consists of more than 8000 pages). These STANAGs are mainly manually written in text using a natural communication language like English, leaving room for (mis-)interpretations and ambiguous definitions (see e.g. standards ambiguity in [MP-IST-01]). To remove the possibility of misinterpretation and ambiguity, verification and validation of the quality and integrity of the STANAG content is required and needs to be supported in an

automated way. The text-based representations of the STANAG do not allow this to happen in an efficient and effective manner.

249. In fact, due to the current status quo, many STANAG standards and implementations may:

- Contain unnecessary errors, since an automated integrity check cannot occur with a STANAG described in a natural language.
- Contain inconsistencies when sections of a STANAG are updated as there is no automated means to check and cue updates that are required for other linked sections of the STANAG.
- Be difficult to browse through without clickable hyperlinks, especially for very large and complex standards.
- Contain duplications and inconsistencies between the definitions of the same data elements across multiple STANAGs.
- Have vague or incomplete definitions of important concepts related to information exchanges, such as data bearers.
- Be subject to restriction from proprietary rights aspects.

250. As STANAGs are currently open to different interpretations, this allows inconsistent implementation of the standards which could lead to interoperability issues when fielded. There is a need for a framework and methodology that supports the transformation of traditional text-based STANAGs into an unambiguous, machine-interpretable format in order to support the automated V&V of STANAG content and implementation quality.

#### **A.5.2.2. Limited resources available for STANAG configuration management (CM)**

251. The traditional approach for STANAG definition and maintenance is that a NATO body "in many cases a NATO working group" is responsible for the definition and maintenance of the STANAG based on a well defined process. There currently are limited resources available for the management and maintenance of current STANAGs. In this era where defence budgets are generally in decline with little, if any, prospect for significant improvements, there exists a need to optimize resources to improve the efficiency and effectiveness of the management and maintenance of existing STANAGs and the development of new ones.

252. The current approach for STANAG configuration management and maintenance is a very manual-intensive, stove-piped process that:

- Results in a tedious and lengthy ratification process.
- Does not leverage on new technologies and methodologies which would support automatic or semi-automatic verification and validation of the STANAG change proposal content, and assessment of impacts and dependencies before implementation.

- Is not designed to optimize resources via the reuse of common definitions to support data harmonization, while increasing quality of the data content.
- Allows duplications and inconsistencies in the definition of the same data elements between multiple STANAGs as there is no automated way to cross-check the definitions.

253. Once current STANAGs are transformed into a machine-readable and machine-interpretable format, automated tools could be developed to help optimize the limited available resources in order to support the management and maintenance of STANAGs. It will also increase the efficiency in the development of new STANAGs as it supports the discovery, reuse and harmonization of common definitions across the various Communities of Interest (COIs) responsible for STANAG development.

### **A.5.2.3. Unaddressed shortcomings of current STANAGs**

254. The need for making data Visible, Accessible, Understandable and Interoperable in an NNEC (SOA) environment is not fully addressed in current STANAGs.

255. Current STANAGs typically:

- Have missing definitions of important concepts related to information exchanges, such as data bearers.
- Do not define how to share information in a Service Oriented Architecture (SOA) environment outside its legacy information exchange stovepipe.
- Are not sufficiently mature to support information exchange within a SOA.
- Do not support or address several necessary requirements such as cross COI and cross-security domain information sharing.
- Do not support object uniqueness and coherent object identification within and between COIs.

256. A structured, layered approach that identifies and captures the gaps and addresses the shortcomings of existing STANAGs in fulfilling the NNEC Data Strategy goals is needed to guide the transformation of existing STANAGs to support information exchange in a SOA environment. It will also assist in future STANAG development to ensure these gaps are addressed at STANAG inception and development rather than costlier and time-consuming changes after the fact.

### **A.5.3. Solution Introduction**

257. In this section, the solution for addressing the identified problem areas and opportunities captured in Section A.5.2, the STANAG Transformation Framework (STF), and its associated layered concepts are introduced. In the following Section A.5.4, the Framework and layers are presented, with an analogy and description per layer that defines the purpose for each layer.

Following, in Section A.5.5, the associated design rules, the methodology, a description of the associated XML Schema Definitions and an XML sample are provided for each layer of the STF. These provide guidance to the end users on how the STF design rules and methodology could be applied to transform existing STANAGs or develop new STANAGs in a layered approach and as machine-interpretable STANAG definition.

### **A.5.3.1. STANAG Transformation Framework (STF) Background**

258. As part of the multi-year standards transformation effort, NCI Agency (formerly NC3A) developed, under sponsorship of ACT, the STANAG Transformation Framework (STF) to address the identified problem areas and opportunities captured in Section A.5.2. The STF concepts were first introduced in the RTO sponsored Lecture Series on Interoperability in November 2009 [RTO-IST-088], and has been further enhanced in detail here. The STF is a framework, a set of design rules and a methodology for transforming traditional text-based information exchange STANAGs into an unambiguous, machine-interpretable XML format and providing a layered approach in addressing the needs for maturing the information exchange STANAGs in the areas identified.

259. The standards transformation concept transforms and augments standards by moving towards a more modular composition of the standards differentiating messages structure, data element dictionary, information exchange business rules and other aspects. To fulfil the emerging NNEC requirements, the current standards will be augmented with additional specifications, such as security cross-domain information exchange definitions.

260. Moreover, the transformation of current standards towards machine-interpretable standards is foreseen as part of the standards transformation concept. The expanding exploration and application of XML into the realm of information exchange is viewed as a major step in support of NNEC. An evolving framework for capturing information exchange specifications in XML is a key element in advancing this technology. As that framework matures it is imperative that it adopts a model which fully supports all types of information exchanges, i.e. binary-, text- and XML-based formats. This will improve quality, maintainability and integrity of the standards and therefore contribute to the NNEC Networking and Information Infrastructure (NII) by improving interoperability.

261. A common framework and methodology applicable to all STANAGs, which are related to the technical interoperability between systems/services, was developed. The combination of the two will allow the NNEC Data Strategy goals to be addressed and they will facilitate the implementation of it from a standardization perspective.

### **A.5.3.2. Concepts**

262. Below a number of concepts specific to the STF set of design rules are described.

- **Layered approach:** The purpose of each layer is to offer services to its neighboring layers, avoiding those layers from being affected from changes in the internal details

of their neighboring layers, and from how the offered services are implemented. The linkages between different layers, is regulated by specific interfaces. The principles used in internetworking can be taken as analogy. As a consequence, layers can also be reused or interchanged.

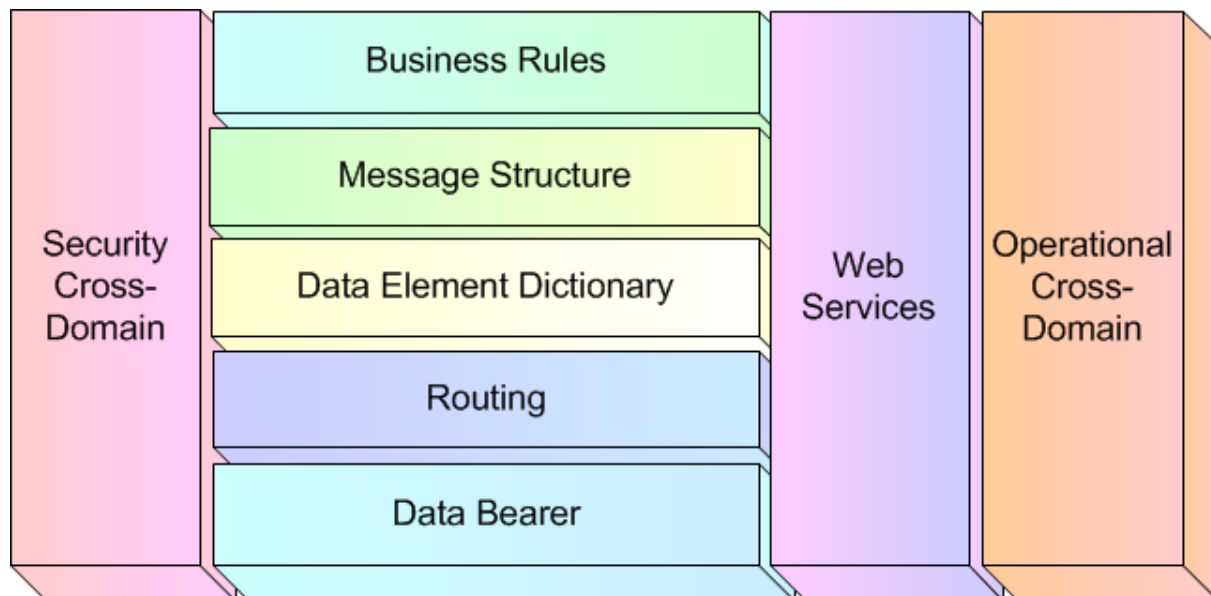
- **Interface:**The place where two different systems interact, normally in accordance with an agreed contract.
- **Human Readable:**A human-readable medium or human-readable format is a representation of data or information that can be naturally read by humans. In computing, human-readable data is often encoded as ASCII or Unicode text, rather than presented in a binary representation. This can also refer to the shorter names or strings that are easier to comprehend or remember rather than the longer, more complex syntax notations, such as some URL strings.
- **Machine Readable:** A machine-readable format or medium of data primarily designed for reading by electronic, mechanical or optical devices, or computers. For example, the binary representation of data used by computers, the UPC barcodes for scanners, or the URL strings.
- **Machine Interpretable:** More than just being readable by machines, machine interpretable data or format contains structured content that can be processed and "understood" by machines.
- **Bit-based:** the information is encoded in a binary representation to optimise bandwidth usage, e.g. Link16 or VMF. This representation is generally not easily human readable.
- **Structured Text-based:** the information is represented as textual values and the structure of the message is governed by other means e.g. line-based and slash delimited like for MTF and OTH-Gold. This representation is typically human and machine readable, but may not be easily machine interpretable.
- **XML-based:** the information is represented as textual values and the structure is governed by an XML Schema Definition (XSD) in line with the [W3C-XML], e.g. MTF-XML or NFFI. This representation is highly machine-readable and machine-interpretable.

#### **A.5.4. STF Layers and Definition**

263. Leveraging the successful application of the layered approach similarly to that of the ISO OSI reference model, the STF is defined using a layered approach to identify and capture the different areas of the information exchange STANAGs that should be specified in order to support various levels of interoperability. The STF layers have been identified based on the analysis of current Information Exchange Requirements and Specifications and emerging requirements for information sharing. The STF defines clear interfaces between the layers, supported by machine-interpretable XML specifications, design rules and a methodology to apply them, in order to support the identification, capture and reuse of specifications within those layers to support information exchange interoperability.



264. The logical view depicted in Figure A.2 provides an overview of the identified STF layers necessary to ensure appropriate data and information dissemination.



**Figure A.2. Layers of the STANAG Transformation Framework**

265. As can be seen, the STF defines five stacked horizontal layers and three vertical layers.

266. The application of the STF layers towards STANAG transformation is based on the intended use and need to support interoperable information exchange within different domains.

267. The horizontal STF layers could be considered Mandatory; their specifications are needed to support interoperable information exchange within a domain. However, a particular system implementation might not need to provide all functionalities described within the STANAG--the functionalities might be implemented by various systems, each playing a different role within the functional scenario. Therefore, the deployment or implementation of a system might cover only a subset of the layers to cover their needs and roles. This way the minimum implementation requirements for each system to achieve interoperability within a functional scenario must specify the requirement to implement parts of each layers to fulfil a specific role in a functional scenario.

268. On the other hand, the vertical layers could be considered Optional specifications based on the intended use and functional scenario. In particular, if it is determined that there is a need to support the exchange of information across different security domains, then the specifications to support that information exchange has to be captured at the Security Cross-Domain layer. If it is envisioned that there is a need to support the exchange of information utilizing web services, then the Web Services specifications have to be captured using the Web Services layer. Finally, if it is deemed necessary to support the exchange of information across operational domains, it is

necessary to map and specify how that information exchange will occur between those domains using the Operational Cross-Domain layer.

269. The horizontal layers leverage concepts that can be loosely mapped to the ISO OSI 7-layer model [[http://en.wikipedia.org/wiki/Iso\\_osi](http://en.wikipedia.org/wiki/Iso_osi)], TCP/IP stack [<http://en.wikipedia.org/wiki/Tcp/ip>] and communication protocol [[http://en.wikipedia.org/wiki/Communication\\_protocol](http://en.wikipedia.org/wiki/Communication_protocol)] specifications.

270. The first two horizontal layers, "Data bearer" and "Routing", deal with physically and logistically "how" the information exchange is occurring between two systems. These two layers can be mapped to the lower 5 layers of the OSI model or the lower 2 levels of the TCP/IP stack, namely the Physical and Data Link layers, and the Network, Transport and Session layers. These deal with getting the data between any two or more systems that need to interoperate with each other.

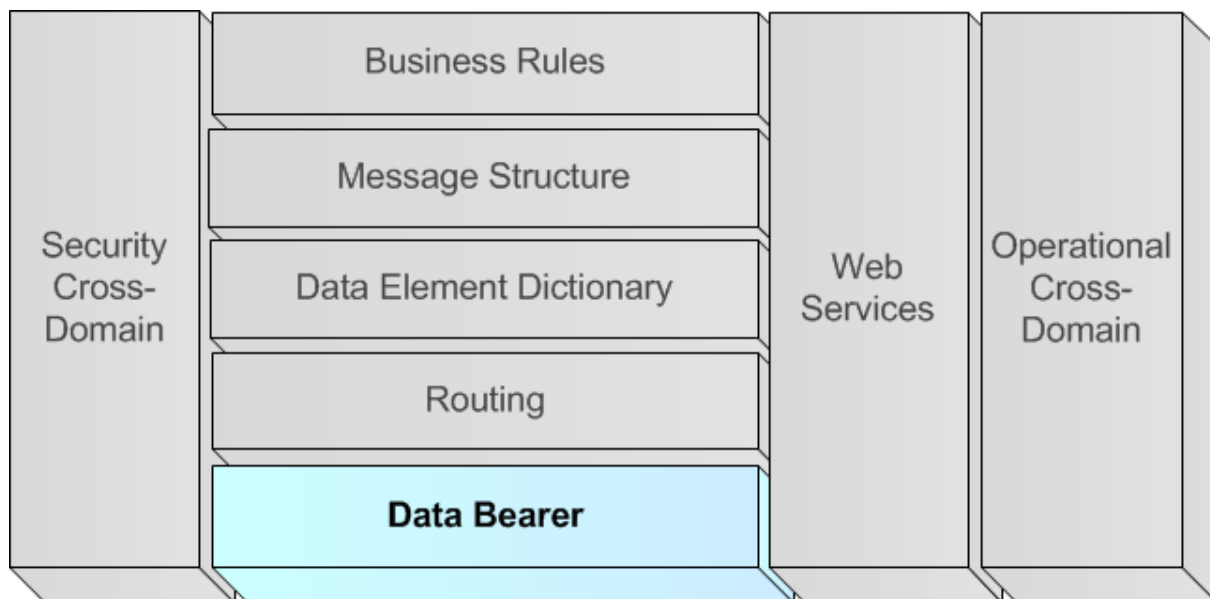
271. The top three horizontal layers defines "what" is being exchanged and the "rules" for exchanging those messages between two or more systems. These layers map loosely to the data definition, data syntax, data semantics and data synchronization concepts used to define communication protocols at the Application layer of the OSI and TCP/IP stack.

- The "Data Element Dictionary" and "Message Structure" define the data representation and syntax of the information exchange which define the context of the information exchange.
- The "TX + RX rules/business rules", focuses on the semantics and synchronization of the data exchange, which defines how to send, receive and interpret the messages so that they make "sense", defining the rules that determine whether the data is meaningful.

272. The STF has been defined in such a way that the layers are generic and applicable to all types of information exchanges. The machine-interpretable XML specifications provide, where required, support for the different types of exchanges by defining a specific adapter of the XML Schema Definition (XSD). In the case of XML-based information exchanges the STF will leverage on the existence of a compliant XSD governing the information exchanges augmented with further required information.

273. The following sections will describe each of these layers starting with an analogy to compare the relevant aspects of automated information exchange with a scenario everyone will be familiar with: natural language communication.

### A.5.4.1. Data Bearer



#### A.5.4.1.1. Analogy

274. The information exchange via a language can be achieved in different ways. The usage of the verbal communication is probably the preferred communication media, either directly in a local discussion or via a transport medium like a phone. Nevertheless, language can also be used to exchange information via textual media (either electronic or paper-based), television and chat.



**Figure A.3. SatCom, Radio, Newspaper, Internet communication bearer**

#### A.5.4.1.2. Definition of Data Bearer layer

275. The data bearer information is composed of the information in the lower 2 layers of the ISO OSI models, which are the physical and data link layers of the OSI network architecture.

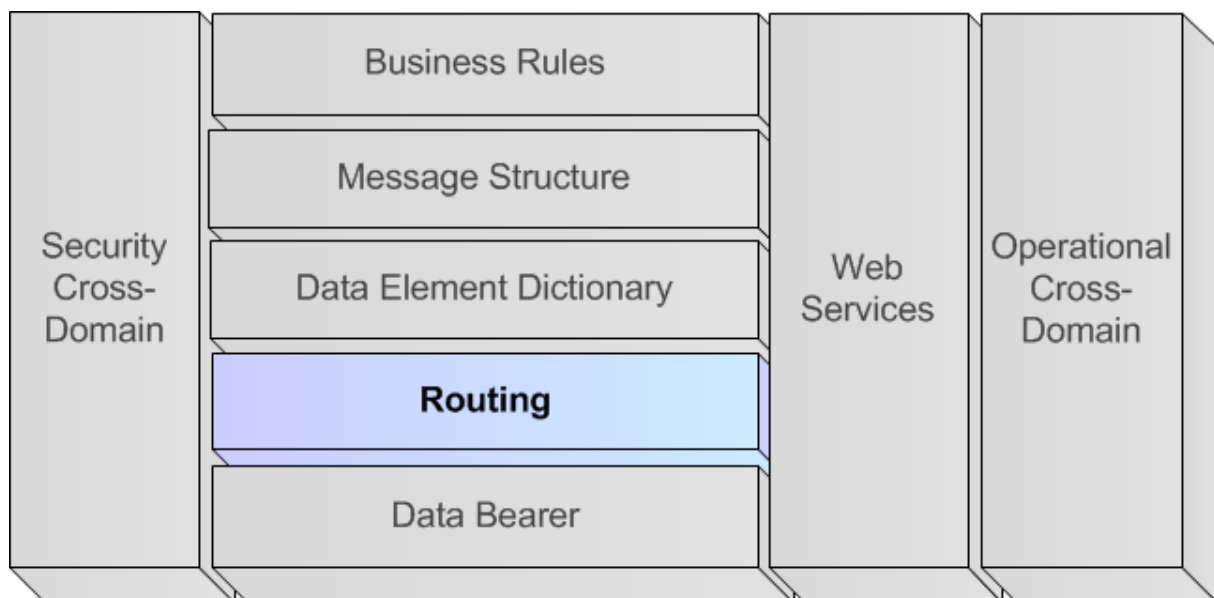
- Physical Layer defines the electrical and physical specifications for devices. In particular, it defines the relationship between a device and a physical medium.

- Data Link Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer.

276. The description within a STANAG of the possible data bearers used within the interfaces is essential to achieve interoperability between system and services.

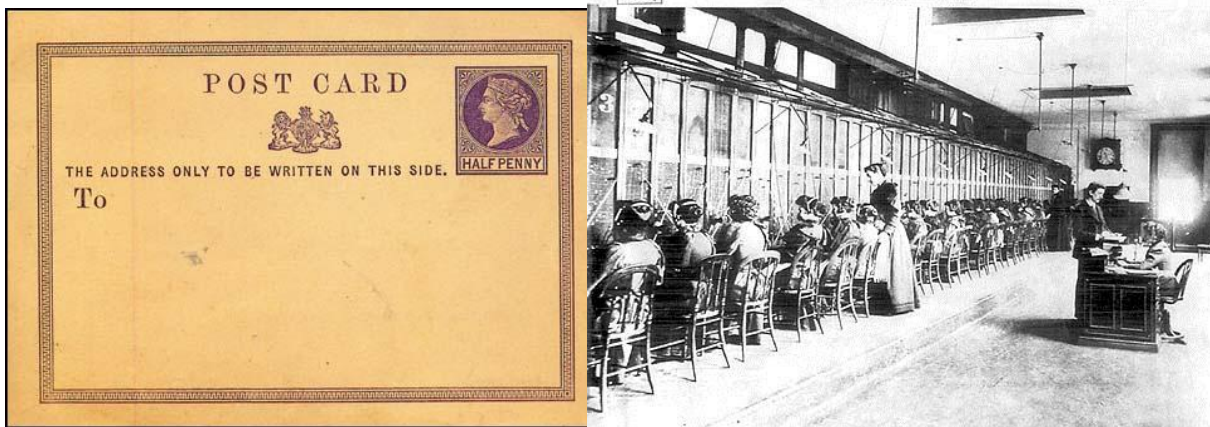
277. In case multiple data bearers can be used for information exchange, all of them have to be described here, including a rationale why the information exchange node should choose one or the other data bearer in specific situations.

### A.5.4.2. Routing (Horizontal Layer)



#### A.5.4.2.1. Analogy

278. *The distribution of information via language is addressed to a specific audience and thus does not occur unconditionally and to everyone. A conversation occurs only in between the participants of the conversation. The chat can be addressed one-on-one or to multiple chat participants, whereas the distribution of the newspaper occurs on a subscription basis.*



**Figure A.4. Britain's first Official Post Card,  
the first commercial telephone switchboard**

#### **A.5.4.2.2. Definition of Routing layer**

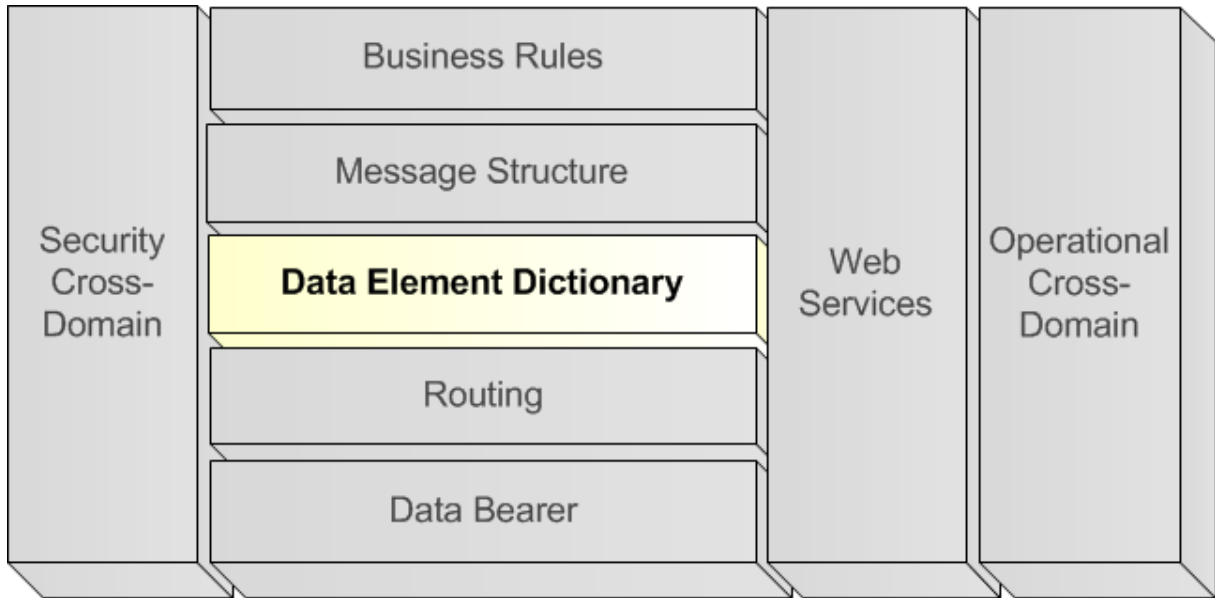
279. The Routing layer overlaps with the 3rd, 4th and 5th layers of the OSI reference model for network communication, which is typically referred to as the Network, Transport & Session layers.

- Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks, while maintaining the quality of service requested by the Transport Layer. The Network Layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors.
- Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. This Layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. This Layer can be thought of as a transport mechanism, e.g., a vehicle with the responsibility to make sure that its contents (passengers/goods) reach their destination.
- Session Layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures.

280. The routing of the information dissemination between two or more parties needs to be explicitly captured within STANAGs.

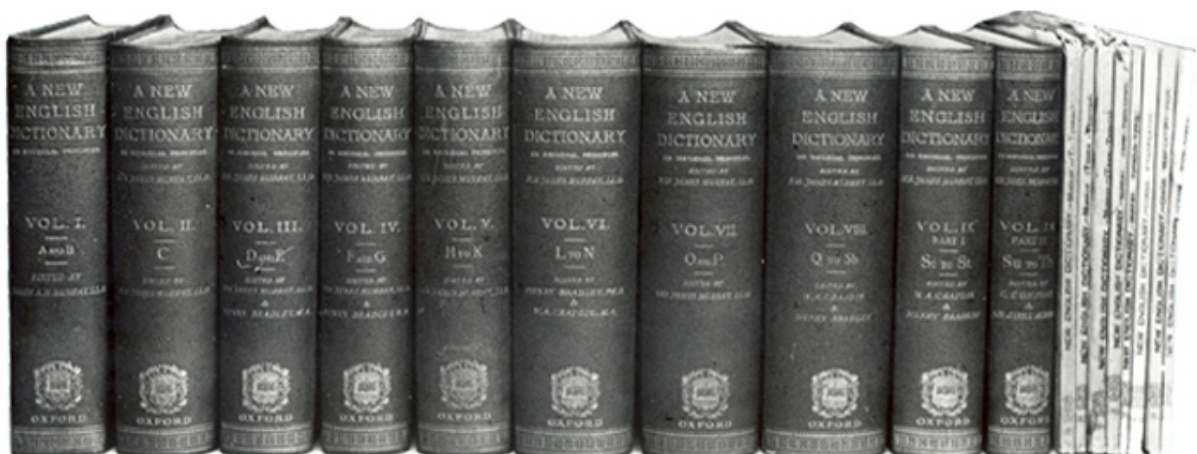
281. Current technology defines the routing of information in heterogeneous ways, which tend not to be interoperable. A lack in specifying the routing mechanism will lead to interoperability issues. In case multiple routing algorithms can be used for information exchange, all of them have to be described within the STANAG, including a rationale why the information exchange node should choose one or the other routing mechanism in specific situations.

### A.5.4.3. Data Element Dictionary (Horizontal Layer)



#### A.5.4.3.1. Analogy

282. *The definitions of words within a language are captured in a dictionary, where each word can have one or multiple meanings in that language. Sometimes the meaning is explicitly stated in the dictionary, in other cases, the meaning of the word is associated with non-verbal communication or tonality of pronunciation. The meaning expressed by a word within a certain language, can be expressed by multiple words within the same language and in other languages.*



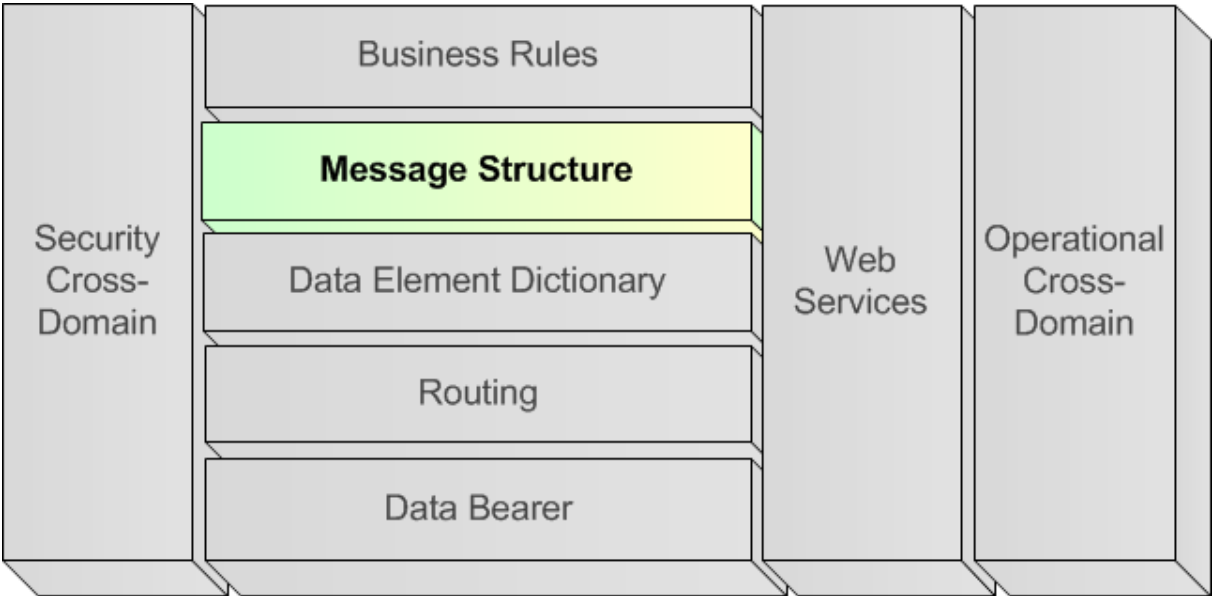
**Figure A.5. Data Element Dictionary**

**A.5.4.3.2. Definition of Data Element Dictionary layer**

283. Within an information exchange STANAG, a data element is the atomic unit of data that has a precise meaning and precise semantics for that domain. Such a data element can be stored or exchanged among computer systems. The catalogue containing all Data Elements within a certain domain is called a Data Element Dictionary (DED) for that domain.

284. It has to be stressed that proper and clear data element definitions [[http://en.wikipedia.org/wiki/Data\\_element\\_definition](http://en.wikipedia.org/wiki/Data_element_definition)] are critical for external users of any data system, since a good definition can ease the process of data element harmonization, where one set of data elements are mapped into another set of data elements.

**A.5.4.4. Message Structure (Horizontal Layer)**



**A.5.4.4.1. Analogy**

*285. Providing words in a non-structured way will pass only very limited information. Every communication language defines the grammar to construct sentences and therefore disseminate the information in an understandable way, to whoever knows the words and the language grammar. The human is capable of interpreting, assuming and correcting grammar mistakes, and thus understanding the information even if not completely properly structured.*



**Figure A.6. Message Structure**

#### **A.5.4.4.2. Definition of Message Structure layer**

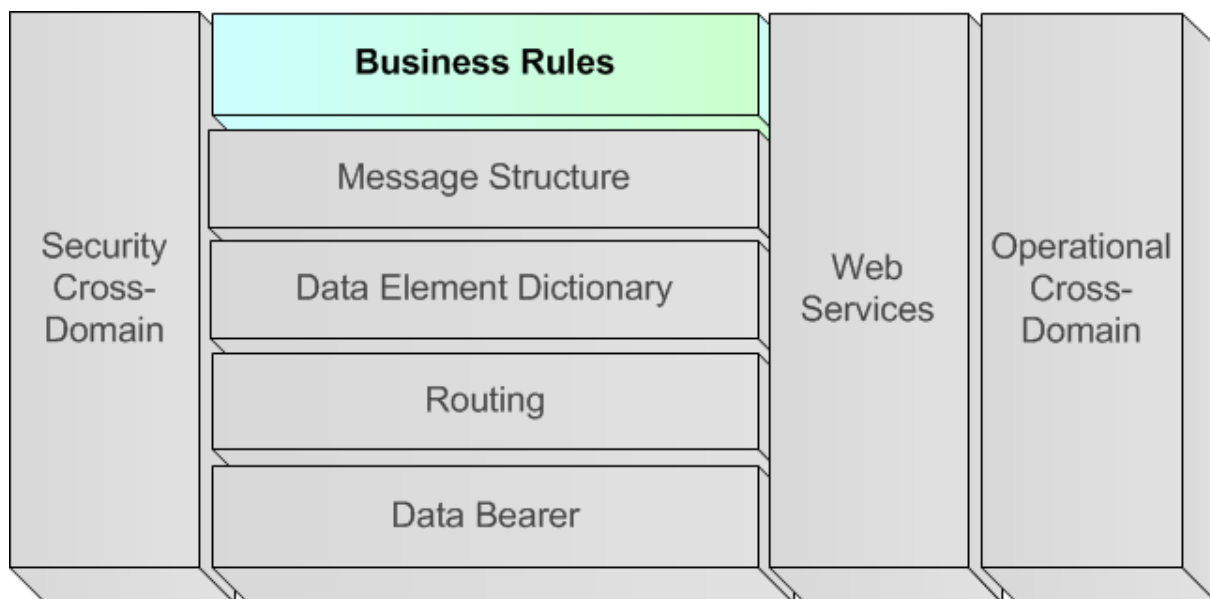
286. To ensure interoperability between systems, it is essential that the data exchange is conforming to specific syntax rules. This syntax is called the message structure, which defines:

- A packaging of one or multiple levels of data elements into logical and/or functional groups, and;
- The sequencing of data elements within each functional and/or logical group.

287. A proper structure will enable the association of data elements with each other, in order to support the binding of data to certain functional or logical objects. For example, the exchange of an altitude without context expresses less information than the exchange of an altitude related to a certain object. By using multiple level packaging, information about multiple objects, or even sub-objects, might be exchanged within one message.

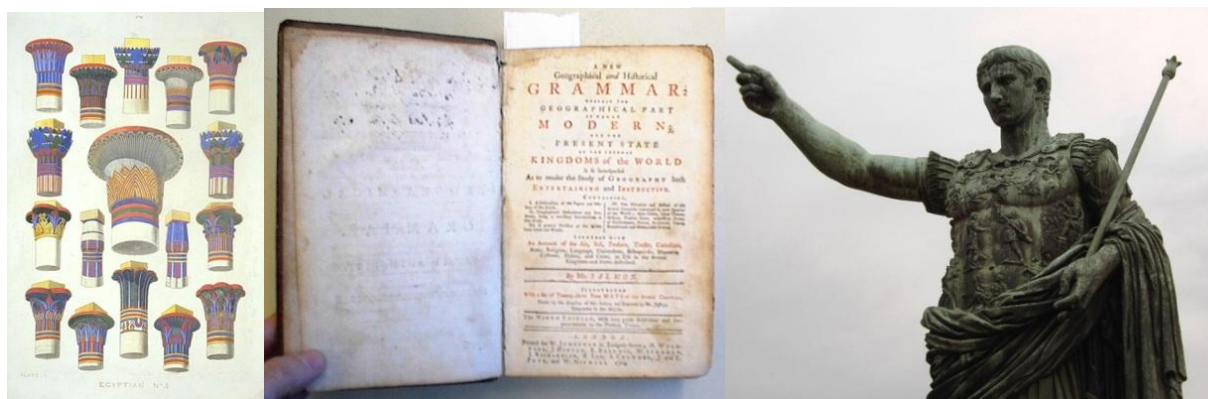


### A.5.4.5. Business Rules (Horizontal Layer)



#### A.5.4.5.1. Analogy

288. *"The Grammar of Ornament", a "new geographical and historical grammar" (London, 1764) and "Augustus as Ruler of Rome" summarize the explicit and implicit aspects of a dialogue. Knowing the available words and the valid sentences (see grammar of the language) that can be formed using these words, does not imply the capability to participate in dialogue. A dialogue follows explicit and implicit rules; if a question is asked, a related answer is expected, if a statement is made, a related statement or follow-up is expected.*



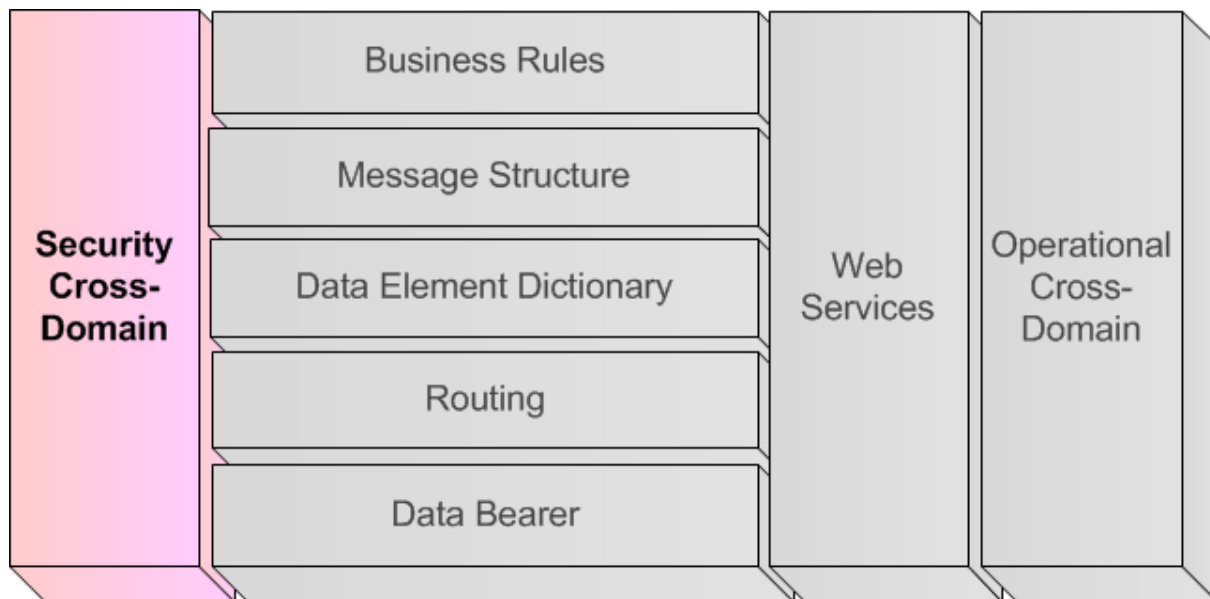
**Figure A.7. Implicit and explicit parts of a dialogue**

#### A.5.4.5.2. Definition of Business Rules layer

289. While the Message Structure and Data Element Definition (DED) provide the more static description of the way messages are constructed and how data elements are coded, the business

rules / transmission reception rules aspect of the standard is defined as what behaviour a system should follow when handling the messages, the interaction with an operator or with the underlying system (e.g. its sensors' output). The business rules / transmission reception rules describe the dynamics of an automated message handling system.

### A.5.4.6. Security Cross-Domain (Vertical Layer)



#### A.5.4.6.1. Analogy

290. *The human tailors the type of information he provides to the audience and to the context, withholding information that is not releasable to (a part of) that audience or in that specific context.*

291. *In a conversation a party can put explicit constraints on the further distribution of provided information. The judgement, whether or not to share information is based on specific rules (e.g. need-to-know principle, personal in confidence attributes) but also on perception.*



**Figure A.8. Past, Current and future security mechanisms**

#### **A.5.4.6.2. Definition of Security Cross-Domain layer**

292. The Security Cross Domain takes into account recommendations provided in Bi-SC Secure C2 Data Strategy with security requirements aspects being subdivided into two categories:

- Requirements for information exchange within the classification at the same level (important if connected to unsecure networks like the Internet), and
- Requirements for the security cross-domain functionalities.

293. The latter can be omitted in case only a single security domain is involved.

294. For security requirements within a homogeneous security domain, the security aspects might contain:

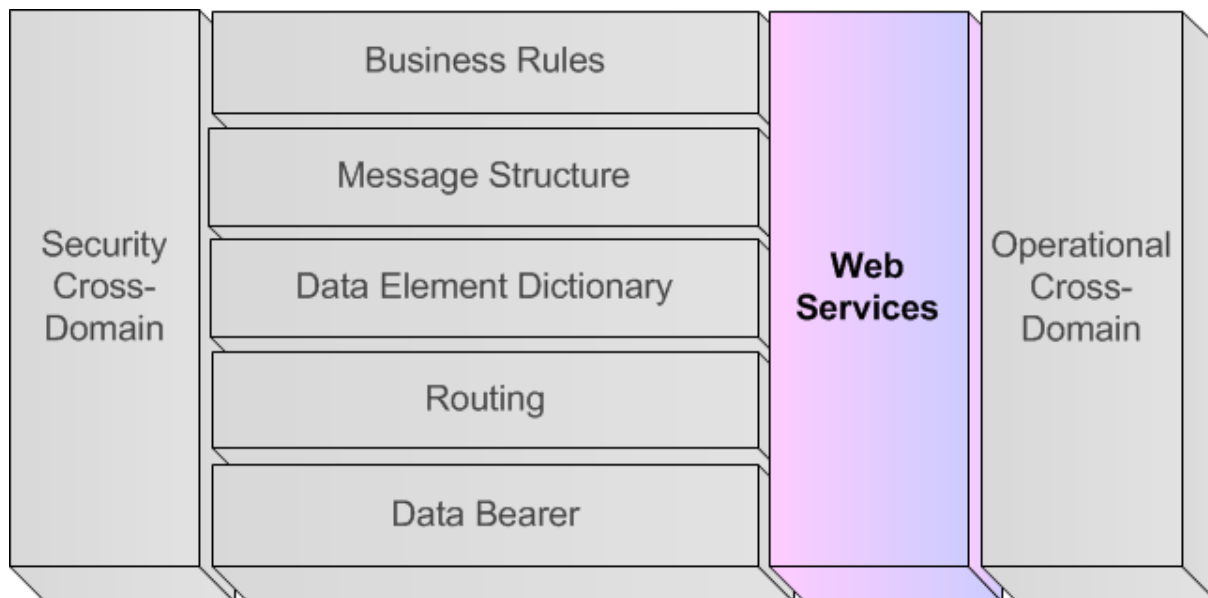
- Information on security related protocols / services (HTTPS).
- Information on data source authentication and authorisation.

295. For cross-domain security, the aspects might contain;

- Appropriate security labeling (in-line with NATO standards [NAC-INFOSEC] and recommendations [RTO-XML-2008] [RTO-XML-2009]) including the specification of what information should be considered classified (at what level) and what information should be considered unclassified
- Possible rules for sanitization of data, defining the manner to downscale the classification of information, e.g. information might be classified during a certain operation or exercise, but unclassified after the operation finished. Sanitization rules should be used to define this.
- Information integrity: If information is labeled with the purpose to exchange it cross-security domain, the boundary device should be able to verify that the information has been labeled

by a trusted device, and that nobody tampered with the label or the data in between the labeler and the boundary device (e.g. Public Key Identifier (PKI)).

### A.5.4.7. Web Services (Vertical Layer)



#### A.5.4.7.1. Analogy

296. *The presence and the wellness of a person, imply that the person is in the position to provide the information in his hands. In addition to being aware of the presence of a person, one should also recognize the person (knowing the person) and know for example his profession or the type of information he can provide, in order to collect useful information from that person. Moreover, a person can attend a meeting for multiple purposes: learn (listening only), actively contribute (active dialogue) or provide information (giving a presentation).*

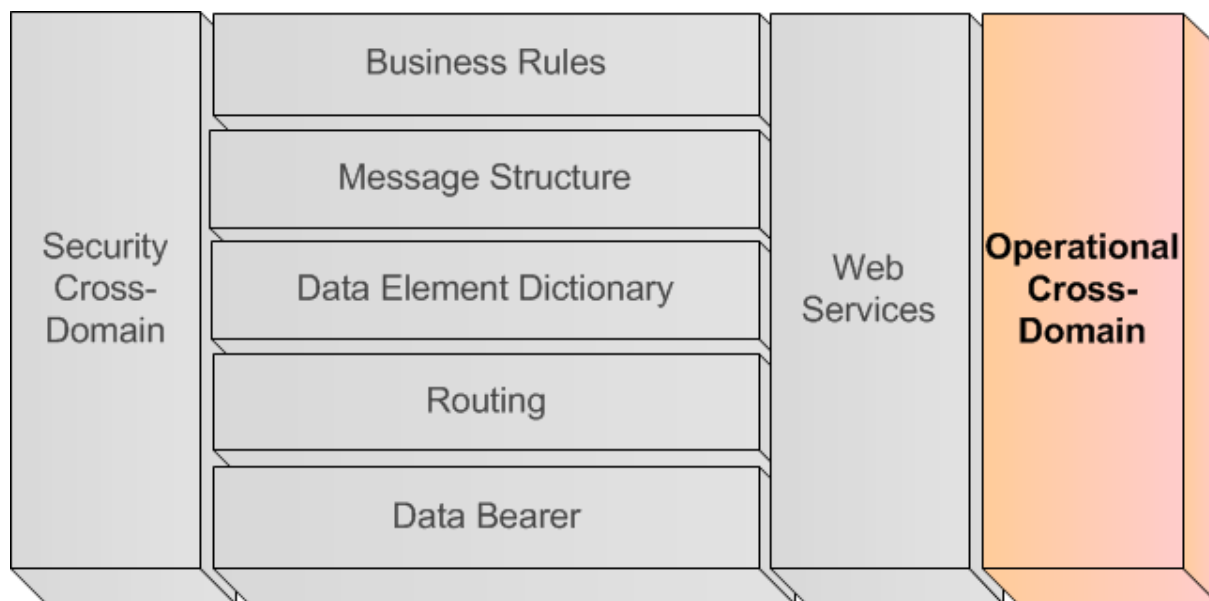
#### A.5.4.7.2. Definition of Web Services layer

297. The web services specification chapter will mainly be used when the information exchange can take place via web-services. The web-services description will contain at least the following components:

- Information exchange scenarios for the Service Oriented Architecture information exchange (containing information on whether data will be pulled or pushed, using mechanisms like publish-subscribe, request-response, etc.).
- A detailed description of the web-services interface, defining the methods that can be called, arguments to be provided and answers to be expected. This part might refer to schemas and WSDL file.

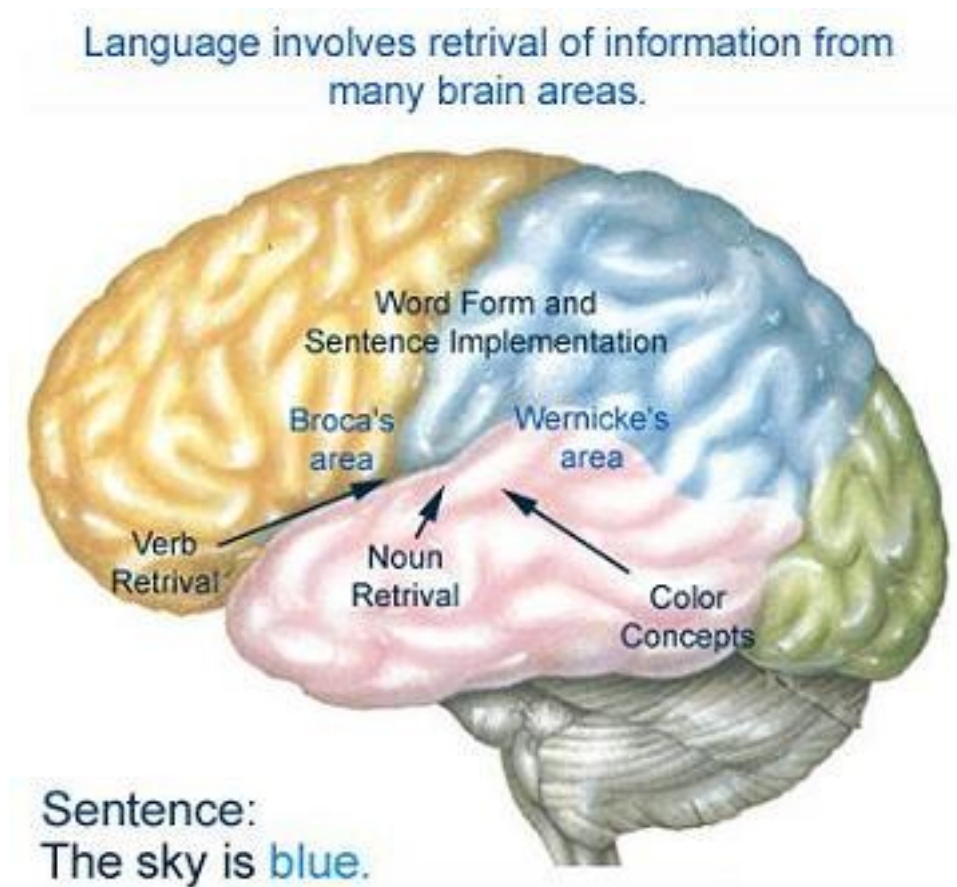
- The Service Metadata specification, which will contain the description of the services based on a set of metadata containing useful information for all COIs, to enable the discovery of the information providers.

### A.5.4.8. Operational Cross-Domain (Vertical Layer)



#### A.5.4.8.1. Analogy

298. *Within the usage of a common language such as English, different users will develop their own vocabulary and associated specific meaning to words related to their core business. If a patient with a basic knowledge meets a doctor and the doctor does not adapt his vocabulary (medical terminology) to the daily vocabulary, the patient will not really understand what the doctor says. Sometimes the patient might have the perception to understand the doctor since he has a vague idea of the meaning of medical terms, but for sure he will not grasp the details. Moreover, a person visiting a foreign country needs a translator to help him communicate with the local people in case he does not speak the local language. Unfortunately, in most of the translations, a loss of information and meaning will occur.*



**Figure A.9. Human Association between different information**

#### **A.5.4.8.2. Definition of Operational Cross-Domain layer**

299. Many information exchange STANAGs are normally developed with usage limited to one specific Community of Interest (COI), leading to the development of ad-hoc vocabularies to fulfil their immediate requirements. The data elements definitions are specifically oriented to the COI with direct impact on quality within the COI specific network and interoperability with other COI specific systems, with little to no consideration of existing STANAGs within or between other COIs.

300. This typically results in a lack of interoperability both within the COI (because of the availability of multiple COI specific standards) and between COIs.

301. The Operational Cross-Domain layer is provided to capture those information exchange specifications between COIs or STANAGs at the necessary levels as identified in the horizontal layers.

302. For example, the data elements defined within two COIs' information exchange specifications could be fully overlapping, disjointed or partially overlapping. It is essential

to associate these data elements and their relationships based on the context and content of the information exchange in order to achieve interoperability between the COIs. The mapping and harmonization of semantically the same data elements and the association of similar data elements has to be captured.

### **A.5.5. STF Design Rules & Methodology**

303. In this section, for each layer of the STF, the design rules are provided together with a description of the supporting XML Schema Definition with examples, followed by the methodology of applying the design rules and utilizing the XML Schema Definition.

304. For STF Version 1.0, the STF Design Rules & Methodology section is scoped to the following:

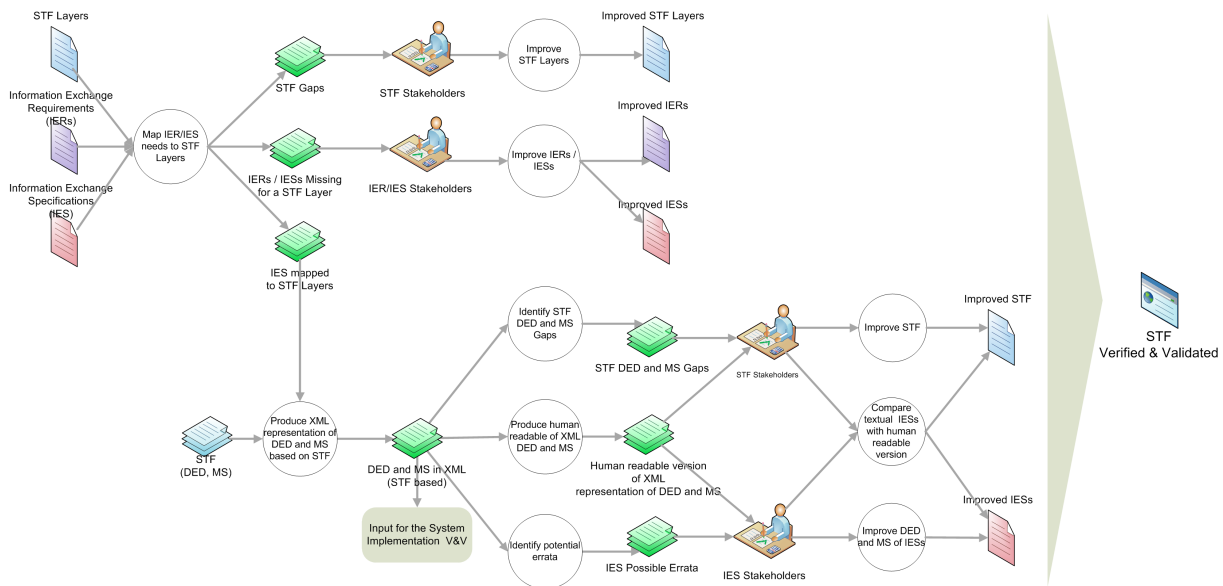
- Data Element Dictionary (DED):
  - Bit-based
  - Structured text-based
- Message Structure (MS):
  - Bit-based, Fixed-length

305. For plans for the STF Design Rules, please consult Section A.12.

#### **A.5.5.1. STF Holistic Process**

306. The definition, application and V&V of the STF layers, design rules and methodology is an on-going process that is handled by the iterative process captured in Figure A.10. This is a Holistic Process that can be applied to the STF itself as well as for the application of the STF in transforming textual IESs into XML. There are explicit points identified for feedback to the STF and IER/IES Stakeholders for possible improvements of their products.

307. For STF Version 1.0, the STF Holistic Process is depicted below. It is anticipated that this Process will be expanded for future versions as additional STF layers are matured and provided. For example, once the Business Rules layer has been expanded upon, an additional step will have to be added to cover that layer.



**Figure A.10. STF - Holistic Process**

308. The STF Holistic Process is detailed in the rigorous steps below:

- **Map IER/IES needs to STF Layers.** Analyze the IERs with regards to the STF layers to identify the need for specifications at those layers (i.e. if there is a requirement to exchange the Information Product via Web Services, then a specification for the Web Services STF layer would be necessary). Based on these needs, identify existing Standards (IESs) that could fulfill those needs. With the STF layered approach, one may find that the same IESs can be reused to fulfil multiple types of IERs as well as find that there will be missing IESs that need to be developed to fill gaps in the STF layers for that IER. The findings can be analysed and corrective actions can be taken by the appropriate stakeholders. In particular, possible outcomes of this step could include the following:
  - Identified STF gaps where no STF Layer captures IER/IES needs, which should be captured and forwarded to the STF Stakeholders for the possible opportunity to **Improve the STF**.
  - Identified IES gaps where no Standards could be found for a particular layer, which should be captured for submission to the appropriate IER/IES Stakeholders for analysis. Results could be the possible opportunity to **Improve current Standards** with the adoption of existing IESs to close the gap or lead to the development of new IESs.
  - Identified IESs to fulfil each identified STF Layer needed to fulfil IER. For the IESs that specify the format and message structures of the information exchange,
- **Produce XML representation of DED and MS based on STF.** Apply the STF XML schemas at the DED and MS Layers to capture the valid data elements that can be exchanged as part of the information exchange, the order in which they can occur,



and constraints on certain aspects of these message exchanges in XML representations. Outcomes of this step could include the following:

- Identified problems/gaps within the STF XML schemas for sufficiently capturing the information exchange DED and MS, which should be captured and forwarded to the STF Stakeholders for the possible opportunity to **Improve the STF**.
- Identified problems within the textual IESs, which should be captured as Possible Errata for submission to the appropriate IER/IES Stakeholders for the possible opportunity to **Improve the Standards**.
- XML files of transformed Standards. Once the Standards have been transformed into XML, the XML files have to be V&V'd to ensure they properly capture the existing IES. Using existing XML Technology and Tools, one is able to perform the following V&V steps on the resultant XML files:
  - **Automatic Conversion to Human-Readable Formats.** Automatically produce the equivalent human-readable documents from the XML files to be provided to the IES Stakeholders to be analyzed for correctness. Results of this could be exploited to **Improve the Standards**.

### **A.5.5.2. Data Bearer Design Rules & Methodology**

309. Not yet addressed within the current version of the STF.

### **A.5.5.3. Routing Design Rules & Methodology**

310. Not yet addressed within the current version of the STF.

### **A.5.5.4. Data Element Dictionary Layer Design Rules & Methodology**

311. The purpose of the Data Element Dictionary layer is to capture the data elements, or vocabulary, of the Information Exchange STANAG.

312. In general, there are different types of Information Exchanges that can occur which can be categorized based on the way the data being exchanged between systems is represented. In particular, within the STF, the following three types have been identified-- bit-based, text based and XML-based, the last being a highly-structured text based information exchange.

313. The STF Data Element Dictionary layer has been defined in such a way that it is applicable to all types of information exchanges. The machine-interpretable STF-related XML specifications provide, where required, support for the different types of exchanges by defining a specific adapter of the XML Schema Definition.

### A.5.5.4.1. DED Concepts

#### 314. ISO/IEC 11179 Data Modelling

315. As considered by ISO/IEC 11179, there are three main relationships related to semantic theory and the basic principles of data modelling that should be addressed when identifying, defining and grouping data elements. These are the following:

- Between generic and more specific concepts (e.g. "Altitude" vs. "Altitude in 25 FT increments above MSL")
- Between a concept and its terminology (e.g. "Location" vs "Position")
- Between a concept and its usage/context (e.g. "Latitude" + "target" = "Latitude of target")

316. Within STF, the first two relationships are captured within the Data Element Dictionary layer. The third relationship can be captured either in the Data Element Dictionary or in the Message Structure layer (see below).

#### 317. Usage vs. Context

318. In Merriam-Webster online dictionary, the word context [<http://www.merriam-webster.com/dictionary/context>] can refer to two slightly different, but related meanings:

- the parts of a discourse that surround a word or passage and can throw light on its meaning
- the interrelated conditions in which something exists or occurs : environment, setting

319. Within STF, the context, or the third data modelling relationship, can be captured either explicitly as a different Data Element or implicitly as a data field within the Message Structure layer. The reason for this is that, often, the specific meaning of a Data Element could be provided by how it is being used (i.e. Latitude of target vs Latitude of shooter). However, the context could also describe the environment in which the data element exists (i.e. Latitude is a data field within the Target Position Message). This could be considered a different usage, hence a different Data Element, but not necessarily so.

320. Furthermore, the type of Information Exchange may have impact on the way the Data Element Concept and Data Elements are defined as e.g. the different representations of bit-based Information Exchanges might be considered different uses.

321. For the purpose of the STF and to support reuse and data harmonization, it is highly recommended that the end user captures the context relationship within the Message Structure layer rather than as an explicit data element.

#### 322. Data Element Concept/Data Elements

323. These are two related concepts within the STF Data Element Dictionary layer that capture the first two relationships. The **Data Element Concept** maps to the generic, "conceptual" concept while the **Data Elements** map to the more specific, "concrete" concepts. In particular,

the Data Elements in the STF DED are organised based on a thesauri, in support of the Data Coherence goal of the NNEC Data Strategy, whereby the Data Element Concepts group together semantically equivalent data elements that might be represented within a STANAG using different terminology and/or granularity. Different possible instantiations of a Data Element Concept are described with the use of one or more Data Elements.

#### 324. **Data Element**

325. A Data Element captures a specific concept with a specific representation, and possibly with a specific usage. It is the atomic unit of data that has a precise meaning and precise semantics for that domain. Such a data element can be stored or exchanged between computer systems.

326. Some important Data Element properties:

- Data Elements are instantiated in the context of a message as a Data Field (see further 5.5.4) in the Message Structure layer.
- As defined, Data Elements are atomic units of data, and therefore are unstructured (e.g. non-complex types). To capture parent-child relationships, data elements should be instantiated as data fields within a Word of a Message Structure.
- Data Elements provide the information on how to handle and interpret the value as exchanged, i.e. how to decode the value as transmitted to something meaningful for computers or humans and how to encode such meaningful value to the representation for transmission. This is similar to the "serialization" concept in information systems.
  - For example, the exchange representation might be some binary or string value, for which the meaningful value might be the altitude in meters or the country name.
- The coding information of a Data Element can specify a mapping between exchanged values and the real values, e.g. mapping the text value NL to The Netherlands for a text-based Information Exchange or mapping the numerical value 3 to FRIEND for a binary Information Exchange.
- For numerical Data Elements, the specification can include a conversion method from the exchanged representation to the meaningful value, e.g. a binary value might indicate the altitude in multiples of 10 meters.
- Additional information is captured on the meaning of the Data Element, e.g. in the case of numerical values which unit the value has (degrees, data miles, meters, etc) and which type (integer or floating point number, boolean, etc).
- In the situation where the coding of a Data Element depends on the value of another Data Element, the DED provides a construct called a CodingSwitch | Coding Switch. The Coding Switch construct allows to capture explicitly which other Data Element (actually, the instantiated Data Field version) should be inspected and depending on its value how the

first Data Element should be decoded/encoded. For example, a Scale Indicator Data Element might control that the Altitude Data Element is reporting the altitude in multiples of 100 or 500 feet increments. This construct is especially used in the binary information exchanges for space optimization.

327. Within the STF, a data element [[http://en.wikipedia.org/wiki/Data\\_element](http://en.wikipedia.org/wiki/Data_element)] is composed of and defined by:

- An identification including the data element name [[http://en.wikipedia.org/wiki/Data\\_element\\_name](http://en.wikipedia.org/wiki/Data_element_name)] and a unique identifier:
  - The name given to the data element within the context of the STANAG, not necessarily unique although recommended.
  - The unique identifier is used to uniquely refer to the Data Element within the context of the STANAG.
- A clear data element definition [[http://en.wikipedia.org/wiki/Data\\_element\\_definition](http://en.wikipedia.org/wiki/Data_element_definition)]:
  - A human readable phrase or sentence associated with the data element within a data dictionary that describes the meaning or semantics of a data element.
- One or more representation terms [[http://en.wikipedia.org/wiki/Representation\\_term](http://en.wikipedia.org/wiki/Representation_term)]:
  - A word, or a combination of words, that semantically represent the data type (value domain) of a data element.
- Optional enumerated values:
  - System of valid symbols that substitute for longer values ISO/IEC 11179 [[http://en.wikipedia.org/wiki/ISO/IEC\\_11179](http://en.wikipedia.org/wiki/ISO/IEC_11179)].
- An optional list of synonyms to data elements in other STANAGs or Metadata Registries:
  - Data elements that are considered semantically equivalent for the purposes of information retrieval.
- Optionally, additional metadata depending on the type of information exchange.

328. It has to be stressed that proper and clear data element definitions [[http://en.wikipedia.org/wiki/Data\\_element\\_definition](http://en.wikipedia.org/wiki/Data_element_definition)] are critical for external users of any data system, since a good definition can ease the process of data element harmonization, where one set of data elements are mapped into another set of data elements.

### 329. **Data Element Concept**

330. The Data Element Concept is the agreed upon term for a generic concept used to represent a set of common data elements.

331. Within the STF, a data element concept is identified by:

- The Name given to the Data Element Concept within the context of the STANAG, not necessarily unique although recommended
- The Data Element Concept Identifier, which is the unique identifier used to refer to the Data Element Concept within the context of the STANAG.

**332. Data Element Dictionary**

333. A collection of data element concepts and associated data elements that are used to specify the message exchange. Within STF, the XML file containing all Data Elements within a certain domain is called a Data Element Dictionary (DED) for that domain.

**334. Data Element Concept/Data Element Identification (DECI/DEI)**

335. To promote reuse, to ease harmonization and to provide meaning to the data elements, it is necessary to be able to uniquely identify each Data Element in an explicit and unambiguous way. Each Data Element Concept is identified by a numerical ID, **data element concept identifier (deci)**, unique within the particular dictionary and each Data Element is identified by a numerical ID, **data element identifier (dei)**, unique within a Data Element Concept.

336. The combination of the DECI/DEI values is used to uniquely reference a particular Data Element. This approach can be easily mapped on that used by various other communities to reference Data Elements, for example:

- the MTF community uses the FFIRN/FUD (Field Format Index Reference Number/Field Use Designator)
- the TDL community uses the DFI/DUI (Data Field Identifier/Data Use Identifier)

**337. Data Element Concept/Data Element Examples**

338. The following table provides some examples of Data Element Concepts and Data Elements.

**Table A.7. Examples of Data Element Concepts and Data Elements**

<b>Data Element Concept</b>	<b>Data Elements</b>
Altitude	Altitude in 25 FT increments, Altitude in 100 FT increments
Heading	Wind direction, Course
Latitude	Latitude (accurate in 0.04 minutes), Latitude (accurate in 0.005 minutes)
Platform	Air platform, Surface platform, Subsurface platform, Land platform, Space platform

### A.5.5.4.2. Data Element Dictionary Logical Model

339. This logical model shows the relationship between these concepts to support the definition of a generic data element dictionary to be used for information exchanges. The attributes shown in the classes denote relevant information that needs to be captured on the classes or indicate a relationship between classes (e.g. dei).

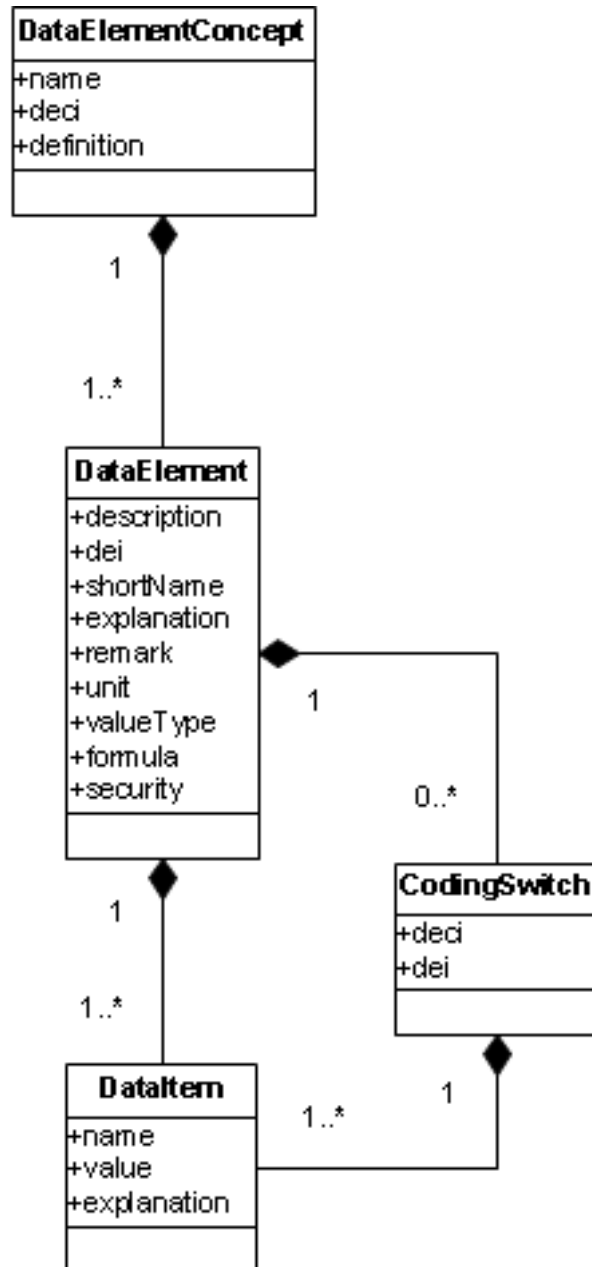


Figure A.11. Data Element Dictionary Logical Model

340. The Data Element Dictionary XML Schemas are derived from this logical model, fully elaborated to include all components (elements and attributes) that are required to model the generic data element dictionaries for all types of information exchanges.

### A.5.5.4.3. Known Limitations

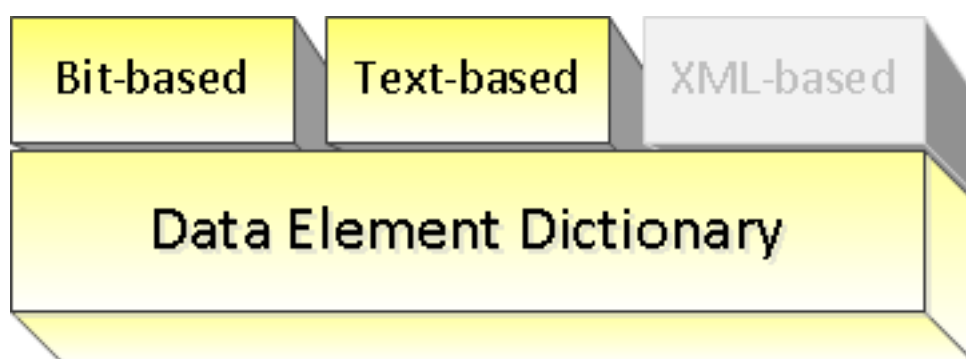
341. There are some known shortcomings in Version 1.0 of the STF Data Element Dictionary XML Schemas and Logical Model in supporting all types of information exchanges. These are described here:

- The logic behind a Formula is not represented in machine-interpretable XML and is therefore still open for interpretation by developers etc. Alternatives are defining standard Formulas (stored in a catalogue) which can be referenced from the data elements. The standard Formula can use XML elements to describe e.g. simple mathematical operations (e.g. multiplication with a certain factor). More complex operations (e.g. for positional information like latitude and longitude) will require more work or maybe even external references.
- The Unit of a DataElement is defined as a simple string (e.g. "METER", "SECOND", "DATAMILE") without any restriction or coupling to external standards. Whenever there is a standard defining such unit there should be a way to link to that.

342. These are being considered although not yet planned for the next version of the STF Design Rules.

### A.5.5.4.4. DED Design Rules

343. Based on the type of information exchange and data representation of the Data Elements, a specific adapter (extension) of the common Data Element Dictionary XML Schema (DataElementDictionary-\*.xsd) shall be used to capture the Data Elements in an XML representation to fulfil the Data Element Dictionary layer of the STF.



**Figure A.12. Data Element Dictionary**

344. Below are the design rules with the methodology on how to apply them to create the STANAG-specific XML file that captures the data element dictionary for a particular information exchange:

345. Rule 1: The DataElementDictionary-BitBased.xsd shall be applied in case the Information Exchange is bit-based, e.g. GMTI, Link16, DIS.

346. Rule 2: The DataElementDictionary-TextBased.xsd shall be applied in case the Information Exchange is based on structured text, e.g. MTF.

347. Rule 3: (Future work) - The DataElementDictionary-XMLBased.xsd shall be applied in case the Information Exchange is based on XML. *This XSD is not provided within the current version of the STF.*

#### **A.5.5.4.5. Methodology for Data Element Dictionary definition**

348. Step 0: Based on the process in place for defining the IES, like [APP-15], decide on the required type of message exchange being bit-based, text-based or XML-based.

349. Step 1: Data Elements Guidance|Identify all Data Elements, being the atomic units of data required for the information exchange.

350. As you are identifying your Data Elements, start to group similar data elements together that share the same functional concept, but have different representation or view. For instance 'Latitude Degrees Minutes Seconds' and 'Latitude Decimal Degrees' both share the same concept 'Latitude', but are expressed by using different data representation types.

351. Step 2: For each Data Element, define the following:

- Identification:
  - Typically the name of the data element as defined in the STANAG, e.g. "latitude" from NFFI or "Country Code" from APP-6A. If the STANAG defines similar data element concepts with the same formats, but use different "labels" or "names" for them, such as "Identification" vs. "ID", they should be defined using the same data element.
  - Assign a Data Element Concept Identifier (number) and a Data Element Identifier (number), consulting the custodian for guidance.
- Data element definition:
  - Text that describes the meaning or semantics from the data element, e.g. "Angular distance north or south of the earth's equator measured in decimal degrees WGS-84" or "Identifies the country with which a symbol is associated"
- Representation terms:
  - Semantically represents the data element covering the data type and, if applicable, the unit, e.g. for a latitude specify double as type and decimal degrees as unit, or specify for Country Code string as a type and no specified unit.
- Enumerated values:



- The list of mappings between symbols and their meaning, if applicable.
- Synonyms:
  - Identify data elements within other STANAGs or meta data registries that are interchangeable in the context without changing the truth value of the proposition in which they are embedded

352. Step 3: If defining a new Data Element, verify whether an existing Data Element can be reused by consulting the preferred data element within the meta-data registry (see Data Elements Guidance| Data Harmonization).

353. Step 4: Depending on the type of information exchange, additionally define the following:

- For bit-based information exchange:
  - Specify the length in bits of the Data Element for exchange
  - For numerical data elements, specify the used bit-coding which captures how a value is represented in binary, in particular relevant for signed numbers (e.g. unsigned, twos-complement, ...).
- For text-based information exchange:
  - Specify the character set allowed for exchange, e.g. only "alphanumeric and dash" and/or a regular expression specifying what values are allowed
  - Specify the minimum and/or maximum length in characters, e.g. 10-30
- For XML-based information exchange:
  - It is supposed that an XSD is defined within the STANAG that defines the XML data elements. If this is not the case, first define this XSD.
  - With respect to the data element dictionary, map every Data Element Concept to the corresponding XML element in the XSD.
  - More specific steps will be provided in STF version 2.

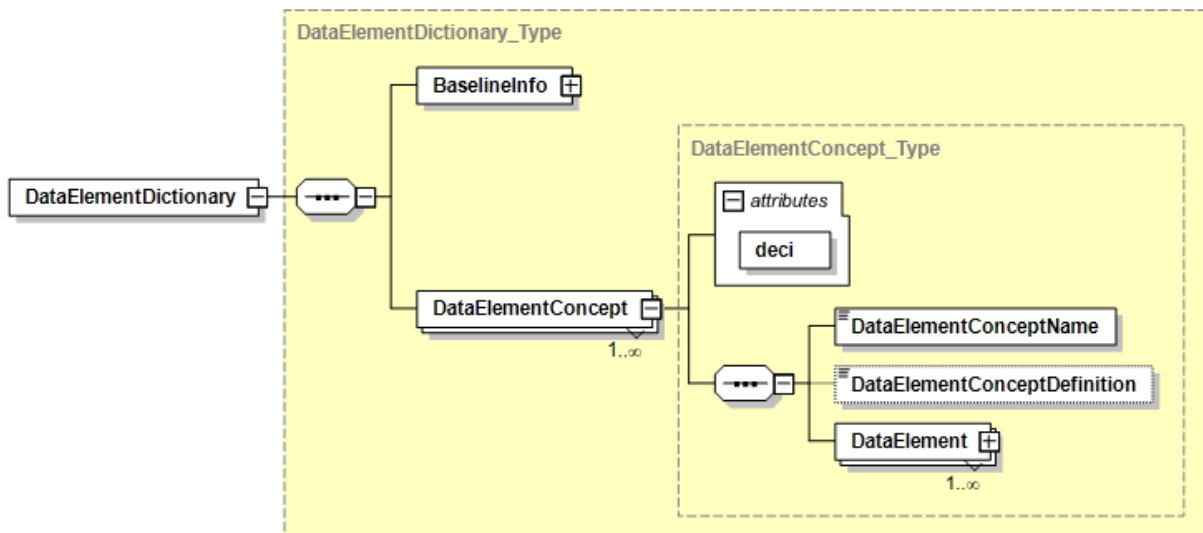
354. Step 5: Once the data elements have been defined create the XML document representing the DED for the STANAG. For that, apply the respective XML Schema as prescribed by the design rules to populate with the information identified above.

#### **A.5.5.4.6. Description of the DED XML Schema Definitions**

355. The following sections describe the XML Schema definitions used to capture the Data Element Dictionary.

### A.5.5.4.7. Base DataElementDictionary XML Schema

356. The base DataElementDictionary XML Schema provides the common elements used for capturing the Data Elements. These common elements are depicted in Figure A.13 followed by a short description.



**Figure A.13. Structure for Data Element Dictionary XML Schema**

1. **DataElementDictionary:** Denotes the top level element containing the Data Element Dictionary for the specific Information Exchange as defined in the BaselineInfo element.
2. **BaselineInfo:** Contains the meta-data for this STANAG like its title, identifier, version, security markings, etc. and is further described below.
3. **DataElementConcept:** Describes a Data Element Concept which includes a single concept and is the generic representation of the Data Elements grouped under it.
4. **DataElement:** Describes a Data Element, which is a representative of the corresponding Data Element Concept. It is further described in the section below.

The example below depicts the top-level elements of the XML instance document of the Data Element Dictionary for STANAG 5516 showing the root element, the BaselineInfo details (explained in the next section) and one of the DataElementConcepts.

```

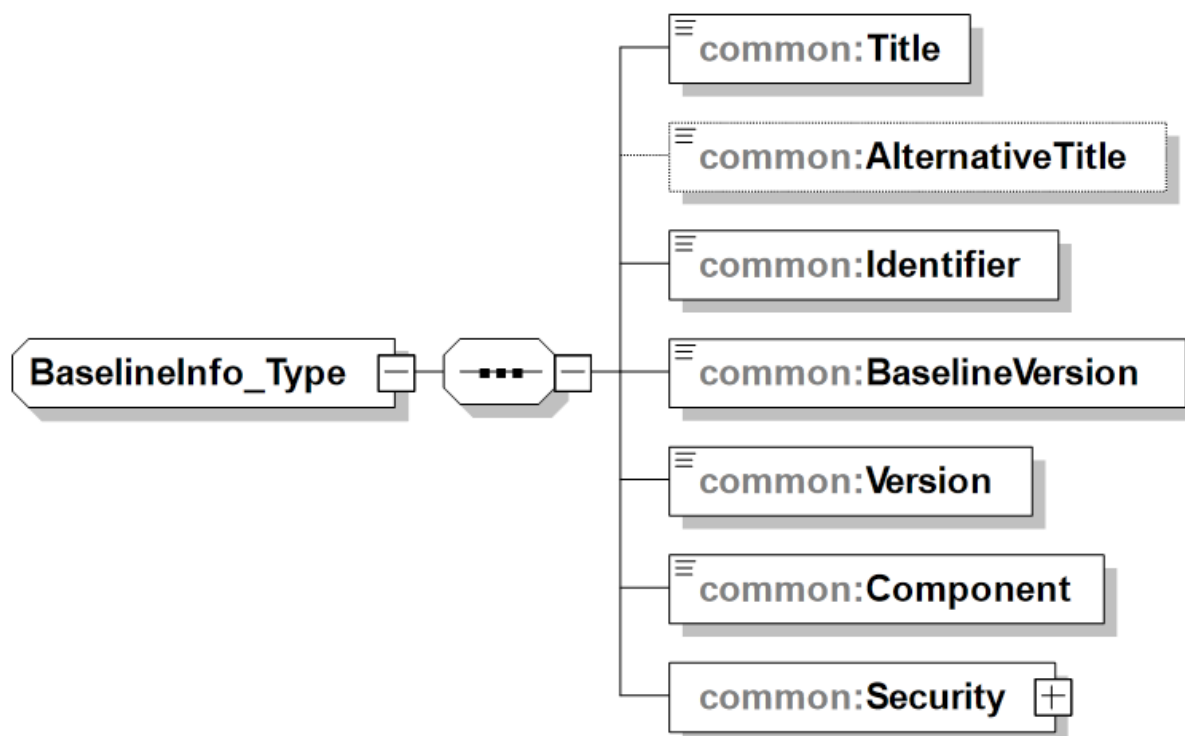
<?xml version="1.0" encoding="UTF-8"?>
<DataElementDictionary
  xmlns="urn:int:nato:stf:generic:dataElementDictionary-BitBased:0:20120824:draft"
  xmlns:common="urn:int:nato:stf:generic:common:0:20120824:draft"
  xmlns:sec="urn:int:nato:stf:generic:security:0:20120824:draft">
  <BaselineInfo>
    <common:Title>LINK16</common:Title>
    <common:Identifier>STANAG 5516</common:Identifier>
    <common:BaselineVersion>edition 6</common:BaselineVersion>
    <common:Version>2012-01</common:Version>
    <common:Component>DataElementDictionary</common:Component>
    <common:Security>
      <sec:PolicyIdentifier>NATO</sec:PolicyIdentifier>
      <sec:Classification>UNCLASSIFIED</sec:Classification>
      <sec:Category type="permissive">RELEASABLE FOR INTERNET TRANSMISSION</sec:Category>
    </common:Security>
  </BaselineInfo>
  ...
  <DataElementConcept deci="292">
    <DataElementConceptName>SPECIAL PROCESSING INDICATOR</DataElementConceptName>
    <DataElementConceptDefinition>INDICATES THAT A MESSAGE REQUIRES SPECIAL PROCESSING.</DataElementConceptDefinition>
    <DataElement dei="002">
  </DataElementConcept>
  ...

```

**Figure A.14. Example of Data Element Dictionary XML instance for Link 16**

#### **A.5.5.4.8. BaselineInfo XML Schema**

357. The **BaselineInfo** element is further detailed in Figure A.15 followed by a short description of its main elements.



**Figure A.15. Structure for BaselineInfo XML Schema**

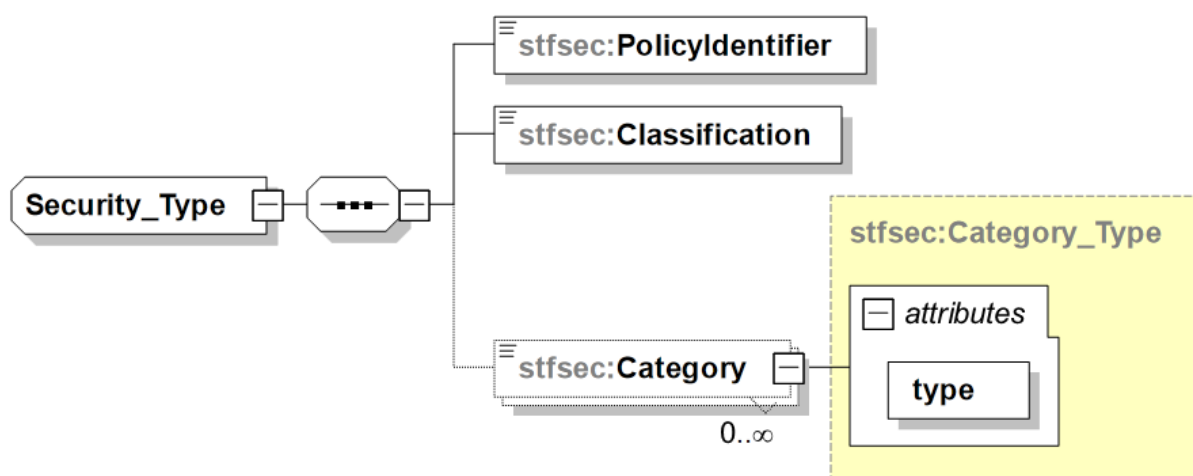
1. **Title:** Provides the name given to the STANAG as Configuration Item (CI). Enables the user to find the CI with a particular title or carry out more accurate searches. The title is commonly used as the key point of reference in the list of search results. Examples are "TACTICAL DATA EXCHANGE - LINK 16" and "NATO IMPLEMENTATION CODES AND RULES".
2. **AlternativeTitle:** Provides any form of the title used as a substitute or alternative to the formal title of the Configuration Item (CI). Examples are "Link16 spec" and "NICR".
3. **Identifier:** Provides an unambiguous reference to the STANAG as Configuration Item (CI) within the context of specific community. An internal, external, and/or universal identification number for a data asset or resource. Examples are "STANAG 5516", "ADatP-31" and "NICR T/1".
4. **BaselineVersion:** Provides the edition or version of the STANAG as Configuration Item. Examples are "edition 5" and "edition 6, first draft".
5. **Version:** Provides the internal version number of the instance document.
6. **Component:** Identifies the STF component of the specification that this instance document contains. This element explicitly indicates what is implied by the root element to support discovery. Examples are "MessageStructure" and "DataElementDictionary".

7. **Security**: Contains the security markings for the instance document (i.e. the specification) and is further described in the next section.

See the section above on the Base DataElementDictionary for an example of the usage of the BaselineInfo element.

### A.5.5.4.9. Security XML Schema

358. The **Security** element provides specific Information Assurance (IA) metadata for data objects; supports typical existing security labels to express policy, classification and category attributes. It is depicted in Figure A.16 followed by a short description of its main elements.



**Figure A.16. Structure for Security XML Schema**

1. **PolicyIdentifier**: Identifies the nation or organization responsible for creating, maintaining, and implementing the security policy to be applied to the information. The security policy is understood as a set of rules for protecting information against unauthorized disclosure, while maintaining authorized access, and preventing loss of unauthorized modification. The policy bodies of different security domains must agree on a common understanding of the handling requirements for information of a particular sensitivity. After the understanding exists, mappings from one security policy to another can be created (see Reference EAPC(AC/322-SC/5)N(2006)0008). For example, NATO, NATO/EAPC, NATO/PFP, NATO/EU, NATO/RUSSIA, NATO/UKRAINE. National use includes: USA, FRA, GBR, NLD, etc.
2. **Classification**: Provides security markings that indicate the sensitivity level of the information (see Reference : EAPC(AC/322-SC/5)N(2006)0008). Examples as defined in AC/322-D(2004)0021 and in "Guidance on the use of metadata element descriptions for use in NDMS" are UNMARKED, UNCLASSIFIED, RESTRICTED, CONFIDENTIAL, SECRET, and COSMIC TOP SECRET.
3. **Category**: Provides an indication of an additional, specific sensitivity, or a dissemination control, or an informational marking on which no automated access control is

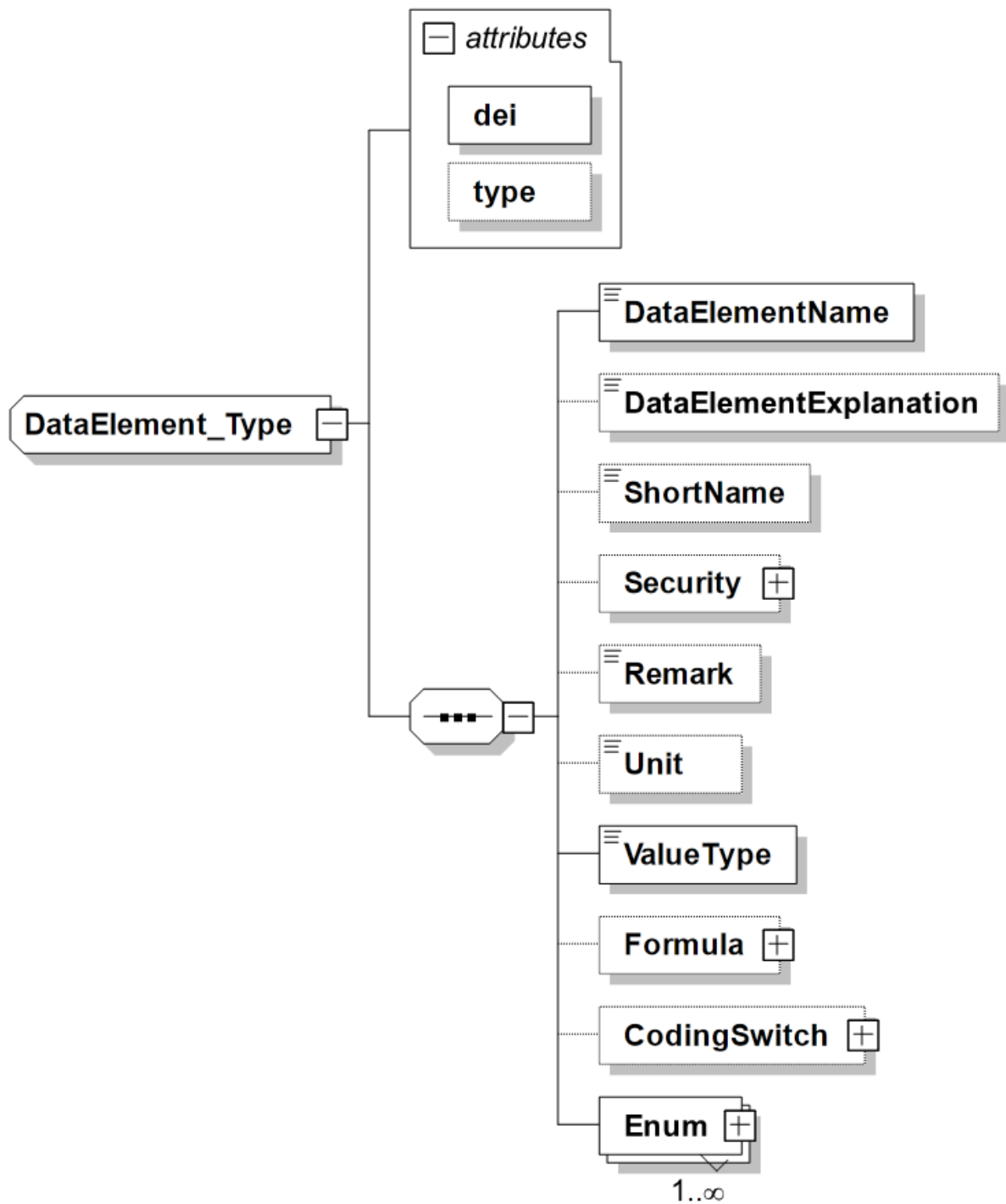
performed (see Reference : EAPC(AC/322-SC/5)N(2006)0008). Special category designator include ATOMAL, CRYPTO, SIOP, SIOP ESI. Dissemination Limitation Markings include EXCLUSIVE, INTELLIGENCE, LOGISTICS, OPERATIONS. Release categories include RELEASABLE TO, RELEASABLE FOR (e.g. RELEASABLE TO ISAF or RELEASABLE FOR INTERNET TRANSMISSION). Administrative markings include MANAGEMENT, STAFF, PERSONAL, MEDICAL, COMMERCIAL.

4. **type** (attribute for Category): Can be one of permissive, restrictive or informational.

See the section above on the Base DataElementDictionary for an example of the usage of the Security element.

#### **A.5.5.4.10. DataElement XML Schema**

359. The **DataElement** XML element describes a Data Element, which is a representative of the corresponding Data Element Concept. It denotes the actual Data Element and contains the Data Items (DIs) used to compose the Data Element. The combination of a Data Element Concept Identifier (deci) and a Data Element Identifier (dei) uniquely defines a Data Element. The **DataElement** XML element is depicted in Figure A.17 followed by a short description of its main elements.



**Figure A.17. Structure for Data Element XML Schema**

- **DataElementName:** Provides the name of this Data Element.
- **dei** (attribute of DataElement): Specifies the Data Element Identifier, which needs to be unique within the parent Data Element Concept.

- **type** (attribute of DataElement): Provides a mechanism to differentiate between types of Data Elements, for example data elements used as spare, disused ones, required for the structure of a message, or holding actual data. The following values are currently supported by STF:

<b>DataElement type</b>	<b>Meaning</b>
spare	Indicates this Data Element denotes a spare; a data element that, on transmissions, will be encoded as zero and shall not be processed upon receipt. Messages shall not be discarded upon receipt of non-zero spare fields.
disused	Indicates this Data Element denotes a disused element which are spare fields that previously had a valid meaning. When transmitted, Disused fields shall be encoded as 0 and shall not be processed upon receipt. Messages shall not be discarded upon receipt of a nonzero Disused field.
structure	Indicates this Data Element is used to define the structure of a message or word. This includes Data Elements that define which message or word is handled (e.g. for the message label) or Data Elements that act purely as a structure switch and do not itself represent any information.
data	Indicates this Data Element is carrying real (tactical) data.

- **DataElementExplanation:** Provides an explanation of how to use this Data Element
- **ShortName:** Provides a short version of the DataElementName, which can be used to refer to the DataElement. It is aimed to make this ShortName unique over all Data Elements, but this cannot be guaranteed at this time.
- **Security:** Provides the ability to provide additional security markings for the DataElement. If none is specified it takes the security markings from the BaselineInfo.
- **Remark:** Provides an optional remark for this Data Element specification.
- **Unit:** Specifies the measurement unit for this Data Element, e.g. Meters, Degrees, Feet. The possible units are specific for a STANAG although preferably units should be used that are defined in standards. If no unit is specified, the value is without unit which is true for all pure enumerations. If the coding for this Data Element utilizes a CodingSwitch (i.e. the coding depends on the value of another Data Field), the unit can be different for different coding variants. In that case the Unit should be specified within the CodingSwitch.



- **ValueType:** Specifies the specific type of value that is represented, e.g. Double, Integer or Enumeration. The current list of types can be extended if required. If the coding for this Data Element utilizes a CodingSwitch (i.e. the coding depends on the value of another Data Field), the value type can also be different for different coding variants. In that case the ValueType should be specified within the CodingSwitch.
- **Formula:** Specifies the Formula needed to decode the decimal value to a meaningful value of a Data Element
- **CodingSwitch:** Defines a decoding switch indicating that, based on the value of the referenced DataField, this DataElement needs to be decoded in a certain way. E.g. the referenced DataElement specifies that this DataElement needs to be interpreted as an altitude in either 1 meter, 10 meters or 100 meters increment.
- **Enum:** Defines a mapping from the exchanged value in a message to its meaning. Mappings can be provided to text (e.g. the reported numerical value 3 means FRIEND, or the reported textual value SV means Surface Vessel), or to the real, meaningful value (e.g. reporting the binary latitude as a double). In case the mapping to a meaningful value is provided, normally not all possible values are enumerated but instead the mapping from a range of binary values to a range of meaningful values (e.g. "0 through 2047" maps to "0 through 511 3/4 data miles"). The enumeration element provides information to encode and decode the exchanged value to a meaningful value for processing or to present as human-readable information. The CodingSwitch and Enum elements are further detailed below.

The example below depicts two examples of the representation of a Data Element, one for a bit-based Data Element from STANAG 5516 and one for a text-based Data Element from STANAG 5500.

```

<DataElement dei="001" type="data">
  <DataElementName>RELATIVE HUMIDITY</DataElementName>
  <DataElementExplanation>THE PERCENTAGE OF WATER VAPOR IN THE ATMOSPHERE.</DataElementExplanation>
  <ValueType>integer</ValueType>
  <Formula name="LinearExpressionIntegerFormula">
    <Parameter name="factor" valueType="integer" value="10"/>
    <FormulaRange>
      <Min>0</Min>
      <Max>10</Max>
    </FormulaRange>
  </Formula>
  <Enum type="data">
    <DataItem>0 THROUGH 100 PERCENT</DataItem>
    <Explanation>IN 10 PERCENT STEPS.</Explanation>
    <BitCodeRange>
      <Min>0</Min>
      <Max>10</Max>
    </BitCodeRange>
  </Enum>
  <Enum type="illegal">
    <DataItem>ILLEGAL</DataItem>
    <Explanation/>
    <BitCodeRange>
      <Min>11</Min>
      <Max>14</Max>
    </BitCodeRange>
  </Enum>
  <Enum type="no statement">
    <DataItem>NO STATEMENT</DataItem>
    <Explanation/>
    <BitCode>15</BitCode>
  </Enum>
  <Length>4</Length>
</DataElement>

```

**Figure A.18. Example of DataElement XML instance for Link 16**

The above example demonstrates how the various elements can be used for a bit-based data element that represent a numerical value (see ValueType element). Note that the Formula that produces the meaningful value for this Data Element only is valid for a specific range of the raw value. The remaining values (so 11..14 and 15) are only valid as enumerations.

The logic of the actual formula is not covered by the STF yet, although a limited number of formulas can be defined, each with its own explicit semantics. In this case, the LinearExpressionIntegerFormula will produce a meaningful value by taking two parameters, offset and factor, and applying the formula: meaningful-value = exchanged-value \* factor + offset. The definition of the formulas is under discussion and will be considered for the next version of the STF.

```

<DataElementConcept deci="1004">
  <DataElementConceptName>MONTH</DataElementConceptName>
  <DataElementConceptDefinition>ONE OF THE TWELVE PARTS INTO WHICH A YEAR IS DIVIDED AS DEFINED BY
  THE GREGORIAN CALENDAR.</DataElementConceptDefinition>
  <DataElement dei="1">
    <DataElementName>MONTH NAME</DataElementName>
    <DataElementExplanation>NAME OF THE MONTH ABBREVIATED WITH 3 CHARACTERS</DataElementExplanation>
    <ValueType>enumeration</ValueType>
    <Formula name="EnumerationFormula"/>
    <Enum>
      <DataItem>JANUARY</DataItem>
      <StringCode>JAN</StringCode>
    </Enum>
    <Enum>
      <DataItem>FEBRUARY</DataItem>
      <StringCode>FEB</StringCode>
    </Enum>
    ...
    <Enum>
      <DataItem>DECEMBER</DataItem>
      <StringCode>DEC</StringCode>
    </Enum>
  </DataElement>

  <DataElement dei="9">
    <DataElementName>MONTH NUMBER</DataElementName>
    <DataElementExplanation>NUMBER OF THE MONTH STARTING WITH 01 FOR JANUARY</DataElementExplanation>
    <ValueType>enumeration</ValueType>
    <Formula name="EnumerationFormula"/>
    <Enum>
      <DataItem>JANUARY</DataItem>
      <StringCode>01</StringCode>
    </Enum>
    ...
    <Enum>
      <DataItem>DECEMBER</DataItem>
      <StringCode>12</StringCode>
    </Enum>
  </DataElement>
</DataElementConcept>

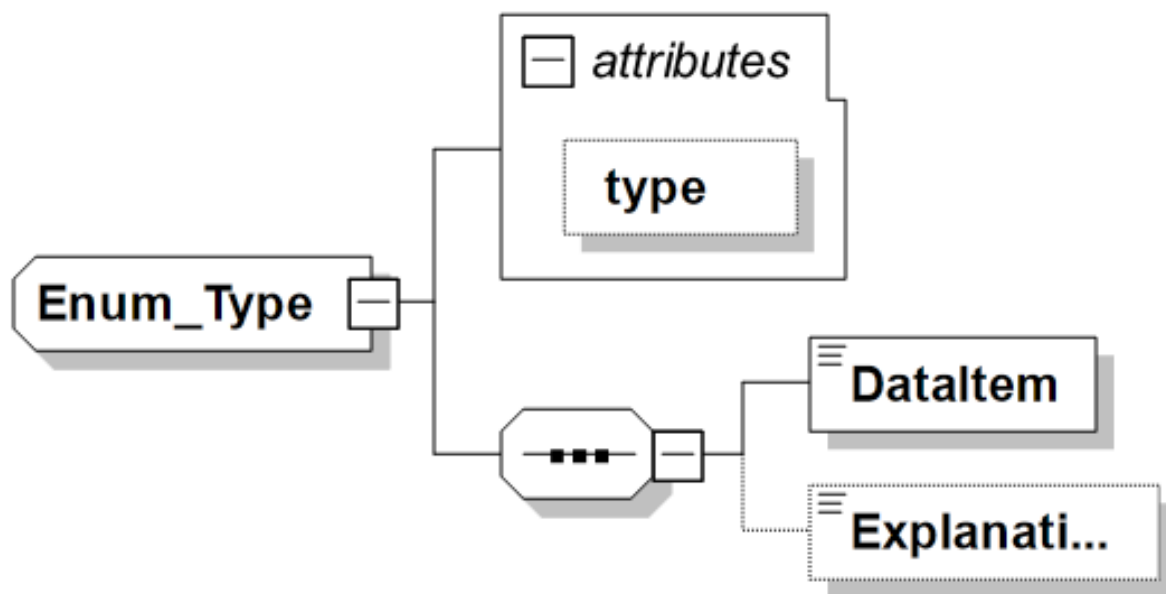
```

**Figure A.19. Example of DataElement XML instance for ADatP-3**

The above example demonstrates the use of the Enum elements for pure mappings, in this case for a text-based format. For the first Data Element, the exchanged value of JAN is decoded as JANUARY, while for the second Data Element, the values are encoded as numbers starting with 01 for JANUARY.

#### **A.5.5.4.11. DataElement Enum XML Schema**

360. The **Enum** XML element defines a mapping from the actual value as exchanged in a message to its meaning. It is depicted in Figure A.20 followed by a short description of its main elements.



**Figure A.20. Structure for Enum XML Schema**

361. The XML Schema does not cover the aspect of the exchanged value as this mapping depends on the type of exchange (bit-based vs. text-based) and therefore the way to describe the exchanged value is type specific and is described in the respective sections.

- **type** (attribute): Provides a mechanism to differentiate between types of Data Items, i.e. values, to further support automated interpretation. Currently the following types are supported:

Enum type	Meaning
disused	Indicates a Data Item value that was previously named but is no longer valid. A DISUSED value cannot be renamed without determining if coordinated implementation is required.
undefined	Indicates a term used to describe a code that has no value currently assigned but may have a value assigned in the future. (This occurs in logically coded Data Elements in which all the Data Items in the Data Element do not have assigned values.)
illegal	Indicates a term used to describe a code that is not a permissible entry into the tactical data system(s) supporting the interface, e.g., a 9 bit Data Element called HEADING that has legal

Enum type	Meaning
	values of 0 through 359 representing degrees has illegal values of 360 through 511.
no statement	Indicates no information on this Data Element is being transmitted. (This does not necessarily indicate that the originator does not have the information.)
unknown	Indicates other values available for this Data Element have not been determined by the originator.
to be determined	Indicates that Data Item design is incomplete. (Data Items and codes will be specified at a later time.)
data	Indicates actual data.
reserved	Indicates that this value is reserved for future use.

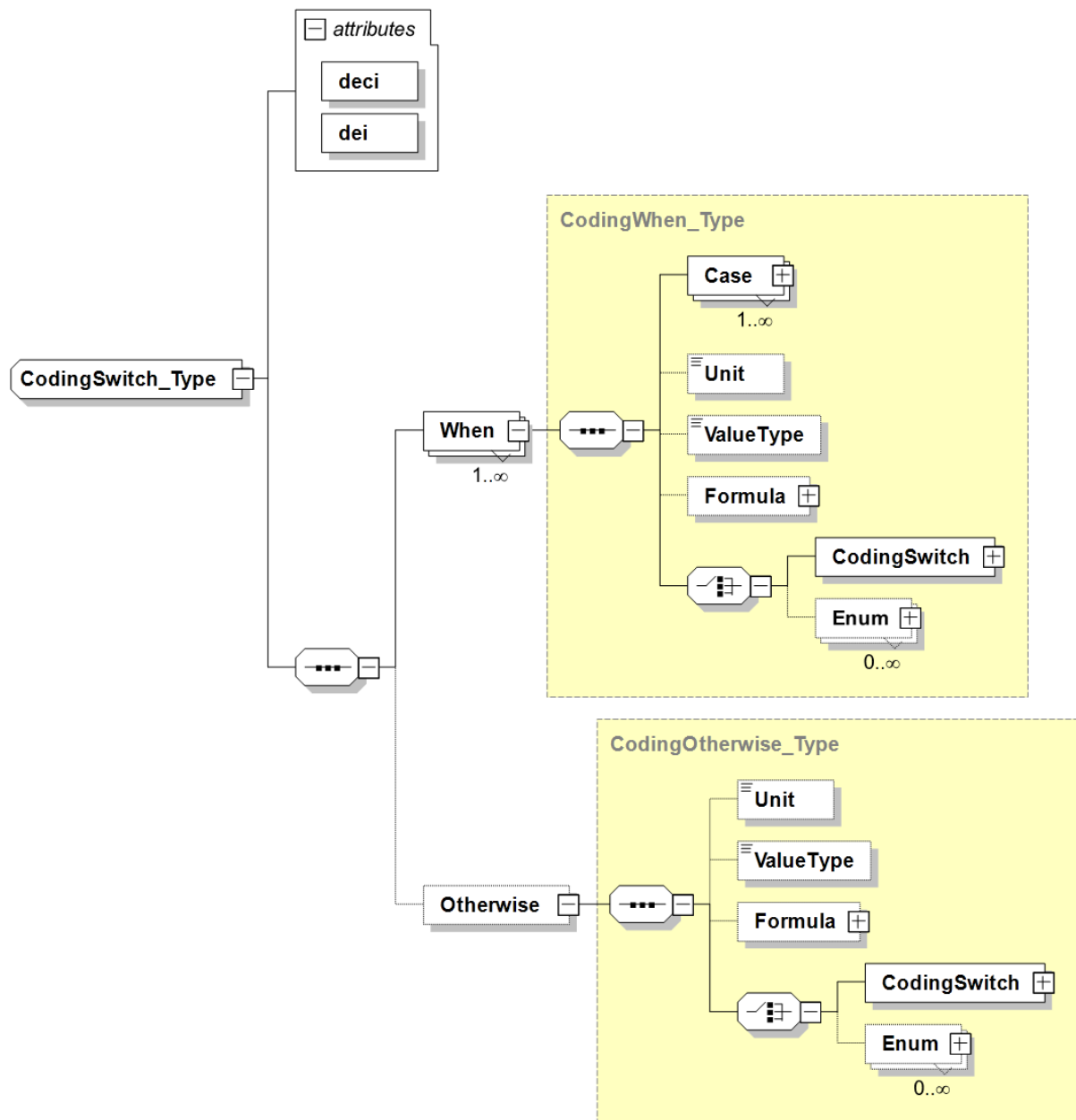
- **DataItem:** Provides the description and/or decoded value of this enumeration.
- **Explanation:** Provides an additional explanation for this Data Item only when necessary for amplification.

See the DataElement example above for examples on Enums, both for bit-based and for text-based information exchanges.

#### A.5.5.4.12. DataElement CodingSwitch XML Schema

362. The **CodingSwitch** XML element provides a way to specify that the encoding/decoding of a DataElement depends on the value of another DataElement. For example, an Altitude DataElement has a value of 5 which means an actual altitude of either 5 meter or 50 meter, indicated by the value of an Altitude Scale Indicator DataElement. Such a construct is typically used within bit-based information exchanges for space efficiency. Note that the **CodingSwitch** can be nested for the situation where the coding is dependent on multiple data elements.

363. The CodingSwitch XML element is depicted in Figure A.21 followed by a short description of its main elements.



**Figure A.21. Structure for CodingSwitch XML Schema**

1. **deci** and **dei**: Indicates the Data Element Concept Identifier (deci) and Data Element Identifier (dei) of the referenced, controlling DataField in the message context whose value is used to switch on.
2. **When**: Encapsulates a specific coding for the DataElement. The enclosed Case element(s) indicate for which value(s) of the referenced DataField this coding should be chosen.
3. **Otherwise**: Encapsulates a specific coding for the DataElement which is chosen if none of the When branches is selected.

4. **Case:** Defines for which value a specific coding applies. This is either indicated with a single value or a range of values, the specifics of which are defined in the type-specific XSD (i.e. bit-based or text-based).
5. **Unit, ValueType, Formula, Enum:** as defined for the DataElement. Their presence within the CodingSwitch will overrule any definition provided at a higher level in the DataElement.

364. The example below for the DEPTH Data Element of STANAG 5516 demonstrates the use of a CodingSwitch where the actual depth is depending of the value of another DataElement that is indicating the multiplication factor.

```
<DataElementConcept deci="366">
  <DataElementConceptName>DEPTH</DataElementConceptName>
  <DataElementConceptDefinition>USED TO REPORT DEPTH IN
    METERS OR A PLAIN STATEMENT.
</DataElementConceptDefinition>
  <DataElement dei="013">
    <DataElementName>DEPTH, TRANSDUCER</DataElementName>
    <DataElementExplanation>WHEN MULTIPLIED BY DEPTH
      INDICATOR (SONOBUOY), EXPRESSES DEPTH OF SONOBUOY
      TRANSDUCER AS MEASURED DOWNWARD FROM MSL AS A
      POSITIVE QUANTITY IN METERS. INTERPRETED ONLY WHEN
      DEPTH INDICATOR (SONOBUOY) IS NOT SET TO ZERO.
    </DataElementExplanation>
    <ValueType>Enumeration</ValueType>
    <Formula name="EnumerationFormula"/>
    <CodingSwitch deci="366" dei="012">
<!-- DEPTH INDICATOR (SONOBUOY) -->
      <When>
        <Case value="0"/>
        <ValueType>Enumeration</ValueType>
        <Formula name="EnumerationFormula"/>
        <Enum type="inconsistency">
          <DataItem>INCONSISTENCY</DataItem>
          <Explanation>CANNOT DECODE THIS COMBINATION
            OF DFI/DUI VALUE(S) AND STRUCTURE-SWITCH
            VALUE(S)</Explanation>
          <BitCodeRange><Min>0</Min><Max>15</Max>
        </BitCodeRange>
        </Enum>
      </When>
      <When>
        <Case value="1"/>
        <Unit>METER</Unit>
```

```

    <ValueType>Integer</ValueType>
    <Formula name="LinearExpressionIntegerFormula">
      <Parameter name="factor"
valueType="Enumeration" value="3"/>
      <FormulaRange><Min>1</Min><Max>9</Max>
      </FormulaRange>
    </Formula>
    <Enum type="no statement">
      <DataItem>NO STATEMENT</DataItem>
      <Explanation/>
      <BitCode>0</BitCode>
    </Enum>
    <Enum type="data">
      <DataItem>DEPTH (METERS X DEPTH INDICATOR)
</DataItem>
      <Explanation/>
      <BitCodeRange><Min>1</Min><Max>9</Max>
      </BitCodeRange>
    </Enum>
    <Enum type="undefined">
      <DataItem>UNDEFINED</DataItem>
      <Explanation/>
      <BitCodeRange><Min>10</Min><Max>15</Max>
      </BitCodeRange>
    </Enum>
  </When>
  <When>
    <Case value="2"/>
    <Unit>METER</Unit>
    <ValueType>Integer</ValueType>
    <Formula name="LinearExpressionIntegerFormula">
      <Parameter name="factor"
valueType="Enumeration" value="30"/>
      <FormulaRange><Min>1</Min><Max>9</Max>
      </FormulaRange>
    </Formula>
    <Enum type="no statement">
      <DataItem>NO STATEMENT</DataItem>
      <Explanation/>
      <BitCode>0</BitCode>
    </Enum>
    <Enum type="data">
      <DataItem>DEPTH (METERS X DEPTH INDICATOR)
</DataItem>

```



```

        <Explanation/>
        <BitCodeRange><Min>1</Min><Max>9</Max>
        </BitCodeRange>
    </Enum>
    <Enum type="undefined">
        <DataItem>UNDEFINED</DataItem>
        <Explanation/>
        <BitCodeRange><Min>10</Min><Max>15</Max>
        </BitCodeRange>
    </Enum>
</When>
<When>
    <Case value="3"/>
    <Unit>METER</Unit>
    <ValueType>Integer</ValueType>
    <Formula name="LinearExpressionIntegerFormula">
        <Parameter name="factor"
valueType="Enumeration"
value="300"/>
        <FormulaRange><Min>1</Min><Max>9</Max>
        </FormulaRange>
    </Formula>
    <Enum type="no statement">
        <DataItem>NO STATEMENT</DataItem>
        <Explanation/>
        <BitCode>0</BitCode>
    </Enum>
    <Enum type="data">
        <DataItem>DEPTH (METERS X DEPTH INDICATOR)
</DataItem>
        <Explanation/>
        <BitCodeRange><Min>1</Min><Max>9</Max>
        </BitCodeRange>
    </Enum>
    <Enum type="undefined">
        <DataItem>UNDEFINED</DataItem>
        <Explanation/>
        <BitCodeRange><Min>10</Min><Max>15</Max>
        </BitCodeRange>
    </Enum>
</When>
</CodingSwitch>
<Length>4</Length>
</DataElement>

```

</DataElementConcept>

#### **A.5.5.4.13. Bit-based Data Element Dictionary XML Schema**

365. The XML Schema for BitBased Data Element Dictionary extends the base Data Element Dictionary XML Schema with the additional information required to capture bit-based Data Elements. In particular, it adds the following:

1. **Length** element to the DataElement element expressed in number of bits
2. **BitCoding** element to the DataElement element indicating how numerical values are encoded. Possible values are unsigned, onesComplement, twosComplement, modifiedTwosComplement, and signMagnitude.
3. **BitCode** element as sub-element of the Enum element. Holds the actual numerical value which can be mapped to its meaning held in DataItem.
4. **BitCodeRange** element as sub-element of the Enum element. Similar to the BitCode element but provides a range of actual values instead.

366. The examples shown before demonstrate the use of these additional elements.

#### **A.5.5.4.14. Structured Text-based Data Element Dictionary XML Schema**

367. The XML Schema for text-based Data Element Dictionary extends the base Data Element Dictionary XML Schema with the additional information required to capture text-based Data Elements. In particular, it adds the following:

1. **CharacterSet** attribute to the DataElement element indicating which characters are allowed in the actual value, e.g. only uppercase alphabetical characters, or only digits. If unspecified, any character is allowed although e.g. for Field or Word separation, specific messages might be excluded.
2. **RegularExpression** attribute to the DataElement element indicating alone or in addition to the CharacterSet the restriction on the actual value of the DataElement by specifying a regular expression, e.g. "[0-9]{3,6}[A-Z]" indicating 3 to 6 digits followed by one uppercase alphabetical character.
3. **MinimumLength** and **MaximumLength** attributes to the DataElement element indicating the minimum and maximum allowed length of the actual value. If unspecified, MinimumLength is interpreted as 0 and MaximumLength as unbounded, although the message or transport might impose a maximum.
4. **StringCode** element as sub-element of the Enum element. Holds the actual textual value which can be mapped to its meaning held in DataItem.

368. The examples shown before demonstrate the use of these additional elements.

#### **A.5.5.4.15. XML-based Data Element Dictionary XML Schema**

369. Not yet addressed within the current version of the STF.

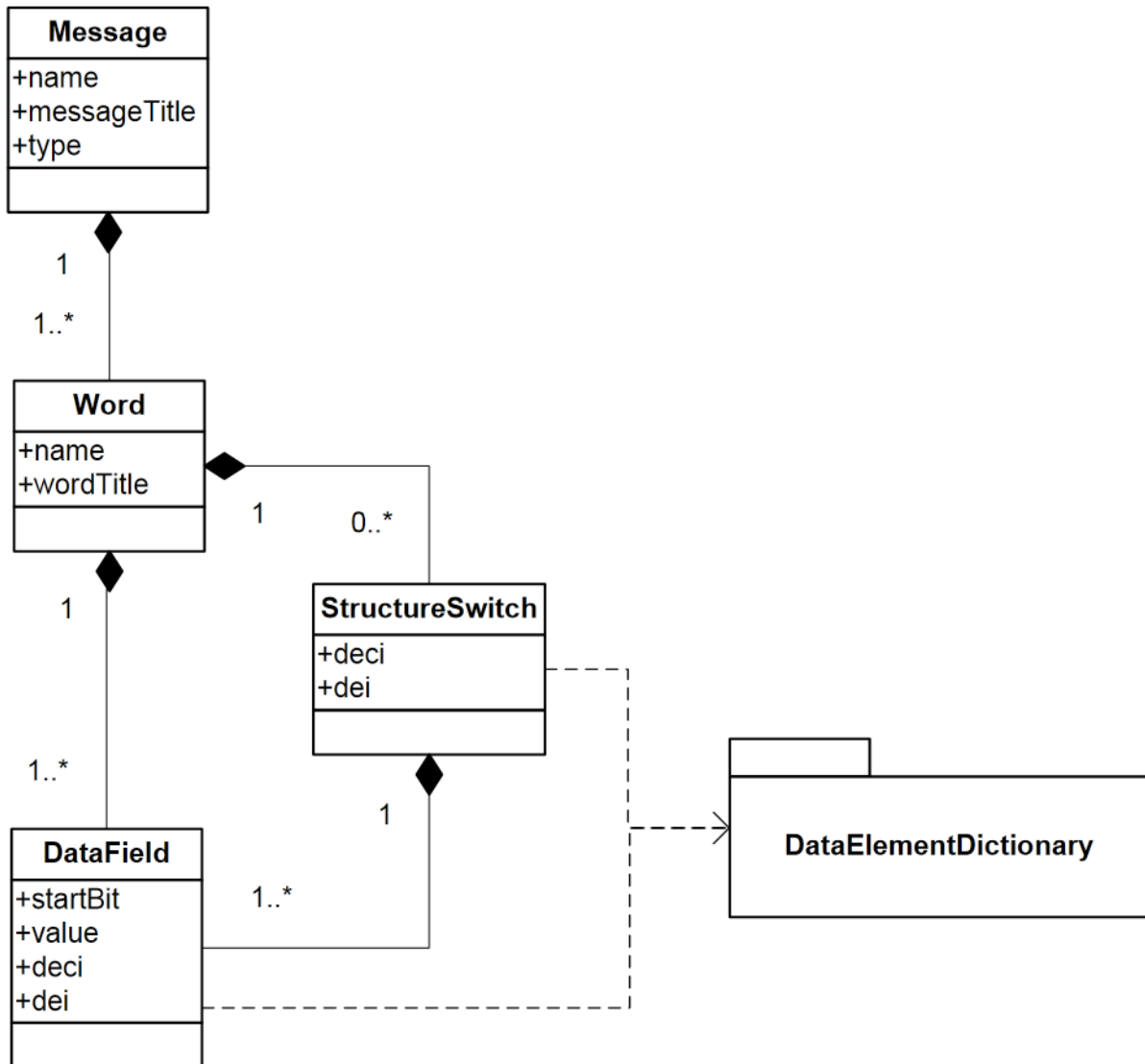
### **A.5.5.5. Message Structure Layer Design Rules & Methodology**

#### **A.5.5.5.1. Message Structure Concepts**

- **Data Field:** The instantiation or use of a data element.
- **Word:** A structured collection, or container, of one or more data fields used to report on a specific aspect.
  - For example, in ADatP-3, within the OWNSITREP message, the LOCATION set provides the Geographic Location of the unit and the LOCAMPN set provides Location Amplification, while in Link-16, within the J3.1 message, the J3.1I word reports on the basic information for an emergency point and J3.1C1 provides the IFF/SIF codes.
- **Message:** A structured collection of one or more words to report a particular set of information.
  - For example, the ADatP-3 OWNSITREP message for reporting information regarding own and subordinate units can contain nested sets including the LOCATION and LOCAMPN sets, while the Link-16 J3.2 message for reporting (the state of) an air track can contain the J3.2I, J3.2E0, and J3.2C1 words.
- **StructureSwitch:** Similar to the concept of a "switch" statement in computer programming, a StructureSwitch is a "conditional construct" that is used as a way to select between alternative data sets within a message structure. It allows for building message structures where the value of a data field defines which following data field(s) are included in the message. StructureSwitches can be nested to support multiple levels of data set selection.
- Within the TDL and JISR community, this would be considered as overlaid sets of data fields, where the value of another, referenced data field, defines which set is present in a word. For example, if in the Link-16 J7.0 message the environment/category data field indicates AIR then the word contains the Air Platform and the Air Platform Activity data fields, while for the GMTI format, if the Segment Type data field specifies Mission Segment the following data is containing the data fields like Mission Plan and Flight Plan.
- **Data Element Dictionary:** The collection of all Data Elements used in the Messages specified by this information exchange STANAG.

### A.5.5.5.2. Message Structure Logical Model

370. This logical model shows the relationship between these concepts to support the definition of a generic information exchange message structure. The attributes shown in the classes denote relevant information that needs to be captured on the classes or indicate a relationship between classes (e.g. dui).



**Figure A.22. Message Structure Logical Model**

371. The Message Structure XML Schemas are derived from this logical model, fully elaborated to include all components (elements and attributes) that are required to model the generic message structures for all types of information exchanges.

### A.5.5.5.3. Known Limitations

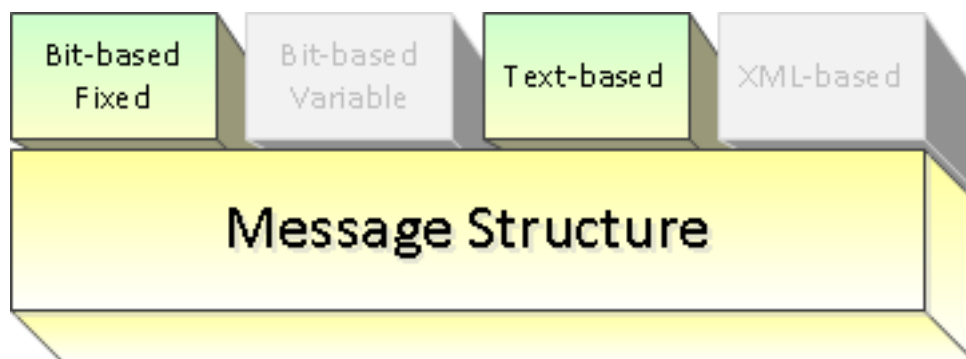
372. There are some known shortcomings in Version 1.0 of the STF Message Structure XML Schemas and Logical Model in supporting all types of information exchange message structures. These are described here:

- Information exchange specifications sometimes do not specify a container-like construct such as the "word" concept defined here. Instead, they define messages as a flat collection of data elements.
- Messages with a more complex structure cannot be represented with the current Message / Word / DataField structure. For example, VMF or the encapsulating protocol for Link 22 messages require more nesting support, such as nesting Words within other Word containers, to get "Sets", "Segments", etc.
- The current structure does not yet support information exchange specifications that define messages of variable length by including optional contents (e.g. VMF, GMTI, DIS, ASTERIX), but will be enhanced to serve this purpose.
- Further details need to be captured in XML on how the data is serialised, e.g. big-endian vs. little-endian, bit-order, character coding.

These are being considered, and extensions, such as the ability to have nested Word elements, to the current model to address these limitations will be provided in Version 2.0 of the STF Design Rules.

### A.5.5.5.4. Message Structure Design Rules

373. Based on the type of information exchange specified by the IES, a specific adapter (extension) of the common STF Message Structure XML Schema (STFMessageStructure\*.xsd) shall be used to capture the Message Structures supporting that information exchange in an XML representation to fulfil the Message Structure layer of the STF, as depicted in Figure A.23.



**Figure A.23. Message Structure with adapters**

374. Below are the design rules with the methodology on how to apply them to create the XML file to capture the message structures for a particular information exchange:

375. Rule 1: The MessageStructure-BitBasedFixedLength.xsd shall be applied in case the Information Exchange is bit-based and the Message Structure type defines messages of fixed length, i.e. no presence of optional contents and use of filler bits.

376. Rule 2: (Future work) -The MessageStructure-BitBasedVariableLength.xsd shall be applied in case the Information Exchange is bit-based and the Message Structure type defines messages of variable length, i.e. presence of optional contents.

377. *This XSD is not provided within the current version of the STF.*

378. Rule 3: The MessageStructure-TextBased.xsd shall be applied in case the Information Exchange is text-based and the Message Structure type is non-XML.

379. Rule 4: (Future work) - The MessageStructure-XMLBased.xsd shall be applied in case the Information Exchange is based on XML. This will capture the Container Elements for each message. The message structure itself is provided by the XSD as defined in the STANAG. The MessageStructure-XMLBased.xsd defines the mapping between the STF Container Elements and the corresponding XSD constructs (e.g. xsd:group, xsd:sequence). *This XSD is not provided within the current version of the STF.*

#### **A.5.5.5.5. Methodology for Message Structure Definition**

380. Step 1: Determine which type of message exchange (bit-based fixed length, bit-based variable length, text-based or XML-based). Based on this, determine the correct STF XML artefact to use and the XML namespace to use for the MS XML instance document that will be created to define the information exchange message structures. Bit-based, text-based and XML-based types each have their own XML namespace.

381. Step 2: Identify all messages to be exchanged.

382. Step 3: For each message, identify the grouping constructs. Depending on the format, terms like word, group, set, container, segment, PDU, etc. may be used.

383. Step 4: For all identified grouping constructs, determine how they should be mapped to the 'Word' abstract concept in the STF MS XML Schema. The mapping does not need to be one-to-one. For example, extra words may be added if they are necessary to group repeated fields even though the specification of the format does not group them.

384. Step 5: For each message, determine the data fields that make up the message using data elements captured within the STANAG-specific DED XML from Section A.5.5.4.

385. Step 5a: If there is a need within a particular message for a StructureSwitch, then for each "switch" pattern, determine the conditions that control the switch.

386. Step 6: Identify all properties of the messages, groupings (words) and data fields, such as DECI and DEI number, name, title, purpose, remarks, start bits if appropriate, fixed and value.

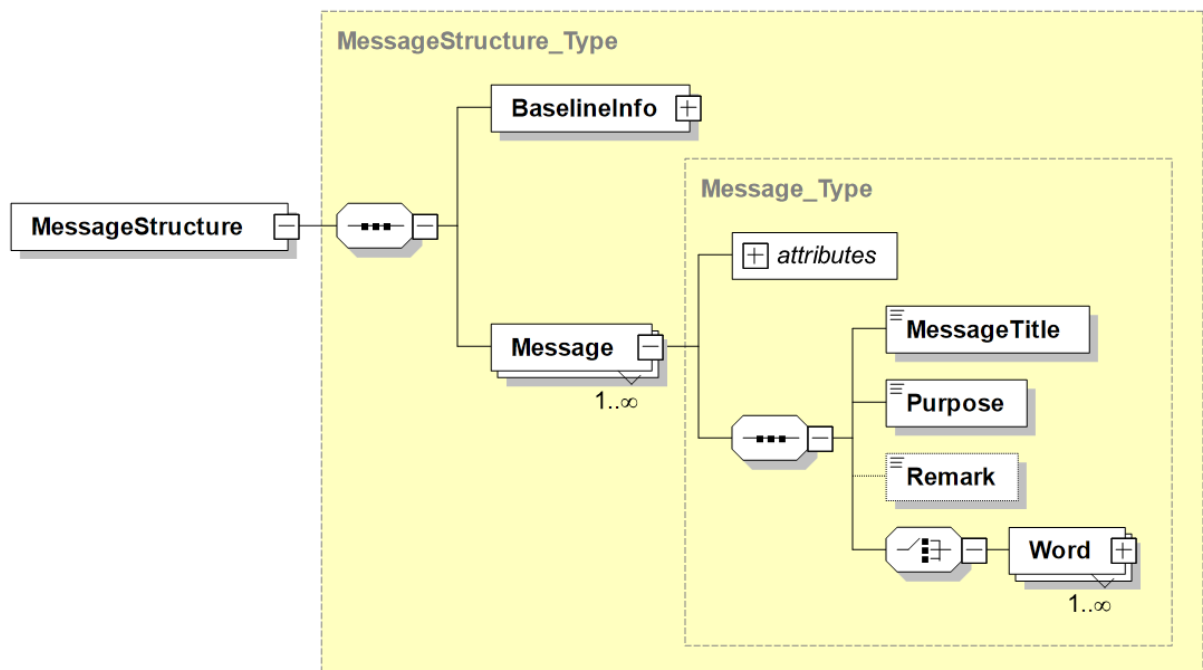
387. Step 7: Create the XML instance document representing the MS, according to the appropriate XML Schema selected in Step 1.

### A.5.5.5.6. Description of the Message Structure XML Schema Definitions

388. The following sections describe the XML Schema definitions used to capture the Message Structure.

### A.5.5.5.7. Base Message Structure XML Schema

389. The base Message Structure XML Schema provides the common elements used for capturing the Message Structure. These common elements are depicted in Figure A.24 followed by a short description.



**Figure A.24. Root level MessageStructure XML Schema Definition**

- **MessageStructure:** Denotes the top level element containing the definition of the structure of the messages for a specific STANAG as defined in the BaselineInfo element.
- **BaselineInfo:** See the section on BaselineInfo XML Schema within the description of the DED XML Schema Definitions

- **Message:** Defines the structure information for a particular Message. A Message has some metadata (like a Name and Title) and consists of Word elements.
- **Word:** Defines the possible Words that are defined for this Message which acts as a container for the actual DataFields. The presence or order of the Words within an exchanged Message is not prescribed here.

The Word element is further detailed in the section below followed by a short description of its main elements.

The example in Figure A.25 depicts the top-level elements of the XML instance document of the Message Structure for STANAG 5516 showing the root element, the BaselineInfo details (explained before) and one of the Messages.

```

<?xml version="1.0" encoding="UTF-8"?>
<MessageStructure
  xmlns="urn:int:nato:stf:generic:messageStructure-BitBased:0:20120824:draft"
  xmlns:common="urn:int:nato:stf:generic:common:0:20120824:draft"
  xmlns:sec="urn:int:nato:stf:generic:security:0:20120824:draft">
  <BaselineInfo>
  <Message name="J3.2">
    <MessageTitle>Air Track</MessageTitle>
    <Purpose>The J3.2 Air Track message is used to exchange information on air tracks.</Purpose>
    <Remark/>
    <Word name="J3.2I">
    <Word name="J3.2E0">
    <Word name="J3.2C1">
    <Word name="J3.2C2">
    <Word name="J3.2C3">
    <Word name="J3.2C4">
  </Message>
</MessageStructure>

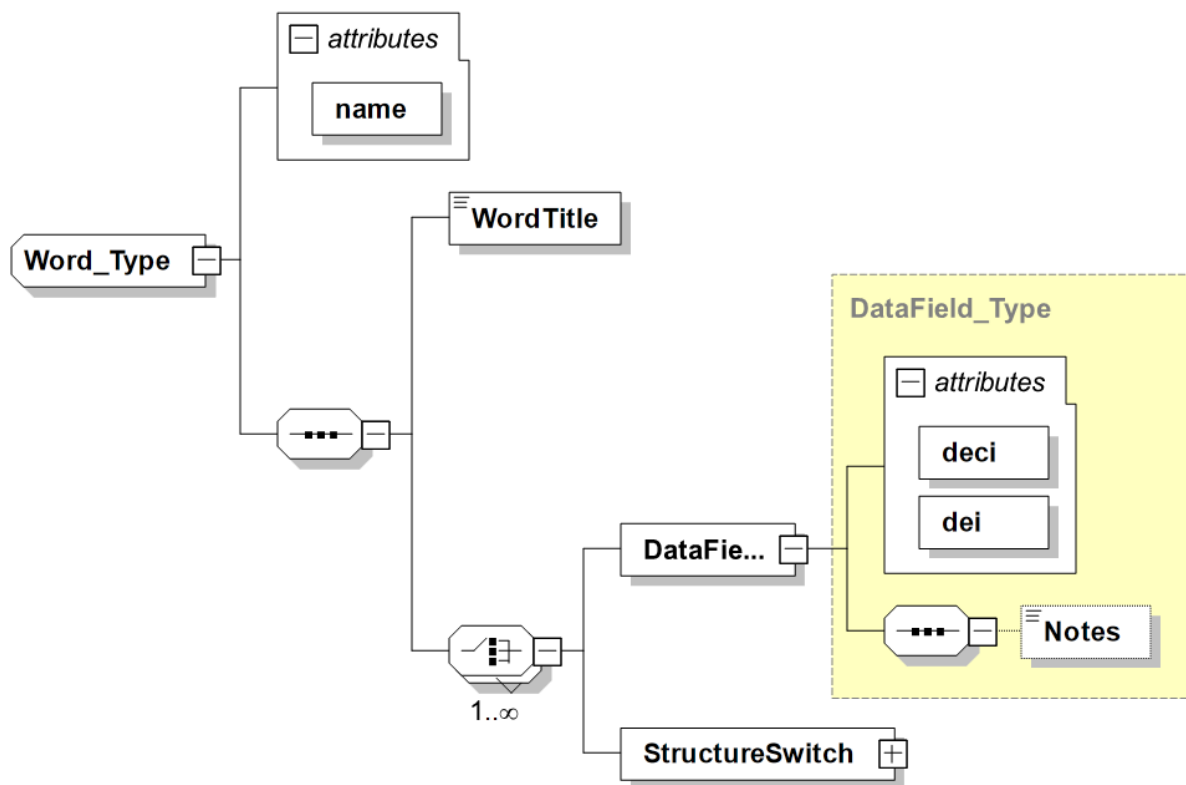
```

**Figure A.25. Word XML Schema**

#### A.5.5.5.8. Word XML Schema

390. The structure of the **Word** element is shown in Figure A.26 followed by a short description of its main elements.






**Figure A.26. Word within the Generic Message Structure XML Schema Definition**

- **name** (attribute): Specifies the name of the Word including specific characters and/or spaces.
- **WordTitle**: Specifies the title of the Word.
- **DataField**: Describes a DataField within a Word holding the actual data. A DataField refers to a Data Element via the deci and dei. The order of the DataFields within a Word is relevant. Optionally a DataField can have a fixed value.
- **StructureSwitch**: Defines a "conditional construct" that is used as a way to select between alternative data sets within a message structure. Based on the value of the referenced DataField one of a set of DataFields is expected. E.g. depending on the value of DataField 'Environment Category' (Air, Ground, Surface, etc), either the 'Air platform', 'Ground platform', 'Surface platform', etc. DataField is present. The StructureSwitch element is built from one or more 'When' entries and an optional 'Otherwise' entry each holding one or more DataFields and/or nested StructureSwitch elements.

The figures below depict examples of the representation of a bit-based Word from STANAG 5516 and a text-based Message and 2 Words for OTH Gold.



```
<Word name="J3.2E0">
  <WordTitle>AIR TRACK EXTENSION WORD</WordTitle>
  <DataField deci="1550" dei="001" startBit="0" value="2"/>
  <DataField deci="756" dei="002" startBit="2"/>
  <DataField deci="281" dei="014" startBit="4"/>
  <DataField deci="758" dei="001" startBit="25"/>
  <DataField deci="756" dei="001" startBit="26"/>
  <DataField deci="282" dei="014" startBit="27"/>
  <DataField deci="892" dei="001" startBit="49"/>
  <DataField deci="371" dei="015" startBit="50"/>
  <DataField deci="367" dei="018" startBit="59"/>
</Word>
```

**Figure A.27. Example of Word XML instance for Link 16**

```

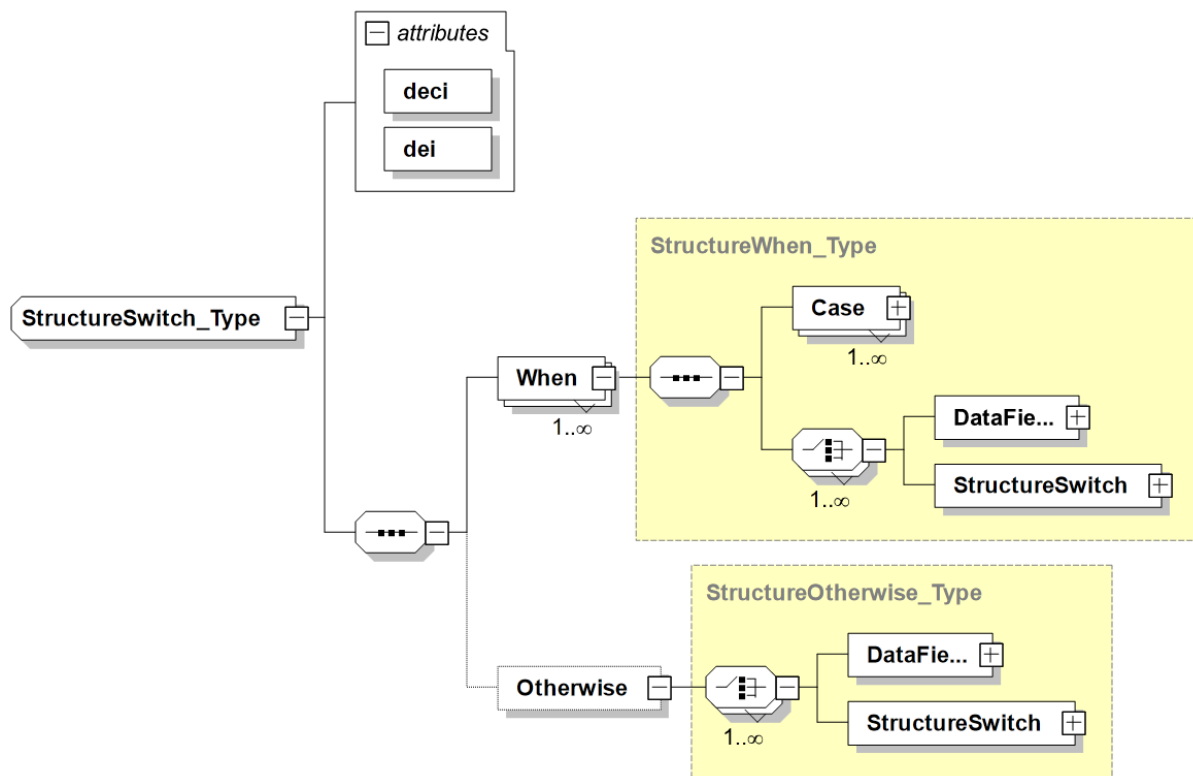
<Message name="JUNIT" type="DATA">
  <MessageTitle>Joint Unit Report</MessageTitle>
  <Purpose>The JUNIT Report message is used to exchange processed unit track data and track management
  sets between computer systems. It contains the identity, location, movement, type, echelon, and threat
  of units.</Purpose>
  <Word name="MSGID">
    <WordTitle>MESSAGE IDENTIFICATION</WordTitle>
    <DataField deci="104046" dei="0" presence="MANDATORY" value="MSGID"/>
    <DataField deci="104046" dei="1" presence="MANDATORY"/>
    <DataField deci="104046" dei="2" presence="MANDATORY"/>
    <DataField deci="104046" dei="3" presence="MANDATORY"/>
    <DataField deci="104046" dei="4" presence="MANDATORY"/>
    <DataField deci="104046" dei="5" presence="OPTIONAL"/>
    <DataField deci="104046" dei="6" presence="OPTIONAL"/>
    <DataField deci="104046" dei="7" presence="OPTIONAL"/>
  </Word>
  ...
  <Word name="JUNIT" cleanname="JUNIT">
    <WordTitle>Joint Unit Report</WordTitle>
    <DataField deci="104046" dei="0" presence="MANDATORY" value="JUNIT"/>
    <DataField deci="104201" dei="106" presence="MANDATORY"/>
    <DataField deci="104040" dei="2" presence="MANDATORY"/>
    <DataField deci="104040" dei="3" presence="OPTIONAL"/>
    <DataField deci="104040" dei="4" presence="OPTIONAL"/>
    <DataField deci="104040" dei="5" presence="OPTIONAL"/>
    <DataField deci="104040" dei="6" presence="OPTIONAL"/>
    <DataField deci="104200" dei="19" presence="OPTIONAL"/>
    <DataField deci="104200" dei="1" presence="MANDATORY"/>
    <DataField deci="104200" dei="13" presence="OPTIONAL"/>
    <DataField deci="104040" dei="10" presence="OPTIONAL"/>
    <DataField deci="104201" dei="109" presence="OPTIONAL"/>
    <DataField deci="104200" dei="31" presence="MANDATORY"/>
    <DataField deci="104200" dei="21" presence="OPTIONAL"/>
    <DataField deci="104201" dei="25" presence="OPTIONAL"/>
  </Word>
  ...
</Message>

```

**Figure A.28. Example of Message and 2 Words XML instance for OTH Gold**

**A.5.5.5.9. StructureSwitch XML Schema**

391. The structure of the **StructureSwitch** element is shown in Figure A.29 followed by a short description of its main elements.



**Figure A.29. StructureSwitch XML Schema Definition**

- **deci** and **dei** (attributes): Indicate the deci and dei numbers of the referenced DataField that is the base of the StructureSwitch. Based on the value of te referenced DataField one of the When blocks applies or alternatively the Otherwise.
- **When**: Defines an alternative set of one or more DataField(s) or nested StructureSwitch(es). The enclosed Case element(s) indicate for which value(s) of the referenced DataField this set should be chosen..
- **Otherwise**: Defines the alternative set of one or more DataField(s) or nested StructureSwitch(es) in case none of the preceding When elements was applied (i.e. none of the indicated Case elements).
- **Case**: Specifies the value for the referenced DataField for which the enclosing When element is selected and therefore the following DataField(s) and/or nested StructureSwitch(es). The value is either indicated with a single value or a range of values, the specifics of which are defined in the type-specific XSD (i.e. bit-based or text-based). Note that a When element can contain multiple Case elements to be able to specify that this When applies for all the specified values.

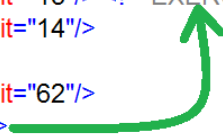
The example below depicts an example of the representation of a StructureSwitch from STANAG 5516. The example specifies that after DataField 758/004, different DataFields can

occur depending on the value of the DataField 385/003. If its value is 0, then the DataField will be 376/007, while if the value is 1, the DataField will be 376/001. Taking the definitions of these DataElements from STANAG 5516 into account, this means that the EXERCISE INDICATOR field controls whether the field is interpreted as either the IDENTITY field or the IDENTITY AMPLIFYING DESCRIPTOR.

```

<Word name="J3.2I">
  <WordTitle>AIR TRACK INITIAL WORD</WordTitle>
  <DataField deci="1550" dei="001" startBit="0" value="0"/>
  <DataField deci="270" dei="004" startBit="2" value="3"/>
  <DataField deci="271" dei="005" startBit="7" value="2"/>
  <DataField deci="800" dei="001" startBit="10"/>
  <DataField deci="385" dei="003" startBit="13"/> <!-- EXERCISE INDICATOR -->
  <DataField deci="839" dei="001" startBit="14"/>
  ...
  <DataField deci="758" dei="004" startBit="62"/>
  <StructureSwitch deci="385" dei="003">
    <When>
      <Case value="0"/> <!-- NON-EXERCISE TRACK -->
      <DataField deci="376" dei="007" startBit="66"/> <!-- IDENTITY -->
    </When>
    <When>
      <Case value="1"/> <!-- EXERCISE TRACK OR UNIT -->
      <DataField deci="376" dei="001" startBit="66"/> <!-- IDENTITY AMPLIFYING DESCRIPTOR -->
    </When>
  </StructureSwitch>
  <DataField deci="1861" dei="001" startBit="69"/>
</Word>

```



**Figure A.30. Bit-based Message Structure XML Schema**

#### A.5.5.5.10. Bit-based Message Structure XML Schema

392. The XML Schema for BitBased Message Structure extends the base Message Structure XML Schema with the additional information required to capture bit-based Message Structures. In particular, it adds the following:

- **startBit** attribute to the DataField element expressed as offset in number of bits from 0.
- Optional **value** attribute to the DataField element for holding the fixed value as an unsigned decimal.
- Decimal **value** attribute of the Case element within the StructureSwitch.

393. The examples shown before demonstrate the use of these additional elements.

#### **A.5.5.5.11. Structured text-based Message Structure XML Schema**

394. The XML Schema for Structured Text-based messages extends the base Message Structure XML Schema with the additional information required to capture text-based Message Structures. In particular, it adds the following:

- Optional **value** attribute to the DataField element for holding the fixed value as a string.
- String **value** attribute of the Case element within the StructureSwitch.
- Optional **presence** attribute to the DataField element to indicate whether an actual value is optional or mandatory.

395. The examples shown before demonstrate the use of these additional elements.

#### **A.5.5.5.12. XML-based Message Structure XML Schema**

396. Not yet addressed within the current version of the STF.

#### **A.5.5.6. Business Rules Design Rules & Methodology**

397. Not yet addressed within the current version of the STF.

#### **A.5.5.7. Security Cross-Domain Design Rules & Methodology**

398. Not yet addressed within the current version of the STF.

#### **A.5.5.8. Web Services Design Rules & Methodology**

399. Not yet addressed within the current version of the STF.

#### **A.5.5.9. Operational Cross-Domain Design Rules & Methodology**

400. Not yet addressed within the current version of the STF.

### **A.5.6. Consequences**

401. To fulfil the information exchange requirements from a mid and a long term view it is essential to plan the implementation of the guidance from a holistic approach. This means the approach needs to achieve improvements which are both efficient and effective. The approach should be modular to enable to reuse, while a spiral approach will allow for continual learning and improvement. The following key success factors for the STANAG transformation need to be considered.

#### **A.5.6.1. Efficiency**

402. The process of STANAG transformation should result in an improved efficiency from multiple perspectives. One of the main aspects of efficiency is to enhance the cost effectiveness

by reducing manual labour. The reduction of manual labour will also provide an advantage by reducing time in STANAG development and maintenance. In particular, this will:

- Lead towards faster implementation of Change Proposals (CP) to the STANAG.
- Facilitate the discovery of ambiguities via automatic verification of both the STANAG and the CPs.
- Cause a reduction in the need for the manual labour-intensive actions (validation, implementation, etc.).

### **A.5.6.2. Effectiveness**

403. The process of transforming the STANAG towards machine readable STANAGs will increase effectiveness:

- By enabling common interpretation of the standards via the non-ambiguous machine interpretable STANAGs.
- Via the enabling of automated standard validation, in order to find possible errors at an earlier stage.
- In the semi-automatic system implementation that are facilitated via the creation of machine interpretable STANAGs. This will reduce the human errors in the system implementation of the STANAGs and thus lead to better implementations.
- In facilitating the semi-automatic validation of system implementation in order to find system failures at an earlier stage. This validation is supported by the STANAGs being machine readable.
- By providing the possibility to generate system documentation in a semi-automated way, based on the machine interpretable STANAG. Allowing the system documentation and system implementation to be always in line for the STANAG implementation part.
- In data harmonization by aligning the machine interpretable STANAG to the Guidance for XML Naming and Design (GXND) and therefore enabling the registration in the NATO Metadata registry and Repository (NMRR) for data element harmonization and vocabulary management.

### **A.5.6.3. Modularity**

404. The STANAG transformation process aims to result into a modular machine interpretable STANAG, which will provide the following advantages compared to the current STANAGs:

- Different modules within the STANAG can be reused within other STANAGs.
- The components must be derived from the requirements of the different scenarios. Nevertheless, after the transformation of the STANAG, it can be applied based on the context.

E.g. if no security context is needed, the security layer can be either not implemented or disabled in specific situations

- Using the modular approach in the STANAG and addressing all different aspects will make the STANAG ready to fulfil unforeseen requirements.

#### **A.5.6.4. Spiral development**

405. The Spiral development will enable the COI to achieve tangible results by adopting early technologies and concepts and learn from their application. This will provide operational and administrative benefits since the first deliverable and lessons learned and feedback can be retrofitted to the administrative community.

406. All consequences of implementing and not implementing a solution whether direct or indirect, wanted or unwanted shall be documented to the extent possible. Consequences for at least the following areas shall be regarded:

- Time
- Cost
- Capabilities
- Security
- Interoperability
- Usability
- Flexibility
- Procedures

#### **A.5.6.5. Benefits of the layered approach**

407. The use of the layered approach is a wide-spread and well-known concept that has been used for years and successful application can be found in the OSI reference model for communication protocols and semantic web interoperability. The adoption of this layered approach introduces multiple benefits:

- **Interoperability:** Currently, solutions based on the standards attempt to provide the overall capability embedded in a single system due to the complexity and unclear separation between the different functional areas addressed by the STANAG. The ability to verify separate functionalities addressed by the current standards is minimal due to their unclear and tangled definitions. By untangling these functionalities and presenting them within a layered approach, the different functionalities can be verified layer by layer independently. This improves the quality of the standard and therefore contributes to overall interoperability.



- **Scalability:** The means to accommodate unforeseen new requirements is enhanced by the application of the layered approach to the STANAG. A new layer can be introduced leveraging on the other layers in a controlled way, e.g. based on emerging requirements.
- **Flexibility:** Each layer describes a specific functionality, where layers can be stacked on top of each other. When a specific functionality is not needed (e.g. Security cross-domain) for a specific deployment or system role, this approach allows clear identification of the parts of the STANAG that do not have to be implemented.
- **Maintainability:** Without using a layered approach, identifying the impact of a change in one part of the STANAG to the other parts of the STANAG is often a challenge. Making changes to one of the layers in a layered approach will affect the other layers in a more controlled and traceable manner.

408. Therefore, the modular approach as adopted within the information exchange STANAG framework allows for maximum reuse of the STANAG layers and a more clear distinction between the different functionalities addressed within the STANAG.

### **A.5.6.6. Consequences of implementing the solution**

409. Current and future operations require and will require interoperability at all levels: from machine-to-machine, to human-to-human via all the transformation steps from data to information. The essential pre-requisite is standardization and well-defined and error-free standards, which are machine-interpretable for ease of implementation and with no opportunity for mis-interpretation. Using the traditional approach to standardization will continue to produce standards that are difficult to maintain and often contain errors, entail long delays before ratification, are ambiguous, and therefore result in non-interoperable systems. The new approach proposed in this document applies to five areas: The application of the layered approach, the configuration management of the standards, the development of systems, the actual interoperability, and the enhanced operational usage in the future. The benefits provided in each of these areas are further addressed in the following sections.

#### **A.5.6.6.1. STANAG Configuration Management enhancements**

410. The current configuration management (CM) of the various STANAGs is handled by their respective Capability Team or Panel (CaT resp. CaP, e.g. TDL CaT for STANAG 5516). Agreed Changes are then incorporated by the custodian (e.g. Defence Information Systems Agency (DISA) for STANAG 5516) using different proprietary tools and methodologies. The process of creating a new STANAG baseline is largely a manual task where changes to the STANAG text are applied to the proper sections; some of the text is maintained in a database as structured data (e.g. the Message Structure and Data Element Dictionary), others are maintained as a collection of plain text (e.g. the body text or the transmit and receive rules). Linkage between one baseline of a STANAG and a previous one is difficult. Furthermore, various STANAGs need to maintain consistency between them, e.g., those defining different Data Links and those that define the conversions between them, or STANAGs and standards which define common elements (e.g. positional definitions or identities (STANAG 1241)).

411. The CM process could leverage on the possibilities introduced by the representation of STANAGs in a machine-interpretable format which is structured and well-defined. Several enhancements are foreseen to the CM process:

- More explicit specification of the components that make up a Configuration Item (CI) which makes these components easier to be discovered and referenced from other areas.
- Automated support for creating a new baseline based on the availability in a machine-interpretable format of both the previous baseline and the changes to be applied.
- Easier tracking of changes to the elements that make up the CI with all relevant aspects like what, when, why and who.

412. The machine-interpretable format of the STANAG can then be used to automatically generate the required STANAG documentation. The quality of this documentation will be greatly improved because of the resulting consistency in internal structure and phrasing, possible different views on the structure, fully hyperlinked to ease navigation, and support for different output formats (e.g. HTML, PDF, and Word). To support these enhancements, the improved standard would provide ways to create references on several levels that can be used:

- Internally in a baseline, e.g., from the message structure to a data element or from the processing actions to a specific message.
- From one baseline to previous ones, e.g. to trace changes to elements.
- To other baselines of related standards, e.g., to data elements in a common or related standard (e.g. variable message format (VMF) and Link-22 reuse data elements from Link-16)).

413. Using these references, the internal and external integrity of the standard can then be validated resulting in increased quality of the produced baseline.

414. The actual changes in an information exchange standard are often part of a Change Proposal (CP) process. CPs are developed and then submitted by Nations and Strategic Commands (SC) represented in the body responsible for the CM of the STANAG in order to modify parts of the STANAGs. CPs could correct errors in the STANAGs or could introduce changes in order to implement new capabilities. As soon as agreement has been reached the CP and supplement sections will be embedded in the next edition of the STANAG.

415. This process could be greatly improved by having both CPs and STANAGs in a structured, well-defined, unambiguous, and machine-interpretable format [NC3A-TN-1391], resulting in the following benefits

- Automated verification of impact and integrity constraints of the CP even before submission
- Automated update of the STANAG based on the agreed CP, including automated referential integrity handling
- Automated verification of changes to interoperability matrices as a result of the CP before agreement

- Possibility to register the changed Information Exchange Specification in the NMRR in machine interpretable format for implementation

416. Several of the aforementioned baseline management activities are supported by the NATO Metadata Registry and Repository (NMRR), which is an NNEC core service for registration, discovery and configuration management of machine-interpretable artefacts. More information on the administrative aspects of the NMRR can be found in [NC3A-TN-1311] [NC3A-TN-1312] [NC3A-TN-1313] [RTO-EN-IST-088]. Besides being visible and accessible to human users, the artefacts registered in the NMRR will also be available to automated clients via a service interface. Due to the machine-interpretable format, services can make use of these artefacts and be notified of changes, thus enabling various advanced use cases. More information on these so-called 'operational' aspects of the NMRR can be found in [NC3A-TN-1367] [NC3A-TN-1368] [NC3A-TN-1369].

#### **A.5.6.6.2. STANAG Implementation & System development enhancement**

417. A structured, well-defined, machine-interpretable standard can be used in various ways. Generation of human readable documentation is one of the most self-evident ones, which could also provide more capabilities than the current human readable standard by using the information provided by the structure. But because of the machine-interpretable aspect of the new specification, its strength is most prominent when it is used as the base for the implementing system's logic i.e., using the specification to generate the system's implementation. In traditional systems, humans read the standard and implement the desired functionality. This is manual work to a large extent without real support for automation. Often engineers will convert certain aspects of the standard to some sort of structured information but each group is basically reinventing the wheel. Furthermore, besides being time-consuming and error-prone, it also requires the human to interpret thousands of pages of text, not always in their native language, while keeping track of the intrinsic linkage between the various sections of the standard. Undoubtedly each company or agency will have developed their own ways of tracking the quality of their work with linkage back to the specification which is a huge effort and therefore represents concrete value and is therefore not easily shared among companies or agencies.

418. Transforming the specification so it can be interpreted by a machine would mean a huge reduction of human interpretation. This can be achieved by defining only a limited and well-defined vocabulary instead of the many ways a natural language can be used to express, e.g., the logic of a system. Different ways of expressing the same thing might be pleasant while reading a novel but will trigger an engineer's brain to wonder whether the different wording might indicate a different behaviour. This is even more applicable when the language at hand is not the engineer's native language.

419. The reduction of human interpretation will have two aspects:

- The level of interpretation will be reduced because of the limited and well-defined vocabulary: just a limited set of constructs needs to be defined with great accuracy and because there is only a limited set, it will be easier to understand.

- The amount of interpretation will be reduced because, once the vocabulary is understood, the whole standard is basically about applying those constructs in a well-defined and repetitive way. That is obviously something a machine is aimed at.

420. When automatically generating systems, ruling out most of the human interpretation together with the increased power and quality of the specification, will have several positive effects on the resulting product:

- Shorter time between specification and implementation: as the standard is now machine-interpretable there is no need to read through all the changes and then find and update the relevant code. In the best case it would be a push-on-a-button to create an updated system ready for testing.
- Cost reduction: shorter time to implement an updated system has a direct impact on the costs. But furthermore, by generating parts of the system the time spent in testing can be reduced because mainly the generation process needs to be validated to produce the correct output.
- Fewer errors: The machine-interpretable aspect means far less human interpretation is required and because of the automatic generation of part of the system less manual work needs to be performed. Both contribute to fewer errors in the final implementation of the system.
- Improved interoperability: Using an unambiguous specification to produce an implementation of higher quality will increase the level of interoperability between systems. More on this subject is covered in the next section.
- Test support: The specification can also be used during the test and validation phases of a system, e.g., to generate automatically test code and scenarios.

421. Obtaining all these benefits will obviously take time to mature but system development will be greatly enhanced resulting in better information exchange systems and increased interoperability which will further be examined in the following section.

### **A.5.6.6.3. Interoperability enhancement**

422. Assessment, verification and validation of the interoperability among platforms is essential in order to achieve situational awareness according to the NNEC Data Strategy. This is especially true in a NATO environment where various nations are collaborating with their own national systems, often developed by different companies and with different requirements. Interoperability shall be verified during various stages of the system's life, each of which can leverage on the machine-interpretable standard.

### **A.5.6.6.4. Paper based interoperability assessment**

423. Originally, a paper-based interoperability assessment involved manually comparing documents against each other; the system's requirements document (SRD) or the interface control document (ICD) against the standard. By capturing the SRD and the ICD in XML in a similar manner to that foreseen for the TDL standard itself, automatic assessment of

interoperability against the standard or another system can be easily achieved. This has a direct positive effect on both the quality of the comparison as well as the time it takes. The paper-based interoperability assessment between the SRD and the standard can be performed even before the system is actually built, reducing the costs associated with later changes. An example of such an interoperability assessment via machine interpretable versions of both the reference document and the ICD can be found in [REF-NC3A-NU/CCS/ADP/2008/331].

#### **A.5.6.6.5. System development**

424. Using the machine-interpretable standard to generate major parts of an implementation system, as explained in the previous section, will positively affect the level of interoperability between these systems. The level of interpretation is reduced because of the well-defined constructs and the limited number of constructs, while the amount of interpretation is reduced because of applying these constructs consistently over the whole standard. Furthermore, if a system interprets a certain construct in a non-standard way (i.e. a bug), this would affect all situations where it is applied which therefore increases the chance of discovering this during tests.

#### **A.5.6.6.6. Interoperability testing**

425. By using the machine-interpretable specification, not only can the system itself, but also test and analyzer tools can be generated to a large extent. The specification will contain all the information like the supported messages, their structure and the protocol for the message exchange. These tools can then be used to rigorously test systems against the standard, both in a one-on-one test and for analyzing the interaction between different systems.

#### **A.5.6.6.7. harmonization of standards**

426. The introduction of machine-interpretable standards will significantly increase the interoperability between systems whose implementation has been derived from the same standard; it will eliminate the need for ad-hoc interfaces and translation of data structures. To ensure interoperability between the systems based on different standards from different COIs, COIs should harmonize their information exchanges and establish common agreed upon operational cross-domain specifications. In the past, this process was often tedious for various reasons, but it is foreseen that this process can be facilitated by the application of the STF and the availability of the future NMRR capability to store and manage those specifications. More information about standardization, the power of metadata, such as the machine-interpretable standards, and the role of the NMRR, can be found in [NC3A-TN-1254] [RTO-EN-IST-088].

#### **A.5.6.7. Consequences of not implementing the solution**

427. The STF can be applied in several ways:

- The STF Layered Framework is used to identify gaps in the IERs and IESs with respect to the NNEC Data Strategy goals.
- The STF Layers are used to structure the evolution and development of IESs.

- The STF Design Rules and XML artefacts are used to transform existing textual IES related to the message formats (DED and MS) into XML representations

428. If the STF is not applied in the evolution and development of IERs and IESs, there is a high risk that the following will occur:

- IERs and IESs will be insufficiently specified, as developers may forget to consider certain aspects such as security cross-domain and operational cross-domain considerations.
- IESs transformed into XML may not have sufficient information to support data harmonization, reuse and semantic interoperability

429. If a common framework is not used to transform the way NATO develops STANAGs for information exchange, it would be difficult to realize the NNEC Data Strategy goals and reach interoperability in the NNEC environment.

### **A.5.7. Limitations**

430. Limitations imposed by the Design Rule or limited conformance to applied standard shall be described in this section.

### **A.5.8. Deviations**

431. There has been cases where IESs for DED and MS have been transformed or captured into XML, but not in-line with the STF XML Schemas for those layers.

432. If the STF Design Rules and STF XML Schemas are not applied to transform existing message formats into XML, there is a chance that the following deficiencies may occur:

- The data element specifications may lack enough detail to support data harmonization.
- Incompatible implementations of frameworks are negating the benefits of a common framework for different message formats.
- Incompatible specifications will make operational cross-domain harder or impossible.
  - For example, when applying STF to the forwarding from format A to format B, every data element from either can be referenced with a consistent and unambiguous triple of Format, deci and dei. This results in a specification for forwarding which is much simpler than taking different specification domain in account.
  - Re-inventing the Wheel: Wasted investment of time and resources to define solutions that are already existing, thought-through, tested, and accepted.

### **A.5.9. Examples**

433. Examples of applying the design rules are provided within the Design Rules & Methodology section for each STF layer.

## **A.6. RELATIONS TO OTHER PRODUCTS**

### **A.6.1. Dependencies**

434. The STF Design Rule have the following dependencies from other products.

- The STF XML artefacts are registered within the NMRR within the STF namespace.
- XML artefacts created by applying the STF design rule shall be registered within the NMRR.
- The STF XML artefacts in the NMRR shall be used to automatically validate the XML artefact created by applying the STF design rule.
- The DED XML artefacts can be used for data harmonization.

### **A.6.2. Impacts**

435. The STF Design Rules impact the evolution and development of STANAGs related to information exchanges. The following table provides an initial list of STANAGs that have been identified so far that should be transformed and improved by applying this design rule. This list is by no means exhaustive and should be expanded as more information exchange STANAGs are identified and used by the NATO community.

**Table A.8. Impacted STANAGs**

<b>Document ID</b>	<b>Date of publication</b>	<b>Issue number / version</b>
[NATO STANAG 5500]: NATO Standardization Agreement 5500, "Concept of NATO Message Text Formatting System (CONFORMETS) - ADatP-3", NATO Standardization Agency, Brussels, Belgium (NATO Unclassified).	25 October 2006	
[NATO STANAG 5501]: NATO Standardization Agreement 5501, Digital Data Link " Link 1 (Point-to-Point)", NATO Standardization Agency, Brussels, Belgium (NATO Unclassified).	28 February 2006	4th Edition
[NATO STANAG 5511]: NATO Standardization Agreement 5511, "Tactical Data Exchange " Link 11/11B", NATO Standardization Agency, Brus-	28 February 2006	5th Edition

<b>Document ID</b>	<b>Date of publication</b>	<b>Issue number / version</b>
sels, Belgium (NATO Unclassified).		
[NATO STANAG 5516]: NATO Standardization Agreement 5516, "Tactical Data Exchange " Link 16", NATO Standardization Agency, Brussels, Belgium (NATO Unclassified).	10 May 2006	5th Edition
[NATO STANAG 5518]: NATO STANAG 5518		
[NATO STANAG 5519]: NATO STANAG 5519		
[NATO STANAG 5522]: NATO Standardization Agreement 5522, "Tactical Data Link " Link 22", NATO Standardization Agency, Brussels, Belgium (NATO Unclassified).	24 September 2004	2nd Edition
[NATO STANAG 5527]: NATO STANAG 5527		
[NATO STANAG 5601]: NATO Standardization Agreement 5601, "Standards for Interface of Data Links 1, 11, 11B and 14"	28 August 2006	3rd Edition
[NATO STANAG 5616]: NATO Standardization Agreement 5616, "Standards for Data Forwarding between Tactical Data. Systems Employing Digital Data Link 11/11B and Tactical Data System Employing Link 16"	09 March 2006	3rd Edition
[NATO STANAG 2183]: NATO STANAG 2183		
[NATO STANAG 2185]: NATO STANAG 2185		
[NATO STANAG 4607]: NATO STANAG 4607		



Document ID	Date of publication	Issue number / version
[NATO STANAG 4609]: NATO STANAG 4609		

### **A.6.3. Interferences**

436. *Describe the interference of the Design Rule with other products.*

### **A.6.4. Replacement**

437. *List what is replaced and why.*

### **A.6.5. Change Request (CR)/Improvements**

438. As this is version 1.0 of the STF Design Rules, no change requests are yet submitted.

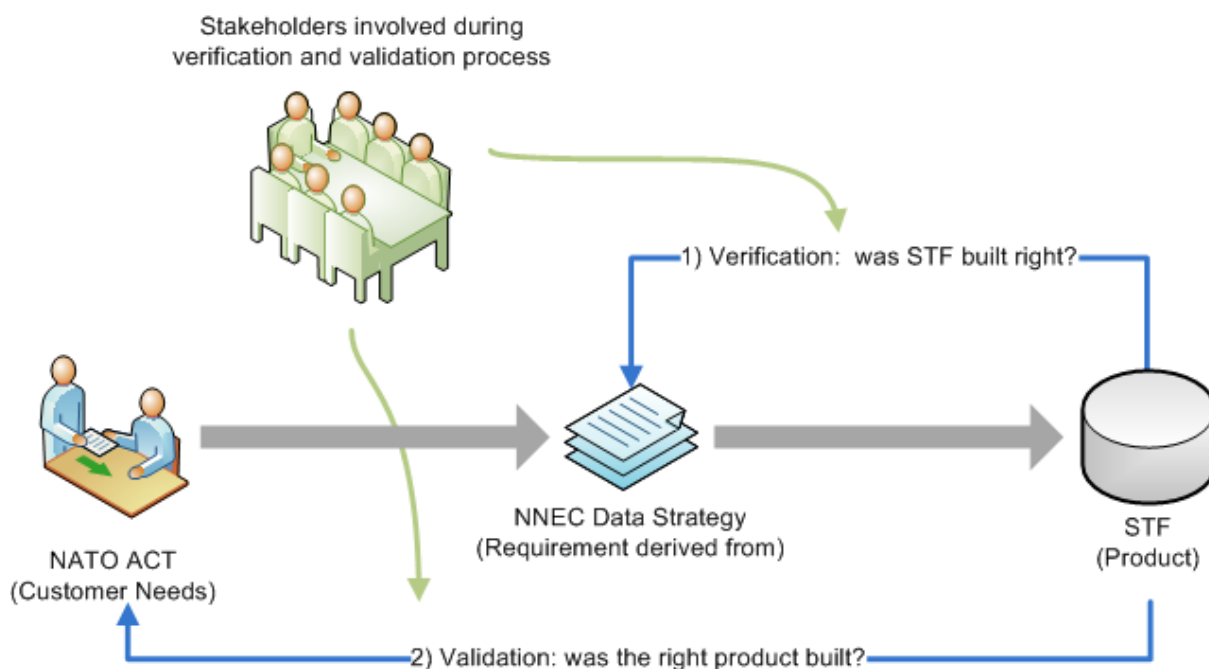
## **A.7. V&V (VERIFICATION AND VALIDATION)**

### **A.7.1. Verification and Validation of STF**

439. Verification and validation together can be defined as a process of reviewing, testing and inspecting the STF components to determine that the STF components produces the expected results based on the expressed requirements.

440. V&V is an on-going process that occurs in several phases with the involvement of NATO and National Stakeholders in multiple venues. The decision to involve external stakeholders at the early stages of the validation process proved to be a success by having obtained buy-in and active contributions from several NATO and National Stakeholders.

441. As the STF is developed based on the spiral incremental approach, the verification and validation process is repeated several times for each component of the STF.



**Figure A.31. STF V&V Process Overview**

442. STF V&V Process Overview depicts the overarching process adopted for the verification and validation.

443. As usual, two questions normally asked when dealing with V&V are the following:

- Validation: Are you building the right thing?
- Verification: Are you building it right?

444. In order to address the first question, the STF product--which includes the layered framework, design rules, XML artefacts and methodology--addresses the requirements expressed by ACT based on the NNEC Data Strategy. In particular, there are requirements to make data Visible, Accessible, Coherent, Assured, Interoperable and Managed Effectively. It is recognized that in order to achieve these goals, many technical and procedural improvements have to be made in the way NATO specifies and manages their Standardization Agreements (STANAGs). The STF is being developed to facilitate both types of improvements by providing a means for transforming and capturing the information exchange STANAGs into a machine-interpretable format, such as XML, to support the NNEC Data Strategy goals.

- In particular, the Validation question will be answered by showing that:
  - The STF layered framework itself is necessary and sufficient to capture the minimum aspects of STANAG specifications in order to support interoperable information exchanges. For example, these should include being able to account for the following:
    - Different data element definitions (bit-based, text-based, XML-based),

- Different message types (fixed vs. variable length; XML-formatted vs. structured text),
- Different transport requirements (TCP/IP, UHF, UDP, etc.),
- Different business rules (transmit/receive rules, transactions, business processes, etc.)
- Different information exchange domain requirements (security, cross-operational, enterprises, etc.)
- The STF design rules and methodology provide a common framework to transform information exchange specifications into XML, a machine-interpretable format, to support reuse, harmonization and semantic interoperability.

445. In order to address the second question, the STF product is continuously being shared with stakeholders to ensure the STF is designed to deliver all functionality. There is a constant feedback to the STF and IER/IES Stakeholders, and the STF is continuously reviewed with walkthroughs and inspection meetings to evaluate the conceptual layers, XML artefacts, design rules and methodology.

- Verification can be addressed by showing that if one applies the STF one is able to:
  - Transform relevant sections of existing information exchange STANAGs into machine-interpretable representations to support the NNEC data strategy
  - Apply it to identify and capture all necessary aspects of information exchange specifications within current STANAGs
  - Either reuse existing specifications or develop new ones to fill in any gaps, such as missing or insufficient specification for the data bearer/routing levels, in a machine-interpretable format
  - Capture and harmonize data elements in a common way to support reuse, data sharing and interoperable information exchanges across communities of interest
  - Specify message structures and business rules in a common way to readily support semantic interoperability

446. This STF V&V process fits into the overarching #STF\_Holistic\_Process | STF Holistic Process, where the STF is being applied to various Case Studies within different communities to transform relevant aspects of their information exchange STANAGs into XML to get the necessary feedback to verify, validate and mature the STF. In this section, these V&V case studies are discussed with a particular emphasis on answering the V&V questions posed above.

### **A.7.2. STF V&V Case Studies**

447. The STF has been applied to various communities of interest including the Asset Tracking (AST), Friendly Force Tracking (FFT), Joint Intelligence, Surveillance and Reconnaissance (JISR) and Tactical Data Link (TDL) communities of interest (COIs).

448. Below is a table that summarizes how the STF has been applied to the various COIs to identify, transform and/or develop relevant STANAGs/Standards to support interoperable information exchanges within those communities.

**Table A.9. STF Applied**

<b>COI</b>	<b>STANAG/Standard</b>	<b>Applicable STF Layers</b>	<b>Information Exchange Aspects</b>
Asset Tracking	5500 [APP-11 (MTF, XML-MTF)]	DED, MS	Text-based and XML-based
	2183 (AAITP-6)	Data bearer, Routing, Security cross-domain, Web services	Draft labeling, SMTP
	2185 (AAITP-4)	Business Rules	
FFT	5500 [APP-11 (MTF, XML-MTF)]	DED, MS	Text-based and XML-based
	5527	Security Cross-Domain, Web Services, Operational Cross-Domain	Draft XML Schemas, Draft service specification (SIP-3)
JISR	4607 (GMTIF)	DED, MS	Bit-based (variable-length)
	4609 ([KLV only])	MS, DED, Routing, Data Bearer	CODEC Formats (e.g. MPEG2, H.264, KLV), Bit-based Data Streams (Video, Audio, Metadata), MPEG-2 Transport Stream
TDL	5501 (Link 1)	DED, MS	Bit-based (fixed)
	5516 (Link 16)	DED, MS	Bit-based (fixed)
	5518 (JREAP)	Data bearer, Routing, DED, MS	Bit-based (variable-length)
	5519 (VMF)	DED, MS	Bit-based (variable-length)

COI	STANAG/Standard	Applicable STF Layers	Information Exchange Aspects
	5522 (Link 22)	DED, MS	Bit-based (fixed-length)
	5601	Operational Cross-Domain	Forwarding rules between Link1 and Link11/11B
	5616	Operational Cross-Domain	Forwarding rules between Link16 and Link11/11B

### **A.7.3. V&V in the Asset Tracking COI**

449. In support of NATO Overarching Architecture 3.1 (OA 3.1) NOV-3 Operational Information Requirement for exchanging Prioritized Critical Assets List (IP632), the Asset Tracking (AST) COI used the AAP-51A (Asset Tracking Business Process Model) to derive NOV-3 Information Requirements specific to tracking of consignments, transport packages and personnel. The STF was applied from the onset to assist in analyzing and identifying the information exchange requirements in support of these Asset Tracking-specific Information Requirements.

#### **A.7.3.1. STF Analysis: Asset Tracking**

450. Based on this analysis, it was determined that the relevant IESs were STANAG 5500 (ADatP-3 XML-MTF format), STANAG 7149 (NATO Message Catalogue APP-11), STANAG 2183 (AAITP-6) and STANAG 2185 (AAITP-4).

451. In particular, it was determined that the structure of messages and the data elements contained within them were to be specified according to STANAG 5500 ADatP-3 following the XML-MTF format, and to be included within the STANAG 7149 Allied Procedural Publication 11 (APP-11), NATO Message Catalogue. The ASTWG developed the corresponding AST-XML-MTF message set, and are to be published later in 2012 with a new edition of APP-11.

452. The STF layers were applied to evolve the AAITP-6 and AAITP-4 specifications to ensure that the data bearing, routing and business rules layers were also covered. In particular, standards for the routing and means of bearing the actual messages appear in AAITP-6 (STANAG 2183) and the business rules are captured in AAITP-4 (STANAG-2185).

453. The Table captures this mapping to illustrate which layers of the STF are covered by which IES specifications.

**Table A.10. Asset Tracking Information  
Exchange Requirement (IER) Analysis**

<b>Required NOV-3 Information Product</b>	<b>Derived Information Product Requirement(s)</b>	<b>Domain(s)</b>
Prioritized Critical Asset List (IP632), Joint Prioritized Critical Asset List (IP634)	Asset Tracking data	Logistics, Security (NATO/Nations)

**Table A.11. STF Holistic Process to Asset Tracking Analysis**

<b>STF Holistic Process &lt;--&gt; Asset Tracking</b>		
<b>STF Layers mapped to IER</b>	<b>IES/Specs per Layer</b>	<b>STF Information Exchange Aspects</b>
Security Cross-Domain	AAITP-6/STANAG 2183	labeling
Business Rules	AAITP-4/STANAG 2185 <i>(plain English statements, not machine readable XML)</i>	NOT XML
Message Structure	part of APP-11 message catalogue (STANAG 7149), ADatP-3 XML-MTF covered by STANAG 5500	XML-based
Data Element Dictionary	part of APP-11 message catalogue (STANAG 7149), ADatP-3 XML-MTF covered by STANAG 5500	Text-based
Routing	defined in AAITP-6	SMTP
Data Bearer		
Web Services	AAITP-6 <i>(guidance is provided, but a specification does not exist, yet)</i>	NOT DEFINED
Operational Cross-Domain	NOT DEFINED	NOT APPLICABLE

### **A.7.3.2. Asset Tracking Conclusions**

454. As highlighted in the table, comparative analysis between the STF Layers and the Asset Tracking information exchange requirements highlighted the lack or incomplete definition related to the following:

- Business Rules are currently formulated in plain English statements, and are not (yet) captured in machine readable XML

- WS (a Web Services guidance is provided but a specification is scheduled for next edition)
- Cross-COI Information Exchange

### **A.7.3.3. STF Overall V&V Conclusions: Asset Tracking**

455. The V&V of the STF Layers as applied to the AST COI did show that the layers provided the necessary components to analyze the information exchange requirements for Asset Tracking messages, and helped to identify gaps in the existing specifications to support that information exchange.

456. The V&V of the STF design rules, XML artefacts and methodology showed that it was able to be applied in the development of two new information exchange STANAGs (2183 and 2185) in support of supporting the Asset Tracking information exchange requirements.

457. Currently, the AST-XML-MTF messages and data elements have been captured in XML in-line with the STANAG 5500 XML-MTF Schemas, but not in-line with the STF XML Schemas. The capture of XML-based DED and MS are out-of-scope of STF Version 1.0, but the need for this has already been identified and captured within the STF Design Rules. It is envisioned that this will be provided in STF Version 2.0.

### **A.7.4. V&V in the Friendly Force Tracking (FFT) COI**

458. The FFT COI initiated a transformation of the specifications related to FFT information exchange: currently the NFFI "D" Document, STANAG-5527 and STANAG 5500 are the relevant documents for this COI.

#### **A.7.4.1. STF Analysis: FFT Phase 1 (NFFI "D" Document)**

459. In the initial analysis of FFT information exchange, it was determined that the only specification available at the time was the NFFI "D" Document. This document was a C3B "Decision" Document that is meant to capture the NFFI format, which is the basic message format used to support FFT.

**Table A.12. FFT Information Exchange Requirement (IER) Analysis**

<b>Required NOV-3 Information Product</b>	<b>Derived Information Product Requirement(s)</b>	<b>Domain(s)</b>
Order Of Battle - Land Forces (IP478), Own Land Forces Situation Report (IP482)	FFT data	Land, Operational Cross-Domain (Joint, Air, Maritime)

**Table A.13. STF Holistic Process to FFT Phase 1 Analysis**

<b>STF Holistic Process &lt;--&gt; FFT Phase 1: NFFI "D" Document</b>		
<b>STF Layers mapped to IER</b>	<b>IES/Specs per Layer</b>	<b>STF Information Exchange Aspects</b>
Security Cross-Domain	NOT DEFINED	
Business Rules	NOT DEFINED	
Message Structure	AC/322-D(2006)0066 - Interim NFFI Standard for Interoperability of FTS	XML-based
Data Element Dictionary	AC/322-D(2006)0066 - Interim NFFI Standard for Interoperability of FTS	XML-based
Routing	NFFI "D" Document	TCP and UDP as defined in IP-1 and IP-2
Data Bearer		
Web Services	NOT DEFINED	
Operational Cross-Domain	NOT DEFINED	

**460. STF Conclusion: NFFI**

461. A comparative analysis between the STF Layers and the NFFI "D" Document highlighted the lack of specifications related to the:

- Business Rules
- Web Services
- Security Cross Domain
- Cross-COI Information Exchange

462. These gaps were brought to the attention of the Stakeholders. It was eventually decided to not use the NFFI "D" Document for the message definitions, but rather move along a different path and to align with the XML-MTF format, as agreed in STANAG 5500. Also, it was decided to develop a new STANAG, STANAG 5527, in-line with the STF so that the gaps could be filled.

**A.7.4.2. STF Analysis: FFT Phase 2 (STANAG 5527)**

463. Based on the decisions based on the STF Conclusions of Phase 1, in Phase 2 NATO began to capture the FFT-related messages in-line with STANAG 5500, with these new messages to be made available in the APP-11 NATO Message Catalogue. Effort was also undertaken to



use the STF layered framework as a basis for developing the specification to support the FFT information exchange in STANAG 5527, where the specification for each layer is captured in different sections on the STANAG.

**Table A.14. STF Holistic Process to FFT Phase 2 Analysis**

<b>STF Holistic Process &lt;--&gt; FFT Phase 2</b>		
<b>STF Layers mapped to IER</b>	<b>IES/Specs per Layer</b>	<b>STF Information Exchange Aspects</b>
Security Cross-Domain	STANAG 5527: Security Cross-Domain XML Schemas	Draft XML Schema used to capture the security Labeling and Sanitizing
Business Rules	NOT DEFINED	
Message Structure	part of APP-11 message catalogue (STANAG 7149), ADatP-3 XML-MTF covered by STANAG 5500	XML-based
Data Element Dictionary	part of APP-11 message catalogue (STANAG 7149), ADatP-3 XML-MTF covered by STANAG 5500	XML-based
Routing	STANAG 5527	Interface Profiles: IP-1 (TCP) and IP-2 (UDP)
Data Bearer		
Web Services	STANAG 5527: Web Services Specification	Draft version of the SIP-3
Operational Cross-Domain	STANAG 5527: Cross-COI XML Schemas	Draft Schemas used to capture mapping details for allowing data transfer between differing standards (i.e. NFFI to FFI MTF and NFFI to OTH-Gold)

**A.7.4.3. STF Overall V&V Conclusions: FFT**

464. The V&V of the STF layers did show that the layers provided the necessary components to analyze the information exchange requirements for FFT, and helped to identify gaps in the existing specifications to support that information exchange.

465. The V&V of the STF design rules, XML artefacts and methodology showed that it was able to be applied in the development of a new information exchange STANAG 5527 in support of supporting the FFT information exchange requirements.

466. Overall, the V&V of the STF showed that

- The STF layered approach helped to identify gaps in the existing specifications to support that information exchange for FFT
- The STF supported the reuse of existing specifications:
  - In the DED and MS layers: STANAG 5500 and STANAG 7149
  - In the Transport/Data Bearer layers: IP-1 (TCP) and IP-2 (UDP)
- The STF supported the development of a new information exchange format: STANAG 5527

### **A.7.5. V&V in the JISR COI**

467. Within the JISR-community, there is a multi-national R&D group, called the Multi-INT All-Source Joint Intelligence, Surveillance and Reconnaissance Coalition (MAJIIC2), that focuses on developing the standards, technologies, processes and policies to support the interoperability and integration of Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) systems within a networked enabled enterprise. Within this enterprise, there is a need to disseminate many different types of ISTAR data products, including, but not limited to, raw and exploited Ground Moving Target Indicator (GMTI), Synthetic Aperture Radar (SAR) and Electro-Optical(EO)/Thermal Imaging (TI) imagery/motion imagery, weapon locating information, Electronic Support Measures (ESM), etc. These different data products may be disseminated via different transport mechanisms (broadcasted on LAN, multicast on WAN, streaming video, still imagery files, tactical data links, via NATO Standard ISR Library Interface servers, etc.) based on the needs and requirements of the end users and functional scenario.

468. As an initial case study, the STF was applied to two of the JISR information exchange requirements, namely GMTI and motion imagery, with the goal to be able to support interoperability testing and validation of these types of information exchanges.

#### **A.7.5.1. GMTI**

469. GMTI is used within the JISR community to detect and report on ground moving targets in support of the NOV-3 Operational Information Requirement to exchange Moving Target Indicator Exploitation Reports (IP660).

470. At the time of the analysis, the relevant documents to specify the information exchange of GMTI were the NATO Ground Moving Target Indicator Format (STANAG 4607), NATO STANAG 4607 Implementation Guide (AEDP-7) and the MAJIIC2 STANAG 4607 Implementation Guides (MAJIIC2 IG)

### A.7.5.1.1. STF Analysis: GMTI Information Exchange

471. Following the STF Holistic Process, the STF layers were used as a guidance to analyze the information exchange requirements for GMTI and to map the contents of the existing IES documents onto the STF layers to help identify possible gaps within the existing specifications.

472. These are shown below:

**Table A.15. GMTI Information Exchange Requirement (IER) Analysis**

Required NOV-3 Information Product	Derived Information Product Requirement(s)	Domain(s)
Moving Target Indicator Exploitation Report (IP660)	Ground Moving Target Indicator (GMTI) data	JISR, Security (NATO/Nations)

**Table A.16. STF Holistic Process to GMTI Analysis**

STF Holistic Process <--> GMTI		
STF Layers mapped to IER	IES/Specs per Layer	STF Information Exchange Aspects
Security Cross-Domain	STANAG 4607: Appendix A (for DED, MS & allowable values) <i>Note: same specification repeated in AEDP-7: Appendix B Not captured in XML</i>	NOT APPLICABLE
Business Rules	AEDP-7, MAJIIC2 IG	NOT APPLICABLE
Message Structure	STANAG 4607	Variable-length
Data Element Dictionary	STANAG 4607	Bit-based
Routing	AEDP-7, MAJIIC2 IG( <i>Guidance, but no specifications</i> )	Embedded within other ISR formats (e.g. STANAG 4545, STANAG 7023)
Data Bearer		
Web Services	NOT DEFINED	NOT APPLICABLE
Operational Cross-Domain	NOT DEFINED	NOT APPLICABLE

### A.7.5.1.2. GMTI Conclusions

- STANAG 4607 specifies the GMTI format

- The STF DED and MS XML artefacts were sufficient and were applied to capture the Data Element Dictionary and Message Structure of the GMTI information exchange, as specified within the STANAG 4607 document.
- STANAG 4607 discusses Data Transmission only with respect to how to handle the messages. There are no sections in this document discussing how to physically transmit the GMTI data.
- The MAJIIC2 STANAG 4607 Implementation Guide was developed by the MAJIIC community for standardizing how GMTI data would be shared amongst the MAJIIC participants. They selected a transport mechanism (UDP Broadcast), which is **not** mentioned within any of the other Standardized documents.
- AEDP-7 provides an Appendix discussing various options for physically sharing the GMTI data. However, there are no specific guidance provided on which are the preferred way, as advised by the STF to provide.
- The MAJIIC2 community is currently transforming their way of business to be interoperable within an NNEC environment. Also, they have identified the need for sharing GMTI between various security domains, across different operational domains and via web services.
- These are identified as Gaps within the STF layers, but are out-of-scope for this V&V assessment.

#### **A.7.5.1.3. STF Applied Conclusions: GMTI**

- STANAG 4607 (GMTI Format) Edition 2 was successfully transformed into XML using the STF design rules & methodology at the DED and MS layers.
- The content of the STANAG 4607 Implementation Guides were analyzed and successfully mapped to the STF layers.
- Gap: Although various Data Bearer/Routing options were identified within the relevant documents, it was not specified when or how to use each option.
- Also, it should be noted that the "UDP broadcast" option was chosen by the MAJIIC community as their GMTI transport mechanism and specified within their Implementation Guide, but this was not provided as an option within the NATO STANAG 4607 or AEDP-7 documents. Therefore, implementations within the MAJIIC community may be interoperable with each other, but might not be interoperable with external communities.
- Recommendation: Improve specification and explicitly capture data bearer/routing requirements within STANAG for interoperable GMTI information exchange.

**A.7.5.1.4. STF V&V Conclusions: GMTI**

473. The STF layers do provide the coverage needed to identify the GMTI information exchange requirements that are needed to support interoperability.

474. The V&V of STF Design Rules & methodology at the DED and MS layers showed that it was sufficient to transform STANAG 4607 (GMTI Format) Edition 2 into XML using the STF XML artefacts.

**A.7.5.2. Motion Imagery (MI)**

475. With MI, the relevant standard is STANAG 4609, which is aimed at promoting interoperability of present and future motion imagery systems within and among NATO nations. Similar to GMTI, MI system implementers have to rely on various implementation guides, the NATO Motion Imagery (MI) STANAG 4609 Implementation Guide (AEDP-8) and the MAJIIC2 STANG 4609 Implementation Guides, in particular, in order to achieve interoperable implementations. There is also a MAJIIC2 Business Rules document available that provides details on motion imagery information exchange interaction requirements, especially with respect on how to utilize the Coalition Shared Data servers.

476. In general, digital MI is composed of two major components, the Data Stream; and the Format. The Data Stream may actually be a set of "elementary" streams such as video, audio, metadata, and subtitles. Each stream type is processed by a specific encoder/decoder (CODEC). The Format is the protocol for transporting the streams through networks or in files. In STANAG-4609, formats available for MPEG2 are Elementary Stream (ES), Program Stream (PS), and Transport Stream (TS). PS and TS formats are capable of carrying multiple synchronized streams.

477. We have mapped the content of those implementation guides to the STF horizontal layers in the table below.

**Table A.17. Motion Imagery Information Exchange Requirement (IER) Analysis**

Required NOV-3 Information Product	Derived Information Product Requirement(s)	Domain(s)
Video Product (IP653)	Full motion video streams, Video clips, Video-on-demand streams (STANAG 4609)	JISR, Security Cross-Domain

**Table A.18. STF Holistic Process to Motion Imagery Analysis**

<b>STF Holistic Process &lt;--&gt; Motion Imagery</b>		
<b>STF Layers mapped to IER</b>	<b>IES/Specs per Layer</b>	<b>STF Information Exchange Aspects</b>
Security Cross-Domain	STANAG 4609	NOT APPLICABLE
Business Rules	AEDP-8, MAJIIC2 STANAG 4609 Implementation Guide, MAJIIC2 Business Rules	NOT APPLICABLE
Message Structure	STANAG 4609 (references SMPTE RP 210; MISB Standard 0801)	CODEC Formats (e.g. MPEG2, H.264, KLV)
Data Element Dictionary	STANAG 4609	Bit-based Data Streams (video, audio, metadata "elementary" streams)
Routing	STANAG 4609	MPEG2 Transport Stream (TS), MPEG2 Program Stream (PS)
Data Bearer	MAJIIC2 STANAG 4609 Implementation Guide, MAJIIC2 Business Rules	UDP, RTP/RTSP, TCP, HTTP/HTTPS
Web Services	NOT DEFINED	NOT APPLICABLE
Operational Cross-Domain	NOT DEFINED	NOT APPLICABLE

### **A.7.5.2.1. MI Conclusions**

- STANAG 4609 DED and MS
  - The STF DED and MS XML artefacts were able to capture the Data Element Dictionary and Message Structure of the KLV "metadata" elementary stream in XML.
  - The STF DED and MS XML artefacts were not used to capture the DED and MS of the other "elementary" data streams, such as the video and audio. These were considered out-of-scope of this case study.
- STANAG 4609 discusses Routing via the MPEG2 Transport Stream and Program Stream. These are slightly different formats for transmitting and storing motion imagery. This could lead to interoperability issues between participants if they do not have the correct implementations to handle both formats.
- The MAJIIC2 STANAG 4609 Implementation Guide was developed by the MAJIIC community for standardizing how MI data would be shared amongst the MAJIIC participants. Within this community, it has been agreed to implement the MPEG2-

TS. Although interoperability would be achieved within the MAJIIC community, interoperability with other STANAG 4609 implementers could not be guaranteed.

- STANAG 4609 does not prescribe how to physically transport the video streams--there are many options as listed in the table, such as UDP, HTTP/HTTPS, RTP/RTSP, etc. It is left up to the end users to decide how to do so. This can lead to non-interoperable implementations of the STANAG.
- The MAJIIC2 community has chosen to use MPEG2-TS over UDP, which is very lossy. They are investigating possibly using RTP/RTSP.
- The MAJIIC2 community is currently transforming their way of business to be interoperable within an NNEC environment. Also, they have identified the need for sharing MI across different operational domains and via web services.
- These have been identified as Gaps within the STF layers, but are out-of-scope for this V&V assessment.

#### **A.7.5.2.2. STF V&V Conclusions: MI**

- Following the STF, it is recommended that the STANAG is improved to provide explicit guidance on which routing and data bearer options should be chosen based to support interoperable solutions.
- The question arose on whether the STF would or should be applicable for capturing the video and audio elementary streams of the STANAG 4609 specification in XML.
  - At first glance, it does not seem that STF would be applicable as Motion Imagery is a **unidirectional** data transfer from a source to a client. It has been stated that STF should be applied only to information exchange, and specifically message exchange, specifications.
  - As MI has no "information exchange" per se, as an information exchange is defined as being a **bidirectional** transmission of data, and is not based on "message exchanges", it would seem like STF would not be applicable.
  - However, further analysis and work would need to be done to determine how applicable the STF could be for capturing the specification to ensure interoperable processing of the full data stream.
- In fact, this is a good case study to use to further elaborate and mature the other layers of the STF so that we get a clearer definition of what it means to transform this type of specification into XML.

#### **A.7.6. V&V in the TDL COI**

478. The STF has been applied within the TDL CaT via tasking to the TDL CaT in XML Syndicate (TDLXMLS) to enable the transformation of TDL-specific STANAGs into XML.

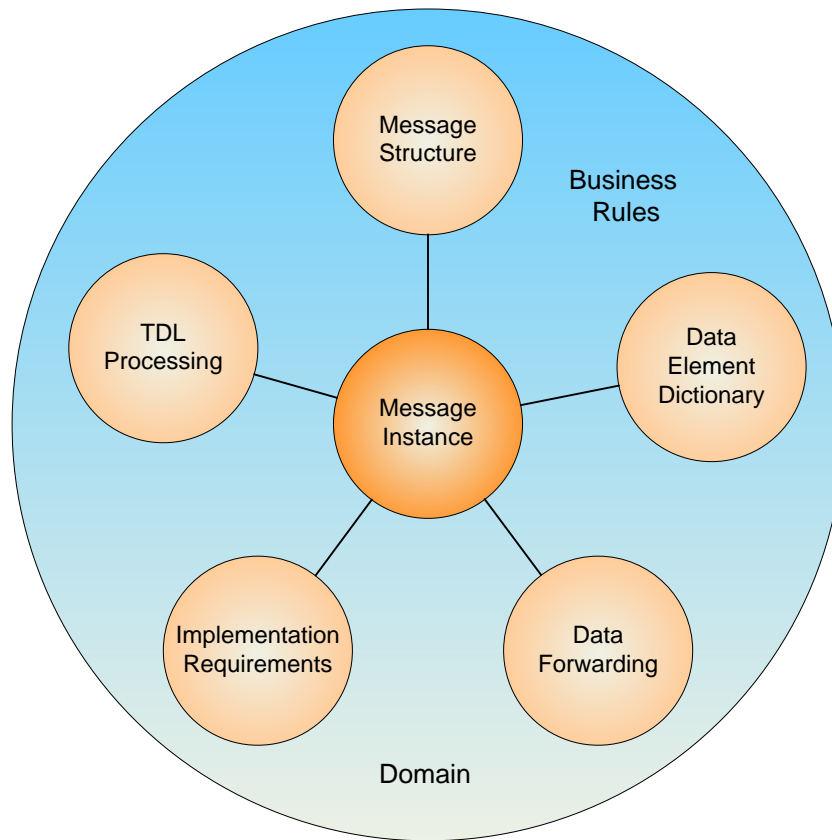
As one of the first applications of the STF, it provided a great forum to mature the concepts and ideas captured within the framework.

479. The application of the STF concept to transform the TDL standards into XML was seen as the appropriate way to go to "preclude the continued independent development of unique solutions for each TDL standard." In particular the following were the standards of interest:

- STANAG 5501 (Link 1)
- STANAG 5511 (Link 11/11B)
- STANAG 5516 (Link 16)
- STANAG 5518 (JREAP) - under ratification
- STANAG 5519 (VMF) - under ratification
- STANAG 5522 (Link 22)
- STANAG 5601 (Data Forwarding between Link 1, 11, 11B and 14)
- STANAG 5616 (Data Forwarding between Link 11/11B and 16)

480. The STF's layered approach easily lent itself to the TDLXMLS's goals by providing a framework whereby the various components, e.g. data element dictionary, message structure, business rules, which characterizes a typical TDL information exchange could be separated out, harmonized and common parts reused. The TDLXMLS developed a framework in line with the STF, focusing on those layers applicable to the current STANAGs (see Figure A.32 below) while a harmonization phase needs to take place to address all STF layers.





**Figure A.32. xTDL Framework**

### **A.7.6.1. Link 16**

481. The work of the TDLXMLS focused on STANAG 5516, while keeping the generic aspect into account when applying the methodology on the other STANAGs.

482. The STF was applied to capture the following aspects of the information exchanges:

- Data Element Dictionary
- Message Structure
- Transmit/Receive Rules (TDL Processing)
- Minimum Implementation (MIN IMP)/Implementation Requirements (IMP REQ)
- Cross-STANAG mapping (Data Forwarding)
- Business Rules

483. Results have been achieved so far for the Data Element Dictionary and Message Structure with on-going effort to capture the TDL Processing in the form of the Transactions as defined

by STANAG 5516. The structure of these Transactions offer a generic approach to model the overall message exchange between systems which is believed to be applicable to other information exchanges as well.

484. To fulfill the STF Operational Cross-COI layer, the Data Forwarding as defined in STANAG 5616 between Link 11/11B and Link-16 Systems is used. This is on-going effort and will also result in feedback to the STF.

485. The STF Data Bearer and Routing layers are, for Link 16, addressed in several ways. Traditionally, Link-16 uses radio frequency (RF) to exchange its J-messages within line-of-sight, although emerging technologies, such as IP and UHF SATCOM, provide the means to pass Link 16 data over long-haul protocols beyond line-of-sight. The traditional RF mechanism is defined in the MIDS standard while the JREAP (Joint Range Extension Application Protocol) standard (STANAG 5518) governs the IP and SATCOM transport. In particular, the JREAP standard defines its own message set and data elements to define the transport level protocol for the exchange of Link 16 J-messages. The JREAP messages and data elements are captured via the STF XML Schemas as well, requiring additional support in the XML Schema to indicate the nesting of Link 16 messages withing the JREAP messages. This enhancement will be retrofitted in the STF XML Schema in version 2. Worthwhile to note is that some of the Link 16 Data Elements are reused within the JREAP DED. Capturing the specific business rules of JREAP is a further action which have to support and tie in with the overall Link 16 business rules.

486. Additionally, the Link-16 Implementation Requirements have been captured in XML with a corresponding XML Schema which will need to be retrofitted in the STF as currently no generic STF XML Schema is provided yet.

**Table A.19. Link 16 Information Exchange Requirement (IER) Analysis**

<b>Required NOV-3 Information Product</b>	<b>Derived Information Product Requirement(s)</b>	<b>Domain(s)</b>
Various incl. Recognized Air Picture (IP82), Joint Target List (IP44), Electronic Warfare Mission Summary (IP326), Target Track Report (IP575), Engagement Of Hostile Aircraft Report (IP302)	Tactical Data Exchange - Link 16 (STANAG 5516)	TDL, Operational Cross-Domain (Joint, Land, Air, Maritime, JISR), Security Cross-Domain

**Table A.20. STF Holistic Process to Link 16 Analysis**

<b>STF Holistic Process &lt;--&gt; Link 16</b>		
<b>STF Layers mapped to IER</b>	<b>IES/Specs per Layer</b>	<b>STF Information Exchange Aspects</b>
Security Cross-Domain	NOT DEFINED	MISSING

<b>STF Holistic Process &lt;--&gt; Link 16</b>		
<b>STF Layers mapped to IER</b>	<b>IES/Specs per Layer</b>	<b>STF Information Exchange Aspects</b>
Business Rules	STANAG 5516	Transactions including Receive/Transmit Tables, Database Records
Message Structure		Fixed length messages
Data Element Dictionary		Bit-based
Routing	STANAG 5518 Joint Range Extension Application Protocol (JREAP), or STANAG 4175 VOL I: Technical Characteristics of the Multifunctional Information Distribution System (MIDS)	Depends on transmission media. Options include JREAP (see table below) for non-LOS or RF for LOS
Data Bearer		IP-based (UDP or TCP), or RF
Web Services	NOT DEFINED	MISSING
Operational Cross-Domain	STANAG 5616	Message and Field forwarding rules between Link 11/11B and Link 16

**Table A.21. STF Holistic Process to JREAP Analysis**

<b>STF Holistic Process &lt;--&gt; JREAP</b>		
<b>STF Layers mapped to IER</b>	<b>IES/Specs per Layer</b>	<b>STF Information Exchange Aspects</b>
Security Cross-Domain	NOT DEFINED	MISSING
Business Rules	STANAG 5518	Not clearly defined; missing guidance on how to handle JREAP management messages (such as, Should management messages be forwarded? How should they be processed? How to avoid circular forwarding? etc.)
Message Structure	STANAG 5518	Variable length messages
Data Element Dictionary	STANAG 5518: APPENDIX D DATA ELEMENT DICTIONARY	Bit-based
Routing		Depends on Transmission Media: see applicable Appendix

<b>STF Holistic Process &lt;--&gt; JREAP</b>		
<b>STF Layers mapped to IER</b>	<b>IES/Specs per Layer</b>	<b>STF Information Exchange Aspects</b>
Data Bearer	Appendix A- Half-Duplex Announced Token Passing Protocol  Appendix B Full-Duplex, Synchronous Or Asynchronous Point-To-Point Connection Protocol  Appendix C Encapsulation Over Internet Protocol (IP)	
Web Services	NOT DEFINED	MISSING
Operational Cross-Domain	STANAG 5518	Forwarding rules between tactical networks in English; needs to be specified in XML

### **A.7.6.1.1. Conclusions of STF applied to Link-16**

487. Capturing the specification of STANAG 5516 in XML has resulted in various relevant results:

- By applying an automated conversion from the Word-based STANAG, many errors have been found ranging from simple typos or layout inconsistencies to wrong references or missing definitions. These have been captured and provided to the TDL CaT for consideration for a DLCP.
- As various editions have been captured, an additional mechanism was available to verify the differences between subsequent versions.
- JREAP is an application-layer protocol & message that enables transmitting Link-16 over IP. Therefore, STF can and was also applied to capture the information exchange requirements for that protocol.
- The STF was applicable for capturing the DED and MS of JREAP in XML.
- It was discovered that within the JREAP specification, STANAG 5518, there were no clear guidance on the roles and responsibilities of JRE Processors for forwarding management messages between JRE Processors networks. There are references to Relay flags, but no explicit business rules for sending and receiving management messages necessary for JREAP network management. This needs to be captured and provided to the JREAP Custodians for consideration.

- Neither STANAG 5516 nor STANAG 5518 provides any specifications or discussions on Security or Web Services. These need to be remedied in order to support the NNEC data strategy goals.

### A.7.6.2. Link 22

488. Link 22 is being developed by the NATO Improved Link Eleven (NILE) Program. The goals of the development of Link 22 included the replacement of Link 11, complementing Link 16 and improvement of the Allied interoperability. As such, the Link 22 Data Elements and the Message Structure reuses many of the Link 16 ones contributing to increased standardization and interoperability.

489. The Link 22 tactical messages and its data elements have been captured using the same XML Schemas as for Link 16. This provided the opportunity to perform an automatic comparison between the two resulting in a number of differences. Both the XML documents and the outcome of the comparison have been provided to the NILE community. Additional work on the messages and data elements used in the transport layer have been captured by NCI Agency-CapDev.

**Table A.22. Link 16 Information Exchange Requirement (IER) Analysis**

Required NOV-3 Information Product	Derived Information Product Requirement(s)	Domain(s)
Various incl. Recognized Maritime Picture (IP84), Maritime Intelligence Report/Summary (IP387/388), Electronic Warfare Mission Summary (IP326), Target Track Report (IP575), Merchant Shipping Situation Report (IP396)	Tactical Data Exchange - Link 22(STANAG 5522)	TDL, Operational Cross-Domain (Joint, Land, Air, Maritime, JISR), Security Cross-Domain

**Table A.23. STF Holistic Process to Link 22 Analysis**

STF Holistic Process <--> Link 22		
STF Layers mapped to IER	IES/Specs per Layer	STF Information Exchange Aspects
Security Cross-Domain	NOT DEFINED	MISSING
Business Rules	STANAG 5522	Not captured as STANAG does not provide transactions (yet) in same format as for Link 16

<b>STF Holistic Process &lt;--&gt; Link 22</b>		
<b>STF Layers mapped to IER</b>	<b>IES/Specs per Layer</b>	<b>STF Information Exchange Aspects</b>
Message Structure	STANAG 5522	Fixed length messages
Data Element Dictionary		Bit-based
Routing	STANAG 4175 VOL I: Technical Characteristics of the Multifunctional Information Distribution System (MIDS)	RF for LOS
Data Bearer		
Web Services	NOT DEFINED	MISSING
Operational Cross-Domain	non-NATO MIL-STD 6020	Data Forwarding between Link 22 and Link 16 not captured as not yet covered in STANAG 5616

### **A.7.6.2.1. Conclusions on STF applied to Link-22**

490. Using the XML representation of both the Data Element Dictionary and the Message Structure, for both Link-16 and Link-22, comparisons have been carried out by NCI Agency to verify that Link-16 Data Elements reused for Link-22 are indeed defined identically. Likewise for the Link-22 FJ-messages, which should be an equivalent version of the Link-16 J-message (with only 1 specific DataField prepended). Differences between the two have been analysed and reported to the NILE-PO.

### **A.7.6.3. Link 1**

491. Link 1 is a point-to-point, duplex, non-encrypted, digital NATO Tactical Data Link (TDL) Standard for the automatic exchange of Track and Strobe data, combined with link and data management messages. It's governed by STANAG 5501 which mainly describes the various messages (S-series) and data elements. The S-series messages are bit-based, fixed length and can be easily captured in the STF XML Schemas. This has actually been done by NCI Agency to demonstrate the usage of the STF on other TDLs.

**Table A.24. Link 1 Information Exchange Requirement (IER) Analysis**

<b>Required NOV-3 Information Product</b>	<b>Derived Information Product Requirement(s)</b>	<b>Domain(s)</b>
Recognized Air Picture (IP82)	Tactical Data Exchange - Link 1 (STANAG 5501)	TDL

**Table A.25. STF Holistic Process to Link 1 Analysis**

STF Holistic Process <--> Link 1		
STF Layers mapped to IER	IES/Specs per Layer	STF Information Exchange Aspects
Security Cross-Domain	NOT DEFINED	MISSING
Business Rules	STANAG 5501, ADatP-31	Not captured as STANAG nor ADatP-31 provide full business rules, specifically not in same format as for Link 16 (transactions)
Message Structure	STANAG 5501	Fixed-length messages
Data Element Dictionary		Bit-based
Routing	RS-232, STANAG 5501	Communication is serial (RS-232) with Link-1 specifics described in STANAG 5501
Data Bearer		
Web Services	NOT DEFINED	MISSING
Operational Cross-Domain	STANAG 5601 (Data Forwarding between Link 1 and Link 11/11B)	Not captured; STANAG does not contain full forwarding logic, e.g. message mapping

**A.7.6.3.1. Conclusions on STF applied to Link-1**

492. Applying the STF to Link-1 demonstrated the following:

- because of its simplicity, Link-1 was an easy information exchange to capture.
- capturing the layers that are actually covered by the STANAG 5501 turned out to be straightforward.
- it clearly highlighted layers that are not covered by any STANAG.
- even though some layers are covered in a STANAG, it also highlighted that these are lacking specific aspects or not detailed enough (so requiring interpretation).

**A.7.6.4. VMF**

493. Variable Message Format (VMF) provides a message catalogue of K-series messages described in STANAG 5519 which is the covering STANAG (to be ratified) for MIL-STD 6017. Together with a header message (described in MIL-STD 2045-47001) and bearer (MIL-STD 188-220) it constitutes a tactical data link. From an STF perspective, this is an interesting format as it clearly separated the STF layers in different standards: one for the message catalogue

(DED and Message Structure layers), one for the header (Routing layer) and one for the bearer (Bearer layer). Furthermore, by nature the messages or a variable length, requiring the STF XML Schemas to support also these types of messages.

494. Even though the current STF version 1.0 does not cater for variable length messages, some experimentation have been done by NCI Agency to extend the XML schemas in preparation of version 2.0. Initially, the various Data Elements of VMF have been captured which has shown to be possible and result in XML instance documents that could be used for documentation purposes and verifications. Because of the nature of the structure of VMF messages, the XML Schema will require extensions to allow for optional DataField and Group of DataFields, and for repetitions of a DataField and a Group of DataFields. This will be added, taking backwards compatibility into account, to the XML Schemas for STF version 2.0.

### **A.7.7. V&V for other information exchanges and COIs**

495. The STF, and in particular the DED and Message Structure schemas have been applied to several other information exchanges as detailed in the following sections.

#### **A.7.7.1. Over-the-horizon Targeting Gold**

496. Over-the-horizon Targeting Gold (OTH-Gold) is a text-based message format, mainly used in the maritime domain. It provides for a message set similar in structure and syntax to ADatP-11 Message Text Format (MTF) messages, with slant-delimited fields making up line-based Sets that are grouped into Messages. It's governed by the "Operational Specification for Over-the-horizon Targeting Gold" published by USA Navy Center for Tactical Systems Interoperability.

497. The STF XML Schemas governing text-based information exchanges have been used to capture the Data Element Dictionary and Message Structure of OTH-Gold, although it's not a NATO STANAG. This demonstrated the following:

- STF can be successfully applied to OTH-Gold for capturing the DED and MS.
- OTH-Gold uses a nesting structure with one Set amplifying the previous. The OTH-Gold Message Structure STF representation can be enhanced to also indicate this nesting aspect. This is foreseen in the next version of the STF.
- The OTH-Gold specification does not provide unique identifiers for its Data Elements. An initial approach has been taken to assign the DECI and DEI numbers although further harmonization is still required.

## **A.8. METHODS**

498. Please refer to the STF Holistic Process for the process for defining, applying and performing V&V of the STF. This Process is applicable both for V&V of the STF itself as well as for the V&V of the STF artefacts produced by the application of the STF Design Rules.



## **A.9. TOOLS**

499. NCI Agency exploited the capability to semi-automatically generate code to create tools to help validate the XML files in support of Interoperability Testing. In particular, the SMACQ/O-ANT tool suite is available that can be used to monitor the information exchange and to report on its compliance to the relevant Standards.

## **A.10. OUTSTANDING QUESTIONS**

500. Not yet addressed within the current version of the STF.

## **A.11. MISCELLANEOUS**

501. Not yet addressed within the current version of the STF.

## **A.12. FUTURE PLANS**

502. Work on the STF will continue with capturing further the missing aspects of current STF layers and adding the Design Rules and Methodology for additional layers including the XML Schemas to support it. The following is a planned list of items to work on:

503.

- Data Element Dictionary and Message Structure for XML-Based information exchanges
- Message Structure for Variable-length Bit-based information exchanges
- Security Cross-domain Layer

This page is intentionally left blank