Stavros Tsakonas
17.02.2022 11:31

Quality of Service requirements (QoS)	-
Complexity	Easy

5.3.6.7 Informal Messaging

Property Name	Description
Identification	Informal Messaging
Classification	TI
Behaviour	This component provides informal and formal messaging services to Users and to NCOP applications and services. This component is the Core BI-SC AIS E-mail services based on Microsoft Exchange.
Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved
Location (Types)	On NATO servers
Interfaces	NCOP interacts with this IC through POP3, MAPI and SMTP protocols
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

5.3.6.8 Core GIS

Property Name	Description
Identification	Core GIS
Classification	TI
Behaviour	A core Bi-SC AIS service, the Geographical Information Service (GIS) server provides a variety of geospatial-related services like Web Map Service (WMS), Web Feature Service (WFS) and Web Coverage Service (WCS).
Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved
Location (Types)	On NATO servers
Interfaces	NCOP interacts with this IC through OGC protocols and http/https end-points
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

In order to provide end-Users with the required GIS functionality, NCOP applications will interface with the GIS Core services provided by the Bi-SC AIS Core by supporting a group of standards and norms for geographic map formats also supported by the Bi-SC AIS Core GIS Services.

The Core GIS WMS, WFS and WCS interfaces are consumed by NCOP in order to display maps in the Geographical COP Editor.

5.3.6.9 Enterprise Management Service

Property Name	Description
Identification	Enterprise Management Service
Classification	TI
Behaviour	This component is the core Bi-SC AIS Enterprise Management Service providing logging and auditing of application events.
Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved
Location (Types)	On NATO servers
Interfaces	This IC interacts with NCOP services through SNMP, http/https … protocols
Collaboration mechanism	-

Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

NATO main tools for Enterprise Management Services are:

- Microsoft SCOM
- Ipswitch WhatsUpGold

These tools are able to retrieve the Windows event logs produced by NCOP components and centralize them for monitoring. The event logs to be retrieved are described in the chapter 5.3.3.1.3 Audit / Log.

In addition to Windows Event Logs, these tools are able to perform checks at the service level, especially http services. To perform basic NCOP service check, the following http access shall be verified periodically by EMS tools:

- access to NCOP Web services (especially JIPS)
- access to the default NCOP maps

5.3.6.10 Security Services and Settings

Property Name	Description
Identification	Security Services and Settings
Classification	TI
Behaviour	This Bi-SC AIS component is a set of approved NATO Security Settings that includes: Account Policies. Password policies, account lockout policies and Kerberos policies; Local Policies. Audit policy, User rights assignment, security options; Event Log Settings. Settings for event log parameters itself (e.g., max size of audit file); Restricted Groups. Membership of security-sensitive User groups; System Services. Start-up and permission for system services; Registry. Permissions for Windows registry keys; File System Permission. Permissions for folders and files; Removal of certain Folders and Files. Removal of some default files and registry keys; Installation of Devices. Settings for installation of specific hardware devices (e.g., floppy drives, microphones, etc.);

	Configuration of Specific Windows Software Modules. Settings for use of security related Windows software modules like DHCP, RAS, etc. BIOS Settings. Security related configuration data for BIOS;
Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved
Location (Types)	Installed on the SharePoint Server, the BizTalk Server, the Application Server, the GeoServer, and the SQL Server
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

The NCIRC 2019 is composed of the following GPO:

- NCSC_W2K19_DomainController_V1.0. It has to be applied on OU « Domain Controllers ».
- NCSC_W2K19_MemberServer_V1.0. It has to be applied on OU « W2K19 Servers » where NCOP SQL, BizTalk, SharePoint, APP and GeoServer servers are defined.
- NCSC_W2K19_UserScreenSaverPolicy_V1.0. It has to be applied on OU “Administrator Accounts” where NCOP administrator accounts are defined.
- NCSC_DomainPolicy_V1. . It has to be applied on OU Root of the domain.

5.3.6.11 Chat

Property Name	Description
Identification	Chat
Classification	TI
Behaviour	This component is the Bi-SC AIS Collaboration service; the Chat uses XMPP (RFC 3920, 3921, 3922, 3923).
Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved
Location (Types)	On NATO servers
Interfaces	NCOP interacts with this IC through XMPP protocol
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-

Quality of Service requirements (QoS)	-
Complexity	Easy

The Collaboration Services component provides the Chat based on the XMPP (Jabber) protocol, the Chat service is a purchaser furnished application integrated as part of the Increment-2, the others services (presence, whiteboard) will be provided later.

The embedded chat application allows the User to:

Launch the chat capability as a separate window;

Access common links as defined for the Organisational Node;

Receive notifications (if configured by the node administrator).

If the collaboration service is not available, NCOP operates in degrade mode (e.g. Chat notification is not available).

5.3.6.12 Document Handling System

Property Name	Description
Identification	Document Handling System
Classification	TI
Behaviour	This component is the Bi-SC AIS Document Handling System. DHS is based on SharePoint and provides a repository to store documents.
Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved
Location (Types)	On NATO servers
Interfaces	NCOP interacts with this IC through http/https end-points to retrieve any document. Each end-point corresponds to a document
Collaboration mechanism	https, https
Local/Configuration data	-
Operating context	TypeScript/JavaScript .NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

The Geographical COP Editor allows displaying BSOs and their links to external documents (located in DHS or in other location) as illustrated in Figure 5-129.

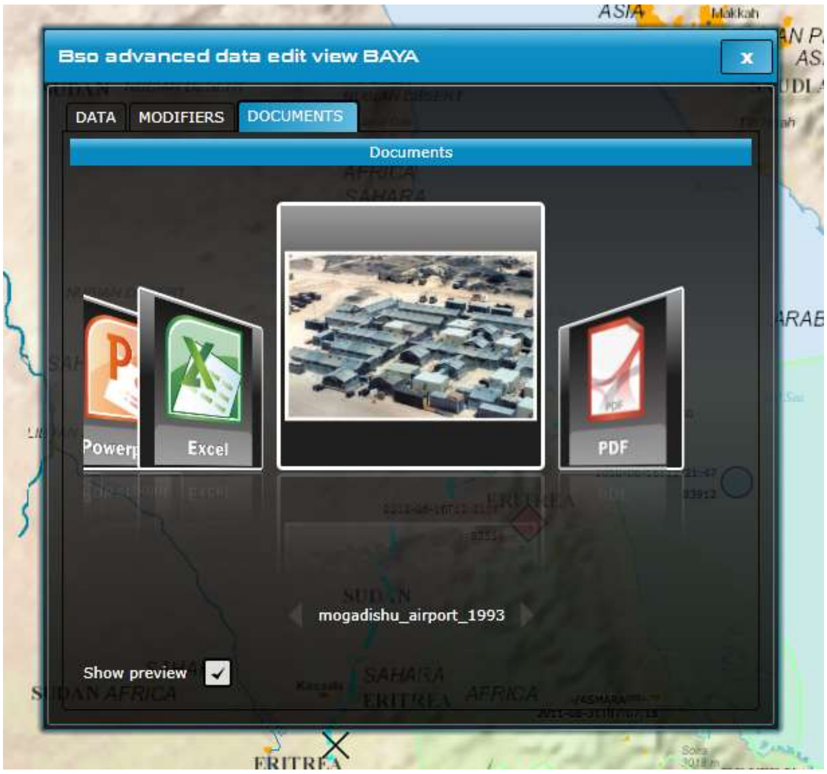


Figure 5-129: External documents (located in DHS …) linked to a BSO

5.3.6.13 NEDS (NATO Enterprise Directory Service)

Property Name	Description
Identification	NEDS
Classification	TI
Behaviour	In the future, NCOP will interact with the NEDS (NATO Enterprise Directory Service) in order to: Register its web services (NCOP as Web Service Provider); Find the available services that it can interact (NCOP as Web Service Consumer).
Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved
Location (Types)	On NATO servers
Interfaces	-
Collaboration mechanism	http, https
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-

Complexity	Easy

5.3.6.14 Identity Provider

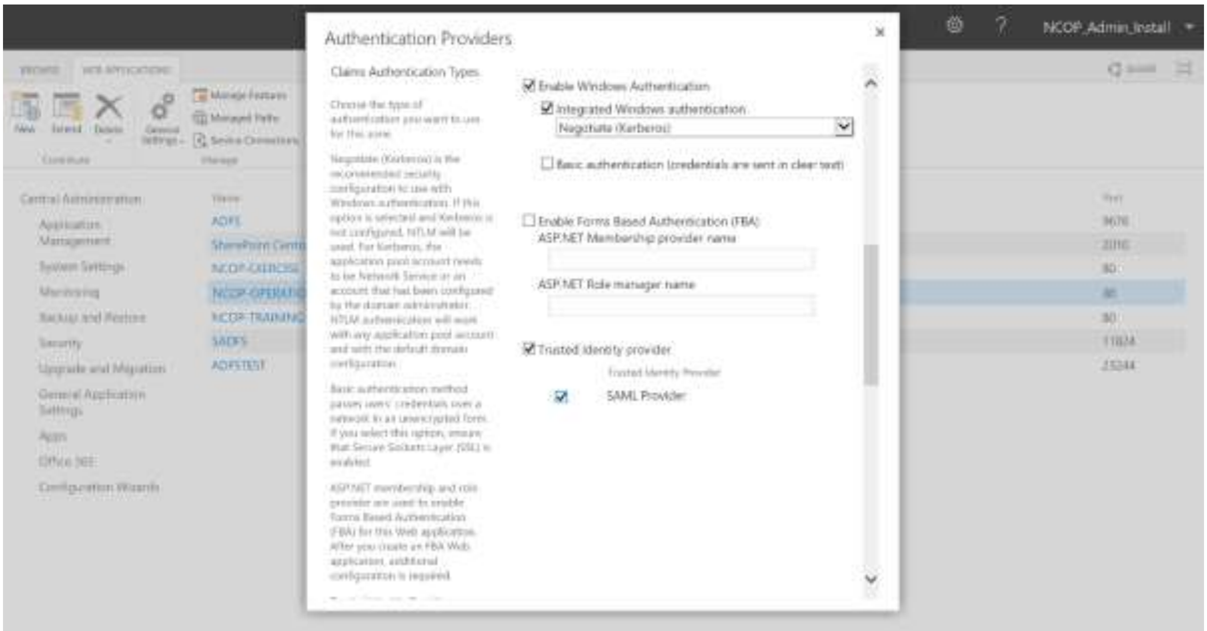
Property Name	Description
Identification	Identity Provider
Classification	TI
Behaviour	Active Directory Federation Services or any IdP (Identity Provider) provides access control and single sign on across NCOP applications. The user authentication and authorization is based on SAML tokens.
Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved
Location (Types)	On NATO servers
Interfaces	NCOP interacts with this IC through https endpoints
Collaboration mechanism	https
Local/Configuration data	Claims attributes
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

The main impacts of a new Identity Provider (any IdP or ADFS/SAML) on NCOP Increment-2 are the following:

- Access to SharePoint NCOP portals will be extended to SAML token (in addition of Kerberos token)
    - Authentication and authorization based on SAML token
    - RBAC will be compliant with users identified by a SAML token
- SAML Delegation
    - Required when NCOP users access SharePoint data from the Geographical COP Editor. The propagation of user credentials is required to allow traceability of user actions as well as authorization and verification of access rights to NCOP Information Elements.
- Claims Enabling Web Services: how to use the claims-based approach with web services, whereby a partner uses a smart client that communicates with identity providers and token issuers using SOAP-based services. The client uses the WS-Trust active federation protocol to obtain a token containing the claims that it needs to access the web service
- Securing REST Services: how to use the claims-based approach with web services, whereby a partner uses a smart client that communicates with identity providers and token issuers using REST-based services

- https: NCOP portals and authenticated NCOP web services will be hosted on https protocol instead of http protocol.

In SAML claims mode, SharePoint accepts SAML tokens from a trusted external Security Token Provider (STS), often known as a claims provider trust. A user who attempts to log on is directed to an external claims provider (for example, ADFS), which authenticates the user and produces a SAML token. SharePoint accepts and processes this token, augmenting the claim and creating a claims identity object for the user.



Authentication Providers

Claims Authentication Types

Choose the type of authentication you want to use for this zone.

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that had been configured by the domain administrator. NTLM authentication will work with any application pool account and with the default domain configuration.

Basic authentication method passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

ASP.NET membership and role provider are used to enable Forms Based Authentication (FBA) for this Web application. After you create an FBA Web application, additional configuration is required.

☑ Enable Windows Authentication

☑ Integrated Windows authentication

Negotiate (Kerberos)

☐ Basic authentication (credentials are sent in clear text)

☐ Enable Forms Based Authentication (FBA)

ASP.NET Membership provider name

ASP.NET Role manager name

☑ Trusted Identity provider

Trusted Identity Provider

☑ SAML Provider

Figure 5-130: NCOP SharePoint Web Application configured to allow Trusted Identity Provider

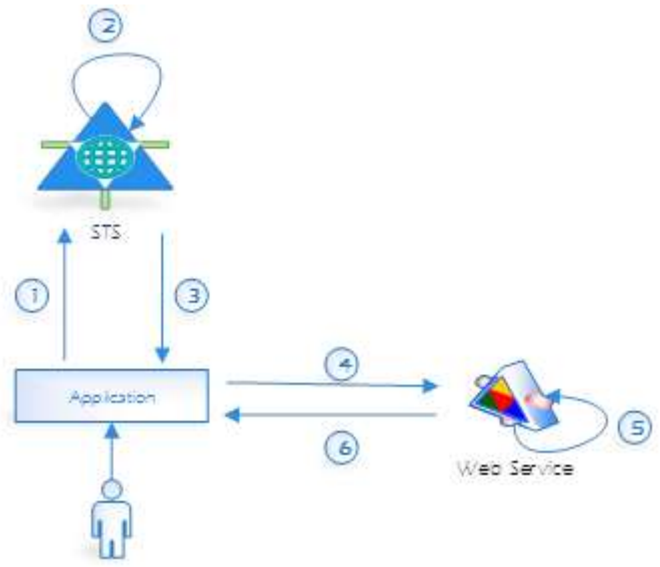


Figure 5-131: Web Service with STS.

1. The client initializes and sends (via application) authentication request to the STS. The request contains client's credentials required to authenticate the client.

2. The STS validates the client's credentials.

3. The STS issues a security token to the client. If the client's credentials are successfully validated, the STS issues a security token (such as a SAML token). The token contains claims which represent user identity.

4. The client (via application) sends a request message to the service. The request message contains the received token.

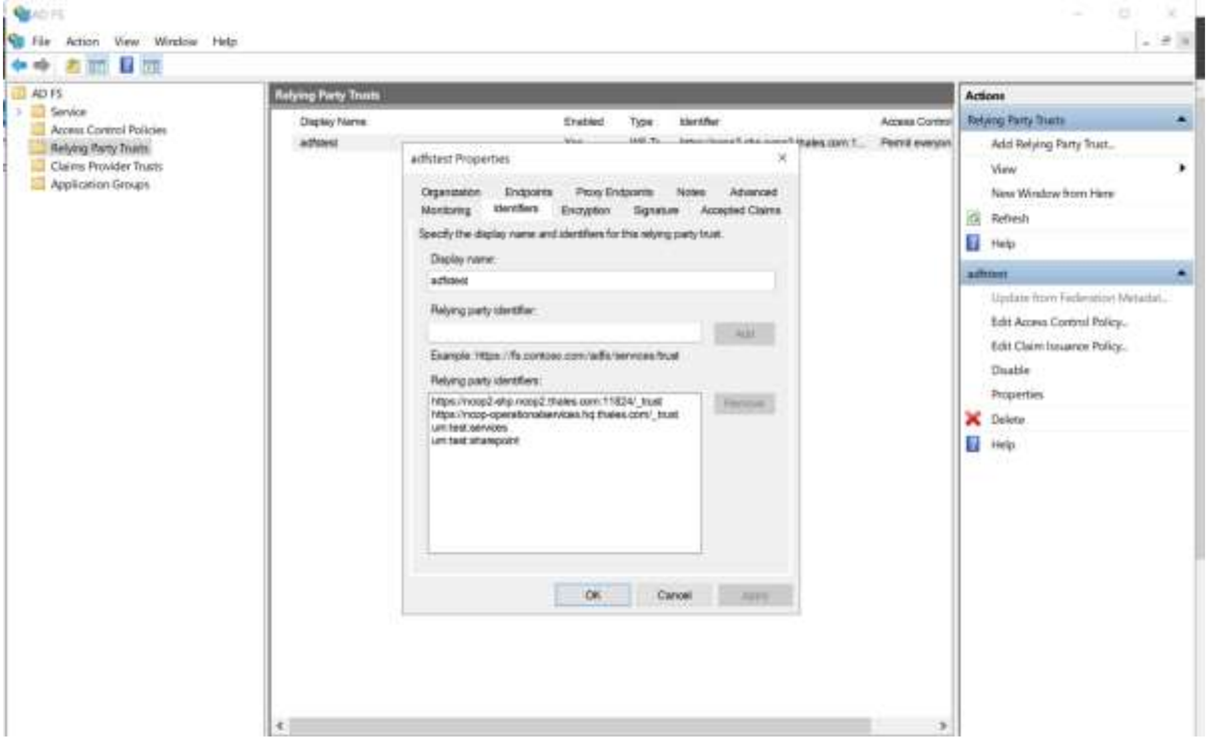
5. The service validates the security token and processes the request. To validate token, connection between service and STS is not necessary – issuer validation is based on PKI

6. (Optional) The service initializes and sends a response message to the client.

The new Identity Provider concerns only user authentication. All NCOP services accounts will remain Windows accounts.

The preferred Identity Provider is ADFS (Active Directory Federation Services).

In this case, each NCOP end-point (NCOP portals hostheaders, Geographical COP Editor services hosheaders) shall be defined as a relying party in the ADFS administration console as illustrated below:



adfstest | Yes | WS-Tr... | https://ncop2-shp.ncop2.thales.com:1... | Permit everyone

Specify the display name and identifiers for this relying party trust.

Display name:
adfstest

Relying party identifier:

Example: https://fs.contoso.com/adfs/services/trust

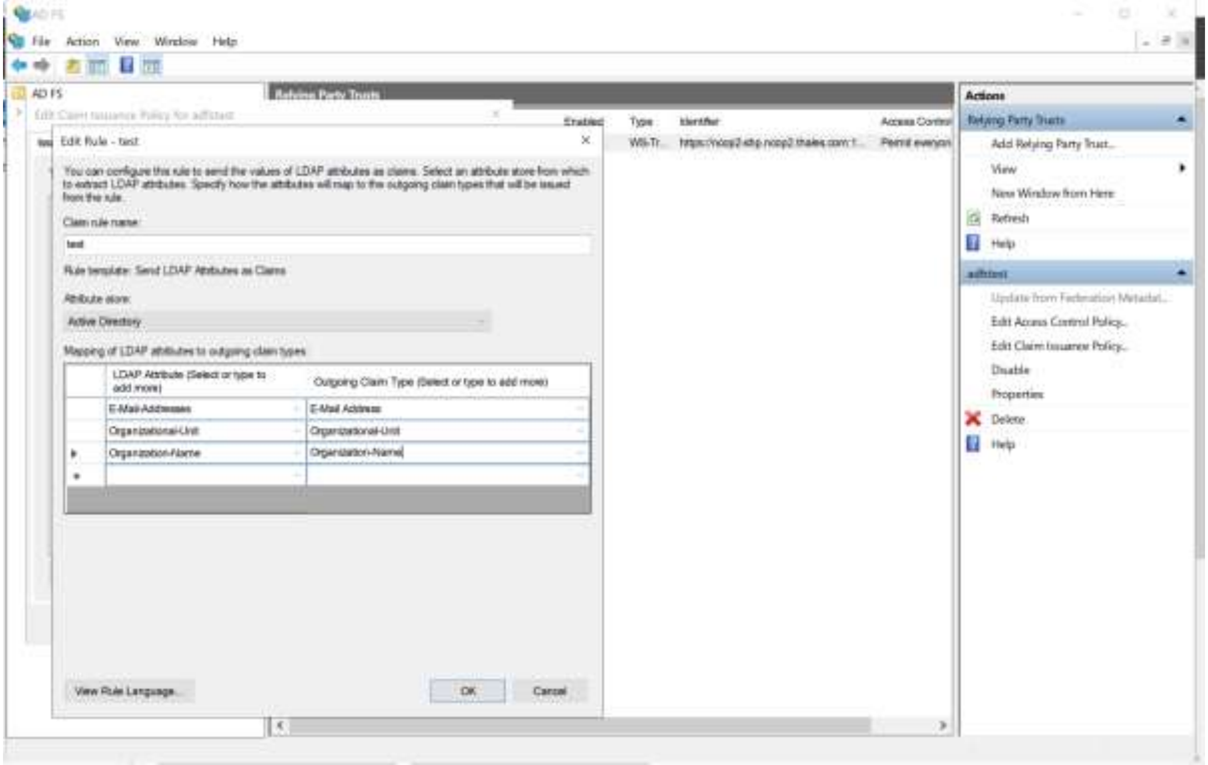
Relying party identifiers:
https://ncop2-shp.ncop2.thales.com:11824/_trust
https://ncop-operationalservices.hq.thales.com/_trust
urn:test:services
urn:test:sharepoint

Figure 5-132: relying party in the ADFS administration console

The claims identity object for the user is based on a set of attributes that shall be defined the “Claim Issuance Policy” on the ADFS administration console. The most relevant attributes seems to be:

- E-Mail Address (mandatory)
- Organizational-Unit
- Organization-Name

They are defined by a mapping from the corresponding LDAP (Active Directory) attributes as illustrated below:



Edit Rule - test

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

test

Rule template: Send LDAP Attributes as Claims

Attribute store:

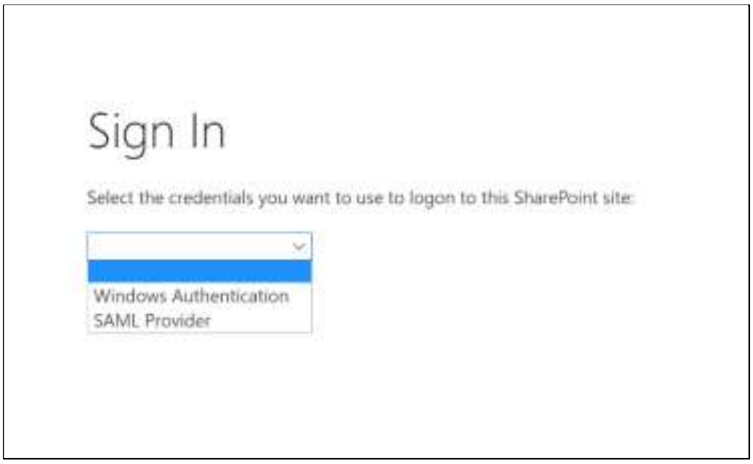
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	E-Mail-Addresses	E-Mail Address
	Organizational-Unit	Organizational-Unit
▶	Organization-Name	Organization-Name
*		

Figure 5-133: Mapping of LDAP attributes to outgoing claim types in the ADFS administration console

In case of double authentication (Kerberos and SAML) the NCOP portal displays the following Sign In options:



Sign In

Select the credentials you want to use to logon to this SharePoint site:

Figure 5-134: Sign In options

In case of Windows Authentication choice (Kerberos), the SharePoint page displays the user account as below:

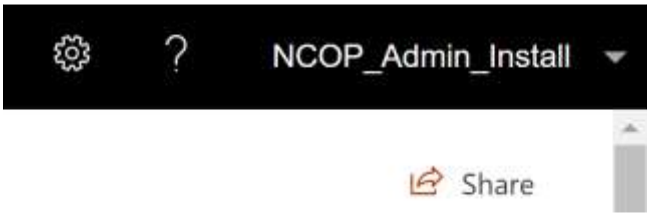
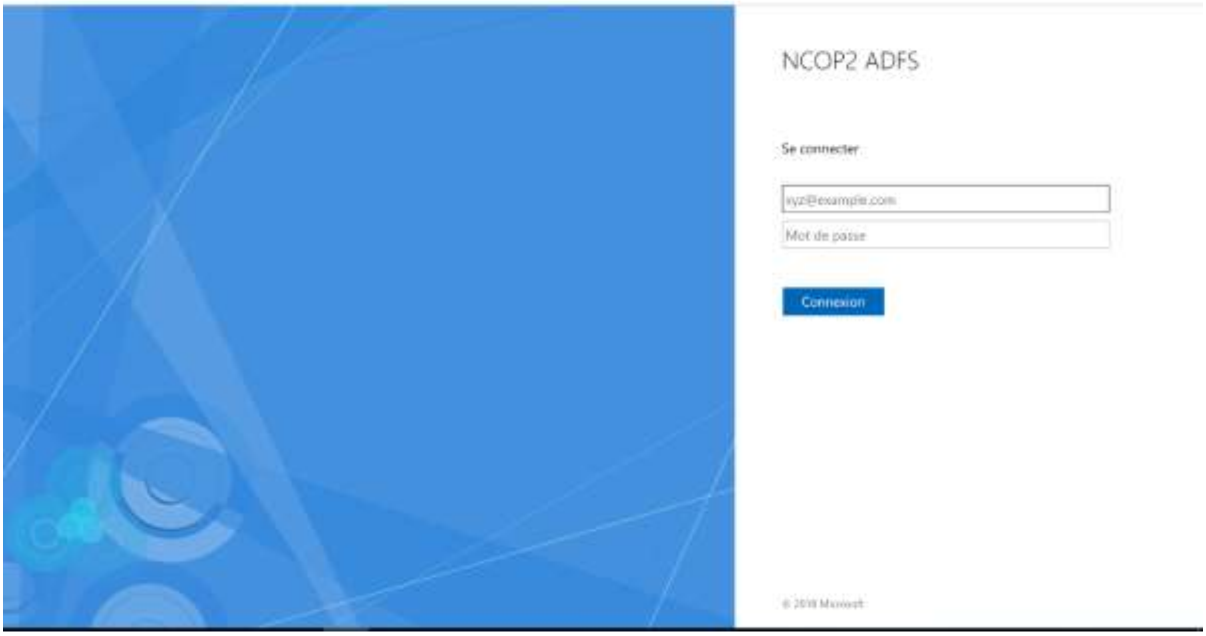


Figure 5-135: User identified with Windows Authentication choice (Kerberos)

In case of SAML provider choice (via ADFS), the user shall input its credentials:



NCOP2 ADFS

Se connecter

xyz@example.com

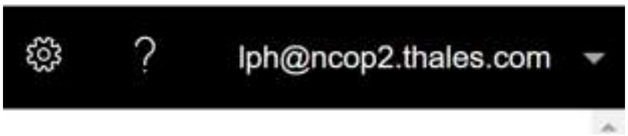
Mot de passe

Connexion

© 2018 Microsoft

Figure 5-136: ADFS authentication form

Then the SharePoint page displays the user account as below (e.g. first claims attribute: email address):



lph@ncop2.thales.com

Figure 5-137: User identified with SAML provider choice (via ADFS)

5.3.6.15 NLB

Property Name	Description
Identification	NLB

Classification	TI
Behaviour	Network Load Balancing is based on PulseSecure Traffic Manager software (preferred) or Microsoft software NLB
Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved
Location (Types)	On NATO infrastructure
Interfaces	NCOP interacts with this IC
Collaboration mechanism	-
Local/Configuration data	-
Operating context	-
References	-
Quality of Service requirements (QoS)	-
Complexity	Low

See 5.4.24 NLB hardware for High Availability Node.

5.3.6.16 Altova MapForce

Property Name	Description
Identification	Altova MapForce
Classification	TI
Behaviour	This component is a Windows-based, multi-purpose IDE (integrated development environment) that enables a user to transform data from one format to another or from one schema to another, by means of a visual, "drag-and-drop" -style graphical user interface that does not require writing any program code.
Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved
Location (Types)	On any Windows 10 workstation
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

5.3.6.17 VMware

Property Name	Description
Identification	VMware

Property Name	Description
Classification	TI
Behaviour	VMware provides a reliable and optimized virtualization solution. This module allows NCOP to operate in a virtualized server environment.
Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved
Location (Types)	On NATO servers
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	Windows Servers and Windows 10 virtual machines
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

5.3.6.18 Microsoft Hyper-V

Property Name	Description
Identification	Microsoft Hyper-V
Classification	TI
Behaviour	Microsoft Hyper-V Server 2019 is a stand-alone product that provides a reliable and optimized virtualization solution. This module allows NCOP to operate in a virtualized server environment.
Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved
Location (Types)	On NATO servers
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	Windows Servers and Windows 10 virtual machines
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

5.3.7 Interfaces

The reader will find a description and identification of the NCOP external interfaces in the Interface Control Document [ICD].

The main Information Exchanges are illustrated below:

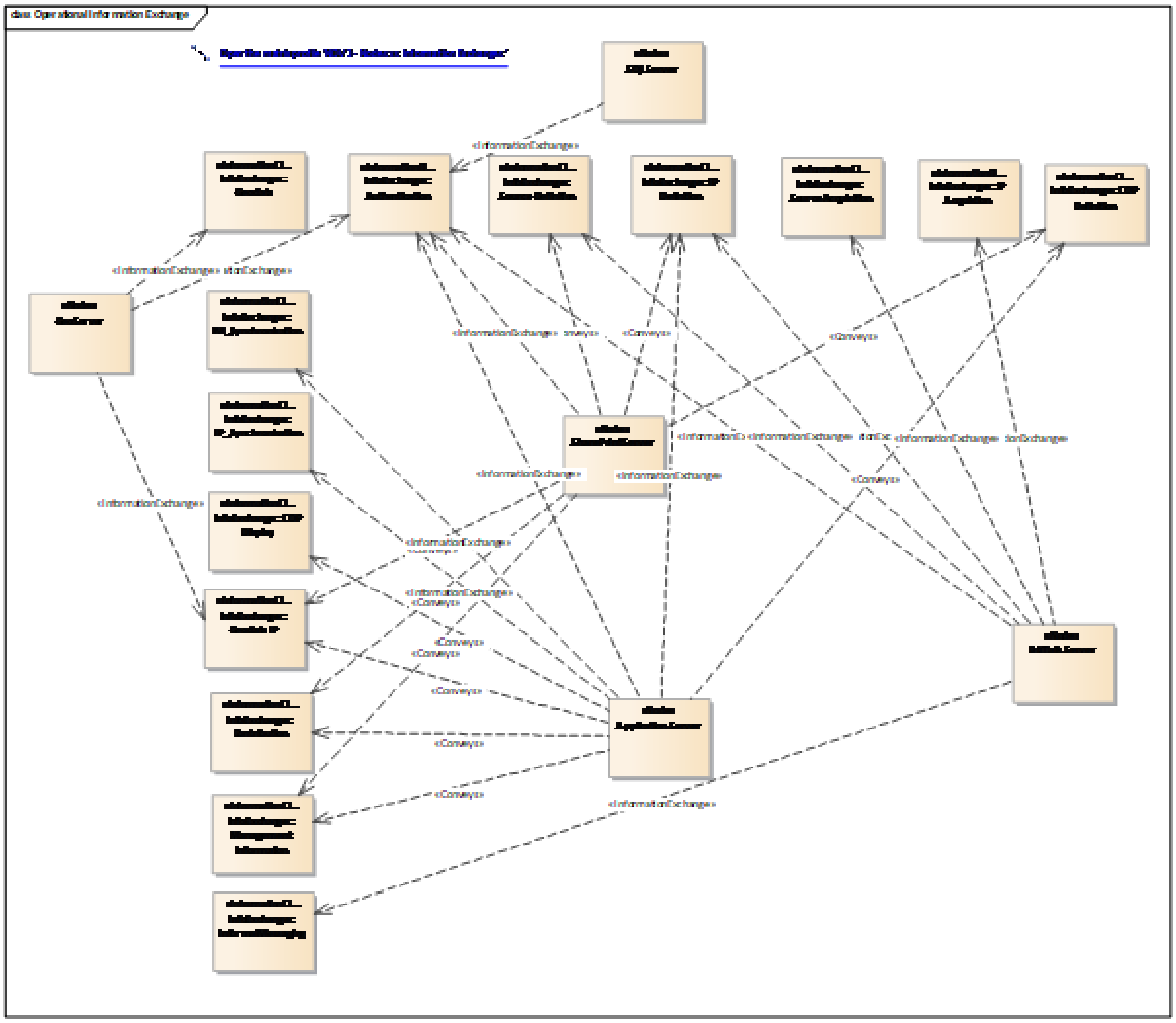


Figure 5-138: Information Exchange vs NCOP Servers

5.4 DESIGN DISCUSSION

5.4.1 Data Model Agility

The architecture is based on the use of a generic, limited-to-core and simultaneously extensible conceptual model for COP.

The derived physical model, named CDF (Common Data Format) is a generic format that takes profit of the already available, extensible XML standard NVG (NATO Vector Graphic), largely used in NATO interoperability.

The NVG data format was created to ease the encoding and sharing of BSO (Battle Space Object) between C2 (Command and Control) systems with particular emphasis placed on military symbology. The NVG data format standard provides C2 system with an easy and lightweight way not only to define but also to contain BSO.

Being based on an XML Schema, NVG has been defined to be easily extended and imported/included in any other XML schema.

As a consequence, the CDF is based on the inclusion of this NVG data format into a set of embedded interrelated XML document dedicated to the definition of each element of the COP: COP structure, COP IP, Annotation, etc.

An agile XML document-based CDF can be designed as follows:

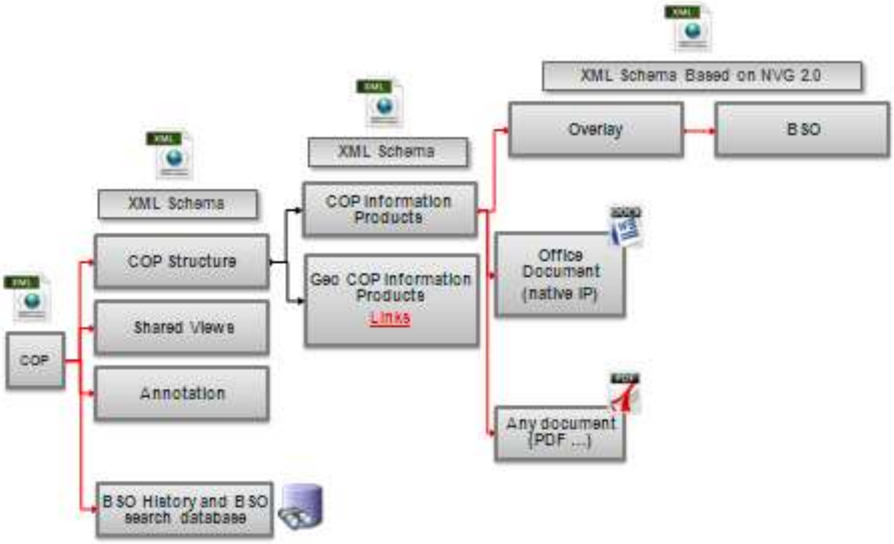


Figure 5-139: CDF Organization

As far as the incorporation of collected native Information Products into CDF COP IP is concerned, it applies with the following policy:

- *For native Information Products containing georeferenced BSO*, the procedure is to:
  - Identify, extract BSOs available in incoming Information Product native format and translate them into BSOs in NVG data format;
  - Create an NVG overlay containing all BSOs;
  - Extract from the incoming Information Product the minimum set of high level information the CDF allowing the identification and classification of the Information Product, to gather it into a COP IP “capsule”;
  - To establish a link between this COP IP capsule, the overlay COP IP and the incoming Information Product in its native format;
- *For other Information Products not containing georeferenced BSO*, such as other non binary (MTF, XML or plain text) or binary (office, jpeg images, etc.) documents that are not related to geographical situational awareness, relational graphs, tables/matrices/lists, the choice is also to:
  - Extract from the incoming Information Product the minimum set of high level information allowing the identification and classification of the Information Product;
  - Gather it into a COP IP “capsule”;
  - To establish a link between this COP IP capsule and the incoming in its native format.

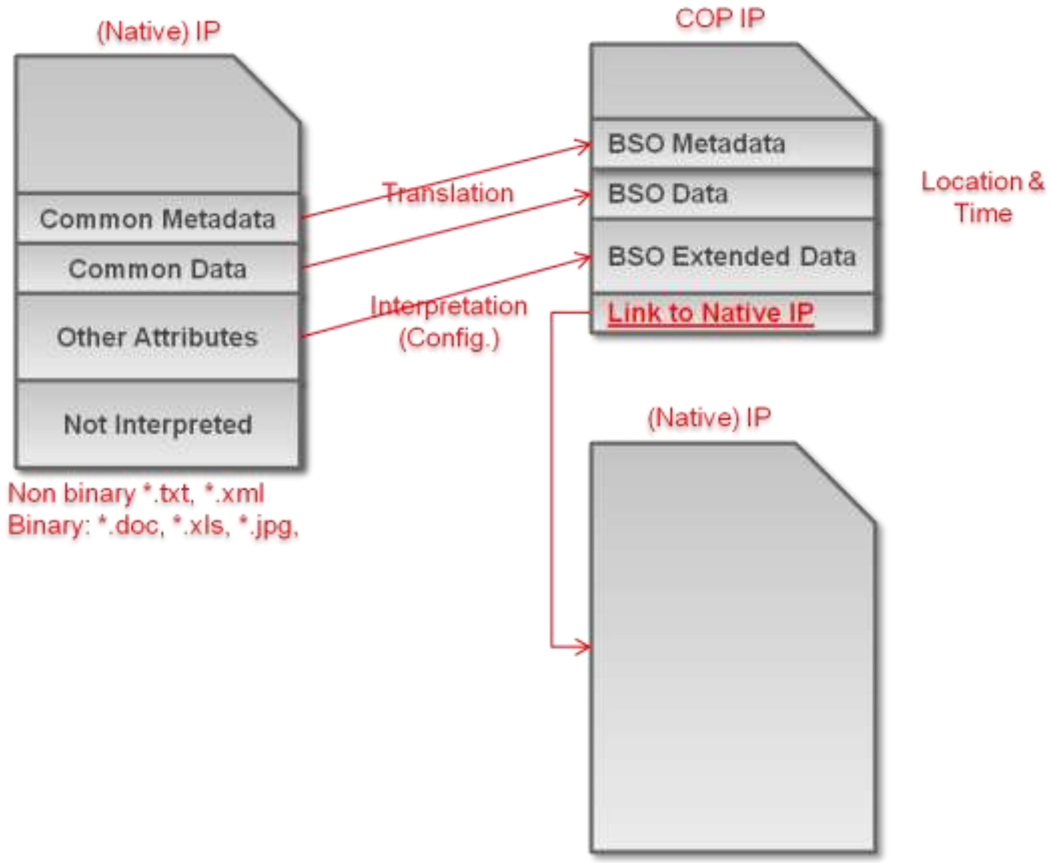


Figure 5-140: Native Information Product extraction and translation into COP IP

Such a choice of NVG XML schema as a base for establishing the NCOP CDF tackles with the potential evolution of the external systems. Those changes may lead to changes in the incoming native Information Product data model and/or integration of new external systems and new native Information Product data model not already known at the date of design of the NCOP system. The CDF principles listed above take these potential changes into account.

5.4.1.1 CDF design

The model used to manage Overlays is based on the NVG 2.0 format specification.

This NVG 2.0 format has the structure and the properties that allow NCOP to store critical information.

5.4.1.1.1 Basic data

Each BSO is at least described by a set of basic data. These basic data specify the BSO type (point, polyline, polygon, circle, etc.), unique identifier, label, coordinates and display symbol.

5.4.1.1.2 Extensible metadata section

For each BSO, the CDF XML schema includes a section dedicated to contain metadata associated to the BSO. This metadata section is designed as a key/value list that is not restricted in terms of metadata number, types or names. Each type of metadata is described in a dedicated section of the CDF.

5.4.1.1.3 Extension section

The CDF XML schema includes at both Information Product and BSO level an extension section designed to contain some additional data that cannot be described using the key/value format of the metadata section.

NCOP uses this section in order to describe:

- Relationships between BSOs within the same Information Product,
- Relationships between BSOs of different Information Products,
- Relationships between Information Products.

Relationships between BSOs are described using the ADEM association types.

5.4.1.1.4 Non geo-localized BSOs

Some BSO are not explicitly geo-localized. Their CDF representation uses the “content-item” object type defined in NVG 2.0. Such CDF elements have no geographical location but can have meta-data and extended data attached as any other BSO.

5.4.1.2 CDF semantics

The CDF is designed to be agnostic of the source data however it is important to include in the CDF model some semantics that allows CDF data to be consistent whatever the source of the information product.

5.4.1.2.1 ADEM attributes

Some metadata are explicitly set during the transformation of incoming data into CDF. These metadata are meant to be common for all Information Products in order to allow the system to perform actions such as filtering or searching across all Information Products.

The ADEM data model which is an extract from the JC3IEDM data model is used as a basis for the CDF common metadata.

The following table lists a set of ADEM metadata that can be set for each BSO of an incoming Information Products:

TABLE 5-12: ADEM TYPES

Metadata identifier	Metadata description	Domain values
ADEM.Type	The type of the object (Unit, Facility, Organisation, etc.)	Yes
ADEM.SubType	The subtype of the object (Airfield, nuclear plant, etc.)	Yes
ADEM.AffiliationGeopoliticalCode	The specific value that represents the identification of the independent first-level geographic-political area and its dependencies, areas of quasi-independence, and areas with special unrecognised sovereignty, including outlying and disputed areas.	Yes
ADEM.ObjectItemHostilityStatusCode	The specific value that represents the perceived hostility status of a specific object	Yes
ADEM.ObjectItemNameText	The character string assigned to represent a specific object	No
ADEM.OrganisationStatusOerationalStatusCode	The specific value that represents the operational status of a specific object	Yes

Using the same principle, it is possible to include semantics of other models into the CDF.

By default all metadata of an incoming Information Product that cannot be semantically mapped to an ADEM metadata is included in the CDF.

5.4.1.2.2 BSO relationships

BSO relationships are described in a specific section, inside the extension section of the CDF.

As defined in the ADEM data model, relationship between BSOs is described in the CDF by:

- A subject (Mandatory),
- An object (Mandatory),
- A subject name (Optional),
- An object name (Optional),
- A subject Information Product (Optional),
- An object Information Product (Optional),
- A subject Information Product Name (Optional),
- An object Information Product Name (Optional),
- An association category (Mandatory),
- A date range of relationship validity (Optional).

The association types are those described in the ADEM data model.

Example of association:

```
<nvg:extension>
      <BSOAssociations>
            <Association>
                  <Object/>
                  <Subject/>
                  <ObjectName/>
                  <SubjectName/>
                  <SubjectInformationProduct/>
                  <ObjectInformationProduct/>
                  <SubjectInformationProductName>
                  <ObjectInformationProductName>
                  <StartDTG/>
                  <EndDTG/>
                  <Category/>
            </Association>
      </BSOAssociations>
</nvg:extension>
```

Example of association defined in AirC2IS interface:

```
<extension>
      <BSOAssociations>
            <Association>
                  <Object>UN^XMN^422                                    SSM
BTL^BALLISTIC_MISSILE^FALSE</Object>
                  <Subject>Group:OP^NCOP-KAMON-ML^NCOP-TEST^PP1-
NCOP/Child:MOA:Kamon(42th)</Subject>
                  <ObjectName>(XMN422) 422 SSM Btl</ObjectName>
                  <SubjectName>MOA:Kamon(42th)</SubjectName>
                  <SubjectInformationProduct>829300c9-5a65-48fc-aebc-
94ebea415839</SubjectInformationProduct>
```

```
                  <ObjectInformationProduct>38469083-1c12-4cf7-90f1-
8c1113bf279c</ObjectInformationProduct>
                  <SubjectInformationProductName>PP1-NCOP-Kamon-
ML</SubjectInformationProductName>
                  <ObjectInformationProductName>ORBAT-OPFOR BM
UNITS</ObjectInformationProductName>
                  <Category>Comes From</Category>
            </Association>
      </BSOAssociations>
</nvg:extension>
```

5.4.1.2.3 Structured Information Products

The use of the NVG as a basis for CDF definition allows the overlay to be structured by the use of the “group” elements. The recursive approach in the XML schema is used in the CDF to represent structured Information Products.

It is the case of some AdatP-3 messages or TOPFAS Information Products that can contain BSOs distributed in multiple paragraphs. Each paragraph shall be mapped to a “group” element containing the text of the paragraph and the BSOs associated.

5.4.1.3 CDF Security classification

The CDF is able to contain security classification information at both Information Product and BSO levels. The security classification information is described in a normalized structure, containing the following elements:

- Identifier,
- Level,
- Category.

The Security Classification included in the CDF version of an Information Product is consistent with the security classification label that is used during a cross domain data exchange. Since the security classification labels are deleted when a message goes through an IEG-C, having this information inside the CDF allows to keep a trace of the security classification of this data when it is received by a consumer.

5.4.1.4 CDF Data signature

The XML schema of the CDF allows the inclusion of a signature in the document itself. This signature is generated by the NCOP system when the CDF is produced. It is then possible for a client that receives a CDF data to verify that the data has not been altered during the transport. The signature is created by the use of an X.509 certificate issued to the NCOP system.

The CDF data signature mechanism requires that a valid certificate be provided by NATO for each site where NCOP is deployed.

Note that this data signature capability can be manually deactivated by an authorized user.

5.4.2 COP Management

This section is related to the §5.3.2.2.1 COP Manager Implementation Component.

The architecture is based on the use of a web-based CMS (Content Management System) provided by Microsoft SharePoint.

Such a choice for CDF management provides NCOP end-users with the following capacities, which are required for COP and related COP IPs management:

- *Document metadata* (user identity, creation, storage and update date, etc.) extraction;
- *Ease of edition and integration of the handled documents* into other application such as office applications;
- *Hierarchical storage management*, indexation (full-text, metadata, etc.) for ease of search and retrieval;
- *Document versioning* and lifecycle workflow (check-in, check-out, version publishing, etc.) management and collaboration;
- *Security* by providing end-users with a unique and secure SSO access to the document repository. Usually in a single AD domain, Kerberos shall be used. In some NCOP deployment configurations (multi domains and local users), ADFS shall be the target for SSO.

Microsoft SharePoint provides all the functions of CMS accessible through a web applications platform. SharePoint's web applications platform allows for managing and provisioning of intranet thin client web portals aside with common EDMS capabilities: document and metadata management, integration, storage, indexation, search, versioning and collaboration processes. Note that it can be used as a rapid web application development platform.

Microsoft SharePoint provides various methods for adaptation and configuration of web application based on CMS to fit customer’s specific requirements. Beyond basic page edition, document storage and user interface customization capabilities, one of the most prevalent forms of configuration in SharePoint is the ability to easily integrate web pages specifically designed in terms of content, appearance and management, named WebParts.

Such a choice of Microsoft SharePoint for CMS and thin client web-based portals development facilities ensure the flexibility of the COP management facilities and web portal-based user interface and its capability to follow evolutions in terms of external systems integration.

5.4.3 Geographical COP Editor

This section is related to the §5.3.1.1.1 Geographical COP Editor Implementation Component.

The architecture is based on the use of a HTML5 cartographic editor called TIMS.js, a Thales product.

The four main features of TIMS.js are:

- *No software installation*: it is a HTML5 client running in any web browser without preliminary installation on the client side;
- *Dissociation from GIS*: it is a generic client independent from any GIS by using standard OGC services such as WMS (ArcGIS REST API can also be used) to display background maps and additional layers. In addition, the internal business model relies on the NVG JSON-based standard for encoding and sharing of BSO;
- Designed to focus on human factors and ease of use; The BSO will be additionally shared in NVG JSON-based standard for HTML 5 JavaScript web clients;
- Built-in with an integration framework allowing easy integration/extension/evolution.

From an operational point of view, TIMS.js is designed:

- To be used in multi-national Joint HeadQuarters: it improves the monitoring of high-intensity and/or disaster-relief operations;
- To be capable of multi-theatre management: Its user-friendly interface and suite of tools also support the briefing of any military or civilian authority on the ongoing situations.

From a technical point of view, the TIMS.js product allows to:

- Display Background maps and additional map layers coming from any OGC WMTS WMS-compatible server, from an ArcGIS server using the ArcGIS REST API, but also from Bing Maps Server (Note that the Bing Maps connectivity is available in the product but is not used in the NCOP context);
- Display joint COP layers such as RAP, RMP and RGP based on NVG data format including:
  - Multiple tactical overlays to be able to follow simultaneously several theatre of operations;
  - APP6-A, APP6-B and APP6-D symbology to represent BSO;
  - BSO detailed information;
  - Quick access to documents linked to specific BSO.

Use multiple projection systems (Geographic latitude/Longitude, UTM, UPS, Mercator and Transverse Mercator), including cartographic projection change at runtime;

- Provide a Situation Awareness capability allowing automatic refresh of tactical overlays.
- Edit overlays from BSO annotation to the creation of missing COP IP element when needed;
- Support APP-6A, APP-6B, APP-6D, MIL-STD B/C/D, and CIMIC symbology to represent BSO;
- Support Level of Details management, Information Panels, Named and Shared Views, time-based filtering.
- The Geographical COP editor displays COPs based on data received from NCOP server sides.

The use of a HTML5 user interface ensures flexibility of COP viewing and editing facilities, its easy integration into web portal-based user interface and its capability to follow evolutions in terms of external systems integration.

5.4.4 Interoperability

This section is related to the §5.3.3.3.1 Microsoft BizTalk Implementation Component.

This section implements the Plugin software pattern for orchestrations, adapters …

The architecture relies on the use of an interoperability functional block, the role of which is to enable the IER (Information Exchange Requirements) with integrated external system acting as Information Product provider Source Entities.

Indeed, this interoperability functional block implements both technical and semantic (operational) interoperability standards and processes to meet the interoperability and IER of the NCOP Increment-2 system, through:

- The use of Microsoft BizTalk Server, which provides the standard technical interoperability protocol and format adaptation facility (SMTP, SOAP/HTTP, several DBMS such as SQL Server, Oracle, text files & binary files such as Office documents, etc.). The provided function ensure that the capability of the NCOP system to evolve easily and to incorporate new external systems as Information Product providers source entity with a limited effort of configuration;
- The integration, through Microsoft BizTalk Server orchestration facility, of operational interoperability components, which implement standard interoperability formats (ADatP-3, OTH-T-Gold) MTF or XML formatted message formats, MIP compliant (C2IEDM, JC3IEDM) XML serialized formats as well as other native XML format (for ex. LC2IS, NCOP, AirC2IS; etc.). These components provide with the capability to directly identify, extract and convert BSOs in native format into BSOs in NVG-based CDF;

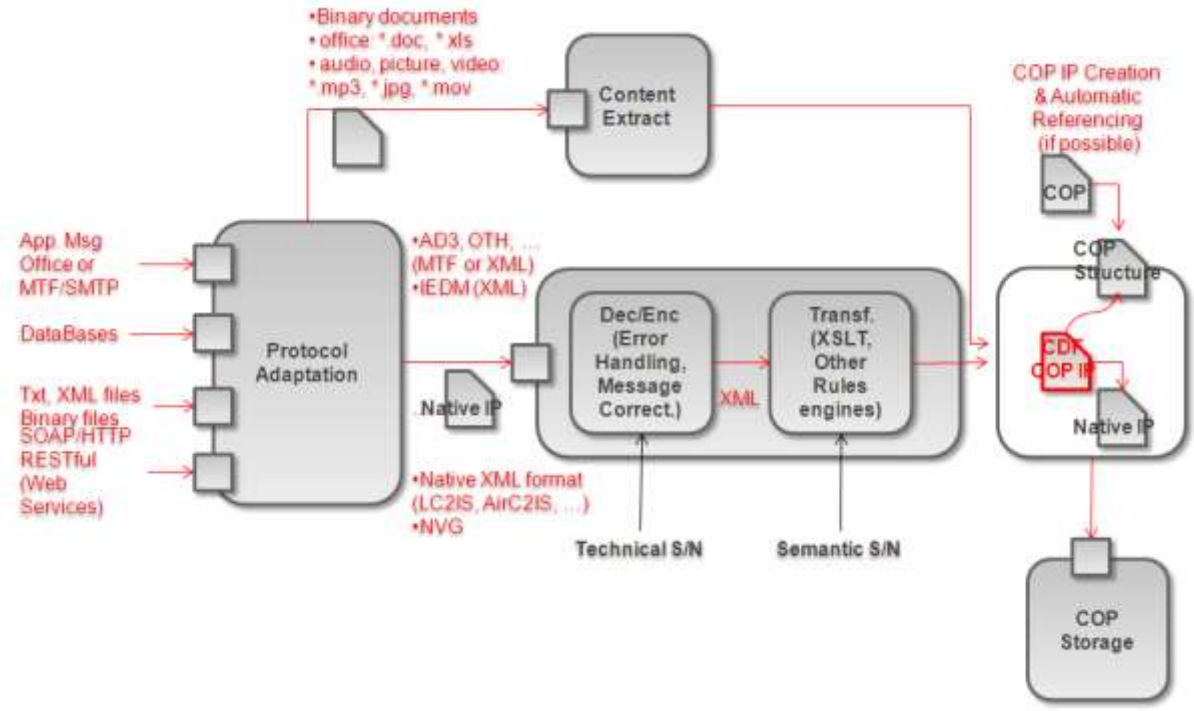

•Binary documents
• office: *.doc, *.xls
• audio, picture, video
*.mp3, *.jpg, *.mov
Content Extract
COP IP Creation & Automatic Referencing (if possible)
COP
App Msg Office or MTF/SMTP
DataBases
Txt, XML files Binary files
SOAP/HTTP RESTful (Web Services)
Protocol Adaptation
•AD3, OTH, ... (MTF or XML)
•IEDM (XML)
Native IP
Dec/Enc (Error Handling, Message Correct.)
XML
Transf. (XSLT, Other Rules engines)
COP Structure
CDF COP IP
Native IP
•Native XML format (LC2IS, AirC2IS, ...)
•NVG
Technical S/N
Semantic S/N
COP Storage

Figure 5-141: Interoperability principles

As shown on the figure above, native Information Products provided by Source entities in binary format (such as office documents, picture or video streams) are kept as is. They are indeed not translated into XML format but encapsulated into COP IP XML-based document.

This technical architecture ensures the flexible integration of NCOP system with any external systems using formatted messages, MIP-compliant serialized XML data format or other native XML data format as interoperability means and allows future integration of any other external system as native Information Product provider Source Entities such as national systems in NRF (NATO Response Force) context.

5.4.5 COP and COP IP relationships

This section is related to the §5.3.2.2.1 COP Manager and §5.3.1.1.10 Relationship Manager Implementation Component.

5.4.5.1 Overview and principles

The following picture presents on overview of the links that can exist between COPs and Information Products.

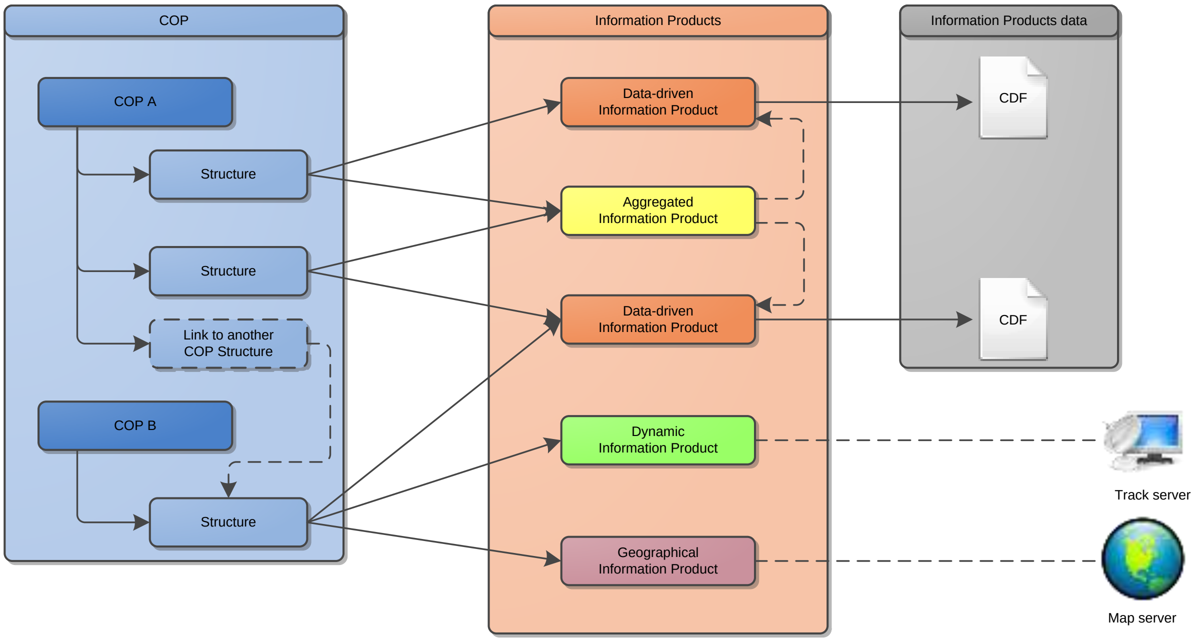

COP
COP A
Structure
Structure
Link to another COP Structure
COP B
Structure
Information Products
Data-driven Information Product
Aggregated Information Product
Data-driven Information Product
Dynamic Information Product
Geographical Information Product
Information Products data
CDF
CDF
Track server
Map server

Figure 5-142: COP and Information Products relationships

NCOP manages the relationships between COPs and Information Products by the use of logical links. COPs and Information Products are defined separately and are stored in separated SharePoint lists. When an Information Product is included into a COP, NCOP only stores the identifier of the Information Product in the COP structure node where the Information Product has been added. This mechanism allows the following configurations:

- A single COP can reference an Information Product multiple times in one or many of its structures
- A single Information Product can be referenced by multiple COPs

A COP only references the configuration part of an Information Product. The content (data) of the Information Product is stored separately:

- Data-driven information products data are stored in a SharePoint document library and associated with the corresponding configuration in the Information Products list.
- Dynamic information products data are not stored in the NCOP storage. The Information Product configuration only references a link to the source server.
- Geographical Information Products are not stored in the NCOP storage. The Information Product configuration only references the geographical data through a URL (WMS layer, KML data, etc.)

5.4.5.2 Aggregated Information Product management

Aggregated Information Products are also managed by the use of references. An aggregated Information Product is defined by the list of constituting Information Products.

The following restrictions apply when defining an Aggregated Information Product:

- An aggregated Information Product cannot reference another aggregated Information Product.
- An aggregated Information Product cannot reference dynamic Information Products
- An aggregated Information Product cannot reference a Geographic Information Product

No data content is stored for an aggregated Information Product. The content of an aggregated Information Product is calculated on-the-fly by concatenating the contents of referenced Information Product data. The result of this aggregation is a CDF file that contains the BSOs of referenced information products. The semantics of all constituting Information Products is kept during the aggregation process by isolating the extended-data schema of each Information Product.

5.4.5.3 Links to other COP structures

NCOP allows that a COP structure contain a node that is a link to a structure of another COP. The content of this particular node is evaluated dynamically when the COP is browsed. This node will appear as a folder that contains subfolders and Information Products like any other folder node.

For data integrity and technical reasons, some restrictions have been introduced for the implementation of this feature:

- Links cannot reference an entire COP or a subfolder of a structure
- It is not possible to create loops (COP A refers to a structure of COP B that refers to a structure of COP A)
- Global links depth cannot be higher than 32

5.4.6 Sources and Information Products

This section is related to the §5.3.2.2.4 COP IP Manager Implementation Component.

5.4.6.1 Information Product and Source relationships

This section implements the Proxy software pattern to manage specific sources: AirC2IS, INTELS-FS …

In NCOP a source is an element that describes the provenance of an Information Product. A source is mainly identified by a name, the data format that it exposes, the protocol used to expose this data and the endpoint or location where this data is made available by the provider system.

If a provider system exposes multiple data formats with different access method, each combination of data format and access method can result in an NCOP source element.

For example, if an LC2IS system offers the following possibilities:

Available data formats:

- Native LC2IS XML
- NVG

Available access methods

- NVG Web Service,
- Native LC2IS Web service,
- File deposit

NCOP allows the COP Manager to declare the following sources for that LC2IS system:

- Native LC2IS XML File deposit,
- Native LC2IS XML via native LC2IS Web service
- NVG file via NVG Web Service
- Etc.

NCOP doesn’t restrict the number and types of sources. For example, if multiple NIRIS servers are reachable by an NCOP node, it is possible to declare multiple sources with the same data format and access protocol combination, each source using a different endpoint according to the target NIRIS server.

Before creating an Information Product it is necessary to create a source. When a source is created, NCOP can if necessary interrogate the associated endpoint and determine if this source exposes capabilities. These capabilities can be used as a basis by an authorized user to identify which Information Products can be created from this source.

When defining an Information Product in NCOP, the COP Manager must start by selection a source. Depending on the source and its capabilities, the user will be able to define a query that will be used by NCOP to acquire the data from the source accordingly. Such queries can have multiple forms depending on the source that is involved:

- SQL request when acquiring data from an SQL source
- Nvg filter when acquiring data from an NVG compliant Web Service.
- Etc.

It is possible to use a single source to create many Information Products. Typically, if a COP Manager has declared a source that exposes an NVG compliant Web service, it is possible to create multiple Information Products from that source by applying different queries, For each Information Product that is declared, NCOP will set up the appropriate orchestration chain that will connect to the source and obtain the data according to the query that has been defined for that Information Product.

5.4.6.2 Management at runtime

NCOP is designed to allow the creation of new sources and new Information Products at runtime.

The creation of a source requires that an authorized user enter the parameters that describe the data to be acquired. The user interface that allows a user to maintain sources is available through the NCOP portal component. When a source item is created, BizTalk connectors and orchestrations are automatically instantiated and if possible the capabilities of the source are acquired.

Once it has been created, a source can be modified but the following parameters cannot be changed for technical reasons:

- Data format,
- Protocol used for data access

For example, it is not possible to modify a source that has been created to connect to an NVG Web Service and turn it into an SQL-based source.

However, it is possible to modify the endpoint (data location) of a source (Web service or file deposit location for example).

The creation of an Information Products requires that an authorized user select a source, optionally specify a query to be applied, and all the acquisition parameters (full/partial update, required update frequency, enforced security classification, etc.) The user interface that allows a user to maintain Information Products is embedded in the geographical COP editor. When an Information Product is created, it is stored in the NCOP storage component and BizTalk connectors and orchestrations are automatically instantiated and the data is being acquired according to the acquisition settings.

5.4.7 COP Persistence

This section is related to the §5.3.4.2 COP and IP storage and §5.3.4.1 COP and IP History storage Implementation Component.

5.4.7.1 Information Elements

All information elements are stored in the SharePoint portal, using lists and document libraries.

Some attributes in the SharePoint lists are XML structures which allows the storage of complex data like COP structures or source capabilities.

Each Information Element is identified by a GUID. These identifiers replace the basic SharePoint identifiers that are not unique across Nodes. GUIDs are identifiers that ensure the uniqueness of an element across all NCOP nodes and that allow a safe way to recreate links when an element is synchronized or restored on a node.

Regarding SharePoint storage, the use of External Blob Storage/Remote Blob Storage feature has been considered but whereas it may increase performances when accessing attached files stored in SharePoint (only Information products in CDF and original format and user feedbacks would be affected), it makes both installation and maintenance (backups) procedures more complex. Therefore, it has been decided to rely on the default storage mechanism where attached files are stored directly in the underlying SQL database.

5.4.7.2 BSO history

The content of this section represent the currently envisioned design and is provided for information purposes only; further technical validation needs to be performed to ensure its suitability before committing to this design. Section 5.4.7.3 contains additional elements regarding the connected BSO Search capability.

5.4.7.2.1 Data structure

To handle BSO history capabilities for NCOP, a relational database is used.

This kind of persistence is more appropriate than the SharePoint storage solution for storing a large amount of data. Indeed, performance issues rise when a SharePoint list contains several thousands of documents. Also, using the native SharePoint versioning mechanism is not satisfying regarding the performances when accessing older versions of a list item.

The data model is directly derived from the application of *Temporal Tables* to a subset of tables shared with the BSO Search capability. The following figure presents the resulting data model:

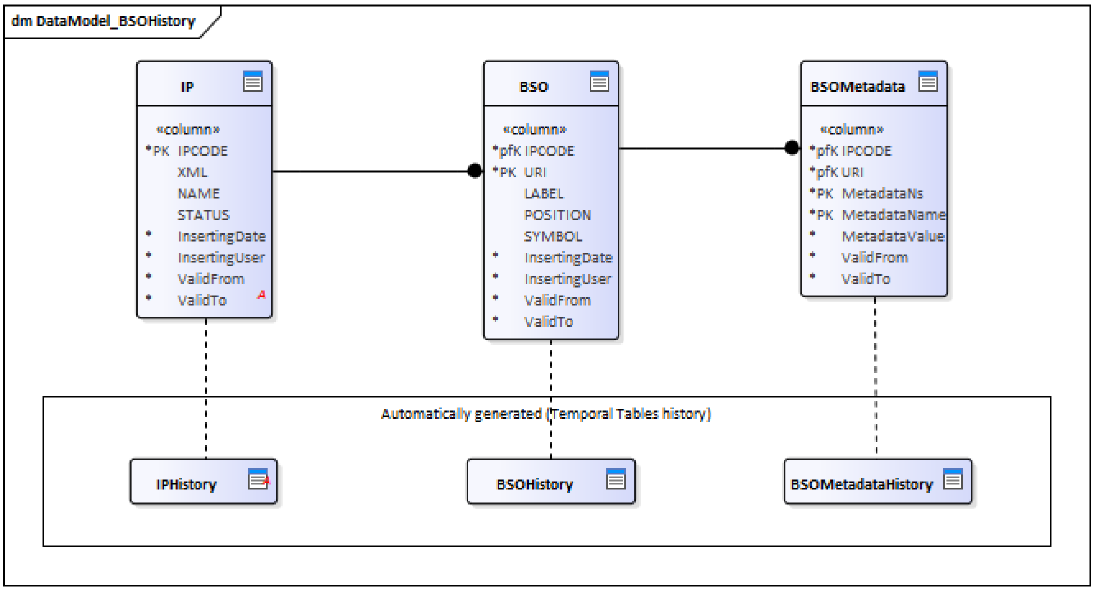


Figure 5-143: BSO History data model

This model defines 3 Temporal Tables, one for each of the central data types: Information Products, BSO and properties of BSOs.

A Temporal Table consists in a *Current* table and a *History* table. The Current table stores the latest version of the data of the Temporal Table. The History table is designed to store all the previous versions of each row from the Current table: right before a transaction updates or deletes a row in the Current table, the database engine persists a read-only copy of that row to the corresponding History table. To manage versioning of its rows, a Temporal Table requires two validity columns representing date-times: the period defined between those values is the time span during which the corresponding row was active. History tables are automatically controlled by the engine.

Throughout this document, and unless specified otherwise, a Temporal Table will be referred to by the name of its Current table.

The main table is the BSO table that stores the successive versions of all BSOs. Each line in the related History table corresponds to a specific version of a specific BSO. For each version, all the properties of the BSO are stored in Temporal Table BSOMetadata, which has its history in table BSOMetadataHistory.

Some of the BSO properties are explicitly stored in dedicated columns to allow fast display and fast search capabilities with search criteria:

- Label
- Position (geometry column to perform spatial searches)
- Symbol

All other properties for a BSO are stored in the BSOMetadata Temporal Table, in a destructured key-value paradigm: each property of a BSO is stored as an individual row.BSOs are identified by a composite key made of the Information Product identifier and the BSO uri within this Information Product. When performing a history search based, the corresponding version of a BSO will be determined by confronting the time constraints to the validity period of the rows.

BSO properties are identified by a composite key made of the Information Product identifier, the BSO uri within this Information Product, and the name of the property.

The IP Temporal Table is designed to store the successive versions of the Information Products' extended-data schema (column CdfRoot). Indeed, across time, an Information Product content can evolve and the same BSO can be described with different attributes from one Information Product update to another. Each line of this table describes the extended data schema at the specific date and time when the Information Product has been acquired by NCOP.

Information Product are identified by a primary key : the Information Product identifier.

It is also important to note that aggregated Information Products are not referenced in this historicized tables. When a historic data for a BSO is requested from an aggregated information product, NCOP searches the BSO with its identifier and the identifier of the original Information Product it belongs to.

When a BSO History request is received, NCOP extracts all BSOs that match the request criteria and creates a CDF file based on the merge of extended-data schema and the aggregation of all matching BSO properties.

5.4.7.2.2 Data acquisition

The BSO and BSOMetadata history tables are filled during the acquisition process of an information product, unless the BSO history capability has been disabled for the Information Product.

Once the incoming information product has been converted into CDF, the CDF is analyzed and all BSOs are extracted. The schema definition for extended data of the instance of information product that is being processed is stored in the IP table. Each BSO is stored in the BSO table and associated with the corresponding entry in the IP table. The BSO properties are further expanded, stored in the BSOMetadata table and associated with the corresponding entry in the BSO table.

The service responsible for filling the BSO History database is described in more details in chapter 6.2.9.

5.4.7.2.3 BSO history consumption

History for a specific BSO can be obtained by using a specific NCOP Web service.

This BSO history Web service allows a COP User to ask the different versions of a specific BSO from a specific Information Product during a specific time range.

The result of this web service call is a CDF JSON made of the aggregation of the successive states of the BSO across time.

If a BSO is part of an aggregated Information Product, the BSO history request always refers to the original Information Product to which the BSO belongs in the first place.

This web service is described more precisely in the NCOP Interface Control Document [ICD].

5.4.7.2.4 Data purge

To prevent the storage from growing indefinitely, NCOP has a purge mechanism that is configurable per Information Product by an authorized user. Unless a user with the COP Manager role has decided to deactivate the BSO history capability for an Information Product, he has to select the period of time for which he wants to keep the history data.

A scheduled job runs periodically in background to delete all data that has expired according to the parameter set by this user.

When an Information Product is deleted, all corresponding BSO History entries are deleted.

5.4.7.3 BSO search

The content of this section represent the currently envisioned design and is provided for information purposes only; further technical validation needs to be performed to ensure its suitability before committing to this design. Section 5.4.7.2 contains additional elements regarding the connected BSO History capability.

5.4.7.3.1 Data structure

To handle the BSO Search capability, NCOP uses a relational database.

This kind of persistence is more appropriate than the SharePoint storage solution for storing a large amount of data. Indeed, performance issues rise when a SharePoint list contains several thousands of documents. Also, using the native SharePoint versioning mechanism is not satisfying regarding the performances when accessing older versions of a list item.

In addition, the BSO search capability requires the ability to perform spatial searches which can be achieved with the MS SQL Server persistence solution and the use of “geometry” columns that allow the creation of spatial indices.

The data model expands on tables used by the BSO Search capability, which will not be presented in detail in this section. The following figure presents the data model:

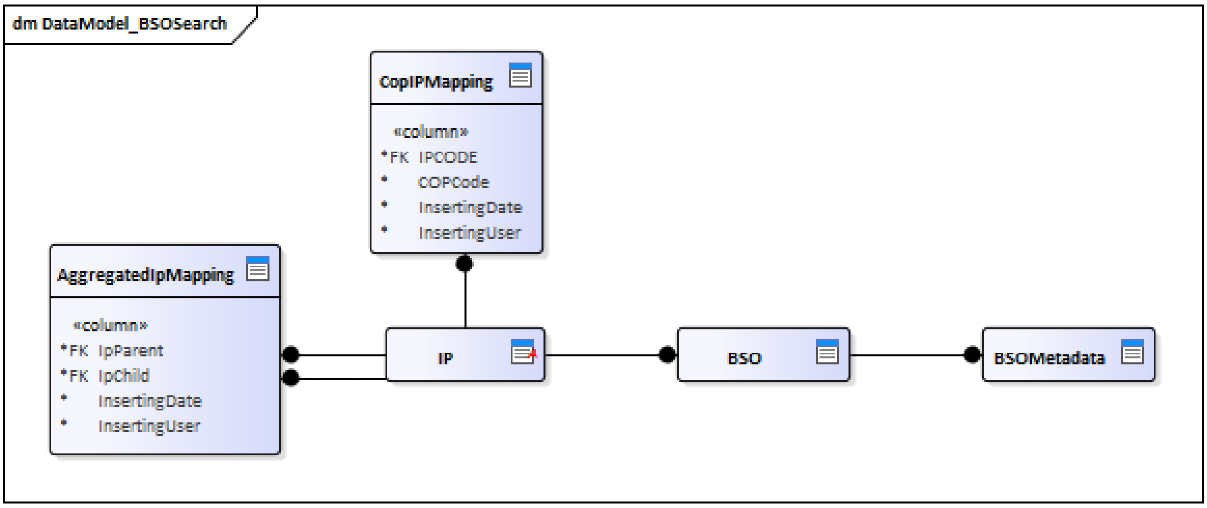


Figure 5-144: BSO Search data model

Since the search for a BSO is done in the context of a COP, the CopIPMapping table is used to identify which Information Products are parts of a COP.

The Information Product table is used to identify the Information Products. The schema column contains an XML fragment that describes the extended-data schema of an information product.

The BSO table contains the description of a BSO. Each line in that table identifies a BSO with some of its properties and the Information Product it belongs to.

Some of the BSO properties are explicitly stored in dedicated columns of this table to allow fast search capabilities with search criteria:

- Label
- Position (geometry column to perform spatial searches)
- Symbol

Metadata and extended-data of the BSOs are stored in the BSOMetadata table. This table is used to perform searches with criteria based on metadata or extended-data.

The AggregatedIPMapping table is used to identify which are the Information Products that are parts of an aggregated Information Product.

5.4.7.3.2 Data acquisition

The tables used for a BSO search request are filled at different times:

- The COPIpMapping table is updated when the structure of a COP changes (Information Product added or removed) or when a COP is deleted,
- The AggregatedIPMapping table is updated when a aggregated Information Product is defined, deleted or modified (directly or indirectly if a constituting Information Product is deleted),

- The BSO and BSOMetadata tables are filled during the acquisition phase of an Information Product, once it has been converted into CDF.

The service responsible for filling the BSO Search database is described in more details in chapter 6.2.9.

5.4.7.3.3 Data consumption

The BSO search capability is exposed by NCOP through the implementation of the search method of the JIPS Web Service.

When NCOP receives a BSO search requests, the request is translated in the appropriate SQL query. The result of the search is created by aggregating the generated CDF JSON fragments of all matching BSOs.

Unlike BSO History management, aggregated Information Products are taken into account during a BSO search. It is necessary to manage the configuration in which a COP contains an aggregated Information Product based on Information Products that are not part of this COP. In such a case, matching BSOs will be presented as being part of the aggregated Information Product in the search results.

The BSO Search web service is described in details in the NCOP Interface Control Document [ICD].

5.4.7.3.4 Data purge

When an Information Product is deleted, all associated BSO Search entries are deleted.

5.4.8 NCOP Node Synchronization

This section is related to the §5.3.3.4.1 Node Synchronisation Implementation Component.

Multiple NCOP Entity nodes of a same NCOP system can be deployed over several sites. The NCOP synchronization capability allows maintaining the COP referential integrity among multiple NCOP Entity nodes. This capability is based on the reuse of Publish / Subscribe NCOP Web Services. It ensures the synchronization of CDF COP information elements (COP, COP structures, COP IP, annotations, shared views, and native Information Products) and CDF Management Information across NCOP nodes.

The publish/subscribe message exchange pattern:

- Allows access to the right information at the right time to the right user role;
- Provides elements/mechanisms to release information from one organization to another (e.g. right to know, Information Product labelling);
- Ensures data dissemination in a distributed environment;

- Reduces overhead and bandwidth consumption between remote sites, focusing on structured data synchronization (bandwidth consumption use can be further optimized through the reduction of metadata synchronization when necessary);
- Provides strong dissemination architecture, using high-level mechanisms, like geospatial topic subscription and publication.

5.4.9 Publish/Subscribe pattern

This section implements the publish/subscribe software pattern.

The publish/subscribe message exchange pattern for Web Services is used in NCOP for the following features:

- User alert/notification

Allows a user to subscribe to specific events that occur in NCOP (operational and/or technical) and to be notified when such an event occurs.

- NCOP IPS

Allows a COP User to be notified when a COP or one of its elements is created, modified or deleted.

- NCOP synchronization

Allows an NCOP node to subscribe to specific COP or Information Products exposed by another NCOP node.

The use of this message exchange pattern optimizes the data exchange process between publishers and subscribers by transmitting data only when necessary.

5.4.9.1 Alert/Notification

Regarding alerts and notifications, the publish/subscribe pattern implementation is based on the WS-Eventing specification. Associated web service methods are described in more details in the NCOP ICD.

Regarding subscription capabilities, a user can subscribe to:

- A category of alerts
- A specific alert
- A specific alert with an additional filter (if applicable)

User subscriptions are stored in a database and are analysed when an event is raised by NCOP.

If a user subscription matches the event, if the user is connected, he will be notified with the appropriate alert and if he is not connected, the alert will be kept temporarily and will be sent to the user the next time he connects to NCOP. If multiple alerts of the same type occur, they are merged to limit the number of entries in the database.

A purge mechanism is provided to delete old alerts and prevent the database from growing indefinitely.

In order to allow a quick definition of subscriptions, it is possible for a user with the “Manage alerts” permission to create subscriptions for NCOP roles. The subscription options are the same as for the users. In this case, when a user connects to NCOP, if he has not defined explicitly its own subscriptions, he will receive alerts based on the subscriptions associated with his roles.

Regarding subscriptions to a category of alerts, since the hierarchy of alerts can be changed by an authorized user, if a category is deleted, the user (or role) subscriptions to this category will also be deleted but if a user (or role) subscription to a specific alert that belonged to this category will be kept.

Regarding to subscription to alerts with additional filters, filter can only be applied to a subset of alerts types. The following table presents the alerts types for which an additional filter can or must be set.

TABLE 5-13: ALERTS TYPES AND FILTERS

Alert type	Filter content	Filter required ?
COP IP changed	Identifier of Information Products	No
BSO relative proximity	Related Information Products Proximity parameter	Yes
BSO entering an area	Identifier of Information Products Geographical area	Yes
Appearance/disappearance of a BSO	Identifier of the Information Product to be analyzed	Yes
BSO attributes value	Identifier of the Information Product to be analysed Attributes and values to be checked	Yes

5.4.9.2 NCOP IPS

5.4.9.2.1 Principles

The NCOP IPS Web service uses the Publish/subscribe message exchange pattern to notify COP Users that a COP or a COP element has been created, modified or deleted. A COP User must use this notification service along with the standard Request/Response-based COP publication service exposed by NCOP to retrieve the appropriate element.

The notification sent to a COP User contains the following information:

- Element type (COP, Information Product, SharedView,…)
- Element action (created, updated, deleted, …)

- Element identifier (unique identifier of the item)

This NCOP Notification service implements the WS-Notification specification. Associated web services methods are described in more details in the NCOP ICD.

5.4.9.2.2 Topic-based subscription and publication

The NCOP IPS web service offers the capability to subscribe to a specific information or set of information by specifying a topic when subscribing. Depending on the subscription topic, the client will be notified only with updates of elements that match the subscription criteria. This Topic-based subscription and publication mechanism is described in more details at chapter 6.2.11.

The Geographical COP Editor is a consumer of the NCOP IPS web services. Its built-in configuration is to subscribe to all types of notifications.

5.4.9.2.3 Subscription and publication monitoring

The NCOP IPS Web service also offers the capability to manage the publication of data by disabling notifications of certain topics for some specific clients.

This capability is accessible through a Web UI that allows:

- The definition of rules to disable publications,
- The monitoring of current subscriptions

This subscription and publication monitoring capability is described in more details at chapter 6.2.11.

5.4.9.3 Synchronization

The NCOP node synchronization process uses the publish/subscribe message exchange pattern.

An NCOP node can subscribe to the following elements:

- COP
- Information Products

When an NCOP node subscribes to a COP, it will receive from the publishing node all the elements related to this COP (the COP element itself and all sub-elements (Information Products, shared views, etc.)

When an NCOP node subscribes to an Information Product, it will receive from the publishing node all the elements related to this Information Product (the Information Product parameter definition, the Information Product instance (cdf),etc.)

When an NCOP node subscribes to an element from another NCOP node, it can specify that the subscription is bi-directional. In this case, a corresponding inverted subscription will automatically be created so both nodes subscribe to each other.

The NCOP synchronization service is based on the implementation of the WS-Eventing specification. Web service methods are described in more details in the NCOP ICD.

5.4.10 Support dynamic connection to nearest WMS server

5.4.10.1 Technical solution

If a COP includes a geographical COP IP located on a specific map server, some clients shall be able to visualize this same information product by interrogating a different map server. The goal of this capability is to improve the performance of geographic data consumption by allowing the clients to use the nearest map server (nearest from the network point of view).

To achieve this purpose, NCOP offers the possibility for a COP Manager to define alternate URLs for each map service that is used by a Geographical Information Product in a COP.

Each alternate map service URL is associated with a network mask that allows NCOP to identify the COP client’s location and expose him the appropriate map service URL. This network mask is compared with the IP address of the client that accesses the NCOP node.

The network mask can be defined in both IP v4 and IP v6 formats and the client IP address is extracted from the HTTP headers of the client’s request.

The published map server URL is calculated when the COP Publication service (JIPS) is invoked by an NCOP client. Therefore, the response of this web service call contains information depending on the location of the client the emitted the request.

5.4.10.2 Sample scenario

The following figure presents the following scenario:

The COP contains a geographical Information Product which has been configured with an alternate URL for NCOP clients whose IP address matches a particular network mask.

Two NCOP clients are accessing this COP. When these clients request the server to obtain the details of the COP, the server analyzes the IP address of the incoming request and according to the rules defined for the Geographical Information Product returns the appropriate URL.

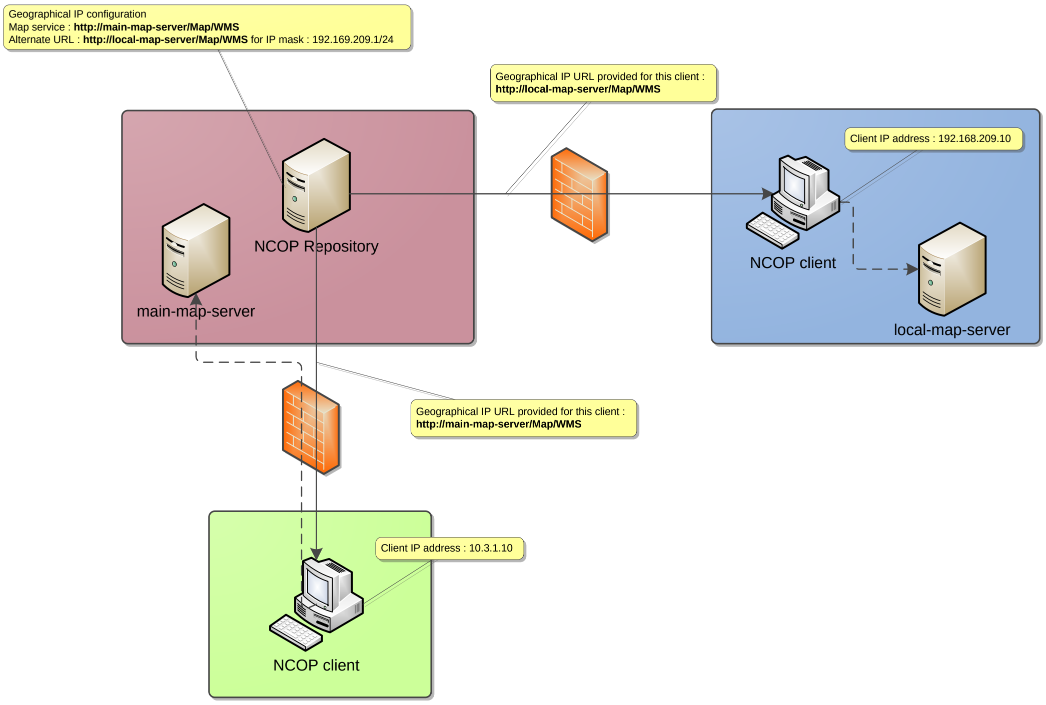

Geographical IP configuration
Map service : **http://main-map-server/Map/WMS**
Alternate URL : **http://local-map-server/Map/WMS** for IP mask : 192.169.209.1/24
Geographical IP URL provided for this client :
http://local-map-server/Map/WMS
Client IP address : 192.168.209.10
NCOP Repository
main-map-server
NCOP client
local-map-server
Geographical IP URL provided for this client :
http://main-map-server/Map/WMS
Client IP address : 10.3.1.10
NCOP client

Figure 5-145: Nearest map server implementation behaviour

5.4.10.3 Limitations

It is important to note that a geographical Information Product is the association of:

- A particular map service,
- A selection of map layers from that particular map service.

Therefore, when a map service is defined with alternate map services URLs it is necessary that these alternate map services expose the very same map layers with the same identifiers. Some clients might not be able to visualize the geographical Information Products of a COP correctly if they are redirected to a map service that does not expose the correct layers.

5.4.11 Configure a new source type on run time

NCOP built-in orchestrations are designed to manage the acquisition of data from well-known interfaces and formats (NVG 1.4 & 1.5, AdatP-3, WISI, etc). They are also designed to be flexible to accept incoming data from different source types and protocols (file deposit, web services, mail exchange, etc.). Data formats and acquisition protocols can be combined to offer multiple possibilities for the acquisition of data. For example, an NVG-based information product can be acquired from a source via a web service, via a file deposit in a shared folder or as an attachment in an e-mail. This kind of combination can be defined when a Source is created in NCOP.

In order to be more flexible, some orchestrations have been designed to be generic so they can be configured at runtime by the COP Manager. These generic orchestrations are the following:

- Excel/SQL/SharePoint-based Information Products
- XML-based Information Products

5.4.11.1 Generic Excel/SQL/SharePoint orchestration

This orchestration has been defined to allow the creation of Information Products based on an Excel file, an SQL database, or a SharePoint list containing BSO properties. This orchestration is configured at runtime by the COP manager when he defines the Information Product. A dedicated panel allows the definition of mapping by identifying source columns and target CDF attributes, include BSO relationships and custom symbols.

The resulting mapping is stored in the NCOP Storage as an XML document that is processed during the conversion step of the acquisition process to produce a CDF document.

5.4.11.2 Generic XML orchestration

This orchestration has been defined in NCOP to allow the creation of an Information Products based on a XML format that is not known in advance. The configuration of this orchestration can be done at runtime when the COP Manager defines the Information Product. During this step the COP Manager must upload an XSLT document that will be applied by the orchestration to convert the XML file into a CDF document.

5.4.12 Definition of a new orchestration

This section is related to the §5.3.3.3.2 Composition / Orchestration Implementation Component.

The definition of a new orchestration can be done in multiple contexts:

- Definition of an orchestration not related to NCOP

In this case, the NCOP BizTalk infrastructure is used to perform actions that are not related to NCOP data processing. Such an orchestration must be developed and deployed as part of a dedicated BizTalk Application. It will have no impact on existing NCOP BizTalk Applications and orchestrations.

- Definition of an orchestration for NCOP

In this case, NCOP BizTalk Applications are enhanced with a new orchestration that will be used to manage a new data format and/or protocol that requires to be acquired. The instructions to create an orchestration that will have to interface with existing NCOP orchestration for data acquisition processing are available in the NCOP Software Build Instructions [SBI].

In both case, it is important to note that creating a new orchestration in BizTalk requires the compilation of new assembly, and the creation of an BizTalk Application package that wil have to be deployed on the target site. Therefore it will probably require a new security accreditation phase and the deployment also have a temporary unavailability impact because an Application is being deployed.

5.4.13 Multi-entities hosting on the same NCOP node

An NCOP node can be configured to identify multiple entities (commands) hosted on this same node.

As described in chapter §5.3.4.3.4 Entities information, an entity is defined by a name and an LDAP search filter that will allow NCOP to identify the Entity(ies) to which a user belongs when this user connects to NCOP. NCOP is designed to allow a user to belong to multiple Entities.

The Entity of a user is exploited by NCOP to determine data access permissions and to identify the owner entity of an Information Element when it is created.

Regarding data creation, the Entity of a user is used to define the owner entity of Information Elements created by this user. If the user belongs to multiple entities, he will be proposed to select one from a list.

Regarding data access, users can visualize all data owned by their entity, and are allowed to visualize data owned by another Entity only if the dissemination settings have been defined accordingly.

5.4.14 Access-rights management across NCOP nodes

For NCOP v1, each NCOP Node describes its local access rights. Roles and permissions are local to a node and are not synchronized across nodes. Also as it is described in the section 5.4.21.1.2, when a user accesses a remote NCOP node, he must authenticate using credentials that are valid in the context of this remote node. Therefore, this user will be given roles and permissions according to the rights that have been set on this remote node.

For NCOP v2, the use of identity federation with the implementation of ADFS/SAML claims based authentication will make possible for a user to connect to a remote NCOP node using its local credentials and rights. This implementation and associated behaviour will be described in a next release of this document.

Regarding visibility rights for COPs and Information Products, Entities and visibility groups are used to allow or deny access to:

- A COP;
- A specific part of a COP (structure, folder or layer);
- An Information Product.

Entities are used to allow or deny access in a dissemination context, whereas visibility groups are used to allow or deny access in a dissemination context or not.

The following scenarios are possible:

- On a node hosting only one Entity, the COP manager has the possibility to restrict access to some COP or information product using visibility groups. In this case, users belonging to the same entity may not be able to visualize the same COPs or Information Products if they do not belong to the same visibility group. In this case, COP and IP dissemination is useless.
- On a node hosting several entities, the COP Manager has the possibility to define access rights by:

    - Using dissemination to allow or deny access to users belonging to a particular entity,
    - Using visibility groups to allow or deny access to specific users,
    - Combining dissemination and visibility groups.

Entities and visibility groups definitions as well as dissemination settings and visibility rules based on visibility groups are synchronized between nodes.

5.4.15 Business rules implementation

5.4.15.1 Information Product status

NCOP offers the capability for COP Managers to create their own rules that will be applied to define the status of an Information Product.

Information Products can have one of the following statuses (each one associated with a colour code):

- OK (green),
- Partially OK (yellow),
- Mostly KO (orange),
- KO (red).

For each Information Product, an authorized user must decide on which conditions an Information Product will have a certain status.

NCOP proposes two different options:

- Statuses based on acquisition failures,
- Status based on data validity duration.

Defining rules for all 4 available statuses is not necessary: for both options some statuses can be discarded and a rule defining only the OK and KO conditions can be created.

In addition of these four status values, the NCOP information quality indicator for an information product shall be calculated from rules that support the following information as new inputs:

- Maximum allowable time since last update of the oldest BSO in the IP, based on source system or NCOP time stamp;
- Minimum and maximum number of BSOs in the Information Product;
- Presence of required fields in each BSO;
- Acceptable values for specific fields in each BSO.

5.4.15.1.1 Status based on acquisition failure

If the user chooses to base the Information Product statuses on acquisition failures, he will define the number of successive acquisition failures that are allowed to be reached for the Information Product to have a certain status.

For example:

- The Information Product has the OK status if the acquisition process doesn’t fail.
- The Information Product has the Partially OK status if the acquisition process fails up to 2 times,
- The Information Product has the KO status above 2 successive failures.

In this mode, NCOP use an acquisition failure counter whose value is updated after each acquisition of an Information Product.

In addition, a scheduled job will update the Information Product status in cases where BizTalk is down and cannot update the acquisition counter. This case only applies to Information Products in “pull” mode and evaluates the acquisition failure counter based on the actual date and time and the required update frequency defined for the Information Product

5.4.15.1.2 Status based on data validity duration

If the user chooses to base the Information Product status on data validity duration, he will define a validity duration since the last correct update of the Information Product, to be acceptable for each status.

For example:

- The Information Product has the OK status if the Information Product was last updated up to 1 hour ago.
- The Information Product has the mostly KO status if the Ip was last updated up to 3 hours ago
- The Information Product has the KO status if the Ip was last updated more than 3 hours ago

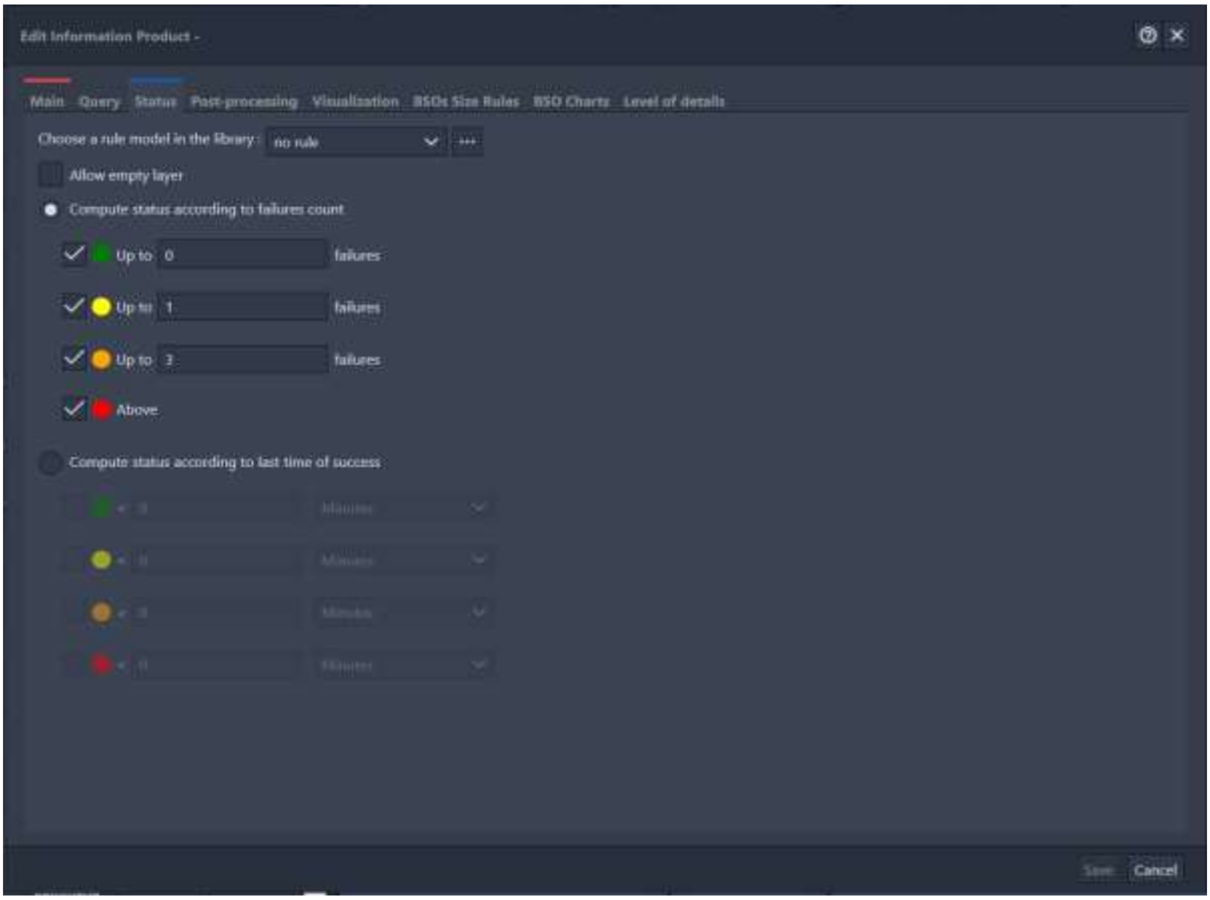
In this mode, NCOP uses a scheduled job that will periodically analyze the NCOP storage content and compare the last acquisition date of an Information Product and the actual date and time with the status rules that have been defined.

5.4.15.1.3 Rules description and storage

All Information Product status rules are described in XML and stored as an attribute of the Information Product itself.

The following figures present the HMI that allows a user to define a status rule for an Information Product:

In this first example, the rule is based on acquisition failures and a status has been explicitly discarded:



Choose a rule model in the library : no rule

□ Allow empty layer

● Compute status according to failures count

☑ 🟩 Up to 0 failures

☑ 🟡 Up to 1 failures

☑ 🟠 Up to 3 failures

☑ 🔴 Above

○ Compute status according to last time of success

🟩 < 0 Minutes

🟡 < 0 Minutes

🟠 < 0 Minutes

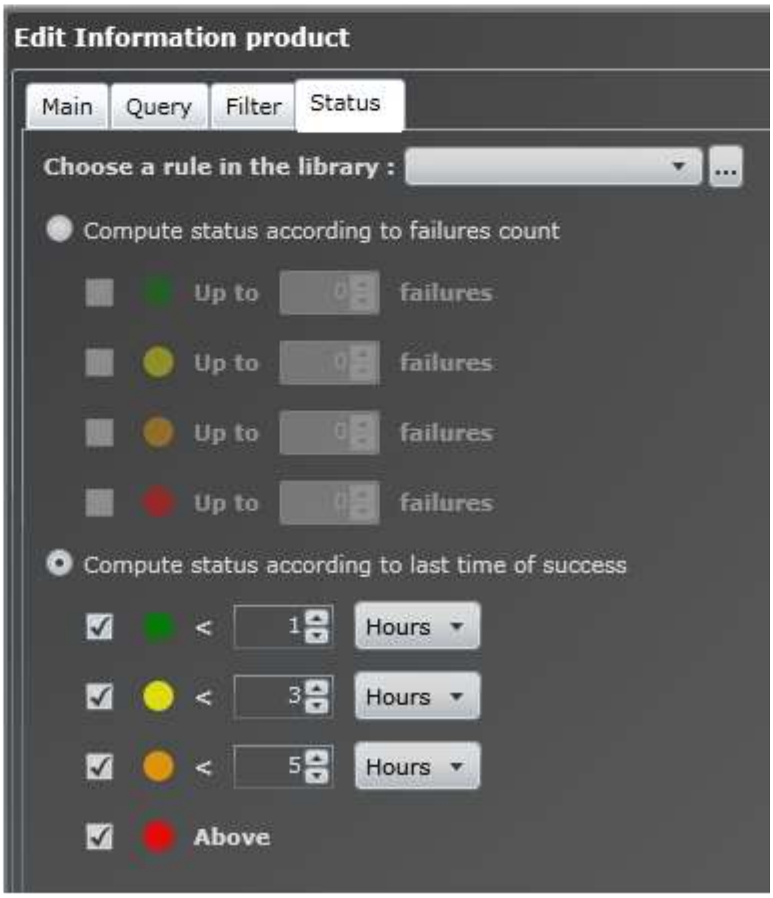
🔴 < 0 Minutes

Figure 5-146: Status rule based on acquisition failures

The corresponding XML representation of this rule is the following:

```
<StatusRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<FailureCountingRule>
<Green UpTo="0" IsChecked="true" />
<Yellow IsChecked="false" />
<Orange UpTo="3" IsChecked="true" />
<Red IsChecked="true" />
</FailureCountingRule>
</StatusRules>
```

In this second example, the rule is based on the validity duration for the Information Product:



Choose a rule in the library :

○ Compute status according to failures count

□ ● Up to 0 failures

□ ● Up to 0 failures

□ ● Up to 0 failures

□ ● Up to 0 failures

● Compute status according to last time of success

☑ 🟢 < 1 Hours

☑ 🟡 < 3 Hours

☑ 🟠 < 5 Hours

☑ 🔴 Above

Figure 5-147: Status rule based on Information Product validity duration

And the corresponding XML representation is the following:

```
<StatusRules xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<SuccessAgeRule>
<Green AgeTo="1" Unit="Hours" IsChecked="true" />
<Yellow AgeTo="3" Unit="Hours" IsChecked="true" />
<Orange AgeTo="5" Unit="Hours" IsChecked="true" />
<Red IsChecked="true" />
</SuccessAgeRule>
</StatusRules>
```

NCOP allows a user to create status rules and save them into a status rules library for later reuse. Reusing a previously saved status rule will automatically fill the status rule definition form with the same parameters.

It is important to note that modifying the parameters of pre-defined rule in the status rules library doesn't modify the status rules that have been previously defined using this pre-defined rule.

5.4.15.2 Operational alerts

NCOP allows any user to define operational alerts.

The following operational alerts have been defined:

- Alerts based on BSO attributes values
- Geospatial alerts
    - Object entering a geospatial area
    - Relative proximity between BSOs in different Information Products
- Appearance and disappearance of a BSO in an Information Product

5.4.15.2.1 Alerts based on BSO attributes values

This type of alert allows a user to define rules that will raise an alert if, for a given information product, one of the BSO has attributes whose values match some criteria defined by the user.

NCOP proposes an HMI that allows a user to declare the match criteria with a set of comparison operators. These criteria are stored using an internal XML schema.

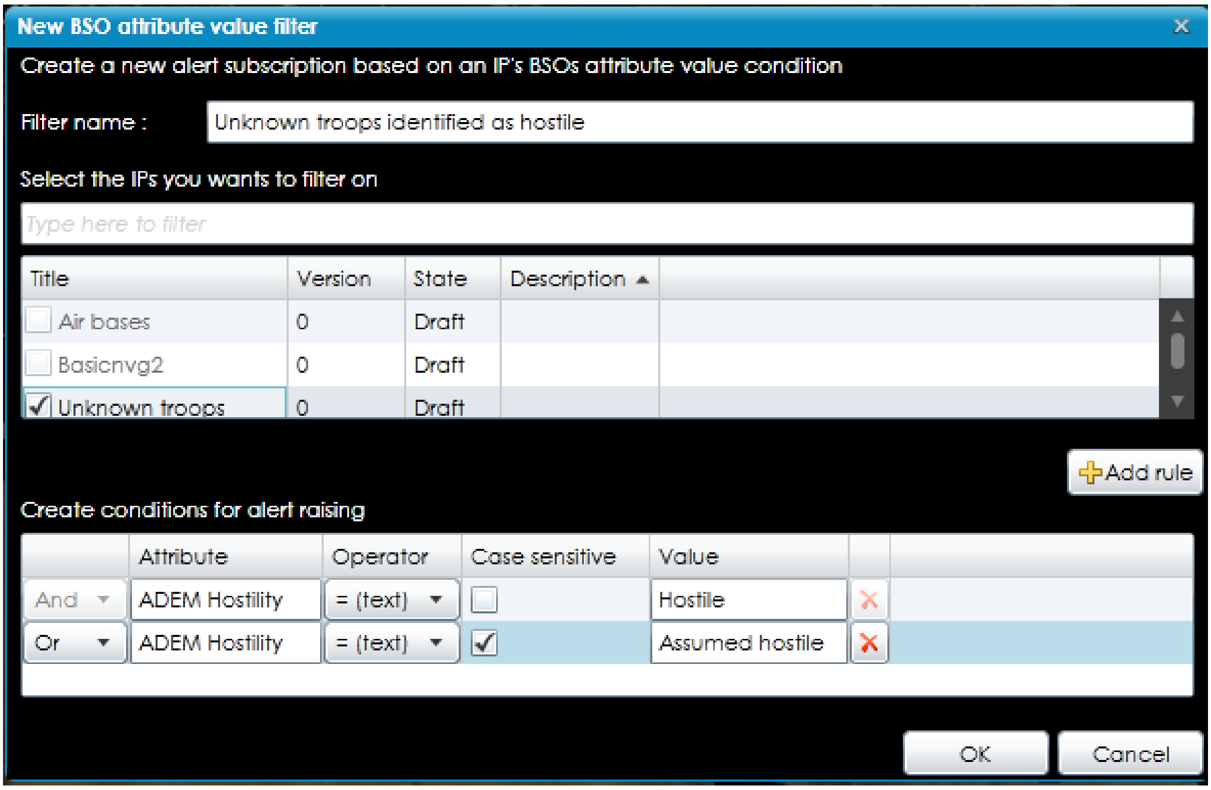
The following is an example of the XML representation for such criteria:

```
<BSOAttributeFilterTable xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="http://ncop.thales.com/2012/09/BSOAttributeFilterTable">

<Rule logic="And" name="Label" value="RADAR" operator="Contains"
ignoreCase="false" />

<Rule logic="And" name="Range" value="12" operator="GreaterThan"
ignoreCase="false" />

<Rule logic="Or" name="Status" value="Operational" operator="NotContains"
ignoreCase="false" />

</BSOAttributeFilterTable>
```

A BSO will match this rule if it has a label attributes that contains the word “radar” and a range attribute with a value greater than 12 or if it has a Status attribute with a value that doesn't contain “operational”.

Note that it is not possible to group criteria with parenthesis.

Embedded in the Geographical Editor, a web user interface allows a user to subscribe to such alerts with personal parameters:



New BSO attribute value filter

Create a new alert subscription based on an IP's BSOs attribute value condition

Filter name : Unknown troops identified as hostile

Select the IPs you wants to filter on

Type here to filter

Title	Version	State	Description ▲
□ Air bases	0	Draft	
□ Basicnvg2	0	Draft	
☑ Unknown troops	0	Draft	

Add rule

Create conditions for alert raising

	Attribute	Operator	Case sensitive	Value	
And	ADEM Hostility	= (text)	□	Hostile	✕
Or	ADEM Hostility	= (text)	☑	Assumed hostile	✕

OK Cancel

Figure 5-148: HMI for defining Alerts based on BSO attribute value

5.4.15.2.2 Geospatial alerts

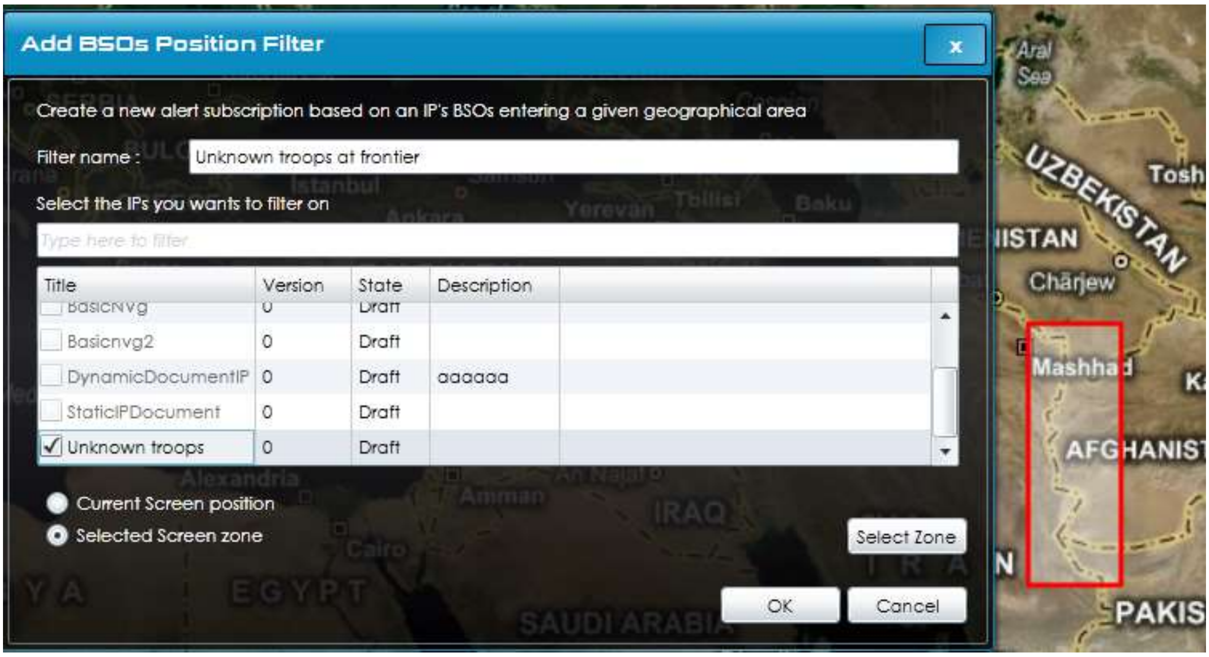
5.4.15.2.2.1 Object entering a geospatial area

This type of alert allows a user to be notified when a BSO enters a particular user-defined area. This rule applies in the context of a particular Information Product identified by the user.

The geospatial area criterion is a rectangular geographical area that can be defined using the Geographical COP Editor.

The geospatial criterion is stored using an SQL geometry attribute in order to take advantage of the spatial search capabilities of SQL Server.

Embedded in the Geographical COP editor, in the Alerts management module, an HMI allows a user to subscribe to such alerts with personal parameters:



Add BSOs Position Filter

Create a new alert subscription based on an IP's BSOs entering a given geographical area

Filter name : Unknown troops at frontier

Select the IPs you wants to filter on

Type here to filter

Title	Version	State	Description
□ BasicNvg	0	Draft	
□ Basicnvg2	0	Draft	
□ DynamicDocumentIP	0	Draft	aaaaaa
□ StaticIPDocument	0	Draft	
☑ Unknown troops	0	Draft	

○ Current Screen position
● Selected Screen zone

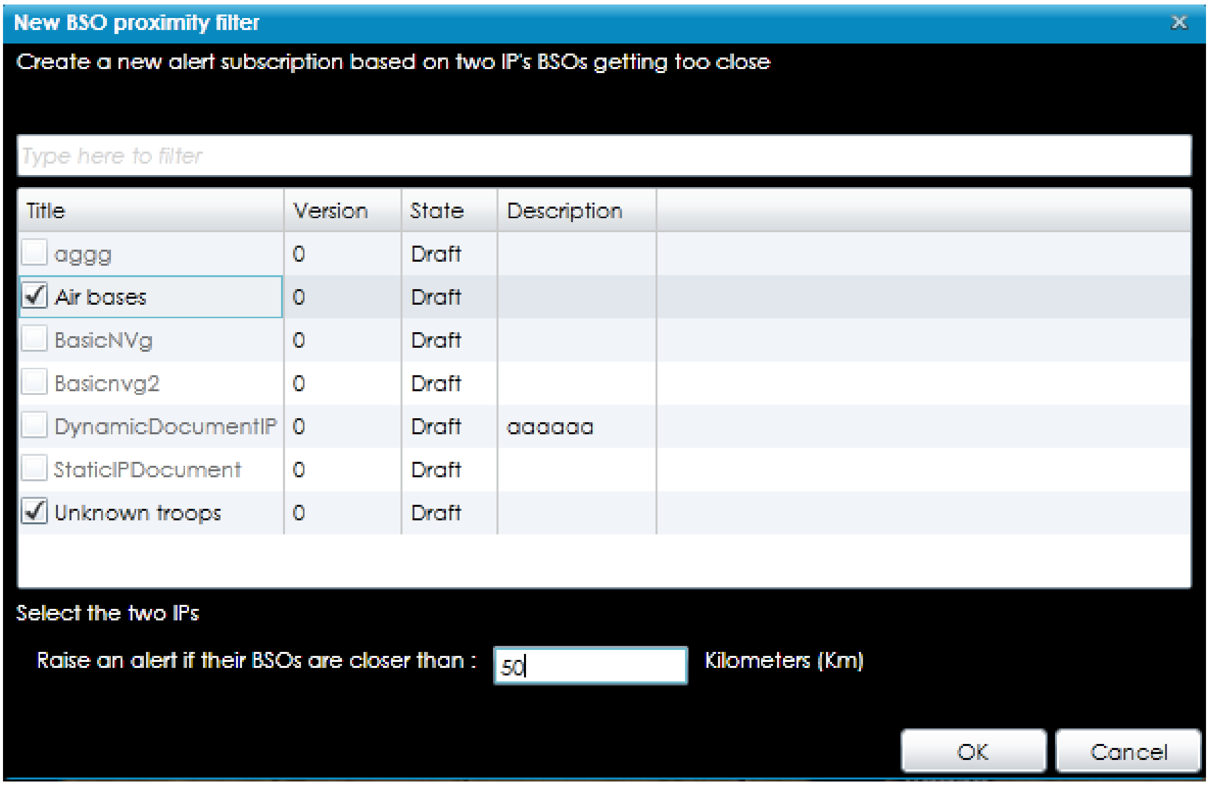
Figure 5-149: HMI for defining alerts based on BSOs entering a geospatial area

5.4.15.2.2.2 Relative proximity between BSOs

This type of alert allows a user to be notified when 2 BSOs (from different Information Products) are close to each other. When defining the rule, the user has to select the two Information Products that need to be analyzed and the distance threshold that will generate the alert.

This type of alert is expensive in terms of data processing because every BSO of an Information Product have to be compared (positions) with every other BSO in each Information Product, which could result in a lot of comparisons according to the number of Information Products involved and the number of BSO per Information Product. That is why a restriction has been set to limit the number of Information Products to be analyzed to 2.

Embedded in the Geographical COP editor, in the Alerts management module, an HMI allows a user to subscribe to such alerts with personal parameters:



New BSO proximity filter

Create a new alert subscription based on two IP's BSOs getting too close

Type here to filter

Title	Version	State	Description
□ aggg	0	Draft	
☑ Air bases	0	Draft	
□ BasicNVg	0	Draft	
□ Basicnvg2	0	Draft	
□ DynamicDocumentIP	0	Draft	aaaaaa
□ StaticIPDocument	0	Draft	
☑ Unknown troops	0	Draft	

Select the two IPs

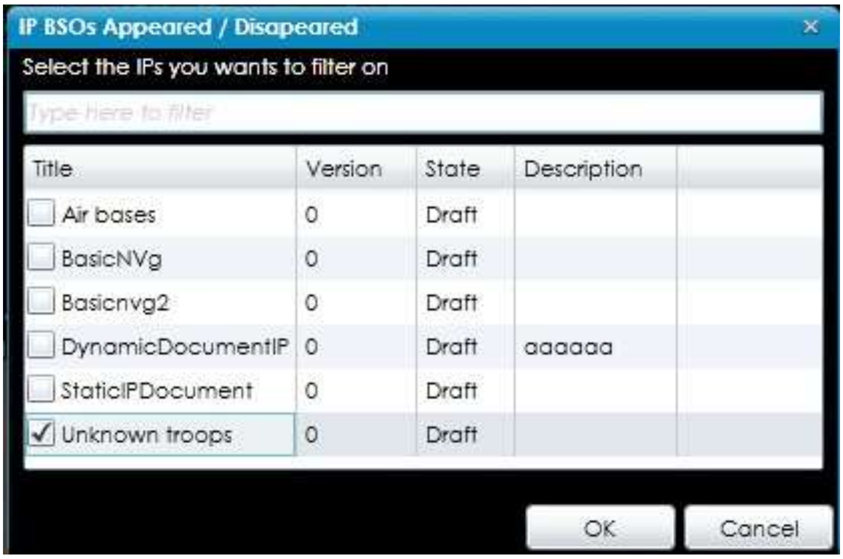
Raise an alert if their BSOs are closer than : 50 Kilometers (Km)

Figure 5-150: HMI for defining alerts based on BSO proximity

5.4.15.2.3 Appearance/Disappearance of a BSO

This type of alert allows a user to be notified if subsequently to an Information Product update a new BSO has appeared or if a BSO has disappeared, compared with the previous version of the Information Product.

Embedded in the Geographical COP editor, in the Alerts management module, an HMI allows a user to subscribe to such alerts with personal parameters:



IP BSOs Appeared / Disapeared

Select the IPs you wants to filter on

Type here to filter

Title	Version	State	Description
□ Air bases	0	Draft	
□ BasicNVg	0	Draft	
□ Basicnvg2	0	Draft	
□ DynamicDocumentIP	0	Draft	aaaaaa
□ StaticIPDocument	0	Draft	
☑ Unknown troops	0	Draft	

Figure 5-151: HMI defining alerts based on (dis)appearance of a BSO

5.4.15.2.4 Rules storage and processing

All the operational alerts business rules defined by the users are stored in Microsoft SQL Server. As described in the previous paragraphs, some rules are defined with XML, some others with a geometry attribute.

These rules are being processed when an “Information Product changed” event is triggered by the NCOP system. Receiving this event, the Business Rules Alerts manager component identifies the rules that need to be verified because they are associated with the Information Product that has been updated.

For each rule that need to be applied, the appropriate processing is launched. Depending on the rule type the processing is different but all of them rely on SQL requests that will use the BSO Search data tables. In fact, these BSO Search data tables contain all the attributes needed to verify if a BSO matches a certain rule (cf. paragraph 5.4.7.3).

If a rule returns a positive response, an event is created by the Business Rules Alerts manager component. This alert will be processed by the Alert/Notification Manager that will notify all the users that have subscribed to the business rule alert.

The following figure presents the different steps and actors involved in the processing of user defined Business Rules alerts:

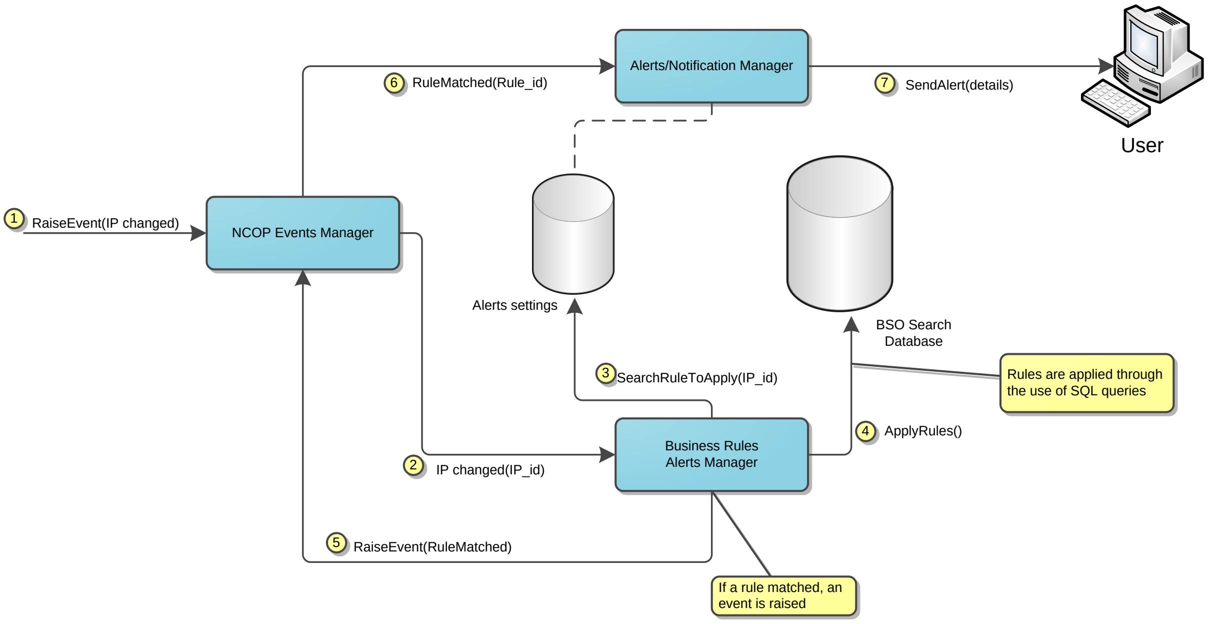

Alerts/Notification Manager
6 RuleMatched(Rule_id)
7 SendAlert(details)
User
1 RaiseEvent(IP changed)
NCOP Events Manager
Alerts settings
BSO Search Database
Rules are applied through the use of SQL queries
3 SearchRuleToApply(IP_id)
4 ApplyRules()
Business Rules Alerts Manager
2 IP changed(IP_id)
5 RaiseEvent(RuleMatched)
If a rule matched, an event is raised

Figure 5-152: Business rules alerts processing

5.4.15.3 Information Product post-processing

5.4.15.3.1 Principles

The purpose of the Information Product post-processing feature is to allow a COP manager to refine the content of an Information Product after it has been transformed into CDF by BizTalk Transformation phase, before it is stored in the NCOP storage.

This post-processing step can be applied to all Information Products that are acquired by BizTalk. Post-processing manipulates the content of a raw CDF file to produce a refined CDF file: it is not dependant on the original Information Product format.

The following figure presents the post-processing step as part of the acquisition process:

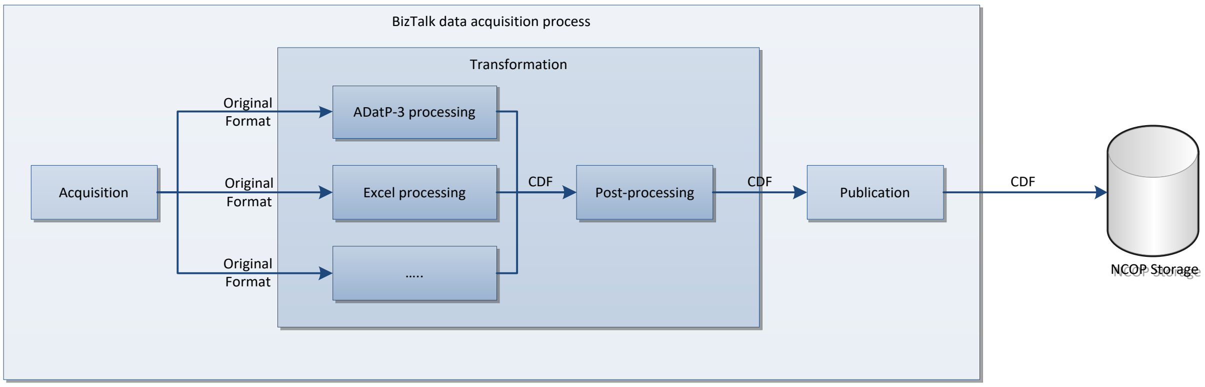


Figure 5-153: Information Product post-processing overview

NCOP proposes multiple refinement types:

- BSO filtering based on BSO properties,
- BSO properties modification to add, modify or remove properties,
- BSO visual modifications,
- Addition of visual augmentations based on BSO properties,
- BSO associations modification

Regarding BSO filtering, it is necessary for sources that don’t provide sufficient filtering capabilities or simply to keep BSOs that are necessary to the operational need.

BSO modification can be used to create or modify properties and therefore refine the generic mapping that has been performed by BizTalk.

Visual modifications can be used to change or set BSO symbols or to modify the style of BSO shapes.

Visual augmentation can be used to add extra shapes in the Information Product depending on BSO properties, for example draw a circle around a radar unit to represent its acquisition range that can be evaluated using its technical properties.

In case where the BizTalk mapping is too generic and won’t identify BSO relationships, it is sometimes possible in the post-processing step to create additional relationships between BSOs using the BSO properties.

5.4.15.3.2 Implementation

Post-processing rules are defined at the Information Product configuration level. A dedicated tab in the Information Product configuration panel allows the COP Manager to define post-processing rules.

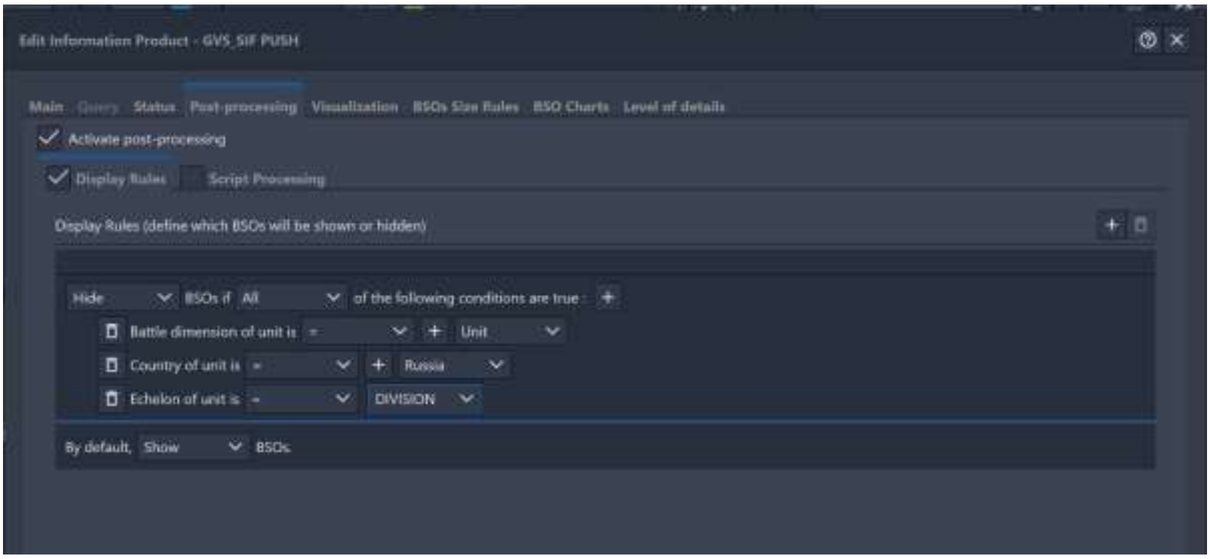
Post-processing rules can be defined using two different approaches:

- Simple filtering rules
- Advanced rules using NCOP scripting

Simple filtering rules are used for BSO filtering only. NCOP proposes an integrated web UI dedicated to the definition of these rules. They can be defined using simple conditions based on the following BSO properties:

- Hostility
- Country
- Echelon
- Headquarter
- Battle dimension
- ADEM type
- Any extended data

The following figure presents the Simple filtering rules UI:



☑ Activate post-processing

☑ Display Rules □ Script Processing

Display Rules (define which BSOs will be shown or hidden)

Hide BSOs if All of the following conditions are true :

Battle dimension of unit is = Unit

Country of unit is = Russia

Echelon of unit is = DIVISION

By default, Show BSOs

Figure 5-154: Post-processing simple filtering rules

Advanced rules can be used for BSO filtering but also for BSO properties modification, BSO visual modification, BSO visual augmentation and BSO associations modification. These rules are defined using the NCOP scripting technology that allows the manipulation of the CDF data model. NCOP proposes an integrated web UI dedicated to the definition of these rules.

The NCOP Scripting technology is described in more details in chapter 6.2.7.

These rules are stored in an XML format that contains both simple filtering rules and NCOP script representing the advanced rules. This post-processing XML definition is stored in the NCOP storage as a property of each Information Product.

During the acquisition of the Information Product, these rules are processed by the post-processing engine invoked by the BizTalk orchestration.

5.4.15.4 Information Product visualization filters

5.4.15.4.1 Principles

The NCOP Information Product visualization filters feature offers the capability for a COP manager to define multiple visual representations for the same Information Product. A COP consumer will then be able to select a specific representation for an Information Product depending on his needs.

The options for defining a specific visual representation are the following

- BSO filtering
- BSO modification of properties and style
- Visual augmentation
- BSO size (fixed or depending on zoom)

- Labels and tooltips configuration

These visualization filters can be applied on demand by a COP Consumer or can be defined as the default representation of an Information Product when a COP manager defines the content of COP.

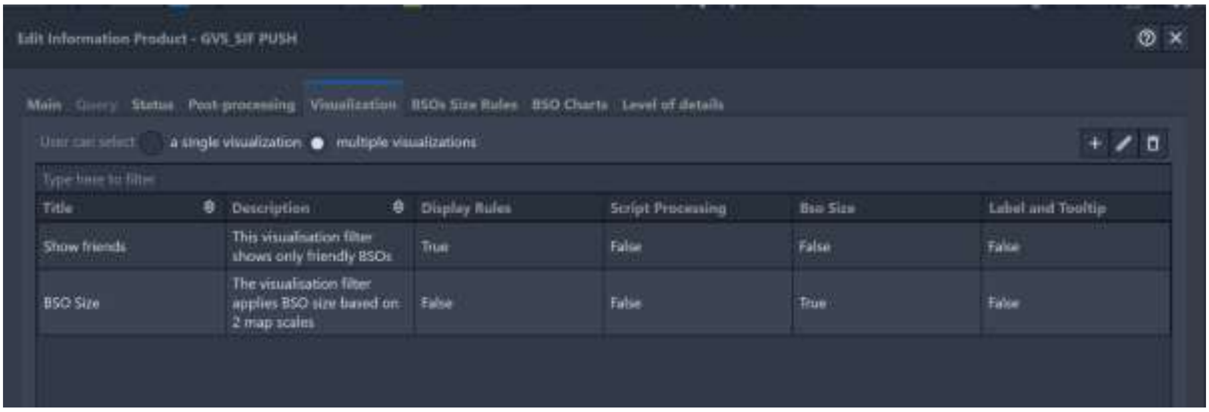
5.4.15.4.2 Implementation

Visualization filters are defined at the Information Product level. A dedicated tab in the Information Product configuration panel allows the COP Manager to define visualization filters. A visualization filter can be made of the following

- Simple filtering rules
- Advanced rules using NCOP scripting
- BSO size rules
- Labels and tooltips configuration

NCOP offers the capability to create multiple visualization filters for a single Information Product. The COP manager has also the capability to allow or forbid COP consumers to combine multiple visualization filters for an Information Product.

The following figure presents the visualization filter definition user interface:



User can select ○ a single visualization ● multiple visualizations

Title	Description	Display Rules	Script Processing	Bso Size	Label and Tooltip
Show friends	This visualisation filter shows only friendly BSOs	True	False	False	False
BSO Size	The visualisation filter applies BSO size based on 2 map scales	False	False	True	False

Figure 5-155: Information Product visualization filters management UI

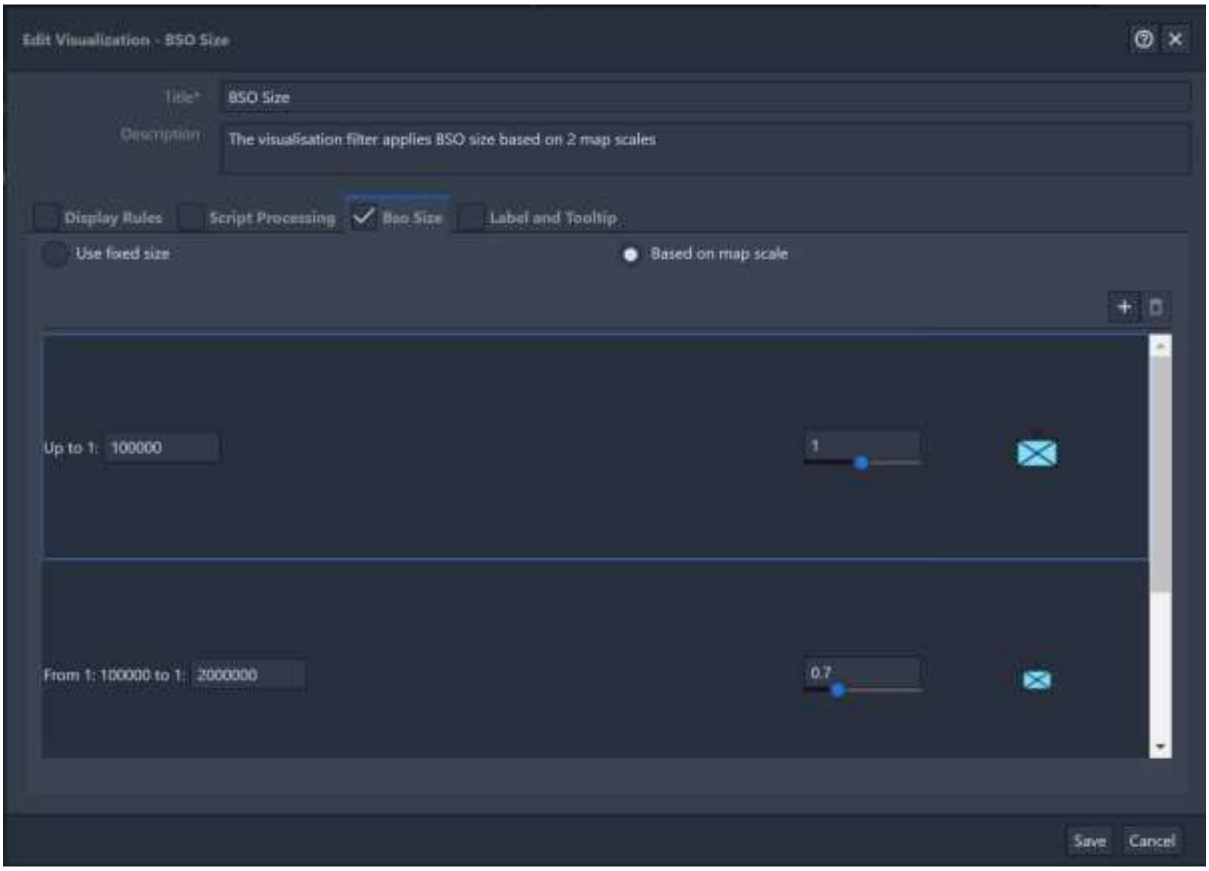
Simple filtering rules are used for BSO filtering only. NCOP proposes an integrated web UI dedicated to the definition of these rules. They can be defined using simple conditions based on the following BSO properties:

- Hostility
- Country
- Echelon
- Headquarter
- Battle dimension
- ADEM type
- Any extended data

Advanced rules can be used for BSO filtering but also for BSO properties modification, BSO visual modification, BSO visual augmentation and BSO associations modification. These rules are defined using the NCOP scripting technology that allows the manipulation of the CDF data model. NCOP proposes an integrated web UI dedicated to the definition of these rules.

The NCOP Scripting technology is described in more details in chapter 6.2.7.

BSO size rules allow the COP manager to define the BSO size. It can be either a fixed size or a variable size depending on the level of zoom. The following figure presents the associated user interface:



Title* BSO Size

Description The visualisation filter applies BSO size based on 2 map scales

○ Use fixed size ● Based on map scale

Up to 1: 100000 1

From 1: 100000 to 1: 2000000 0.7

Figure 5-156: Visualization filter BSO size rules configuration panel

Labels and tooltips can be configured by the COP manager who will select the properties to be used for tooltips and labels. The list of available properties is based on the content of the latest acquired information product instance. The following figure presents the associated user interface.

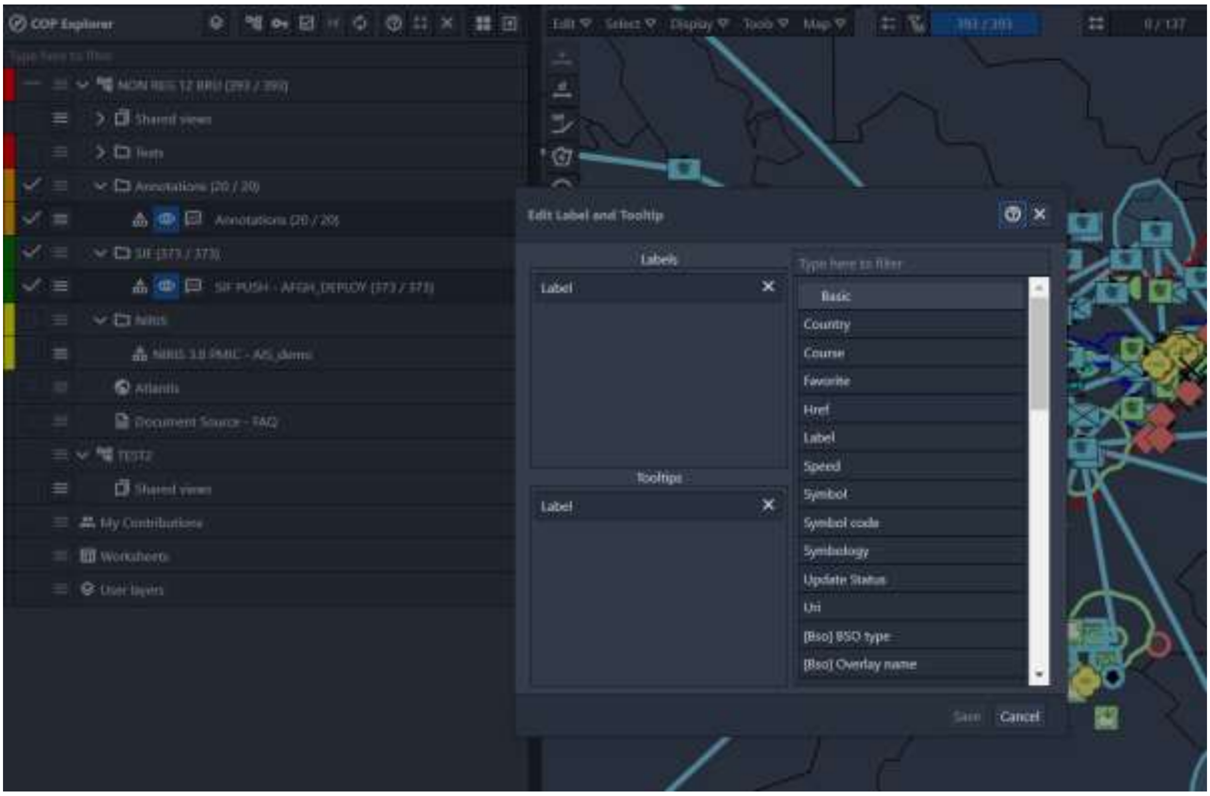


Figure 5-157: Visualization filters labels and tooltips configuration panel

Visualization filters are stored in an XML format, attached as a property to the corresponding Information Product item in the NCOP storage.

Visualization filters are processed in two parts:

- Simple filtering rules and advanced rules defined using NCOP script are processed on the server side by the NCOP publishing service (NCOP IPS). These two types of rules modify the CDF content of the Information Product and the resulting CDF is cached in order to minimize NCOP storage access and data processing, therefore optimizing consumption by all COP consumers.
- Tooltips and labels configuration and BSO size rules are processed on the client side, because they have no impact on the CDF content and are completely dependant on the visualization of the information.

5.4.15.5 Information Products level of details

5.4.15.5.1 Principles

A Level of detail (LoD) is a representation of an Information Product for a particular usage. Depending on the user objectives using the COP, the required LoD will differ.

Taking this into account, the following concepts have been implemented to manage LoD in NCOP.

- LoD

  It is a display configuration for an Information Product. It is made of the following:

  - BSO filtering rules based on BSO properties and relationships
  - BSO display aggregation rules based on BSO properties and relationships
- LoD type

  It is a set of individual LoDs. More precisely, it contains the following:

  - A set of ordered individual LoD, used for manual selection of a specific LoD
  - A set of individual LoD associated to a particular zoom level, used for automatic LoD selection based on the current map zoom scale.
  - Association with an Entity, used for automatic selection of the correct LoD type to be used depending on the user's entity.

5.4.15.5.2 LoD definition

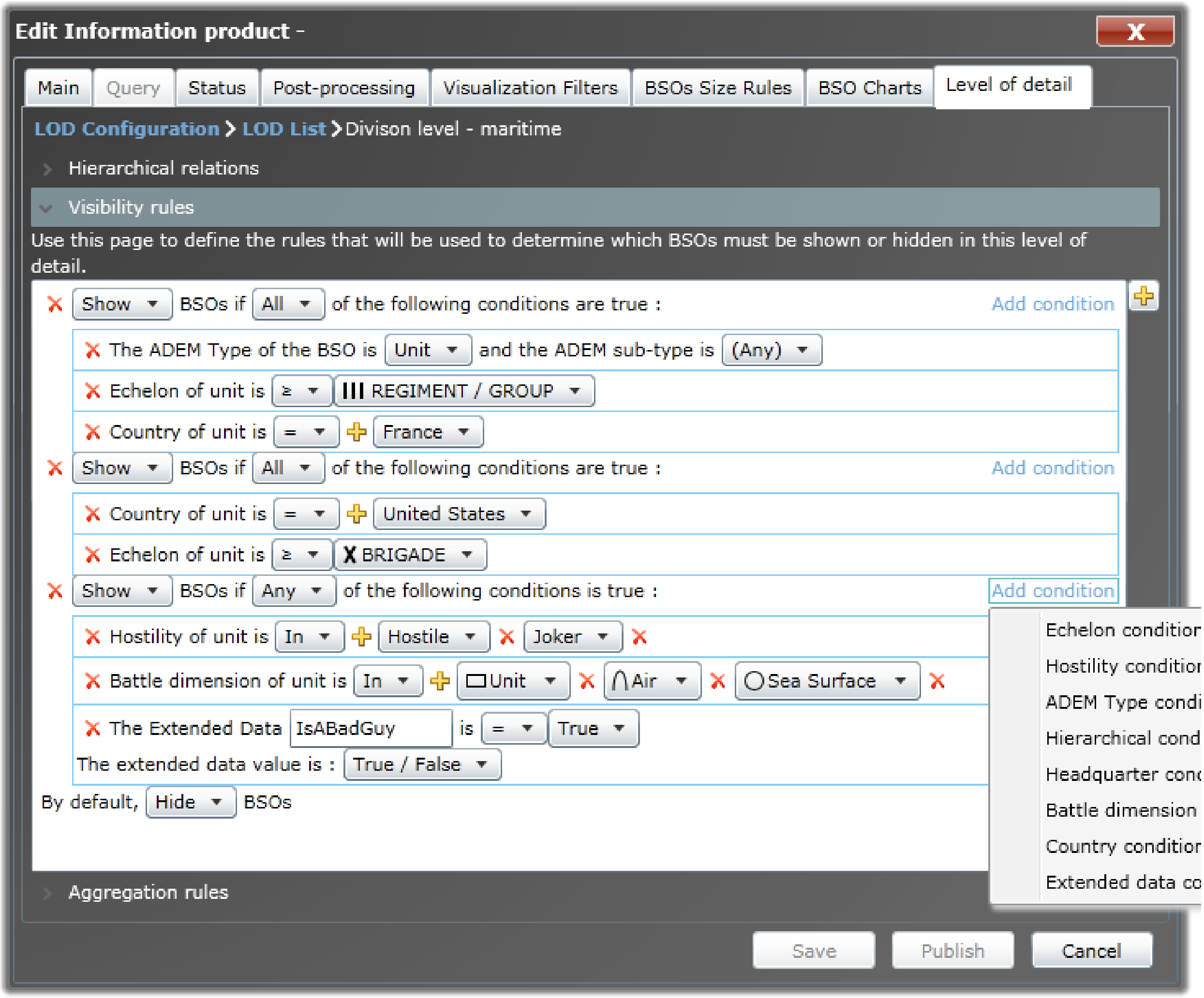
Regarding BSO filtering, NCOP offers the possibility to define rules based on the following properties:

- Echelon
- Hostility
- Headquarter
- Battle dimension
- Country
- Hierarchy level (based on a selected relationship type)
- ADEM BSO Type
- Any BSO extended data

For the hierarchy level conditions, a relationship type must be selected beforehand by the COP Manager. This relationship will be used to define rules such as: don't display a BSO if it is below level 3 in the relationship tree. The typical use case is to define rules based on the order of battle relationship to voluntarily hide BSOs of a certain hierarchical level.

Multiple rules and condition can be defined and ordered, providing maximum flexibility for the definition of filtering rules.

The following is a screenshot of the filtering rules definition UI in the Level of Detail configuration panel in the Information Product edition form:



LOD Configuration > LOD List > Divison level - maritime

Hierarchical relations

Visibility rules

Use this page to define the rules that will be used to determine which BSOs must be shown or hidden in this level of detail.

Show BSOs if All of the following conditions are true : Add condition
- The ADEM Type of the BSO is Unit and the ADEM sub-type is (Any)
- Echelon of unit is ≥ III REGIMENT / GROUP
- Country of unit is = France

Show BSOs if All of the following conditions are true : Add condition
- Country of unit is = United States
- Echelon of unit is ≥ X BRIGADE

Show BSOs if Any of the following conditions is true : Add condition
- Hostility of unit is In Hostile, Joker
- Battle dimension of unit is In Unit, Air, Sea Surface
- The Extended Data IsABadGuy is = True
  The extended data value is : True / False

By default, Hide BSOs

Aggregation rules

Figure 5-158: Level of Detail filtering rules definition panel

Regarding BSO display aggregation rules, NCOP proposes options to define the behaviour of the clustering feature when displaying BSOs on the map. Depending on the BSO nature and properties the following behaviours could be expected when a BSO overlaps with others when they are disaplayed on the map:

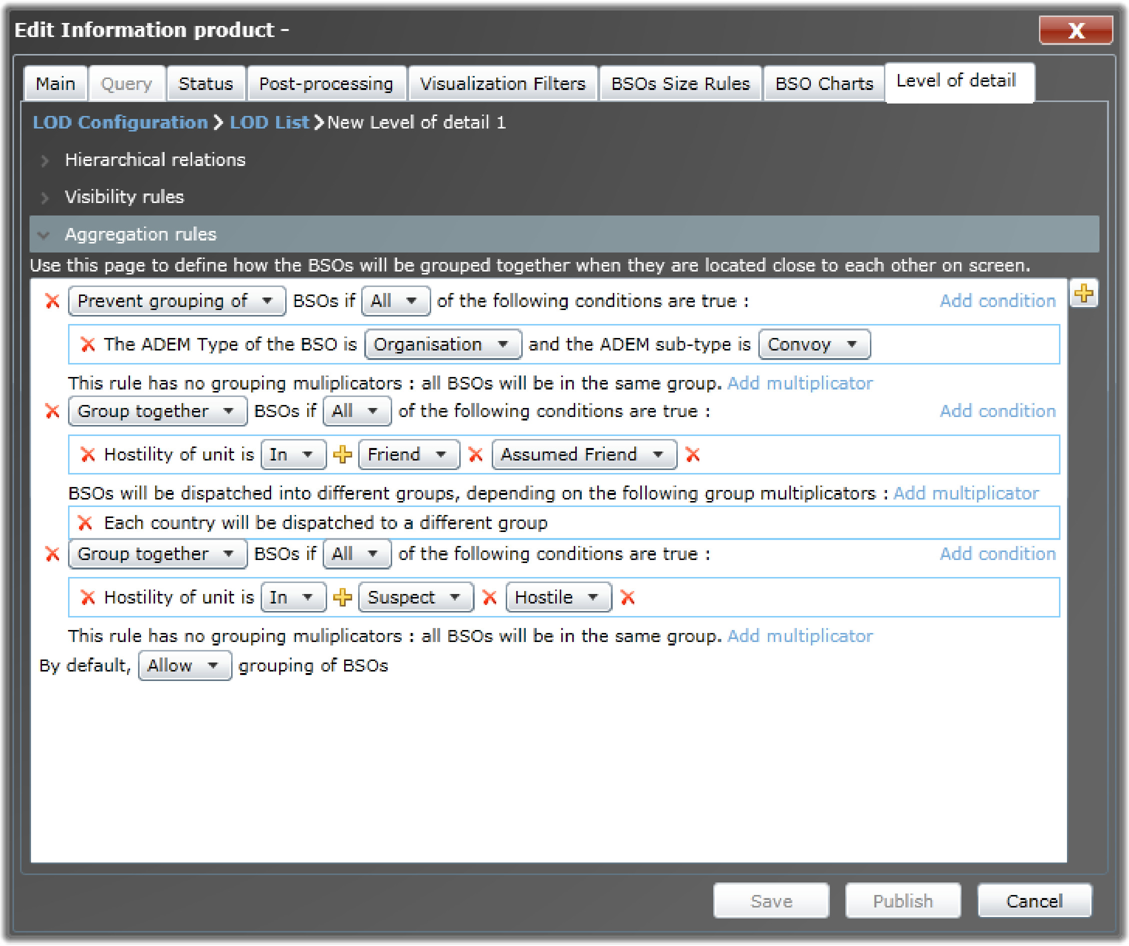
- The BSO must be displayed independently of the others
- The BSO can be grouped with others, with the following sub-options:
  - A single group can be created
  - Objects must be differentiated in a group based on BSO properties

When a single group is created, only one symbol is displayed on the map.

When objects are differentiated in a group, one graphical object will be drawn on the map but its visual representation is based on the various symbols of the BSOs it contains

It is important that when BSOs are aggregated with the decluttering mechanism, they will not be displayed at their real location.

The following is a screenshot of the aggregation rules definition UI in the Level of Detail configuration panel in the Information Product edition form:



Use this page to define how the BSOs will be grouped together when they are located close to each other on screen.

✕ Prevent grouping of ▾ BSOs if All ▾ of the following conditions are true : Add condition

✕ The ADEM Type of the BSO is Organisation ▾ and the ADEM sub-type is Convoy ▾

This rule has no grouping muliplicators : all BSOs will be in the same group. Add multiplicator

✕ Group together ▾ BSOs if All ▾ of the following conditions are true : Add condition

✕ Hostility of unit is In ▾ + Friend ▾ ✕ Assumed Friend ▾ ✕

BSOs will be dispatched into different groups, depending on the following group multiplicators : Add multiplicator

✕ Each country will be dispatched to a different group

✕ Group together ▾ BSOs if All ▾ of the following conditions are true : Add condition

✕ Hostility of unit is In ▾ + Suspect ▾ ✕ Hostile ▾ ✕

This rule has no grouping muliplicators : all BSOs will be in the same group. Add multiplicator

By default, Allow ▾ grouping of BSOs

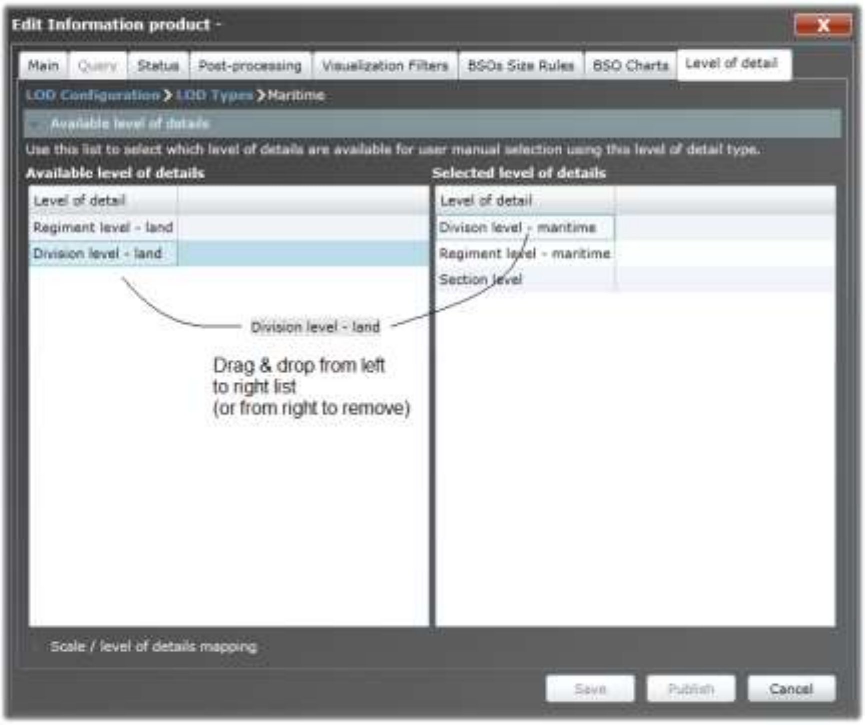
Figure 5-159: Level of Detail aggreation rules definition panel

5.4.15.5.3 LoD type definition

Defining a LoD type consists in:

- Selecting individual LoDs, to be used for manual LoD application by consumers

  This is done with a dedicated UI allowing the COP Manager to select LoDs from the list of all available LoDs. This UI is presented in the following figure:


Edit Information product -
X
Main
Query
Status
Post-processing
Visualization Filters
BSOs Size Rules
BSO Charts
Level of detail
LOD Configuration > LOD Types > Maritime
Available level of details
Scale / level of details mapping
Save
Publish
Cancel

Use this list to select which level of details are available for user manual selection using this level of detail type.

Available level of details

Level of detail
Regiment level - land
Division level - land

Selected level of details

Level of detail
Divison level - maritime
Regiment level - maritime
Section level

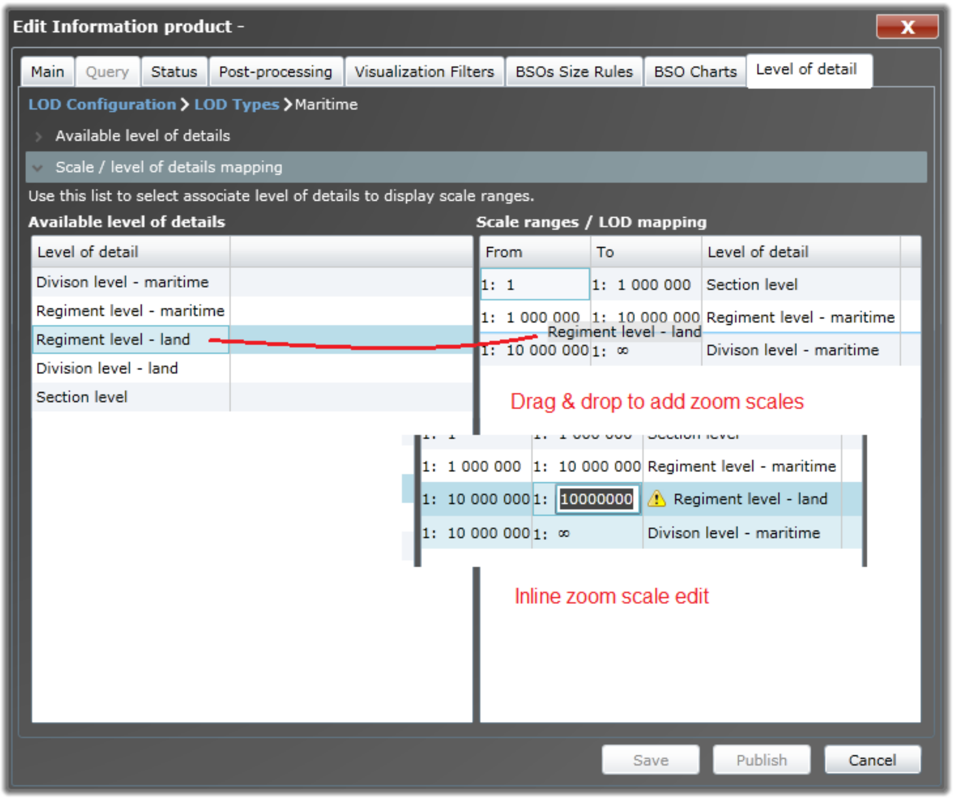
Division level - land

Drag & drop from left
to right list
(or from right to remove)

Figure 5-160: Level of Detail type definition panel (1/3)

- Associating individual LoDs to map scales, to be used for automatic LoD application based on the current map zoom scale

  This is done with a dedicated UI allowing the COP Manager to select LoDs from the list of all available LoDs. This UI is presented in the following figure:



LOD Configuration > LOD Types > Maritime

Available level of details

Scale / level of details mapping

Use this list to select associate level of details to display scale ranges.

Available level of details

Level of detail
Divison level - maritime
Regiment level - maritime
Regiment level - land
Division level - land
Section level

Scale ranges / LOD mapping

From	To	Level of detail
1: 1	1: 1 000 000	Section level
1: 1 000 000	1: 10 000 000	Regiment level - maritime
1: 10 000 000	1: ∞	Divison level - maritime

Regiment level - land

Drag & drop to add zoom scales

1: 1	1: 1 000 000	Section level
1: 1 000 000	1: 10 000 000	Regiment level - maritime
1: 10 000 000	1: 10000000	⚠ Regiment level - land
1: 10 000 000	1: ∞	Divison level - maritime

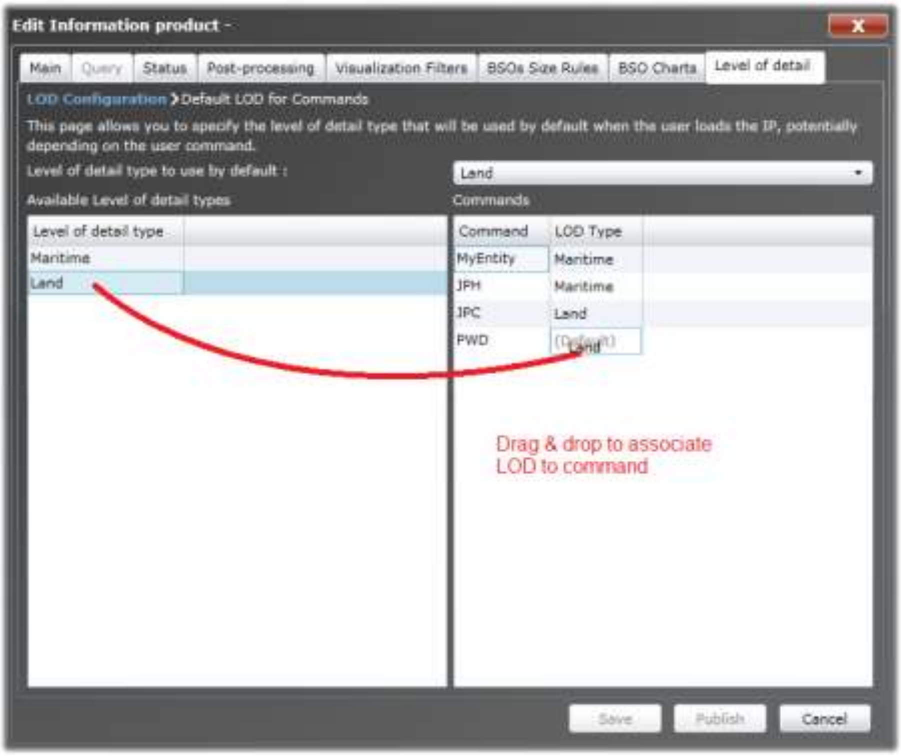
Inline zoom scale edit

Figure 5-161: Level of Detail type definition panel (2/3)

- Associating a LoD type to a specific entity.

  A single LoD type can be associated to multiple entities. It is also possible to define a default LoD type. It will be associated with entities that don't have a specific LoD type defined.

  Association to entities is done with a dedicated UI presented in the following figure:



LOD Configuration > Default LOD for Commands

This page allows you to specify the level of detail type that will be used by default when the user loads the IP, potentially depending on the user command.

Level of detail type to use by default : Land

Available Level of detail types

Level of detail type
Maritime
Land

Commands

Command	LOD Type
MyEntity	Maritime
JPH	Maritime
JPC	Land
PWD	(Default)

Drag & drop to associate LOD to command

Figure 5-162: Level of Detail types definition panel (3/3)

5.4.15.5.4 Level of Details templates

For similar Information Products, the COP Manager could want to reuse existing LoD instead of defining a LoD from scratch. Therefore NCOP offers the capability to save a LoD as a template for a later reuse. Reusing a LoD template will only create a copy of an LoD definition: modifying a LoD template will not affect LoD that have been previoulsy created from this template. It also allows the COP Manager to start from a LoD template and refine it based on the Information Product specificities. LoD templates can be organized with folders to reflect their content and simplify the search of a specific template.

In order to simplify the LoD definition process, NCOP also offers the possibility to create or copy a LoD from LoDs currently being used by other Information Products.

In addition, the COP manager has also the capability to copy a full LoD configuration from one already defined for another information product. This option will copy the whole LoD configuration: individual LoD and LoD types.

5.4.15.5.5 Level of details configuration storage

A LoD configuration is stored using an XML representation that contains:

- all filtering and aggregation rules of each LoD
- all parameters of each LoD type

The corresponding XML document is stored as a property of the associated Information Product. If the Information Product is synchronized between two NCOP nodes, the LoD configuration is also synchronized with the Information Product item. This XML representation is used by the Geographical COP Editor to configure LoD application when the Information Product is visualized.

LoD templates are stored using a similar XML representation but are stored in a dedicated SharePoint list in the NCOP portal. LoD templates remain local to an NCOP node and are not synchronized to remote nodes.

5.4.15.5.6 LoD application in the Geographical COP Editor

When an Information Product is loaded in the Geographical COP Editor, the XML representation of its LoD configuration is used to apply the visualization settings. Settings are applied by taking into account the following elements:

- Automatic application
    - Based on the user entity, the corresponding LoD type will be automatically selected
        - Depending on the current zoom scale, the corresponding LoD will be automatically applied
            - BSOs are filtered depending on the LoD settings and BSO properties
            - BSOs are clustered depending on the LoD settings and BSO properties
- Manual application
    - The consumer selects the LoD type
        - The consumer selects the LoD from those available for the selected LoD type
            - BSOs are filtered depending on the LoD settings and BSO properties
            - BSOs are clustered depending on the LoD settings and BSO properties

The BSO filter used when a LoD is being applied is not visible from the user a standard BSO filter. The filtering is performed before the BSOs are displayed. Therefore, hidden BSOs don’t appear in the list of BSOs contained in the information product. However for user understanding, BSO counters in the COP Explorer take this filtering into account and display:

- Number of BSOs of the original Information Product
- Number of BSOs once the LoD filter has been applied

5.4.15.5.7 Level of Details use case

The following is an explanation of a sample use case involving the Level of Details feature in a basic scenario:

Two entities want to consume the same information product. Because of their activities they don't require to display the same information: MARCOM is a maritime HQ and will focus on maritime units whereas CCOMC will want to display units of all types. From this information two LoD types should be created:

- 'Maritime' will contain LoDs that are appropriate for Maritime-oriented visualization.
- 'Global' will contain LoDs that are appropriate for a visualization requiring the display of all units' categories

For each LoD type, specific filtering options could apply depending on the visualization zoom scale:

- At the country level, only enemy units could be displayed
- At the city level, all units should be displayed

From these requirements, specific LoDs will be defined and associated with the corresponding LoD types:

- Display maritime units
- Display enemy maritime units
- Display everything
- Display enemies

When those LoD are selected to be part of the LoD type, the COP Manager will decide to associate them with a zoom scale:

- 'Display maritime units' and 'display everything' will be associated with a zoom scale range corresponding to a country level
- 'Display enemy maritime' units and 'display enemies' will be associated with a zoom scale range corresponding to a city level

The following figure presents an overview of this scenario:

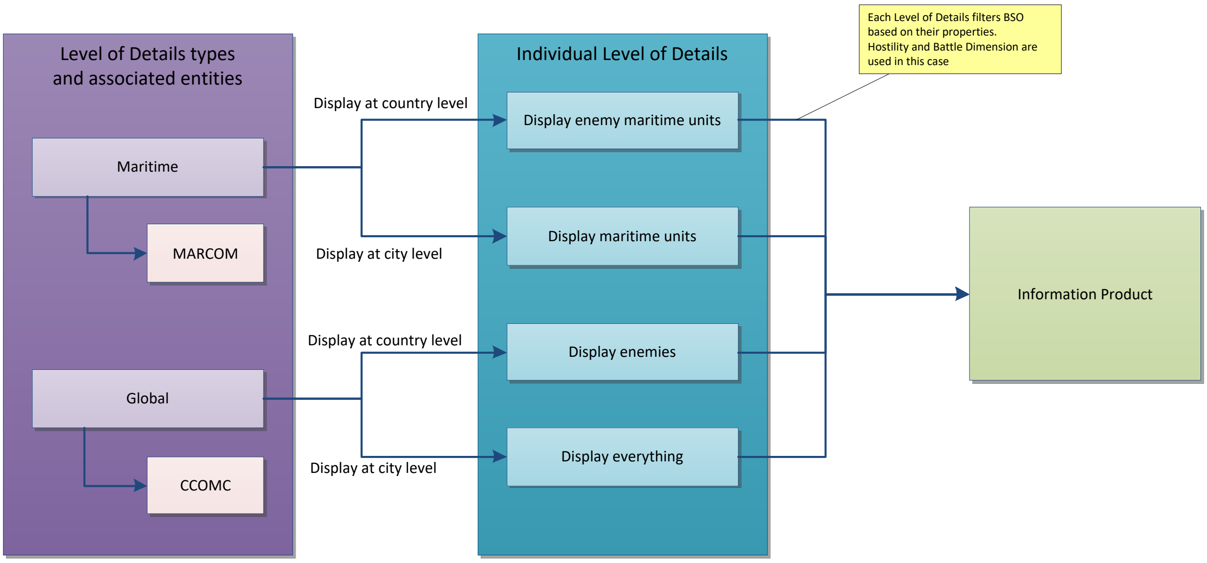

Level of Details types and associated entities
Maritime
MARCOM
Global
CCOMC
Display at country level
Display at city level
Display at country level
Display at city level
Individual Level of Details
Display enemy maritime units
Display maritime units
Display enemies
Display everything
Each Level of Details filters BSO based on their properties. Hostility and Battle Dimension are used in this case
Information Product

Figure 5-163: Level of Detail basic scenario overview

5.4.16 Using an external SQL server

In case of deployment on the Data Centre, a dedicated team is in charge of the SQL servers installation (not specific to NCOP). All the other servers (SharePoint, BizTalk, GeoServer…) are in the scope of the NCOP team in charge of the NCOP deployment.

However all NCOP servers are dedicated to NCOP (SQL, SharePoint, BizTalk, GeoServer) contrary in 5.4.23 Mutualization of servers (SQL and SharePoint) where the SQL Server is shared between several FAS.

5.4.17 Anonymous access to NCOP

5.4.17.1 NCOP home page

The home page presented in the NCOP portal does not require that the user be logged in. It exposes COPs and Information Products that have been explicitly declared by the owner entity as publicly accessible to the users that have been authorized by the bearer network: the dissemination settings are configured to authorize the “Everyone” virtual entity to view these COPs

This page proposes to the user:

- A list of available COPs
- A list of recently updated Information Products
- A shortcut to launch the Geographical COP editor
- A login option

Until the user explicitly logs in, he has a read only access and no administration function is available.

5.4.17.2 Geographical COP Editor

From the NCOP Home page, it is possible to launch the Geographical COP Editor anonymously. When launched anonymously, the Geographical COP Editor allows the users to browse the list of available “public” COPs and visualize the contents of the associated Information Products. The user can use the same functionalities as the basic default role and also, the Geographical COP Editor does not include the alert/notification functionalities.

5.4.17.3 NCOP Web services

It is possible for external systems to consume NCOP Web services anonymously. The following services are available with anonymous access:

- COP consumption based on JIPS (JCOP IP Publishing Service):
  - JIPSonSteroid (iGeoSIT consumers)
  - JIPS
- COP consumption based on NCOP IPS (NCOP IP Publishing Service):
  - NCOPIPS (WCF SOAP XML)
- COP consumption based on Geographical COP Editor Services
  - Geographical COP Editor Services (REST API)

Regarding the visibility of COPs and Information Products, the same rules are applied than for the content exposed in the public home page of NCOP, meaning that anonymous consumption of these web services allows the system to access information that has been explicitly declared as “public” by the owner entity.

5.4.17.4 Disabling anonymous access

It is possible to disable anonymous access by modifying the configuration of the Web server where NCOP Web services are hosted. This remains a manual operation that consists in disabling the ‘Anonymous authentication’ scheme for the web application folder in IIS. The procedure is described in the NCOP System Administration Manual.

5.4.18 BizTalk organization

This section is related to the §5.3.3.3.1 Microsoft BizTalk Implementation Component.

5.4.18.1 Applications

As described above in the document, NCOP uses four (4) different BizTalk applications. BizTalk applications are a way to isolate portions of code having in mind software maintenance. Each Application can be deployed as a single deployment package, independently of the others. Therefore, if some orchestration requires an update, it is not necessary to re-deploy all the Applications but only the Application that handles this specific orchestration.

Regarding resources (mainly CPU and memory) and manipulated data, BizTalk Applications are not impacted:

- Hosts instances are the technical mean to optimize resources,
- Data can go from one orchestration to the other independently of BizTalk Applications because in NCOP BizTalk Applications share the same message box.

5.4.18.2 Host instances

BizTalk offers a lot of flexibility regarding the optimization of resources by the use of host instances. Host instances can be created as required by an administrator in order to isolate some orchestrations, receive ports or send ports in terms of CPU and memory usage and optimize the use of these resources on each BizTalk server.

By default, the NCOP factory settings have isolated some critical parts of the data acquisition orchestrations but these settings can be refined at run-time by an authorized user. A host instance can be created on the server and be associated with orchestrations and ports independently of their hosting Application.

Note that in a BizTalk Group configuration (multi-server environment), BizTalk introduces the Host concept that is the abstraction of all corresponding host instances that are running on each server of the BizTalk Group.

5.4.18.3 Data acquisition behaviour

Regarding data acquisition, NCOP allows the declaration of Information Products in “pull” mode. In this configuration, BizTalk orchestration will be triggered periodically, according to the schedule settings defined in the Information Product by the COP Manager.

The way BizTalk initiates the acquisition of pulled data is handled by a process that will periodically (Every one (1) second) determine which Information Product must be acquired. This process determines the Information Product to acquire by:

- Identifying the most urgent Information Product to be acquired (regarding the schedule parameter),
- Avoiding launching another “pull” acquisition for an Information Product if the previous process for that Information Product is still in process.

The last bullet of the list is a mechanism that is designed to avoid bottlenecks in the acquisition processes that could happen by launching multiple acquisitions of the same data at the same time. A side effect of this mechanism is that if an acquisition process for an Information Product takes some time, the next iteration of the pull mechanism might cause the data to arrive later than it is planned by the schedule parameter. But this behaviour is a lesser evil compared to a saturation of all data acquisition processes because of one Information Product that takes to much time being processed.

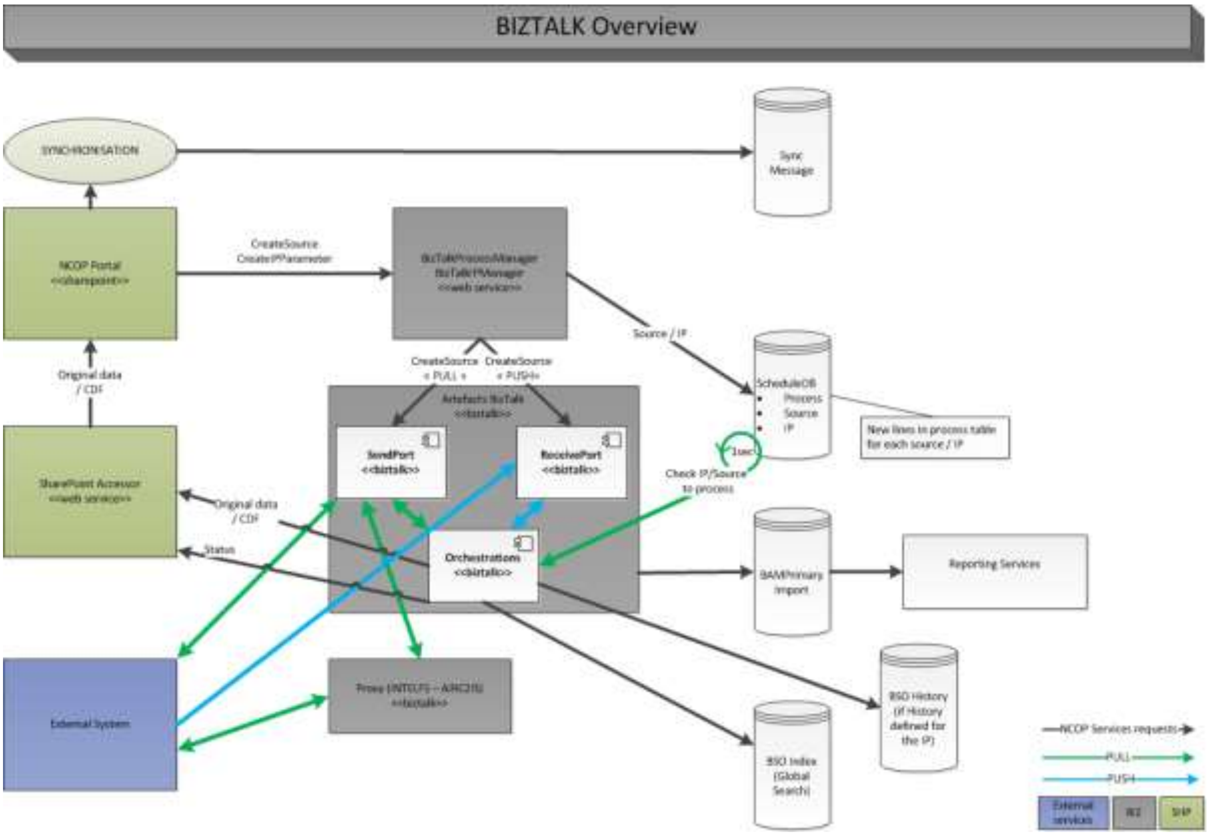


Figure 5-164: Overview of data acquisition performed by BizTalk

5.4.19 Dynamic Information Products

5.4.19.1 Principles

NCOP offers the capability to define dynamic Information Products and include them into a COP. An information product can be considered dynamic for the following reasons:

- Information update is too frequent

This is the case of tracking data provided by NIRIS, MCCIS and other tracking systems. The refresh rate of the information provided by these systems would flood and saturate the data acquisition channel and the NCOP storage component

- Information is too big

This is the case of documents such as videos that would take a lot of place in the NCOP storage component whereas they would be preferably made available using streaming protocols

- Information doesn't require to be stored in NCOP

This is the case of Geographical data such as background maps and geographical information that are maintained and exposed by external map providers (mainly CoreGIS)

Therefore, the fact that an Information Product is considered dynamic is enforced by the nature of the source itself.

When an Information Product is dynamic, NCOP will only store the necessary information that will allow a user to consume the information product directly from the source.

5.4.19.2 Track-based Information Products

5.4.19.2.1 Acquisition and consumption mechanisms

Tracks Information Products can be defined in NCOP using the same principles than any other Information Product: at first a source must be created, and then Information Products can be created using that source.

However, in the case of such dynamic Information Products, BizTalk is involvement is a bit different. Unlike data-driven information products, for performance reasons described above, it is not desirable that the data follow the same processes (feeding BSO history and BSO search database tables, publication in the NCOP storage).

BizTalk involvement in the management of Dynamic Information Products is the following:

When a source is created in the NCOP storage, BizTalk is notified and appropriate connectors and orchestrations are instantiated in order to acquire the capabilities of the source.

When an Information Product is created in the NCOP storage, BizTalk is notified and propagates the Information Product settings to the appropriate dynamic source connector. These dynamic source connectors are components whose job is to:

- Subscribe to sources according to Information Product settings,
- Convert into CDF the incoming tracks published by the source,
- Forward the CDF tracks to the NCOP Dynamic Source Server.

Dynamic source connectors are implemented as Windows Services. They are implemented this way to avoid the processing of dynamic data in BizTalk orchestrations. Some refresh rates of incoming tracks could have an impact on the other BizTalk processes and slow down the processing of data-driven Information Products.

The NCOP Dynamic source server is a component that:

- Receives CDF tracks from all dynamic source connectors,
- Keep an internal cache of tracks for each Information Product,
- Receives Information Product subscriptions from COP Users

- Forward the CDF tracks to all subscribed clients.

The internal track cache for each Information Product is used:

- To transmit the current state of an Information Product as the first update packet after a client subscribes to that Information Product.
- To manage BSO deletion when a track has not been refreshed after a certain period of time (configurable)
- To offer the capability in NCOP to convert a Dynamic Information Product into a data-driven Information Product

The following figure presents the communications between the various actors involved in the tracks-based dynamic Information Product consumption process:

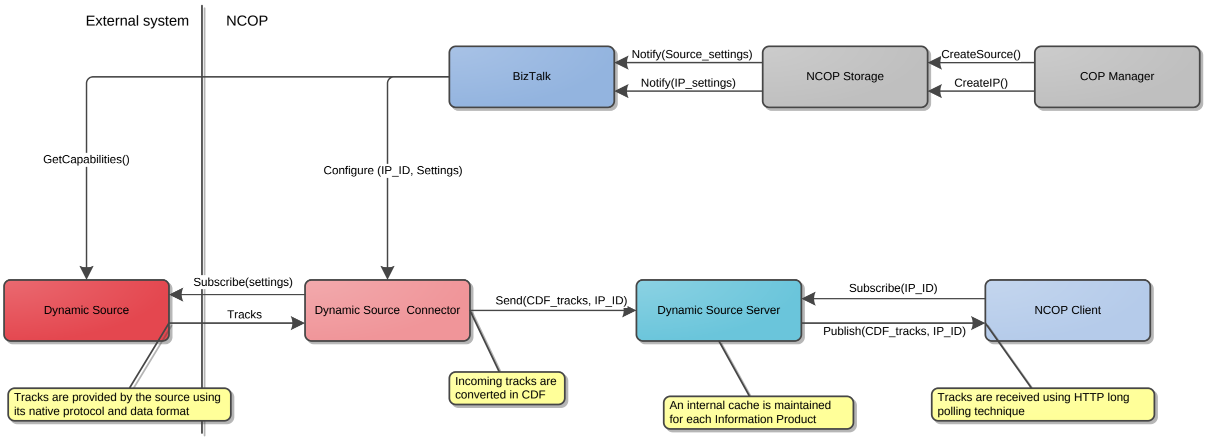

External system
NCOP
BizTalk
Notify(Source_settings)
Notify(IP_settings)
NCOP Storage
CreateSource()
CreateIP()
COP Manager
GetCapabilities()
Configure (IP_ID, Settings)
Dynamic Source
Subscribe(settings)
Tracks
Dynamic Source Connector
Send(CDF_tracks, IP_ID)
Dynamic Source Server
Subscribe(IP_ID)
Publish(CDF_tracks, IP_ID)
NCOP Client
Tracks are provided by the source using its native protocol and data format
Incoming tracks are converted in CDF
An internal cache is maintained for each Information Product
Tracks are received using HTTP long polling technique

Figure 5-165: Tracks-based Dynamic Information Products consumption process

When NCOP is installed in high availability mode, the dynamic source connector and dynamic source server are instantiated multiple times providing:

- Failover for data acquisition by the dynamic source connectors
- Failover for data data consumption from the dynamic source servers
- Load balancing for data consumption from the dynamic source servers

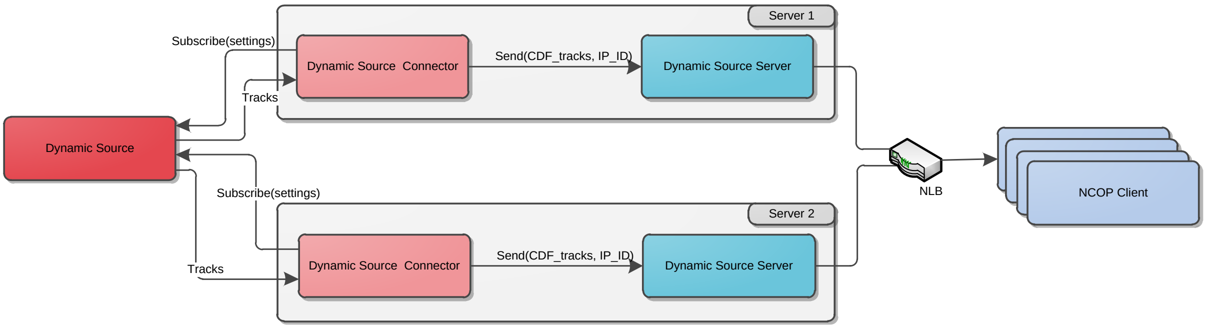


Figure 5-166: Dynamic Information Products consumption with high availability

In the case of a NIRIS connector installation on dedicated servers, the data flow is described in the following diagram:

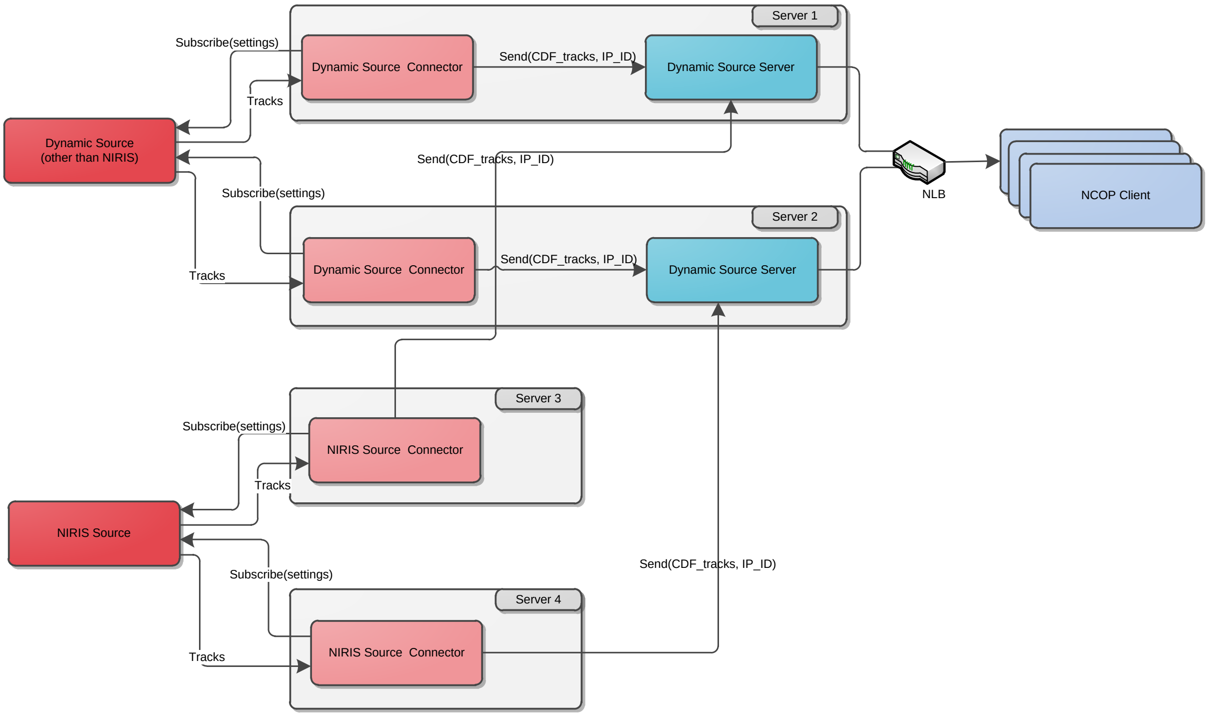


Figure 5-167: Dynamic Information Products consumption with high availability and NIRIS connectors installed on dedicated servers

Each dynamic source connector windows service allows the connection to multiple source servers: for example, the same MCCIS connector is used to connect to multiple MCCIS servers (each MCCIS server being declared as a source in NCOP). Dynamic source connectors will instantiate as many connections as required to the remote source servers and will receive data coming from all the connected sources. All received tracks are sent to the Dynamic source server component that is in charge of sending the appropriate tracks to the clients.

5.4.19.2.2 Conversion into a data-driven Information Product

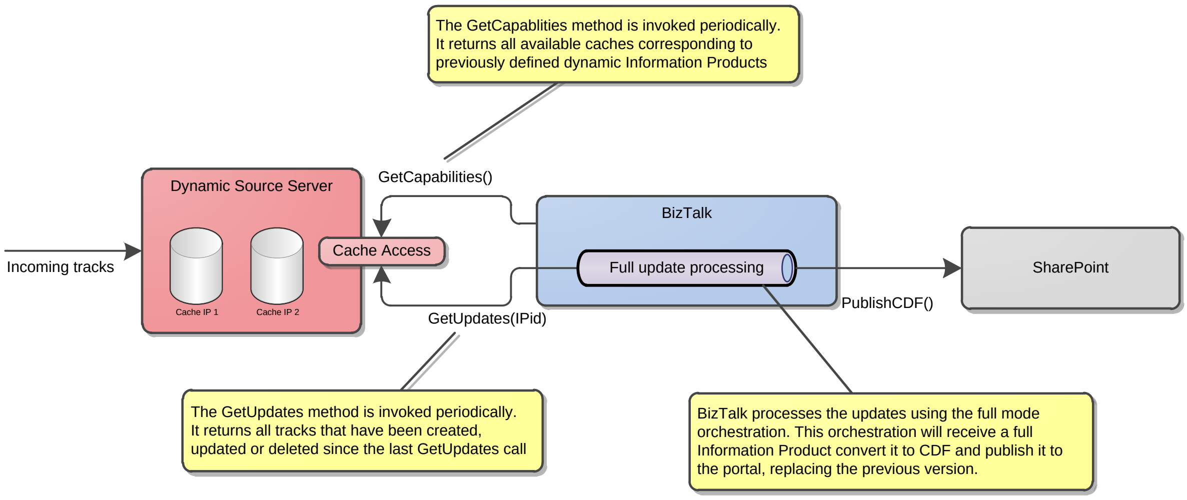
NCOP offers the possibility to convert any existing track-based dynamic Information Product into a data-driven Information Product.

For this purpose, an internal NCOP source is created during NCOP installation. This source allows the creation of data-driven Information Products based on any existing track-based Dynamic Information Product. This source is in fact the Dynamic Source Server that:

- Exposes its capabilities corresponding to its available internal caches (one per Information Product)
- Provides Information Products updates upon request by return its cache contents.

Data acquisition for this source is configured to be done periodically. Updates are provided in full mode, in order to avoid processing differential updates which might lead to performance issues even impacting the acquisition of other Information Products and Sources.

The following figure presents how track-based dynamic information products are converted into data driven Information Product:



The GetCapablities method is invoked periodically. It returns all available caches corresponding to previously defined dynamic Information Products

The GetUpdates method is invoked periodically. It returns all tracks that have been created, updated or deleted since the last GetUpdates call

BizTalk processes the updates using the full mode orchestration. This orchestration will receive a full Information Product convert it to CDF and publish it to the portal, replacing the previous version.

Figure 5-168: Dynamic to data-driven conversion

When a dynamic Information Product is created by a COP Manager, an automatic process will create the corresponding data-driven Information Product from the Dynamic Source Server built-in Source and associate both Information Products.

This “technical” data-driven Information Product is not visible as such by the COP manager and Users. It is an internal Information Product for which data acquisition will follow the same steps as any other data-driven Information product (feeding BSO search, BSO history database and publishing a CDF version of the data into the NCOP portal). This “technical” information product will be used by COP Users that do not have the appropriate connector to consume dynamic information products.

To be more specific regarding the consumption of dynamic Information product the process will be the following: when browsing the COP with NCOP web services, the COP Users will see the Information Product in the structure of the COP and identify its dynamic capability. If the COP User has the appropriate dynamic Information Product connectivity it will be able to subscribe and consume the Information Product dynamically from NCOP. If the COP User doesn’t have the appropriate connector, it will be able to consume the information product as data-driven (using the GetProductContent method from the JIPS web service for example).

5.4.19.3 Geographical Information Products

NCOP handles several types of Geographical Information Products:

- KML/KMZ files
- WMS layers

KML or KMZ files can be declared as a geographical Information product by declaring the URL at which the file is available. When the COP is exposed by NCOP, this same URL is used to define the location of the information product so that the clients can access the file.

A WMS-based Geographical Information Product is defined in NCOP using two steps:

First, a Map Service must be declared. The Map Service is an element that is able to provide multiple Map Layers. Map Services are defined by a URL made available by a Geographical Map Server (a map server can expose multiple Map Services).

Once a Map Service has been defined, it can be used to create a geographical Information product by selecting the required map layers with their associated style.

When the COP is exposed by NCOP, WMS-based Information Products are described the following elements:

- Map Service URL
- List of Map Layers
- List of Map Layer styles

This information can be used by any consumer so he can create the appropriate WMS request to obtain the data.

5.4.19.4 External documents

In NCOP, external documents can be declared as Information Products. These documents will be identified with the URL at which they are exposed by an external system. When the COP is exposed by NCOP, these Information Products will be described by this same URL.

Depending on the protocol associated with the resource’s URL (http, rtsp, mms, etc.), a COP User requires the appropriate tools in order to access and display the data.

5.4.20 NCOP behaviour in degraded mode

This chapter is dedicated to the description of NCOP behaviour when:

- Network is not available
- NATO infrastructure service is not available
- NCOP service is not available

5.4.20.1 Network failures

Network failures can happen at various levels depending on the network topology of sites.

The following figure presents a high level view of connections that can exist in a typical deployment scenario for NCOP:

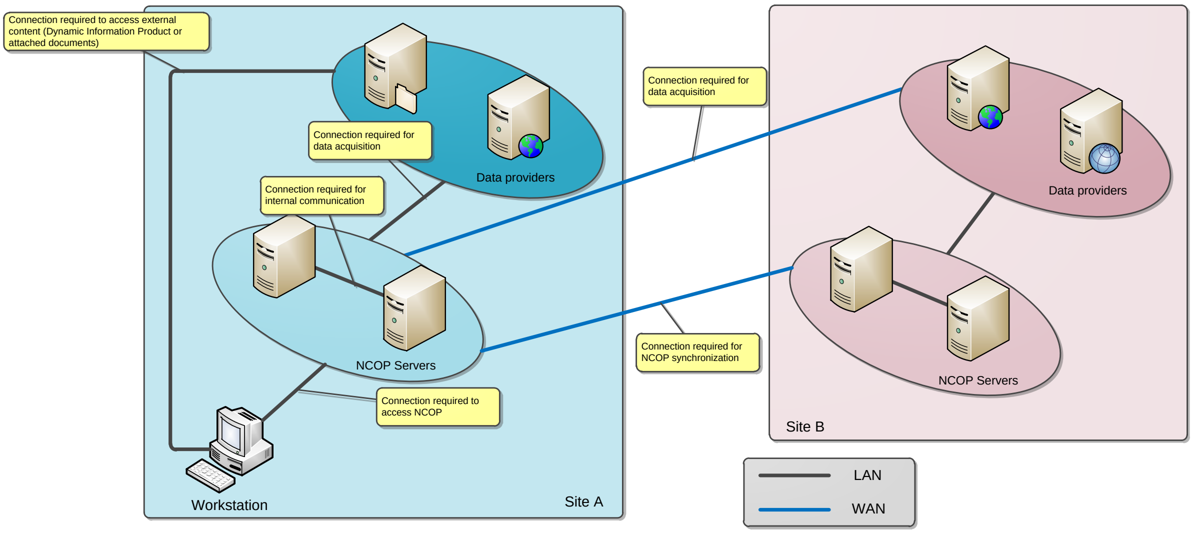

Connection required to access external content (Dynamic Information Product or attached documents)
Connection required for data acquisition
Data providers
Connection required for internal communication
NCOP Servers
Connection required to access NCOP
Workstation
Site A
Connection required for data acquisition
Data providers
Connection required for NCOP synchronization
NCOP Servers
Site B
LAN
WAN

Figure 5-169: LAN and WAN connectivity sample scenario

The following chapters describe the impact of a loss of network connectivity for LAN and WAN.

5.4.20.1.1 LAN connectivity failure

The impact of a network failure on NCOP depends on network failure location.

1. Network failure between workstations and NCOP servers:

If the network failure impacts the communication between workstations and NCOP hosting servers, it is considered as a major failure because in this case, NCOP users won’t be able to use the Geographical COP Editor to visualize the COP or manage it.

However, the acquisition mechanisms should still be running and sources and information products that have been configured should still be acquired.

2. Network failure between workstations and data providers or between hosting servers and data providers:

If the network failure impacts the communication between workstations and external servers or data providers, NCOP remains operational regarding COP management and COP consumption. However, in this case, dynamic information products, external documents lookup and map data based on external servers can’t be visualized.

3. Network failure between NCOP hosting servers:

If the network failure impacts the communication between NCOP hosting servers, NCOP is simply unusable. If BizTalk Server cannot reach SQL Server, information products cannot be acquired. Also, if SharePoint cannot reach its SQL database, the portal is unusable and it is impossible to connect to it or get information from it, which forbids the COP management or COP consumption activities.

4. Network failure between NCOP hosting servers and external servers:

If the network failure impacts the communication between NCOP hosting servers and external servers, data providers are unreachable and Information Products cannot be acquired. In this case, users are still able to use NCOP and visualize COPs and associated Information Products: last versions of data-driven Information Products are still available because they have been stored in the NCOP Storage. If data providers are unreachable and Information Products cannot be acquired, authorized users will receive alerts/notifications indicating it. Also, because the Information Products cannot be acquired, the associated status will be updated according to status rules that have been defined by the COP Manager. COP Users will then be aware that the Information Products they are viewing are fresh and reliable or not.

5.4.20.1.2 WAN connectivity failure

If the network failure impacts the WAN connectivity for an NCOP node, the NCOP functionalities remain operational from within the node. However it has an impact on the following:

- NCOP Synchronization between nodes is not working which mainly means that a client node won’t receive updates from source nodes.
- External data providers are unreachable which will cause the raise of alerts indicating that information Products cannot be acquired. The Information Products status will also be updated accordingly.
- Dynamic Information Products and geographical data (background maps and layers) cannot be visualized by the COP Users.

5.4.20.2 NATO Infrastructure services unavailability

5.4.20.2.1 Active Directory unavailability

This service is critical because it is used by the authentication process of many services. It is used to authenticate the users but also the technical services accounts that are used by the COTS that are part of the NCOP solution.

If this service is not available, NCOP won’t be usable.

When this service is available again NCOP functionality will be available again

5.4.20.2.2 Identify Provider unavailability

This service is not critical for NCOP because it is used by the authentication process of external users (as a supplement to Active Directory). It is used to authenticate the external users but NOT the technical services accounts that are used by the COTS that are part of the NCOP solution.

If this service is not available, NCOP will be usable for Active Directory users.

When this service is available again external authenticated with SAML tokens will be available again

5.4.20.2.3 Informal Messaging service unavailability

This service is not critical for NCOP it is only used in the following contexts:

- Message based Information Products
- Alert/Notifications through e-mail

If the messaging service is not available, message based Information Products that have been declared won't be able to be acquired by NCOP. It will result in alerts being raised indicating a connectivity failure with the messaging system. The status of these Information Products will be updated according to the status rules that have been defined.

If the messaging service is not available, alerts/notification that have been configured to be sent by email to the subscribers won't be sent. Such alerts will be kept back and sent when the messaging service is available again.

5.4.20.2.4 CoreGIS service unavailability

The CoreGIS service is not critical for NCOP.

CoreGIS unavailability has an impact on the visualization of maps that have been configured to use this service.

Non geo-data Information Product can still be visualized by NCOP users.

Also, NCOP's GeoServer server and provided default maps can be considered as a fallback solution for the visualization of background maps.

5.4.20.2.5 Chat service unavailability

The Chat service is not critical for NCOP.

However, its unavailability has an impact on the following:

- XMPP based Information Products
- Alerts/Notifications through XMPP

If the Chat service is unavailable, Information Products that have been configured to use this service as a source won't be updated. It will results in alerts being raised indicating a connectivity failure and Information Products statuses will be updated according to the rules that have been defined by the COP Manager.

If the Chat service is unavailable, Alert/Notifications that have been configured to be sent using the NATO Chat service won't be sent. Such alerts will be kept back and sent when the messaging service is available again.

5.4.20.2.6 Enterprise Monitoring System unavailability

The NATO EMS service is not critical for NCOP because they are integrated with loose coupling. The unavailability of this service won't forbid the use of the NCOP end-user functionalities.

Local monitoring will still be available on the NCOP hosting servers and logs will be kept back on the servers for a later use when the EMS service is available again.

5.4.20.2.7 Document Handling System unavailability

This service is not critical for NCOP.

However, it can impact the following:

- Information Products based on DHS as a source
- Attached documents to a BSO

Regarding Information Products, Depending on if they have been configured as data driven or dynamic, the impact is not exactly the same.

If an Information Product has been configured to use DHS as a source dynamically, it will result in the impossibility for COP Users to access and visualize these Information Products.

If an Information Product has been configured in a data-driven mode, COP Users will be able to access it and visualize it if it has been previously acquired and therefore stored in the NCOP Storage. If DHS is temporarily unavailable, the acquisition of such Information Product will fail and result in alerts being raised indicating a connectivity failure and Information Products statuses will be updated according to the rules that have been defined by the COP Manager.

Regarding attached documents to a BSO, they are described as links in the BSO properties. Therefore, in this case, the unavailability of DHS will result in the impossibility to access and visualize these attached documents. COP Users will still be able to visualize the Information Products and associated BSOs.

5.4.20.2.8 NPKI service unavailability

This service is not critical for NCOP.

NPKI is the service that acts as a certificate authority allowed to:

- Provide and publish certificates
- Maintain and publish the Certificate Revocation List (CRL)

The unavailability of this service can impact NCOP in different ways:

If the NPKI is unavailable during the NCOP installation process, the certificates needed for NCOP cannot be provided. It won't forbid the installation of NCOP but will require some adaptations:

- Deactivation of the data signing process for incoming and outgoing information products (see chapter 5.4.1.4 for more details)

Both of these features can be activated later when the NPKI is available again and the certificates are provided.

Once NCOP has been installed with appropriate certificates provided, the unavailability of NPKI will result in the expiration or unavailability of the CRL and the impossibility to check the validity of certificates. It mainly has an impact on the connection to secured sources such as https web sites.

For NCOP certificates management, the target service that will be used is NPKI. However, the Interim-NPKI currently available in the MS/NS environment should be sufficient for to support NCOP requirements.

5.4.20.2.9 NEDS

The NATO Enterprise Directory Service is not critical for NCOP.

It is mainly used as a repository which contains useful information on external systems and FAS to allow a COP Manager to create Sources and Information Products. But if this service is unavailable, Sources and Information Products can still be created manually.

This repository is also used by NCOP to describe and expose its services so they can be used by external consumers. The information related to NCOP services (location and description) can be provided using another method.

5.4.20.3 NCOP Services unavailability

5.4.20.3.1 SQL Server unavailability

SQL Server is a critical resource for NCOP because this service is required by BizTalk and SharePoint. If this service is not available, it will result in the impossibility for users to use NCOP and for data to be acquired.

Only the background maps exposed by NCOP's own GeoServer server and the Geographical COP Editor (disconnected from back-end) will remain available.

5.4.20.3.2 BizTalk Server unavailability

BizTalk is a key and critical element in the NCOP architecture. Its unavailability will impact the acquisition process of NCOP but will not forbid the consumption of NCOP. Regarding COP Management, it is not possible to create new Sources or Information Products when BizTalk is unavailable. Also user Information Product contribution is not possible in this case.

When BizTalk server is unavailable, COP Users will still be able to visualize COPs and associated Information Products. The failure of the acquisition process will result in the Information Products status being degraded because the data is not updated.

5.4.20.3.3 SharePoint server unavailability

SharePoint is a key element in the NCOP architecture. Its unavailability has a major impact on NCOP functionalities. The acquisition process handled by BizTalk will fail because Information Products cannot be published in the NCOP Storage. Also the COPs and Information Products cannot be accessed and visualize by users or external system because the NCOP storage where the Information Elements are stored is not accessible.

5.4.20.3.4 Application server unavailability

Application server is a key element in the NCOP architecture. Its unavailability has a major impact on NCOP functionalities. The Geographicail COP Editor cannot be accessed and visualize by users.

5.4.20.3.5 GeoServer Server unavailability

The GeoServer server is not critical for NCOP.

If the GeoServer server provided as part of the NCOP solution is unavailable, users won’t be able to use the default maps provided by NCOP. The Geographical COP Editor can be configured to use CoreGIS instead.

If the GeoServer server is unavailable, COP management functions remain available. COPs and Information Products remain accessible for the COP Users.

5.4.21 NCOP authentication strategy

NCOP requires authentication at the following levels:

- HTTP access
- SQL access
- File system access

5.4.21.1 HTTP access

HTTP access is used by the end users to access NCOP (NCOP Portal, Geographical COP Editor and Web services). It is also used internally by the NCOP components to communicate using Web services.

Windows authentication is activated on all NCOP sensitive web sites hosted in IIS. What are meant by sensitive web sites are all web sites that expose data and web sites that host web services that have read and write permissions to NCOP data.

The privileged authentication method for HTTP access is Kerberos. However in some configurations NTLM authentication could be required. NTLM authentication is required in the case where the client doesn’t have sufficient connectivity (network or DNS) to reach the KDC (Key Distribution Center).

The HTTP Negotiate extension is used to convey authentication tokens (Kerberos or NTLM).

5.4.21.1.1 NCOP components authentication

NCOP components use the HTTP access in the following contexts:

- Within an NCOP node to communicate with other NCOP components through Web services,
- Across NCOP nodes when COP synchronization is configured and running.

Within an NCOP node, because NCOP uses service oriented architecture, components communicate through web services. Each component is run using a dedicated Windows account. This account is used for authentication of HTTP requests using Kerberos.

When COP synchronization is configured and running, some NCOP components must authenticate when they invoke a web service on a remote node. Depending on the network configuration and Active Directory topology, Kerberos or NTLM authentication can be used. Authentication in NCOP synchronization contexts is more detailed in the chapter 6.2.1.

5.4.21.1.2 End-user authentication

End-user can use Kerberos or NTLM as an authentication method depending on how NCOP is accessed, from a network point of view. Kerberos is the privileged method but NTLM is necessary if the user cannot obtain Kerberos tickets (KDC unreachable for example).

When a user accesses NCOP he must use credentials that can be validated against the Active Directory domain in which the NCOP hosting servers have been registered. When accessing a remote node, a local credential can be used if the NCOP is in the same AD domain or in a different domain with a trust relationship with the user’s Windows domain.

5.4.21.2 SQL access

SQL access is used only internally for NCOP COTS and services to access their data. Authentication for SQL access is performed using Windows authentication (Kerberos or NTLM). SQL accesses are made by the technical service accounts that are used to run the COTS (BizTalk and SharePoint) and NCOP Web Services. This avoids having logins and passwords written in configuration files.

5.4.21.3 File system access

File system access is required by all NCOP COTS and services for temporary persistence and logs persistence. File system is only accessed by the technical service accounts that are used to run the COTS and services.

5.4.21.4 Authentication delegation requirements

Since NCOP uses Windows credentials for user authentication and implements a Service-Oriented Architecture, some actions require the usage of delegation in order to use the user's authentication token throughout the chain of services call.

In accordance to NATO recommendations regarding Kerberos delegation, NCOP installation documentation describes how to configure the minimal and sufficient settings to activate Kerberos delegation for NCOP. The following principles are applied:

- Only constrained delegation is used,
- Only standard Microsoft settings are used.

Delegation is required in NCOP for two specific purposes:

- When NCOP users are accessing SharePoint through business web services from the Geographical COP Editor,
- When BizTalk needs to provide credentials to be used when accessing the Intel-FS source.

The following figure presents the usage of Kerberos delegation when NCOP users access SharePoint data from the Geographical Editor. The propagation of user credentials is required to allow traceability of user actions as well as authorization and verification of access rights to NCOP Information Elements:

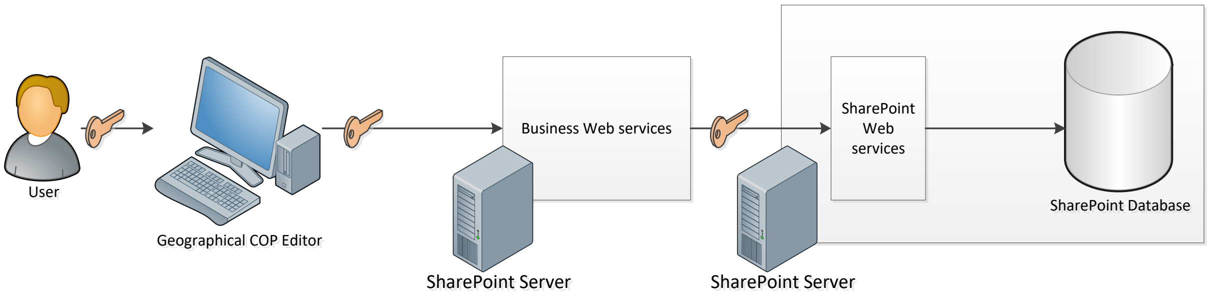


Figure 5-170: Kerberos delegation usage for NCOP users access from the Geographical COP Editor

In order to enable delegation for this purpose, the technical service account used to run business services application pool in IIS has to be configured to allow delegation towards SPNs associated with SharePoint web services. For this technical service account, the delegation must allow authentication protocol transitioning because users can authenticate to NCOP using not only Kerberos but also NTLM is some cases (see chapter 5.4.21.1.2).

Regarding delegation required for BizTalk when accessing the Intel-FS source, the following figure presents the components involved when BizTalk needs to authenticate when accessing the Intel-FS server:

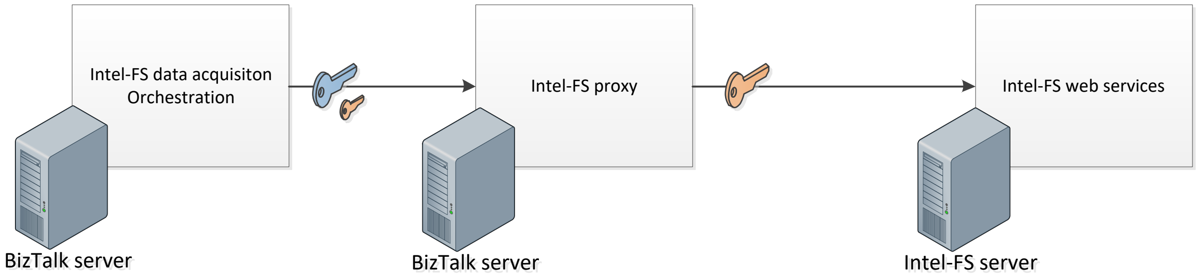


Figure 5-171: Kerberos delegation usage for BizTalk access to Intel-FS source

In this case, the BizTalk orchestration initiates a connection to an internal Intel-FS proxy. This connection is authenticated using Kerberos and uses a particular binding that allow the transmission of additional credentials that will be reused by the proxy. In the end, the Intel-FS proxy will use these credentials to connect to the Intel-FS web service. To enable this behaviour, the technical service account used to run BizTalk host instances must be configured to allow delegation towards BizTalk SPNs. This delegation does not require protocol transitioning and can be set to ‘Use Kerberos only’. Also, the connection between the data acquisition Orchestration and the Intel-FS proxy is done using the loopback network (localhost) to ensure that no sensitive data is sent over the network.

Regarding delegation required for BizTalk when accessing the AirC2IS source, the following figure presents the components involved when BizTalk needs to authenticate when accessing the AirC2IS server:

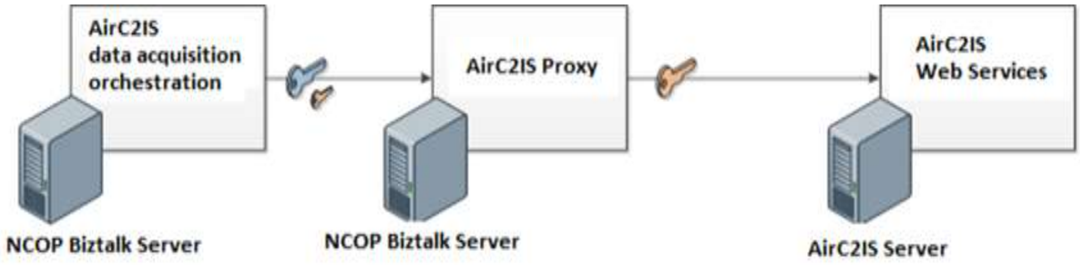


Figure 5-172: Kerberos delegation usage for BizTalk access to AirC2IS source

In this case, the BizTalk orchestration initiates a connection to an internal AirC2IS proxy. This connection is authenticated using Kerberos and transmit the "source code". In the end, the AirC2IS proxy will get the credentials to connect to the AirC2IS web services using the "source code". Also, the connection between the data acquisition Orchestration and the AirC2IS proxy is done using the loopback network (localhost) to ensure that no sensitive data is sent over the network.

5.4.22 IT Modernization

The key assumptions of IT Modernization:

- 2 Data Centres will replace the current IT infrastructures of the HQ
    - Mons
    - Lago Patria
- Mons Data Centre is normally active and is providing a virtualized environment for the FAS. Lago Patria Data Centre is used as back-up by using VM replication.

The IT Modernization will have the following main impacts on NCOP application:

- For the 2 Data Centres, only one NCOP Increment-2 node is installed instead of one NCOP node per HQ in NCOP Increment-1
- ITM will use a single NCOP Operational portal URL (instead of one per HQ in NCOP Increment-1)
- NCOP SharePoint server is split into:
    - SharePoint Web Front End server. NCOP SharePoint solutions (.wsp) will be deployed on it but no installation package will be deployed on it
    - NCOP Application server. The “NCOP Web application” installation package will be deployed on it to install the Geographical COP Editor, The Globe View, the NCOP Web services …
- NCOP Increment-2 can be based on several SharePoint Web Front End servers and several NCOP Application servers
- NCOP Increment-2 can be installed on a NCOP dedicated SharePoint farm (as in NCOP Increment-1) or on an existing SharePoint farm shared by several systems and hosted on ITM infrastructure.

At least two scenarios were initially identified. Only one scenario is still relevant:

- As illustrated Figure 5-173:

- Active NCOP Application servers are only hosted on the first Data Centre. The second Data Centre hosts replicated “NCOP Application servers” virtual machines (they are passive and represented by yellow colour in the following Figure). In case of unavailability of the first Data Centre, the passive “NCOP Application servers” will become active (replacing the servers hosted on first Data Centre)
- Active SharePoint servers are only hosted on the first Data Centre. The second Data Centre hosts replicated “SharePoint servers” virtual machines (they are passive and represented by yellow colour in the following Figure). In case of unavailability of the first Data Centre, the passive “SharePoint servers” will become active (replacing the servers hosted on first Data Centre)
- Active NCOP BizTalk servers (2 max) are only hosted on the first Data Centre. The second Data Centre hosts replicated “NCOP BizTalk servers” virtual machines (they are passive and represented by yellow colour in the following Figure). In case of unavailability of the first Data Centre, the passive “NCOP BizTalk servers” will become active (replacing the servers hosted on first Data Centre)
- Active NCOP SQL servers (2 max) are only hosted on the first Data Centre. The second Data Centre hosts replicated “NCOP SQL servers” virtual machines (they are passive and represented by yellow colour in the following Figure). In case of unavailability of the first Data Centre, the passive “NCOP SQL servers” will become active (replacing the servers hosted on first Data Centre)

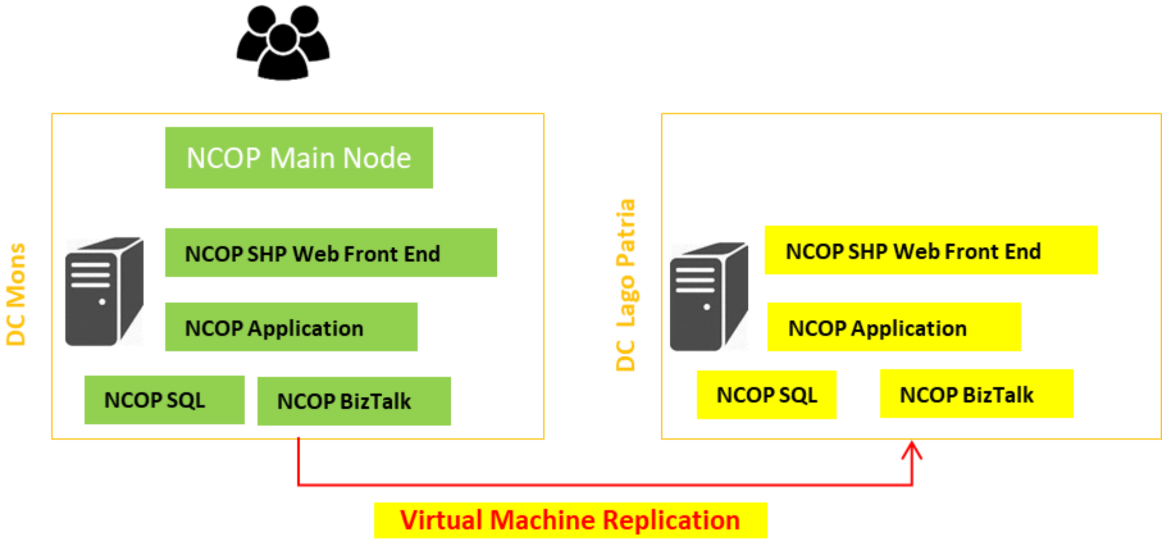


Figure 5-173: NCOP deployment on ITM: (only NCOP Servers in Mons DC are active)

In synthesis, the replication is based on an active / passive mechanism with cold recovery in case of first DC unavailability. Data Centre: NCOP VM shall be installed only on the active Data Centre.

5.4.23 Mutualization of servers (SQL and SharePoint)

NCOP Increment-2 application can use a dedicated SQL server (as currently done in Increment-1) or use a “mutualized” SQL server.

The “mutualized” SQL server is shared by several systems (DHS, LC2IS …). NCOP application uses dedicated SQL instances (and not the default SQL instance) to avoid contradictory needs between systems sharing the same SQL server:

- NCOP-CMN for NCOP Common applications and services
- NCOP-BIZ for NCOP BizTalk applications and services
- NCOP-SHP for NCOP SharePoint web applications and services
- NCOP-HIS for NCOP History applications and services

NCOP Increment-2 application can use a dedicated SharePoint server (as currently done in Increment-1) or use a “mutualized” SharePoint server.

The “mutualized” SharePoint server is shared by several systems (DHS, LC2IS …). In that case, a single SharePoint farm will be used but NCOP will continue to use its own 3 SharePoint Web Applications (Operational, Training and Exercise). SharePoint server and SharePoint farm can be shared but not the NCOP SharePoint Web Applications.

Limitations

For NCOP, the SharePoint Web Applications relies on Kerberos authentication or SAML and not on NTLM authentication.

5.4.24 NLB hardware for High Availability Node

In NCOP Increment-1, the High Availability NCOP Node was installed and based on Microsoft software NLB.

In NCOP Increment-2, the High Availability NCOP Node will be based on PulseSecure Traffic Manager software (preferred) or Microsoft software NLB .

5.4.25 Distributed COP Maintenance

In NCOP Increment-1, the maintenance of a COP (and COP Structure) by multiple COP Managers at the same time is not allowed. A save conflict error occurs when multiple “Save” actions are performed simultaneously (Only the first “Save” is completed).

NCOP Increment-2 will allow:

- Concurrent editing of a COP in the same NCOP node
- Concurrent editing of a COP synchronized between 2 NCOP nodes

The COP Edition Information Panel will be notified when a COP is updated by another COP Manager from another workstation. The Event managing system of NCOP Increment-1 currently used, for example, to update the COP Explorer Information Panel (see §5.3.1.1.8) will be reused to update the COP Edition Information Panel. In case of conflict (same COP Structure element modified by several COP Managers) a “Resolve Conflict” Information Panel will be displayed to keep or discard the conflicting changes.

5.4.26 Triton C4ISR-Viz Reusable Software

When available, the Triton C4ISR-Viz Reusable Software will replace the TIMS Web Client (HTML 5 TIMS.js) Subordinate Configuration Item.

The interface between the NCOP HMI and the Triton C4ISR-Viz Reusable Software will be based on the NATO-specific CMAPI: NATO Map Application Programming Interface (NMAPI). This NMAPI interface is an extension of the Common Map Application Programming Interface 1.3.0 (CMAPI) [C4ISR-VIZ].

The migration of HTML 5 TIMS.js to Triton C4ISR-Viz Reusable Software will be facilitated due to NMAPI interface already defined in the TIMS Web Client.

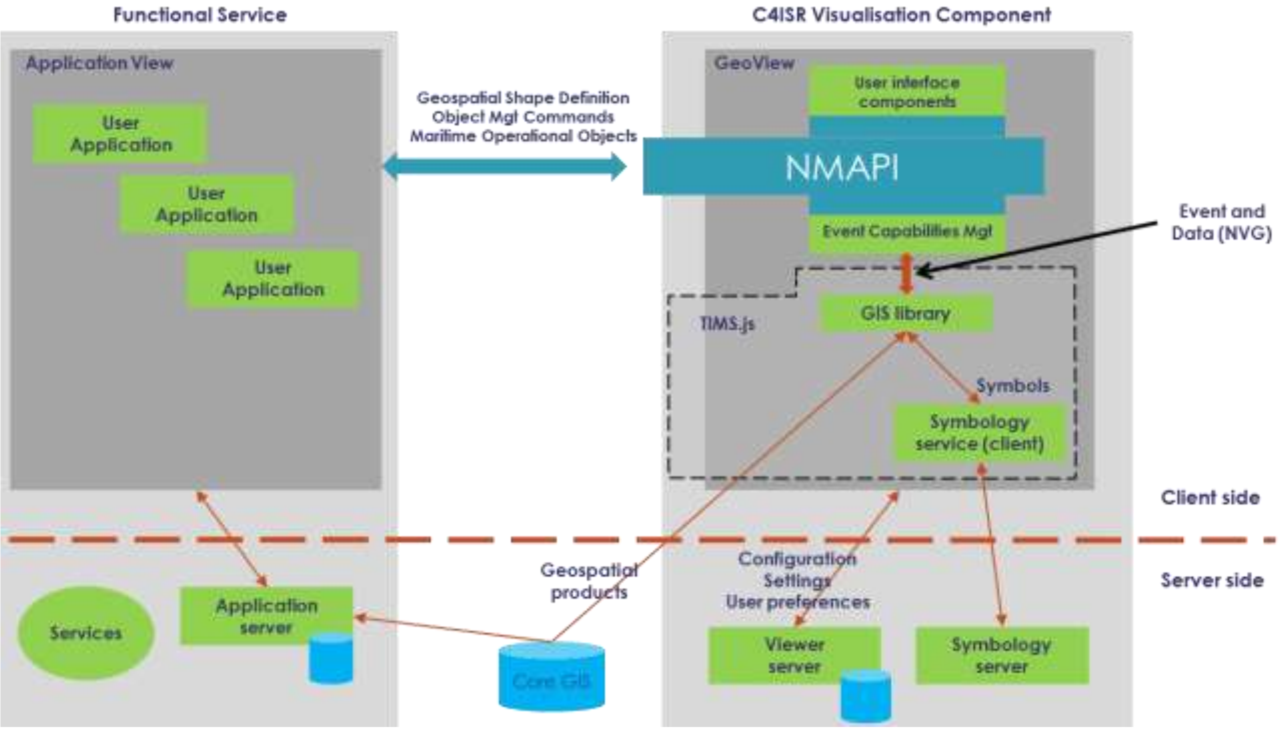


Figure 5-174: NMAPI interface in HTML 5 TIMS.js

The detailed integration of the C4ISR-Viz in NCOP will be described at a later stage.

6 DETAILED DESIGN

6.1 SAMPLE UML DIAGRAMS

6.1.1 Sequence diagrams

The following sequence diagram shows the interactions between SA when executing the “Manage Roles” Use Case. Although not shown on the diagram, the SA belong to the IC identified in the High level detail for the same Use Case.

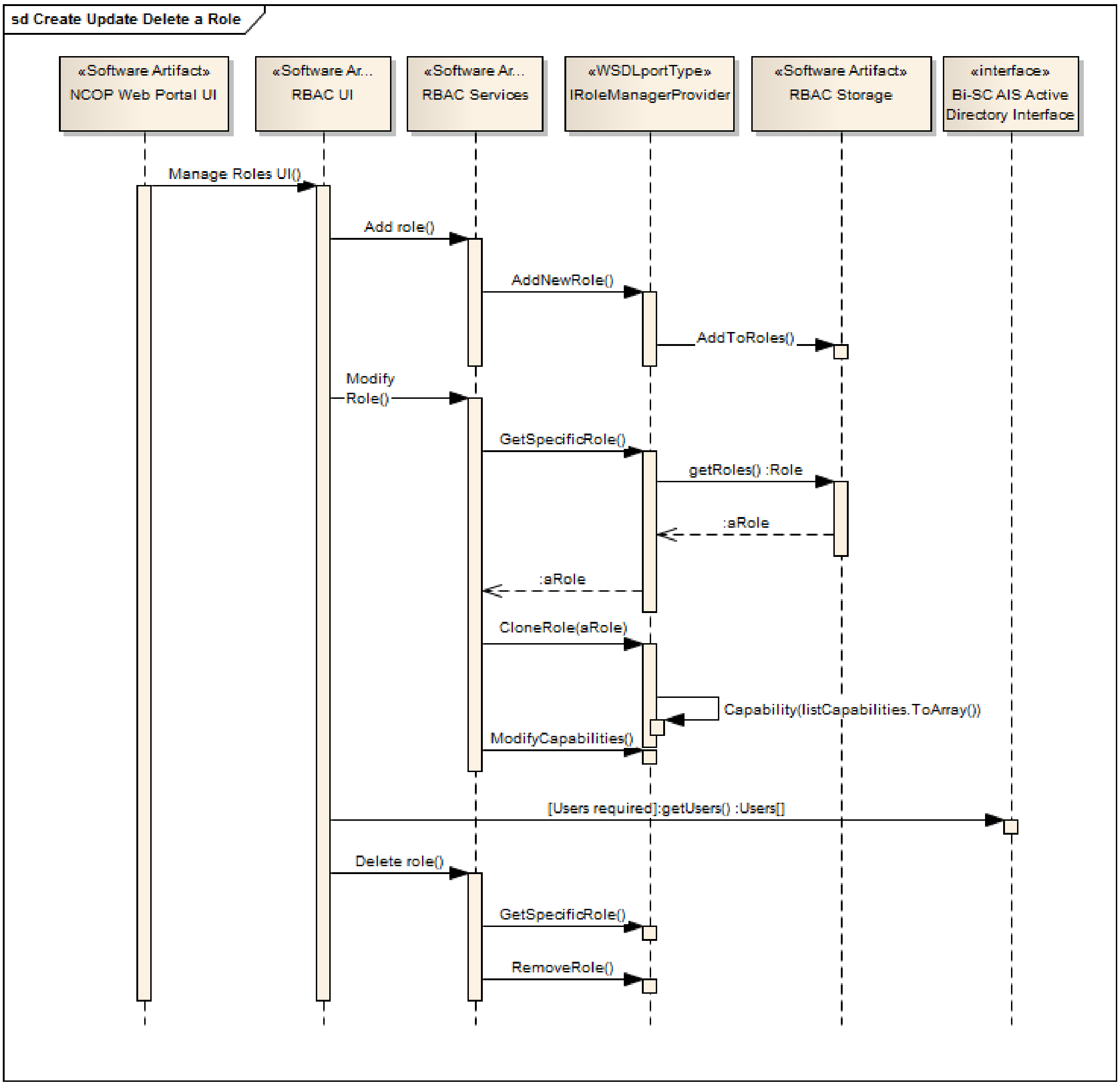

sd Create Update Delete a Role
«Software Artifact» NCOP Web Portal UI
«Software Ar... RBAC UI
«Software Ar... RBAC Services
«WSDLportType» IRoleManagerProvider
«Software Artifact» RBAC Storage
«interface» Bi-SC AIS Active Directory Interface
Manage Roles UI()
Add role()
AddNewRole()
AddToRoles()
Modify Role()
GetSpecificRole()
getRoles() :Role
:aRole
:aRole
CloneRole(aRole)
Capability(listCapabilities.ToArray())
ModifyCapabilities()
[Users required]:getUsers() :Users[]
Delete role()
GetSpecificRole()
RemoveRole()

Figure 6-1: Detailed sequence diagram for the “Manage Roles” Use Case

A logical model view of the storage is presented in the annex B.12

6.2 DETAILED DESIGN TOPICS

6.2.1 Synchronization

This section is related to the §5.3.3.4.1 Node Synchronisation Implementation Component.

6.2.1.1 Implementation details

6.2.1.1.1 Initialization phase

When an NCOP node subscribes to a COP or an Information Product on a remote node, the client node will receive initialization package that contains the current state of the item that is being subscribed to. Therefore if that node has subscribed to a specific COP, it will receive a package containing the current COP definition (metadata, structure, dissemination settings, etc.), the associated Information Products (configuration and CDF data, including data history and original data), metadata of sources associated with the information products, SharedViews, Annotations, etc.

This package is provided through a Web Service using Zip compression to minimize the size of the package and optimize the data exchange.

When the package is received by the client Node, all items contained are being recreated in the NCOP storage component. However, in this case, the creation of Sources and Information Products won't provoke the instantiation of BizTalk connectors and orchestration on this client Node. Indeed, the source that has been declared and used on the remote node is not necessarily reachable on the client node, and even if it was reachable, it would provoke multiple acquisition of the same data that would result in conflicts because the Information Product would be updated by the synchronization process from the remote node and by the local acquisition process that would be running because a source has been instantiated.

The goal of this initialization is to obtain quickly the same objects on the nodes that are being synchronized without having to replay all individual events that have to the actual version of the COP and its related items.

6.2.1.1.2 Event-driven processing

Once the client node has been initialized with the latest version of each subscribed items, the event-driven process is set up and the client is notified whenever an item related to the COP or Information Product it has subscribed to is changed on the source node.

The event-driven processing works as follows:

1. When an item is modified on an NCOP node, an event is triggered in the Event Manager component (cf. chapter 5.3.3.2.1)
2. This event is propagated to the synchronization manager and recorded as a synchronization event in the synchronization database.

Note: A synchronization event only contains the type of event (creation/update/deletion), the type of item (COP, Information Product, Shared View, etc.) and reference (unique identifier) of the item.

3. Then the synchronization broker service
    a. analyses all incoming synchronization event,
    b. identifies the associated COPs or Information products,
    c. obtains the data from the NCOP storage
    d. Identify the target nodes according to subscriptions
    e. Verify that the target node is authorized to receive the data according to its security classification and dissemination settings that have been defined
    f. creates one broker messages for each node that match the subscriptions and authorization criteria
4. The synchronization SyncManagement service will then:
    a. process the broker messages,
    b. Send the data to the subscribed node by invoking the synchronization client service on this remote client node.

In order to handle connectivity loss between two nodes, all synchronization events and broker messages are kept and can be replayed later.

6.2.1.1.3 Data exchange protocol

All data sent from one node to another is sent by using HTTP SOAP (default) or RestFull HTTP GET (if configured for the remote node) Web Services.

During the initialization phase, the SOAP request is described in XML but contains a Base-64 encoded element representing a Zip file that contains multiple XML files. Each XML file represents a synchronized item (COP, Shared view, etc.) with all its properties

When the event-driven mechanism is in place (after the initialization phase), each SOAP (resp. GET) request contains an individual XML (resp. JSON) document that describes the item that is being synchronized.

The following figure summarizes these behaviours:

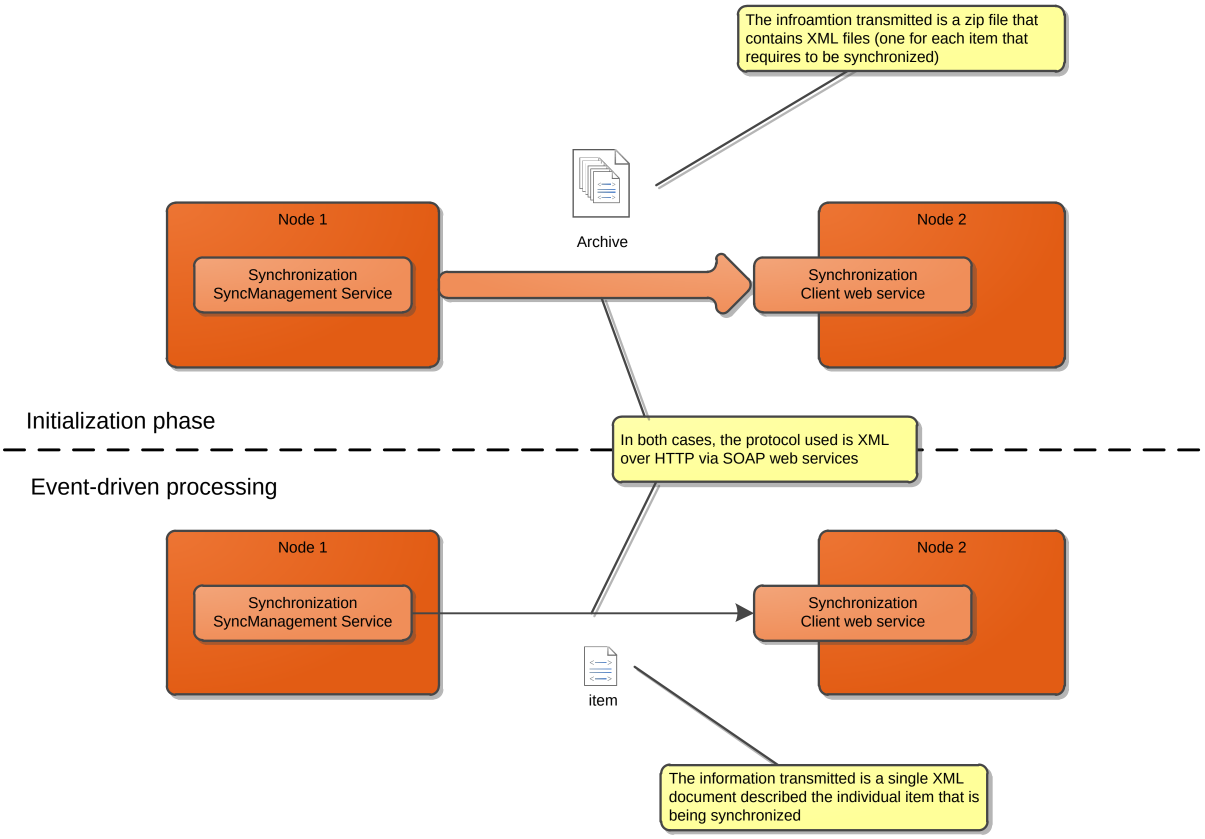

The infroamtion transmitted is a zip file that contains XML files (one for each item that requires to be synchronized)
Node 1
Synchronization SyncManagement Service
Archive
Node 2
Synchronization Client web service
Initialization phase
In both cases, the protocol used is XML over HTTP via SOAP web services
Event-driven processing
Node 1
Synchronization SyncManagement Service
Node 2
Synchronization Client web service
item
The information transmitted is a single XML document described the individual item that is being synchronized

Figure 6-2: Synchronization data exchange protocol

6.2.1.1.4 Mono-directional synchronization

NCOP supports mono-directional synchronisation where only one NCOP node is able to initiate any connection to the other nodes because of network settings. It is the case when NCOP nodes are in different security domains but no IEG is available. In this case, the IEG may be replaced by a firewall with specific settings and rules.

When mono-directional synchronization is used, the data is not pushed automatically by the source node, but periodically requested by the target node; the synchronization is then in ‘pull’ mode. The synchronization is event-driven and based on web services but in this case:

- events are kept on the source node until the client node requests the updates,
- data exchange pattern is ‘request/response’ instead of ‘publish/subscribe’,
- Information Elements are not sent one by one but several at a time in order to minimize the amount of requests.

The usage of this pull mode is declared when defining partner nodes and the ‘pull’ interval can be set per subscription. The following figure presents the two phases of the synchronisation process when using the mono-directional synchronization:

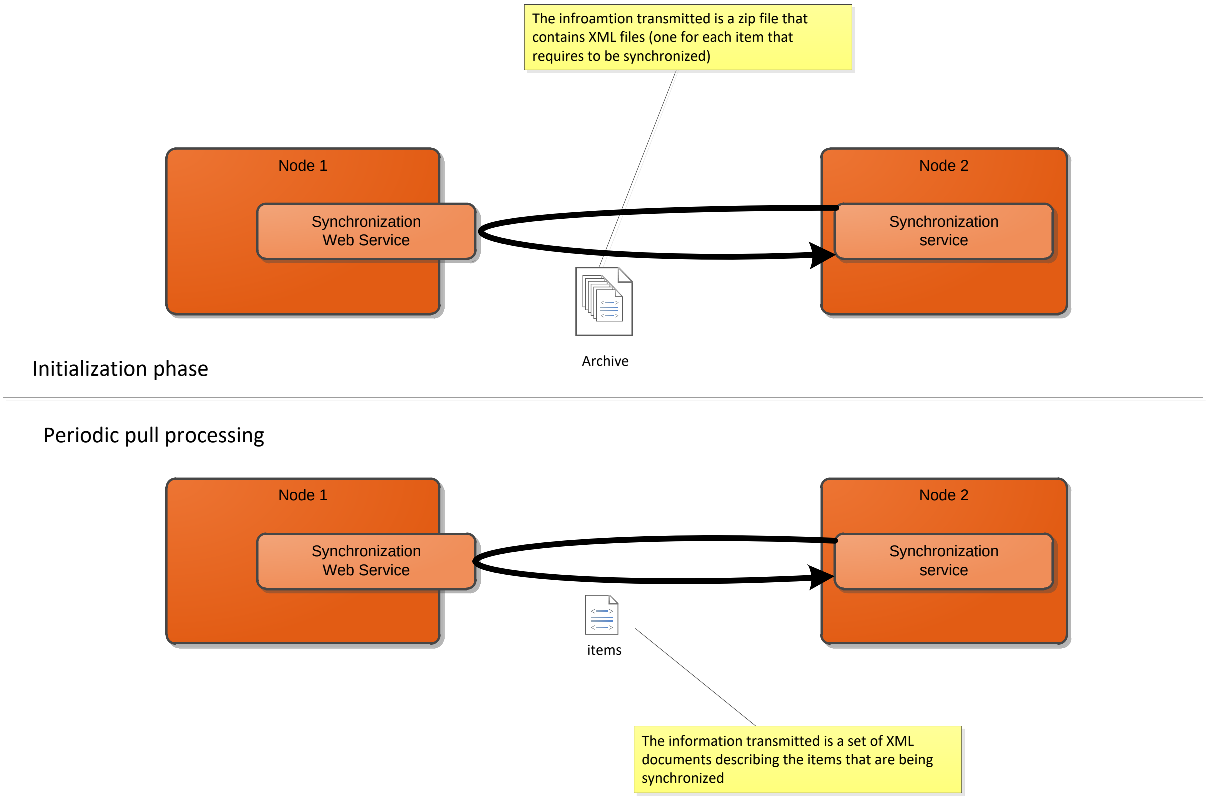

The infroamtion transmitted is a zip file that contains XML files (one for each item that requires to be synchronized)
Node 1
Synchronization Web Service
Node 2
Synchronization service
Archive
Initialization phase
Periodic pull processing
Node 1
Synchronization Web Service
Node 2
Synchronization service
items
The information transmitted is a set of XML documents describing the items that are being synchronized

Figure 6-3: Synchronization data exchange protocol when using mono-directional synchronization

6.2.1.2 Authentication across nodes

Authentication is required when node communicates with another during the synchronization process. The following scenarios have been taken into account:

Both nodes are registered in the same AD domain or forest.

Nodes are registered in separated AD domains with no trust relationship.

In order to handle these configurations, NCOP proposes a way to:

- Securely store the credentials to be used to invoke a remote synchronization service,
- Select the appropriate authentication method: Kerberos or NTLM.

Regarding credentials, NCOP proposes a Web user interface that can be used to declare and store credentials to be used in the synchronization: for each external node that is declared on an NCOP node, the credentials to be used when the synchronization web service are being invoked must be selected from the secure store. These credentials must be valid in the context of the target node.

The storage of synchronisation credentials is based on the native SharePoint credentials storage. A certificate is required to encrypt the credentials in this storage.

In order to secure the synchronization client service, access restrictions can be explicitly declared at the Web site level to allow only identified users to use the synchronization client web service. The authorized users must be those that are being used by the SyncManagement service to connect to remote client web services.

The following figure presents how credentials are used to access the Synchronization client web service:

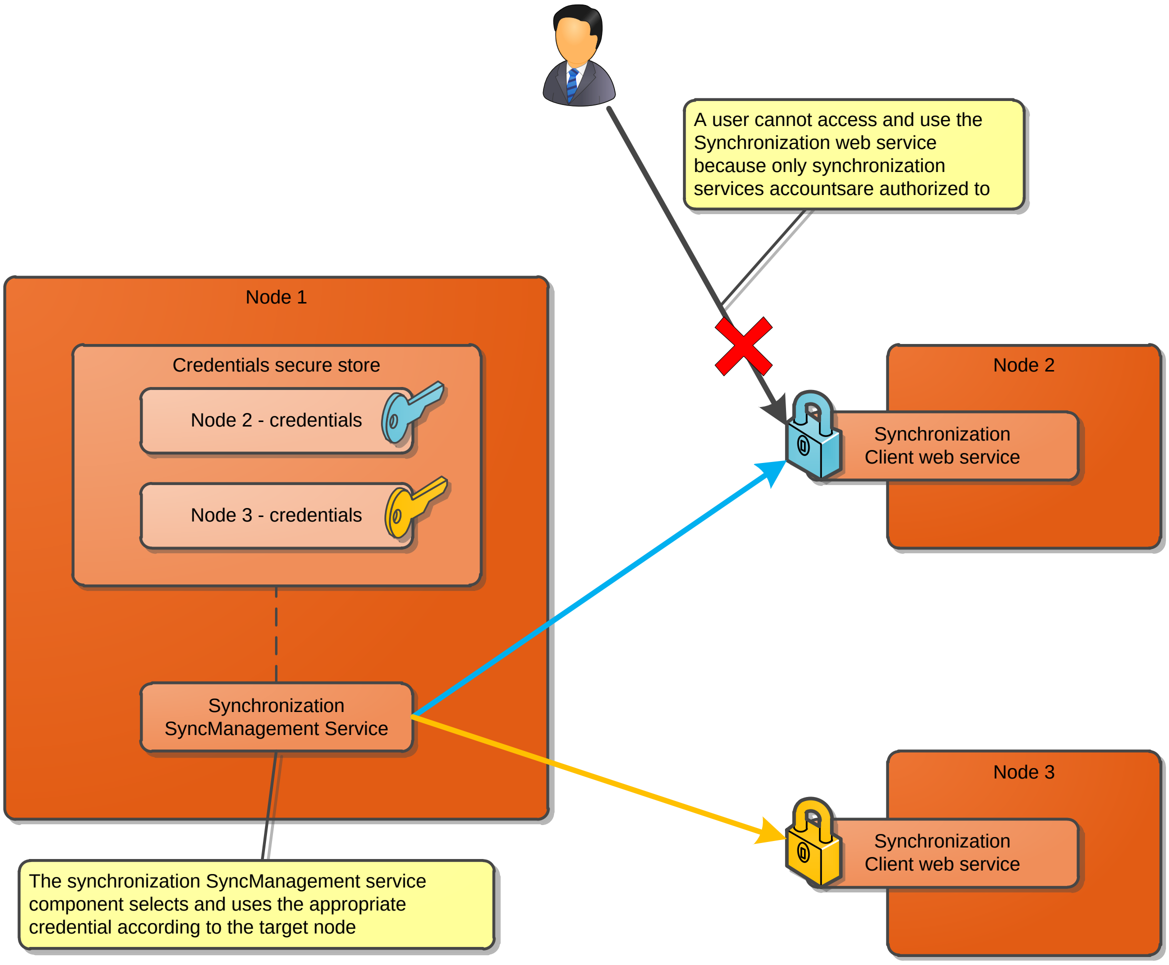

A user cannot access and use the Synchronization web service because only synchronization services accountsare authorized to
Node 1
Credentials secure store
Node 2 - credentials
Node 3 - credentials
Synchronization SyncManagement Service
Node 2
Synchronization Client web service
Node 3
Synchronization Client web service
The synchronization SyncManagement service component selects and uses the appropriate credential according to the target node

Figure 6-4: Synchronization security implementation

With the implementation of ADFS and claims-based authentication, the local storage of credentials to access a remote node will not be required. NCOP ADFS implementation is planned for NCOP Increment-2 and will be described in a later release of this document.

In addition to these authenticated Web services, anonymous applications are installed for cross-nodes dialogs through IEG-C/XML-GUARD that do not support HTTP 1.1 Challenge/Response dialogs (401 HTTP Response rejected). For a given node, these installed anonymous web applications can be stopped (to be inaccessible) when no IEGC will be ever used to access this node.

6.2.1.3 Synchronization failure management

6.2.1.3.1 Connectivity issues

Because permanent connectivity between synchronized nodes cannot be guaranteed, NCOP synchronization mechanism uses a local database to store the broker messages that are produced to be sent to client nodes. The messages are stored using a queue mechanism, with on queue for each target node. If a message cannot be sent to a client node (network or authentication failure for example), the message returns in the queue and the synchronization SyncManagement service will try to send it again later.

6.2.1.3.2 Synchronization conflicts

In order to manage synchronization conflicts that can happen in complex scenarios where multiple nodes are involved, NCOP uses a revision attribute for each item that can be synchronized (COP, Shared view,, Annotation, etc.)

The revision attribute value is made of the following:

- Owner node

  Identifier of the node on which the object has been created,

- Previous nodes

  List of identifiers of the nodes through which the item has passed during previous synchronization steps. This is required to avoid sending the same item to a node that has already received it from another node.

- Version number

  Value based on the native SharePoint version number

- Modification date time (UTC)

When an item is received, the local item will be updated in the following cases:

- If the object doesn't exist in the local NCOP storage
- If the incoming version number and modification dates are greater than the local one for this item.

NCOP uses the following policies to identify and manage conflicts when a synchronized item arrives on a client node:

- If the incoming item has the same version number and modification date as the corresponding item in the local NCOP storage, then the incoming item is discarded.
- If the incoming item has a version number that is greater than the version number of the corresponding item in the local NCOP storage then:

    - The local item is updated if the client node has subscribed in read only mode (the source node item version always prevails in this case)
    - The local item is not updated if the client node has subscribed in read/write mode (in this case, the client node also acts as a source node and the version of this item will be sent to other client nodes)
- If the local item version number is lower than the received item version number and the local modification date is greater than the received modification date then the local item won't be updated and an NCOP alert is raised (Synchronization conflict)

6.2.1.3.3 Failure recovery

If a node needs to be resynchronized because it has been disconnected for a long time, NCOP offers the capability to enforce synchronization. This option is available per subscription and the re-synchronization mechanism is based on the same initialization described in the chapter above: Instead of sending all missed individual synchronization message, the client node will receive a zip package containing all required data. The client node will then replace its local content with the contents received from the source node.

6.2.2 Security classification handling of incoming Information Product

This section is related to the §5.3.3.2.4 Security Classification Manager and Cross Domain Manager Implementation Component.

6.2.2.1 Principles

Regarding the security classification of Information Products, the behaviour of NCOP is based on the following rules:

- A security classification must be normalized before being stored in the NCOP storage
- An Information product cannot be stored in the NCOP storage if the security classification normalization step fails
- If the security classification of an Information Product has been enforced by a COP Manager, this enforced classification will prevail compared to the incoming security classification
- The NCOP storage component always stores both incoming and normalized security classification for an Information Product

6.2.2.2 Security classification normalization

Security classification normalization is a step that is run during the acquisition phase: all incoming Information Products are analyzed and the associated security classification is extracted.

Because information products come from many external systems, it is not guaranteed that the security classification of all incoming Information Products be homogeneous, in terms of data structure and values.

Regarding the data structure, depending on their format, some Information Products can present their security classification in one simple text value or in a structured data set with multiple text values by separating the security policy, identifier and category.

Regarding the values, each system may have its own dictionary for security classifications. Therefore, NCOP can receive incoming Information Product security classifications with different values that could have in fact the same meaning.

In order to be able to publish COP Information Products with consistent security classifications, NCOP must normalize all incoming security classification using its own security classification repository.

To handle the heterogeneity of incoming security classifications, each NCOP security classification is enhanced with a set of aliases to define alternate values for the same security classification.

For example, the NATO SECRET security classification can be defined as follows in NCOP:

- Policy: NATO
- Identifier: SECRET
- Category/Caveats: *none*
- Aliases: NATO SECRET, NS, NATO - SECRET

The list of aliases for each security classification can be updated as required by an authorized user.

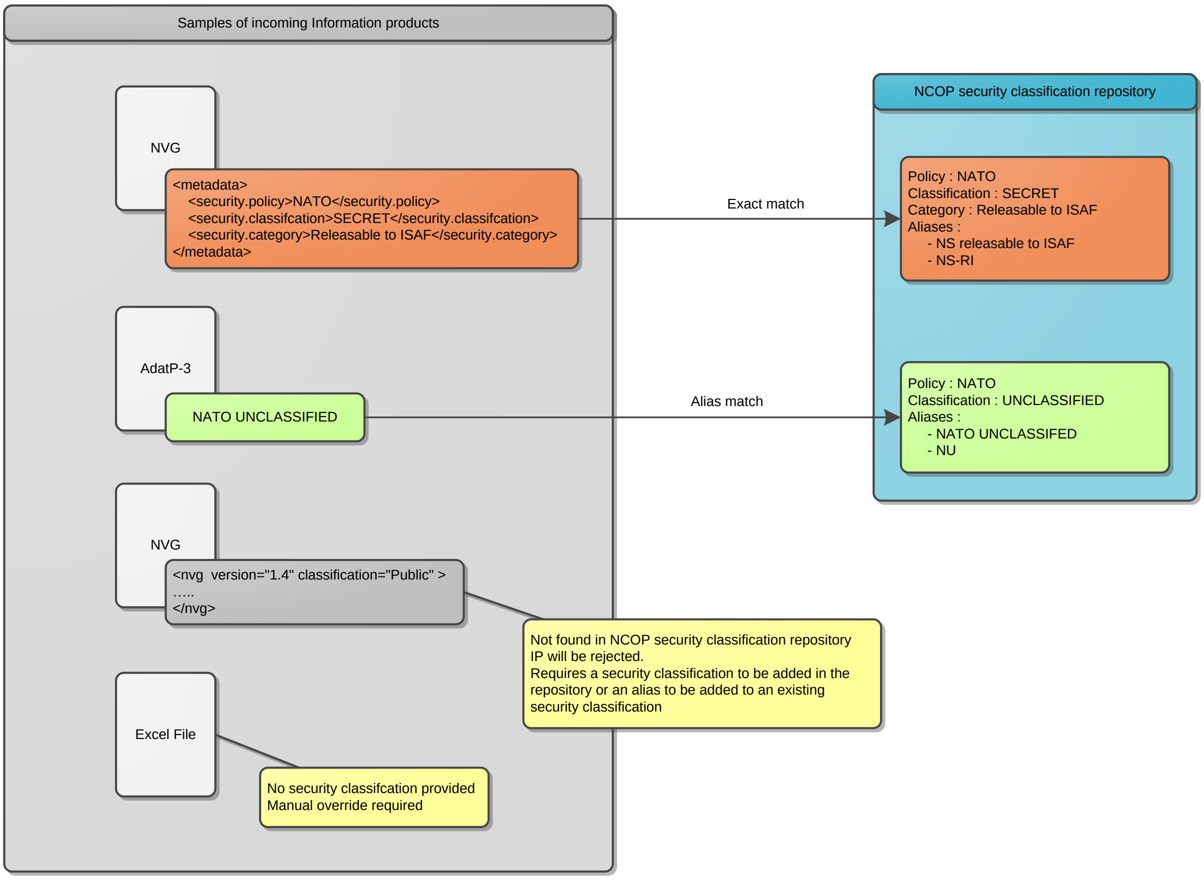

Samples of incoming Information products
NVG
<metadata>
<security.policy>NATO</security.policy>
<security.classifcation>SECRET</security.classifcation>
<security.category>Releasable to ISAF</security.category>
</metadata>
AdatP-3
NATO UNCLASSIFIED
NVG
<nvg version="1.4" classification="Public" >
…..
</nvg>
Excel File
No security classifcation provided
Manual override required
Exact match
Alias match
NCOP security classification repository
Policy : NATO
Classification : SECRET
Category : Releasable to ISAF
Aliases :
- NS releasable to ISAF
- NS-RI
Policy : NATO
Classification : UNCLASSIFIED
Aliases :
- NATO UNCLASSIFED
- NU
Not found in NCOP security classification repository
IP will be rejected.
Requires a security classification to be added in the repository or an alias to be added to an existing security classification

Figure 6-5: Security classification normalization

If an incoming information product has no security classification or a wrong one, it is possible for an authorized NCOP user to enforce a specific security classification by selecting one in the NCOP security classification repository.

The following figure describes the workflow used to determine the security classification of an Information Product during the acquisition phase:

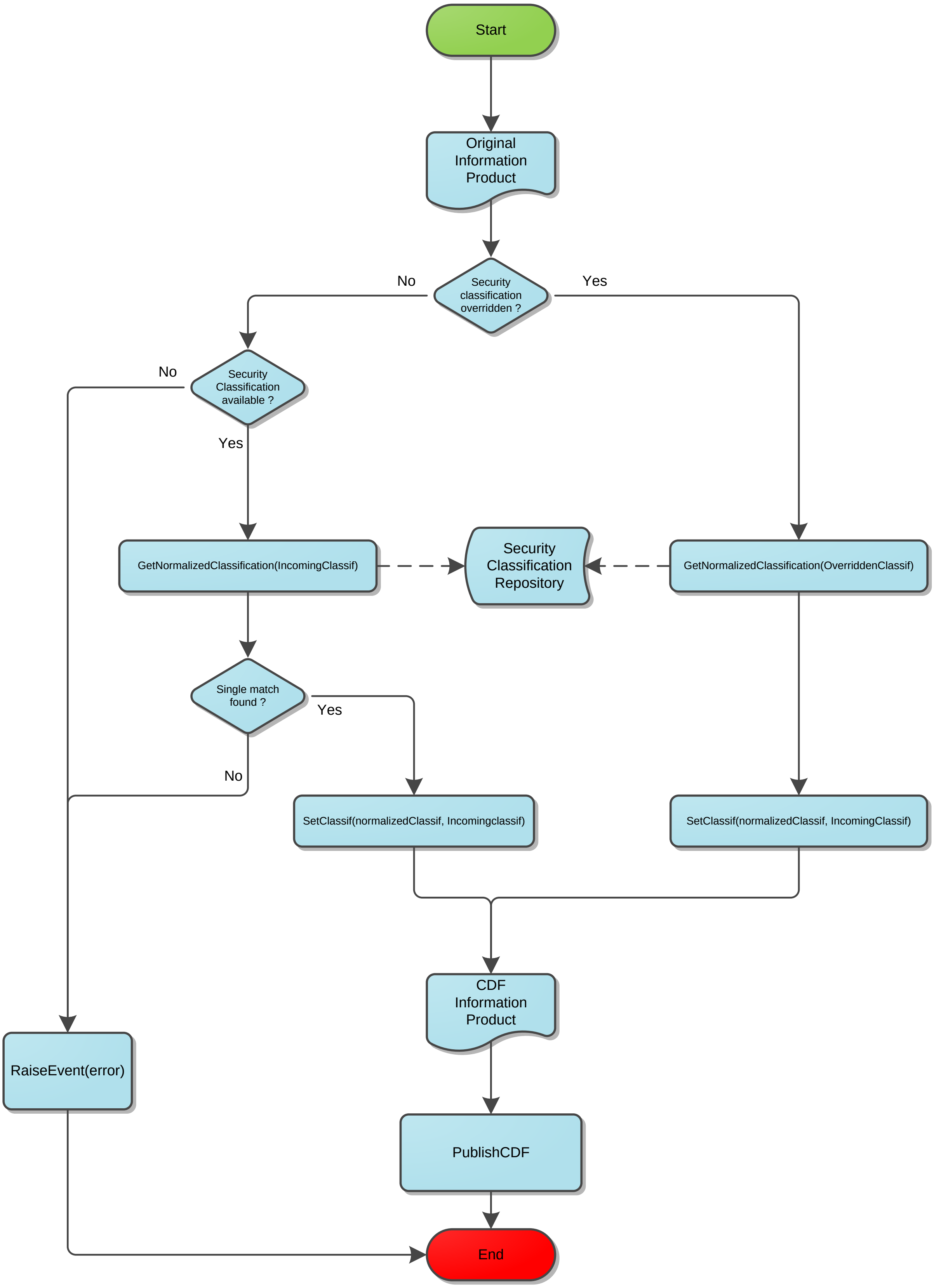

Start
Original Information Product
Security classification overridden ?
No
Yes
Security Classification available ?
No
Yes
GetNormalizedClassification(IncomingClassif)
Security Classification Repository
GetNormalizedClassification(OverriddenClassif)
Single match found ?
Yes
No
SetClassif(normalizedClassif, Incomingclassif)
SetClassif(normalizedClassif, IncomingClassif)
CDF Information Product
RaiseEvent(error)
PublishCDF
End

Figure 6-6: Security classification computation workflow

6.2.2.3 Alerts and actions

An incoming security classification can be normalized only if there is a single match in the NCOP security classification repository. No match or multiple matches is considered as an error and will require an action from an authorized user. Any error in the normalization process will raise an event that will result in a notification for the authorized users.

The following errors can be triggered during the normalization process:

- No security classification defined in incoming Information Product
- Incoming security classification not found in NCOP security classification repository
- Multiple matches found for incoming security classification in NCOP security classification repository

For each error, one of the following actions is required to solve the problem and allow the incoming Information Product to be stored and published by NCOP:

- Add a new entry in the NCOP security classification repository,
- Add aliases for an existing entry in the NCOP security classification repository,
- Enforce a security classification for an Information Product.

6.2.3 Details of BizTalk mappings

Details of BizTalk mappings are described in the NCOP Interface Control Document [ICD].

This section is related to the §5.3.3.3.2 Composition / Orchestration Implementation Component.

6.2.4 TIMS.js extensions

This chapter describes the technical solution used by NCOP to create extensions that can be added in the TIMS.js product. These techniques are used by NCOP to:

- Add management panels that are independent from the TIMS.js product
- Add panels and functionalities that will interact with the TIMS.js product through its public API

TIMS.js MMI Interface details can be found in chapter Appendix F.

This section is related to the §5.3.1.1.1 Geographical COP Editor Implementation Component.

6.2.5 ADatP-3 mapping management

Details of ADatP-3 mappings are described in the NCOP Interface Control Document [ICD].

This section is related to the §5.3.3.3.5 ADatP-3 and OTH-T Gold Message Processing Implementation Component.

6.2.6 Automated unit testing, coding rules and code reuse

6.2.6.1 Automated unit testing

Automated unit testing has been implemented for some critical projects that are part of the NCOP solution. For example, the source code of the NCOP Synchronization components, the Events manager component, or the generic internal data access layer classes contain specific classes dedicated to automated unit testing.

The standard Microsoft Visual Studio Unit Testing framework is used to implement these automated unit tests.

The complete list of Implementation Components using automated unit testing is described in the following table:

6.2.6.2 Coding rules

The same coding rules are applied to all the source code of NCOP Visual Studio projects and solutions.

The following standard coding rulesets are applied:

- Microsoft Basic Correctness Rules
- Microsoft Basic Design Guideline Rules
- Microsoft Extended Correctness Rules
- Microsoft Extended Design Guideline Rules
- Microsoft Minimum Recommended Rules
- Microsoft Security Rules

6.2.6.3 Code reuse

For the MCCIS Overlays and Tracks interfaces, NCIA has provided the source code that is being used in JCOP. Some parts of this source code has been reused and integrated in NCOP MCCIS connector source code. The source code that has been reused covers the following aspects:

- Network connection
- Data filtering
- Conversion of the MCCIS data model to NVG

The following table lists the source code file containing reused code:

TABLE 6-1: LIST OF SOURCE CODE FILES CONTAINING NCIA REUSED CODE

MCCIS Connector activity	Source code file

Network connection	Nato.NCOP.Mccis2Nvg/Overlays/NvgOverlayService.cs Nato.NCOP.Mccis2Nvg/Tracks/TrackTracer.cs Nato.NCOP.Mccis2Nvg/Tracks/MCCISConnection.cs
Data filtering	Nato.NCOP.Mccis2Nvg/Overlays/Overlayfilter.cs Nato.NCOP.Mccis2Nvg/Overlays/Overlays.cs Nato.NCOP.Mccis2Nvg/Overlays/OverlaysStructure.cs Nato.NCOP.Mccis2Nvg/Overlays/NvgOverlayService.cs Nato.NCOP.Mccis2Nvg/Tracks/Publicator.cs
conversion of the MCCIS Data model to NVG	Nato.NCOP.Mccis2Nvg/Overlays/Item.cs Nato.NCOP.Mccis2Nvg/Overlays/OverlaysStructure.cs Nato.NCOP.Mccis2Nvg/Tracks/Track.cs Nato.NCOP.Mccis2Nvg/Resources/FunctionID_MCCIS.Type_Map.txt

Regarding the data conversion, NCOP has developed additional code to generate extended data required for NCOP CDF needs: the ADEM attributes (described in chapter 5.4.1.2.1).

6.2.7 NCOP scripting technology

This section is related to the §5.3.2.2.4 COP IP Manager Implementation Component and in particular:

- §5.3.2.2.4.3 Information Product post-processing
- §5.3.2.2.4.4 Information Product visualization filters.

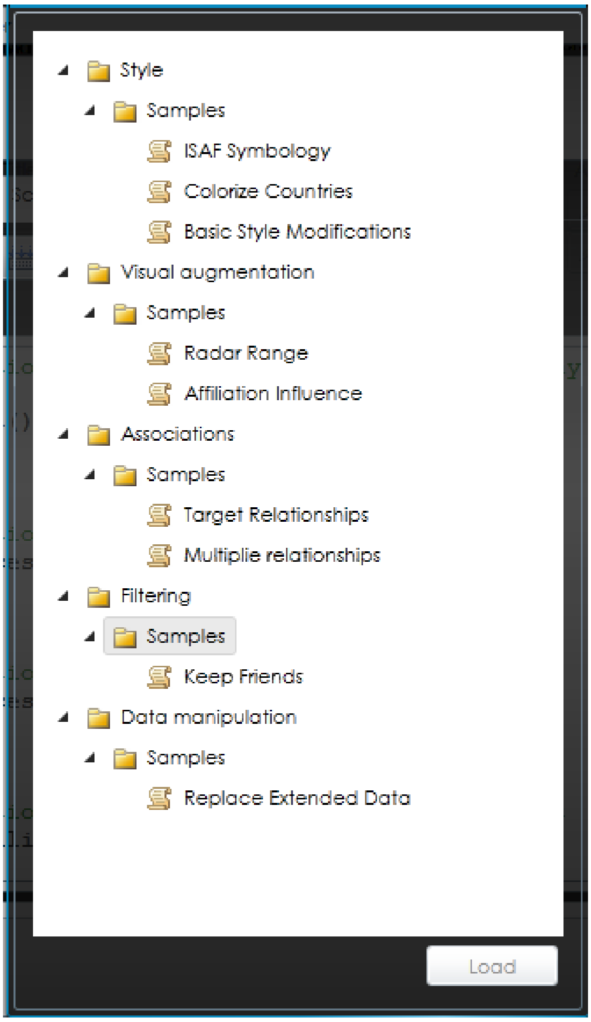
6.2.7.1 Principles

For the implementation of post-processing and visualization filter features, the first approach was to provide a set of graphical UI controls to allow the definition of rules that would have been used to transform a CDF. However, because the CDF remains an open format (unlimited number and types of properties for a single BSO) and because the rules can be based on any property that cannot be known in advance, creating such an HMI would have been too complex to implement but also to be used by the user. To avoid implementing a simple HMI that would have been too limited in terms of possibilities, the NCOP solution relies on a scripting language: the NCOP scripting technology.

This scripting technology is dedicated to the manipulation of CDF files. It offers a lot of flexibility to manipulate BSOs in terms of properties and style.

Because creating a script to modify the content of an Information Product requires some computer programming notions, factory samples are provided as part of the NCOP solution. Each sample is a commented script that presents specific operations that can be performed: manipulating BSO properties, modifying BSO style or symbology, manipulating associations, etc. Some specific scripts are also provided like the script that applies the ISAF symbology to BSOs that come from an LC2IS Information Product.

The following figure presents the list of sample scripts that are provided as part of the NCOP installation:



- Style
  - Samples
    - ISAF Symbology
    - Colorize Countries
    - Basic Style Modifications
- Visual augmentation
  - Samples
    - Radar Range
    - Affiliation Influence
- Associations
  - Samples
    - Target Relationships
    - Multiplie relationships
- Filtering
  - Samples
    - Keep Friends
- Data manipulation
  - Samples
    - Replace Extended Data

Figure 6-7: List of sample NCOP scripts

In addition to these samples, the scripting language comes with an integrated help module and is also documented in the NCOP Online Help.

6.2.7.2 Scripting language presentation

NCOP scripting technology is based on the ConScript scripting language and engine. This programming language follows the principles of managed code (like .NET) ensuring execution isolation and safety. The engine that processes the scripts can be hosted in a .NET application. For NCOP needs, three execution engines have been instantiated in order to be executed in the following environments:

- Post-Processing engine
  - Implemented inside an web service
  - Invoked by BizTalk during the acquisition process of an Information Product

- Visualization Filter engine
  - Implemented inside the COP publishing services (NCOP IPS)
  - Invoked when a visualization filter has to be applied on an Information Product
- Script preview engine
  - Implemented as an add-in to the Geographical Editor
  - Invoked from the Information Product edition panel when using the script editor UI

Based on the generic ConScript language, the NCOP Script language has been enhanced and specialized in order to comply with NCOP needs. In particular a lot of built-in functions have been provided to perform CDF-specific operations. The following chapters present the main capabilities of the language.

6.2.7.2.1 General presentation

The scripting language itself is a high-level C-like language. It is able to manage local and global variables, loops, functions, etc. It uses an object-oriented approach through the use of associative arrays to represent object properties.

NCOP scripts are used to take a CDF file as an input and to generate another CDF as an output file. The script processing engine automatically calls specific functions as it processes the CDF input file elements. Therefore, an NVG script must contain the following mandatory functions:

Function	Arguments	Description
init	*N/A*	Initialisation function invoked when the script is being executed. It allows the declaration and initialisation of global variable that will be used throughout the script
processInformationProduct	• Information Product	Invoked when an Information Product is being processed. The information Product being processed is the argument of the function.
processBSO	• Information Product • BSO	Invoked for each BSO present in an Information Product, the information Product and BSO being processed are the arguments of the function.
finalize	*N/A*	This function is invoked at the end of the script.

In addition to these mandatory functions, an NCOP script can contain custom internal functions that can be called by the script.

The following is a sample script that transforms an Information Product by keeping only “Friend” BSO based on their APP6A symbol:

```
/*
 * This script sample removes all BSO that are
 * not affiliated to Friend
 */

// This function is called on script startup and may be used to initialize
global variables
function init()
{
}

// This function is called on the root of the IP
function processInformationProduct(ip)
{
}

// Custom function used to find if we should remove the BSO
// (this is our business rule)
function ShouldRemoveBso(bso)
{
  if (bso.IsSymbolizedContentType == true)
  {
    var symbol = bso.symbol;
    // affiliation is only supported for app6a
    if (symbol.type == "app6a")
    {
      // Remove all bso that are not friends
      if (UpperCase(symbol.Affiliation) != "F")
      {
        return true;
      }
    }
  }
  return false;
}

// This function will be used to process all bsos inside a group or composite
function processSubBso(container)
{

  // here, we modify the collection while we iterate.
  // therefore, we do not use foreach statement that would
  // lead to unpredictable results
  // instead we iterate using index and starting with the end
  var index;
  for (index = container.Items.size - 1; index >= 0; --index)
  {
    var subBso = container.Items[index];
    if (ShouldRemoveBso(subBso))
    {
      container.Items -= subBso;
    }
    if (subBso.IsCompositeType == true || subBso.IsGroupType == true)
    {
      processSubBso(subBso);
    }
  }
}

// This function is called on each BSO
function processBso(ip, bso)
{
  if (ShouldRemoveBso(bso))
  {
    // to remove a BSO from the root of the IP, we use DetachBso
    DetachBso(bso);
  }

  if (bso.IsCompositeType == true || bso.IsGroupType == true)
  {
    // If the BSO is a group or a composite, it may contain
    // bso to remove too
    processSubBso(bso);
  }

}


// This function is called at the end of the script
function finalize()
{
}
```

6.2.7.2.2 CDF-oriented capabilities

The NCOP scripting language provides a set of functions and capabilities dedicated to the manipulation of CDF elements.

It provides a full read-write access to all BSO properties:

- Basic data (including style properties)
- Metadata
- Extended-data
- Associations

Properties are based on the CDF model which is an extension of the NVG 2.0 data model. A BSO variable has some additional properties that give access to military symbology properties (country, hostility).

Combined with the built-in functions, these CDF-oriented capabilities can be used to perform the following operations:

- Add/remove/modify BSO properties
- Define BSO symbol and/or style
- Create any type of NVG element, including composite objects
- Filter BSOs based on their properties
- Create/update/delete BSO associations

6.2.7.2.3 Built-in functions

The following table presents the main categories of built-in functions that can be used in an NCOP script:

TABLE 6-2: MAIN CATEGORIES OF BUILT-IN FUNCTIONS

Category	Description
Trigonometry	Contains all buil-in functions related to trigonometry (sin, cos, etc.) as well as a fromMGRS function that returns the longitude/latitude corresponding to an MGRS coordinate.
String	Contains all built-in functions dealing with String manipulation (trim, replace, compare,etc.)
Guid	Contains the Guid() function that returns a unique identifier

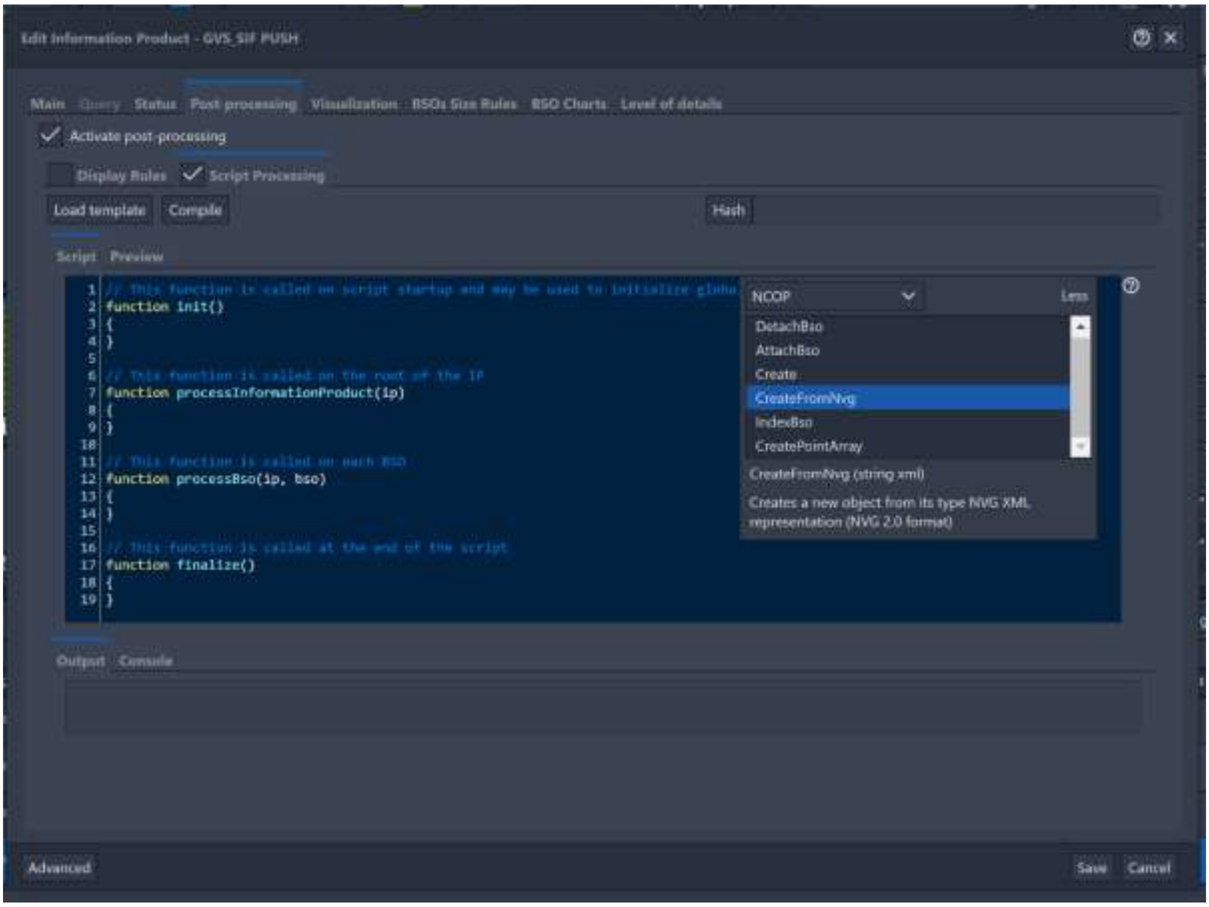
Cast	Contains all built-in functions that will convert a string value into an integer, or a double, or a date, etc.
Date	Contains all built-in functons that deal with dates, such as extracting the year, month, day,etc.
Data	Contains all built-in functions dedicated to the manipulation of CDF extended-data.
Debug	Contains the Print and Dump functions used for debugging purpose
Domain Values	Contains all built-in functions required to retrieve Domain Values stored in the NCOP storage
NCOP	Contains all built-in functions used to manipulate BSOs (create, createFromNVG, remove, index)

6.2.7.3 Script editor presentation

This editor is embedded in information product edition panels for post-processing and visualization filter definition. It has the following features

- Automatic syntax colorization
    - Bring out key words, similar to Visual Studio editor
- Integrated help
    - Quick help module displaying and briefly explaining built-in functions
- Preview panel
    - Allows the user to test a script by providing a sample CDF file. The resulting CDF file is presented in a sub panel to verify that the script is working correctly
- Debug console
    - Provides feedback when the script is executed
        - Compilation errors
        - Runtime errors
        - Print & Debug output

The following figure presents the NCOP Script editor embedded in the Visualization Filter definition module:



☑ Activate post-processing

□ Display Rules ☑ Script Processing

```
// This function is called on script startup and may be used to initialize globa
function init()
{
}

// This function is called on the root of the IP
function processInformationProduct(ip)
{
}

// This function is called on each BSO
function processBso(ip, bso)
{
}

// This function is called at the end of the script
function finalize()
{
}
```

CreateFromNvg (string xml)

Creates a new object from its type NVG XML representation (NVG 2.0 format)

Figure 6-8: NCOP script embedded editor UI

6.2.7.4 Error management

Two different error types can occur:

- Compilation errors
- Runtime errors

Compilation is a necessary step before the script can be executed. It will check that the script syntax and grammar are correct and generate the byte code that will be executed. During the script edition, the ‘compilation’ button can be used to perform this verifications and a compilation report will be provided to the user in the console with details such as line number where the error was detected and nature of the error (missing parenthesis, undeclared variable, etc.). Compilation is also performed on the server side whenever a script has to be executed. If any compilation error occurs, the script can’t be executed.

The script execution stops automatically when errors occur at runtime. If these error occur when using the preview feature in the geographical COP editor, the error cause and location will be displayed in the debug console. When the script is executed on the server side two behaviours must be considered depending on the component that processes the script:

- When post-processing scripts are executed
  - BizTalk will raise an NCOP alert but will publish the original CDF Information Product without transforming it.
- When visualization filters are applied
  - The NCOP IPS, will raise an error and no Information Product will be published.

6.2.8 COP exposition as OGC services and formats

6.2.8.1 Principles

The purpose of this feature is to allow the consumption of COPs and Information Products by clients that don't implement an NCOP IPS (or JIPS) consumption interface but are able to consume WMS services and WMC files.

NCOP Information Elements are translated into OGC objects using the following mappings:

NCOP Information Element	OGC concept	Comment
COP	Map service	
COP structure	Folders	
Information Product	Map layer	• CDF information products are converted into a map layer • Geo-Information Products (WMS and KML) are referenced using their original URL/location
Shared View	WMC file	The resulting WMC file contains links to the appropriate information element in its OGC format
Shared Views list	WMC catalogue file	The file references all individual WMC file corresponding to the Shared Views

It is important to note that the COP structure is kept during the conversion. It is recreated by organizing Map layers in folders that match the COP Structure. These folders are then exposed as part of the Map Service definition.

More details are provided regarding the exposed properties and values in the NCOP [ICD].

The following figure presents an overview of the process and the actors involved in the conversion process:

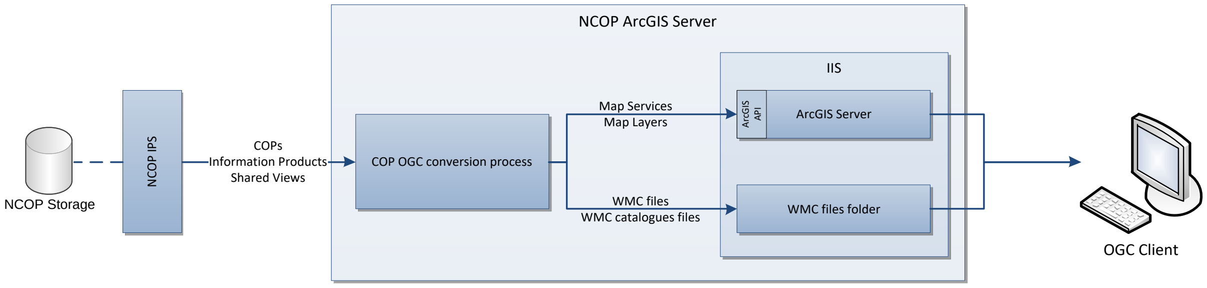


Figure 6-9: Overview of the 'COP exposition as OGC services' process

6.2.8.2 Conversion process

The conversion is performed by an autonomous scheduled process that uses the NCOP IPS service to retrieve NCOP Information Elements from NCOP Storage. Because the WMS layers will be consumed anonymously, only public Information Elements are retrieved, using the same rules as when a COP is exposed for NCOP IPS anonymous consumption.

The following presents the algorithm used for the conversion of Information Elements into OGC services and WMC files:

```
•  Retrieve COPs list
•  For each COP :
       o  Retrieve COP definition
       o  Create a Map Service
       o  For each Information Product :
              -  Retrieve Information Products definition
              -  If the Information Product is based on CDF:
                     •  Retrieve Information Product data (CDF)
                     •  Convert CDF into KML
                     •  Create a map layer from KML
                     •  Add the map layer to the COP Map service
              -  Else (Geo-Information Product):
                     •  Add a reference to Geo-Information Products (KML/WMS) to
                        the COP Map Service
       o  Publish the Map Service
       o  Retrieve COP shared views
       o  For each shared view:
              -  Create a WMC file containing links to appropriate Map Layers from
                 the COP Map Service
       o  Create a WMC catalogue file referencing all Shared Views WMC
```

OGC Map services are published in the NCOP GeoServer server in a dedicated NCOP folder.

The NCOP [ICD] specifies the URL that must be used to consume these WMS services.

The WMC catalogue file and the corresponding WMC files are created in a dedicated folder on the NCOP GeoServer server. This folder is exposed as a standard Web site using IIS.

The NCOP [ICD] specifies the URL formats that must be used in order to:

- retrieve the WMC Catalogue corresponding to a specific COP
- retrieve the WMC file corresponding to a specific Shared View of e specific COP

NCOP uses one conversion process and one output folder per NCOP site in order to isolate COPs and Information Products depending on the environment where they have been instantiated (operational, training and exercise).

6.2.9 BSO indexing service

This section is related to the §5.3.4.1 COP and IP History storage Implementation Component.

When an Information Product is acquired on an NCOP node, the BSO it contains must be extracted and stored in the BSO Index database. It is required for the usage of the following capabilities:

- BSO History
- BSO Search
- User layers

The BizTalk acquisition process includes an indexing orchestration which is performed when an Information Product is acquired. However, when the Information Product is synchronized or imported/restored from an archive, the data is not processed by BizTalk in order to minimize processing (incoming data is already in the CDF format). In order to have access to the functionalities mentioned above, an additional BSO indexing service is implemented to build the BSO history and index.

This indexation is performed by a dedicated windows service. This service runs in background to provide decoupled indexing. Its activities are scheduled and based on the comparison of data available in the SharePoint portal (CDF files of the information product instances) and the data available in the BSO history and index database.

When an updated data is detected, the service performs the following actions:

- Retrieves the associated CDF,
- Extracts each BSO properties,
- Stores each BSO in the BSO Index database
    - Only the latest version of a BSO is kept in this database
- Stores each BSO in the BSO History database unless the BSO history feature has been deactivated by the COP Manager when the Information Product has been defined
    - Previous versions of the BSO are kept according to the retention policy for the Information Product

To provide flexibility, there is one indexing service per NCOP site (operational, training and exercise). They are activated by default but could be stopped by an authorized user if required. However, stopping this indexing will impact the functionalities listed above: BSO search, BSO history and User layers will not provide up to date information. For each service, the schedule can be configured.

Also, the indexing services can be temporarily configured to perform a full indexation of the NCOP storage. This configuration must be activated only when necessary: in cases where data has been restored in NCOP at the database level only.

These indexing services are deployed on the SharePoint server to optimize access to the CDF files. Indexing services are designed to be run in a high-availability environment. In this case services are deployed and run on both SharePoint servers.

6.2.10 User layers management

This section is related to the §5.3.1.1.3 User Layer Manager Implementation Component.

6.2.10.1 Principles

A "user layer" is a user-defined layer that contains references to individual BSOs coming from COP Information Products. It allows a user to store in an individual layer a set of BSOs of interest. When this user layer is loaded in the Geographical COP Editor, the latest version of each BSO is loaded on the map like any other COP Information Product.

COP consumers have the ability to define multiple user layers and organize them by creating folders.

A user layer is personal but can be shared by the owner. When a user layer has been shared, other COP Consumers are able to select it as a favorite and import it as a reference in their own user layers.

6.2.10.2 Storage

User layers management uses a combination of storage backend with both SharePoint lists and pure SQL storage.

Two SharePoint lists are used to store the definition of user layers:

- User Layers
- User favorite user layers

The "**User Layers**" SharePoint list stores the main definition of user layers. The following properties are used to characterize a user layer item:

Attribute	Description
GUID	Unique identifier of the user layer
Title	Name of the user layer
Path	Location in the user layer tree *(e.g. /Ground/Radars)*.
Classification	Security classification of the user layer
Shared	Boolean value indicating if this user layer is shared to other COP consumers
Owner	User that owns the user layer

The security classification of a user layer is determined by identifying the highest security classification defined among all contained BSO. If no security classification is defined at the BSO level, the security classification of the originating Information Product is used.

The “**User Favorite User Layers**” SharePoint list stores the shared user layers links when they are defined as favourites by another consumer. A favorite user layer is seen as a link to a shared user layer. This link is visible in the User layer tree and can have a different name than the original user layer. The following properties are used to characterize a favorite user layer item:

Attribute	Description
GUID	Unique identifier of the favorite user layer
Title	Name of the favorite user layer
Path	Location in the user layer tree *(e.g. /Ground/Radars)*.
User Layer	Identifier of the linked User layer (lookup field pointing to the user layer item in the “User Layers” list.)
User	User that owns the favorite user layer

The SQL storage is used to store the following elements:

- List of references to BSOs contained in each user layer
- BSO properties

The list of references to BSOs contained in each user layer is stored in a simple table with the following SQL columns:

TABLE 6-3: USER LAYER TABLE

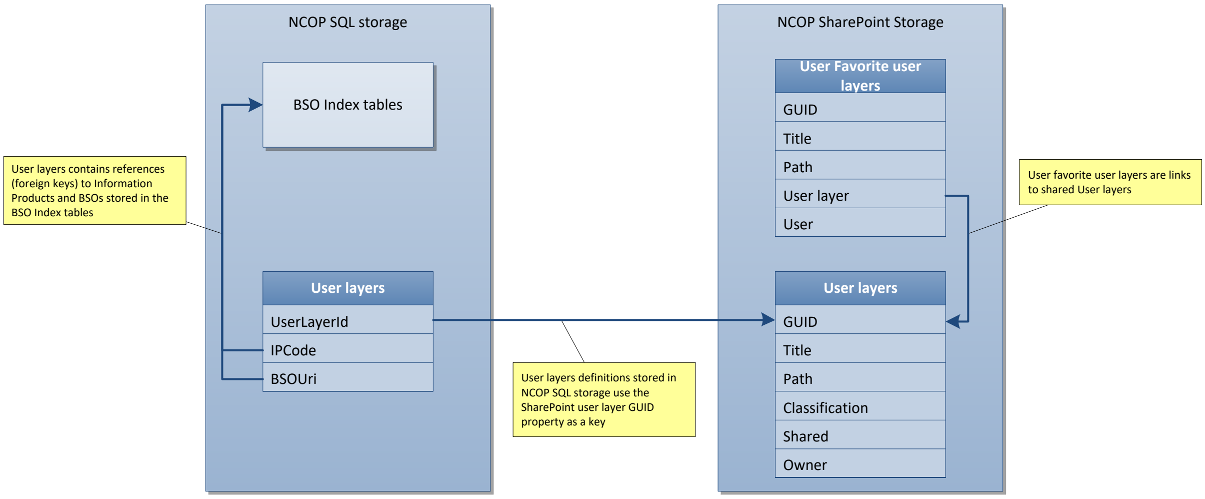
Column name	Description
UserLayerId	Unique identifier of the User layer, as defined in the SharePoint “User layers” list described above.
IPCode	Unique identifier of the originating Informaiton Product
BSOUri	Identifier of the BSO as defined in its originating Information Product

The User Layer management reuses the BSO Index tables defined in chapters 5.4.7.2 and 5.4.7.3 as the storage tables for BSO properties.

This hybrid storage configuration has been designed to address the following:

- Reuse of the existing BSO index database to avoid duplication of information
- Optimize performance when retrieving BSO property using standard SQL ‘join’ feature.

The following figure presents an overview of links between items involved in User layers management:



User layers contains references (foreign keys) to Information Products and BSOs stored in the BSO Index tables

User layers definitions stored in NCOP SQL storage use the SharePoint user layer GUID property as a key

User favorite user layers are links to shared User layers

Figure 6-10: User layers storage overview

6.2.10.3 Definition, consumption and sharing

End user activities related to User layers are performed using from the Geographical COP Editor. The following actions can be performed:

- Create (rename, delete) a user layer
- Create (rename, delete) folders
- Organize user layers in folders (with drag & drop)
- Add the currently selected BSOs to a specific User layer
- Share a user layer
- Browse shared User layers
- Add as a favorite a user layer shared by another user.
- Load an user layer for display

All these actions use web services to read and write appropriate items in the NCOP storage. These web services are described in more details in the NCOP [ICD].

When a user layer is loaded in the Geographical COP Editor, it is automatically refreshed when one of the BSO it contains is updated. This mechanism is based on the NCOP eventing system: When an Information Product is updated by a source and acquired by NCOP, an “Information Product content changed” event is raised internally. Depending on the impacted Information Product the associated user layers are identified and a notification is sent to the Geographical COP Editor so it can refresh the user layers.

6.2.10.4 Limitations

The following limitations exist for User layers:

- BSO Links are not stored in a user layer

  The reason is that a user layer only contains BSOs selected by the end user. Storing the BSO links in the user layer definition would have required storing *also the linked BSOs for a correct exploitation of those links. It would have led to include additional BSOs in the user layer which is not expected by the end-user.*

- A Shared View cannot contain User layers (User layers can be contained by Named Views only)

  User layers definitions are stored and accessible only on the node on which they were created. They are not synchronized on remote NCOP nodes since they don't belong to any COP. Therefore if they were included in a Shared View, user layers content may not be visible by all consumers depending on their location. To avoid such inconsistency a contributor is not allowed to create a Shared View that contains a user layer.

6.2.11 NCOP IPS Topic-based subscription and publication management

6.2.11.1 Principles

NCOP provides flexibility for subscription to Information Elements updates. It is achieved by allowing NCOP IPS consumers to subscribe to the publication service by specifying a topic. As a result, the consumer will receive notifications only for Information Elements that match the topic specified.

In addition, an authorized NCOP user has the possibility to define publication restriction rules. With such a configuration, the NCOP IPS will not send notifications to a consumer based on the type of notification and on the consumer identity. These publication restriction rules are associated with Systems that represent a category of consumers (As an example, if AirC2IS clients consumed NCOPIPS directly, they would register themselves as consumers of the AirC2IS system). It is therefore possible to disable notifications for all consumers that are instantiated in the same System.

Both subscription and publication rules can be defined by specifying the following target Information Elements:

- COP
  - Structure node (structure and folders)
  - Information Product
    - Annotation
  - Shared View
- Information Product
- Shared View

NCOP IPS topic-based subscription and publication rules are hierarchical:

If the user subscribes to a specific COP, he will receive notifications for all modifications in the Information Elements attached to this COP (e.g. Shared View created, COP structure change, COP Information Product content changed, etc.)

If the user subscribes to a specific node in the structure of a specific COP, he will only receive notifications related to Information Elements located under this specific structure node (e.g., COP Information Product content changed (if the COP Information Product location in the COP structure matches the subscription topic)).

6.2.11.2 Topic definition language

For subscription and publication rules definition, a specific language must be used. This language is widely based on the standard XPath expression language:

- It is adapted to the hierarchical structure of NCOP Information Elements,
- It allows the use of the * wildcard,
- It allows filtering based on Information Element attributes
- Specific keywords have been introduced to satisfy NCOP needs.

The specific keywords that have been introduced are the following

Keyword	Description
/#cops	The next element in the expression is a COP: e.g. /#COPS/MyCOP
/#information products	The next element in the expression is an Information Product. (e.g. /#IP/
/#shared views	The next element in the expression is a Shared View. (e.g. /#SharedViews/MyView
/#kml maps	The next element in the expression is a kml map
/#maps	The next element in the expression is a WMS map
/#annotation	The next element in the expression is an annotation layer

Some additional details and samples for this language are provided in the NCOP [ICD].

6.2.11.3 NCOP IPS information storage

The NCOP IPS web service requires storing the following elements:

Element	Content description
Consumer subscriptions	The list of current subscribers, with associated system, subscription topic and publication endpoint
Publication restriction rules	The list of publication restriction rules with their associated system
NCOP content image	The hierarchical representation of the NCOP Information Element structure based on the content of the NCOP Storage

Consumer subscriptions are stored in the memory of the process attached to the NCOP IPS Web services. They are maintained based on consumers' activities (subscribe, unsubscribe, renew).

Publication restriction rules are stored using an SQL Server-based persistence. They are maintained based on the administrator activities performed using the dedicated web UI for publication restriction rules management. The implementation of this storage is using two SQL tables which are described hereafter:

The SQL table ‘IPSRules’ contains the publication restriction rules definition:

TABLE 6-4: IPSRULES SQL TABLE

Column	Type	Description
ID	Numeric	Internal SQL identifier
System	Numeric (Foreign key)	Identifier of the system for which the publication restriction rule has been defined
Active	Boolean	Indicates if the publication restriction rule is taken into account or not by the notification engine
IPSRule	Text	The textual definition of the topic for which notifications shall not be published

The SQL table ‘IPSSystems’ contains the list of NCOP IPS Client Systems for which publication restriction rules have been defined:

TABLE 6-5: IPSSYTEMS SQL TABLE

Column	Type	Description
ID	Numeric	Internal SQL identifier
Label	Text	Name of System

NCOP content image is a memory image of the structure of all Information Elements defined on the NCOP node. This data is used by the notification processing engine to forward the appropriate notifications to the appropriate subscribers. Its internal model is based on tree structure that exactly matches the NCOP Information Elements organisation based on the current NCOP Storage content. This tree structure is used by the notification processing engine which more detailed in the next chapter. The usage of process memory storage instead of SQL-based persistence is required to optimize performances.

6.2.11.4 Topic-based processing engine

The topic-based processing engine is made of 3 main components:

- Event analyzer

  This component receives events generated by the NCOP Events Manager component (cf. chapter 5.3.3.2.1). Based on this event, the event analyser component will start with updating the NCOP content image to be in sync with the NCOP Storage, and then the event will be declined in a list of impacted elements with a name that reflects the hierarchy in the NCOP storage.

  For example, considering an ‘Airbases’ information product that is present:

  - *twice in the structure of COP COPx,*
  - *in a Shared View contained in COPx*
  - *once in the COP COPy,*

An incoming "Information Product content changed" event will identify the following impacted elements:

- *○ /#cops/COPx/Structure/Folder1/Airbases*
- *○ /#cops/COPx/Structure/Folder2/Airbases*
- *○ /#cops/COPy/Structure/FolderA/Airbases*
- *○ /#information products/Airbases*
- *○ /#cops/COPx/#shared views/View1*

- Consumer resolver

  This component analyses the notifications generated by the 'Event analyzer' component and searches for matches with current consumer subscriptions. Once subscribers have been identified based on their subscriptions, the component checks if there are any publication restriction rules that should be applied. In the end valid notifications are sent to the 'Notifier'

- Notifier

  This component is in charge of sending notifications to the valid consumers identified by the 'Consumer resolver'.

The following figure presents an overview of the processing of an incoming event:

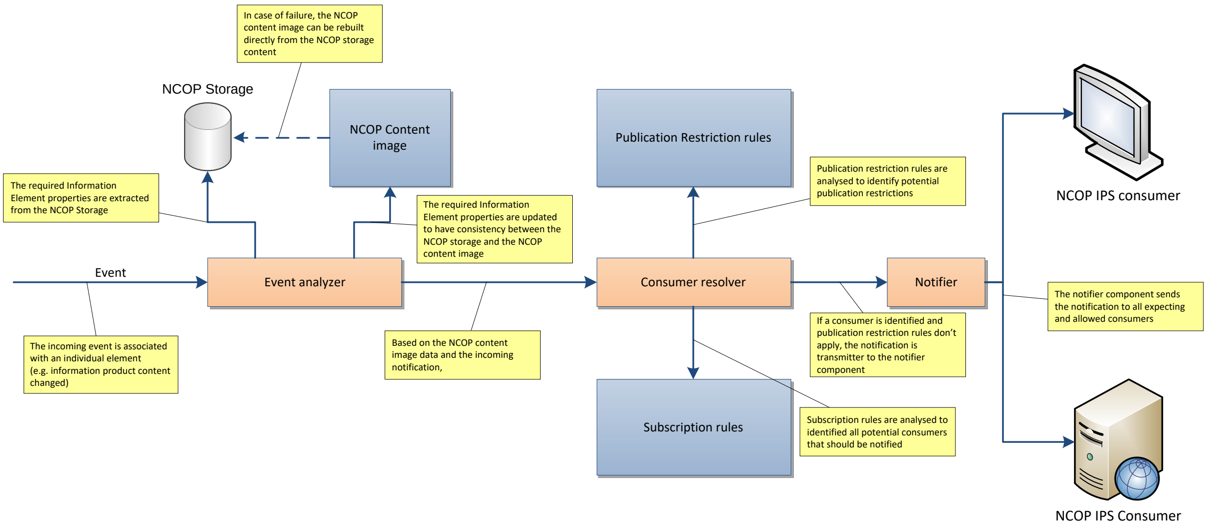

In case of failure, the NCOP content image can be rebuilt directly from the NCOP storage content
NCOP Storage
NCOP Content image
Publication Restriction rules
NCOP IPS consumer
The required Information Element properties are extracted from the NCOP Storage
The required Information Element properties are updated to have consistency between the NCOP storage and the NCOP content image
Publication restriction rules are analysed to identify potential publication restrictions
Event
Event analyzer
Consumer resolver
Notifier
The notifier component sends the notification to all expecting and allowed consumers
The incoming event is associated with an individual element (e.g. information product content changed)
Based on the NCOP content image data and the incoming notification,
If a consumer is identified and publication restriction rules don't apply, the notification is transmitter to the notifier component
Subscription rules
Subscription rules are analysed to identified all potential consumers that should be notified
NCOP IPS Consumer

Figure 6-11: NCOP IPS event processing for topic-based publication

6.2.12 COP Worksheet data acquisition mechanism

6.2.12.1 Implementation principles

The purpose of the COP Worksheet is to allow COP contributor to rapidly capture data using a tabular tool for defining BSOs. From this COP Worksheet, multiple layers will be created by using BSO properties to dispatch BSOs in those layers. NCOP implementation for the COP worksheet feature is based on the following principles:

- Excel is used as the tool for capture and as the storage format of the data
- Each COP Worksheet is represented with a single Excel file (NCOP supports the definition of multiple COP Worksheet)
- Each COP Worksheet to a single Information Product in NCOP
- COP Worksheets are stored in a dedicated SharePoint document library in the NCOP Storage.
- COP worksheet Information Products are processed using the standard NCOP Excel-based Information Product acquisition process to be converted into CDF.
- Visualization filters are defined and used to dispatch BSOs into multiple layers (each visualization filter creating a different representation of the same Information Product)

6.2.12.2 COP Worksheet Storage

Each COP Worksheet is implemented in NCOP as an Excel file stored in a dedicated SharePoint document library in the NCOP portal. This implementation proposes the following advantages:

- The Microsoft Excel tool provides easy data manipulation
- The Excel data format is a format for which the acquisition process is already taken into account in the NCOP acquisition interfaces
- SharePoint storage allows the Excel file to be opened directly from the SharePoint and saved directly into the portal thanks to native SharePoint/Excel integration.

6.2.12.3 COP Worksheet data access

From the COP explorer, a dedicated section allows contributor to access already existing COP Worksheets or to create new one.

Creating a COP Worksheet consists in uploading an initial Excel file and defining a basic mapping of CDF BSO properties.

Editing an existing COP Worksheet is also initiated from the COP Explorer. The ‘edit’ action will download the Excel file and open it in Excel. Then the user can use native Excel capabilities to update the data. The ‘Save’ option in Excel will save the COP Worksheet automatically in the NCOP portal.

6.2.12.4 Creation of layers from a COP Worksheet

Since a COP worksheet corresponds to a single information Product, some actions are necessary to instantiate multiple COP layers from a single COP Worksheet. This is achieved by the COP Manager defining multiple visualization filters for each COP Worksheet Information Product. For example, if the COP Worksheet data contains land and maritime units, the COP Manager is able to define 2 visualization filters to create two different representations of the data: one for displaying land units and the other for displaying maritime units.

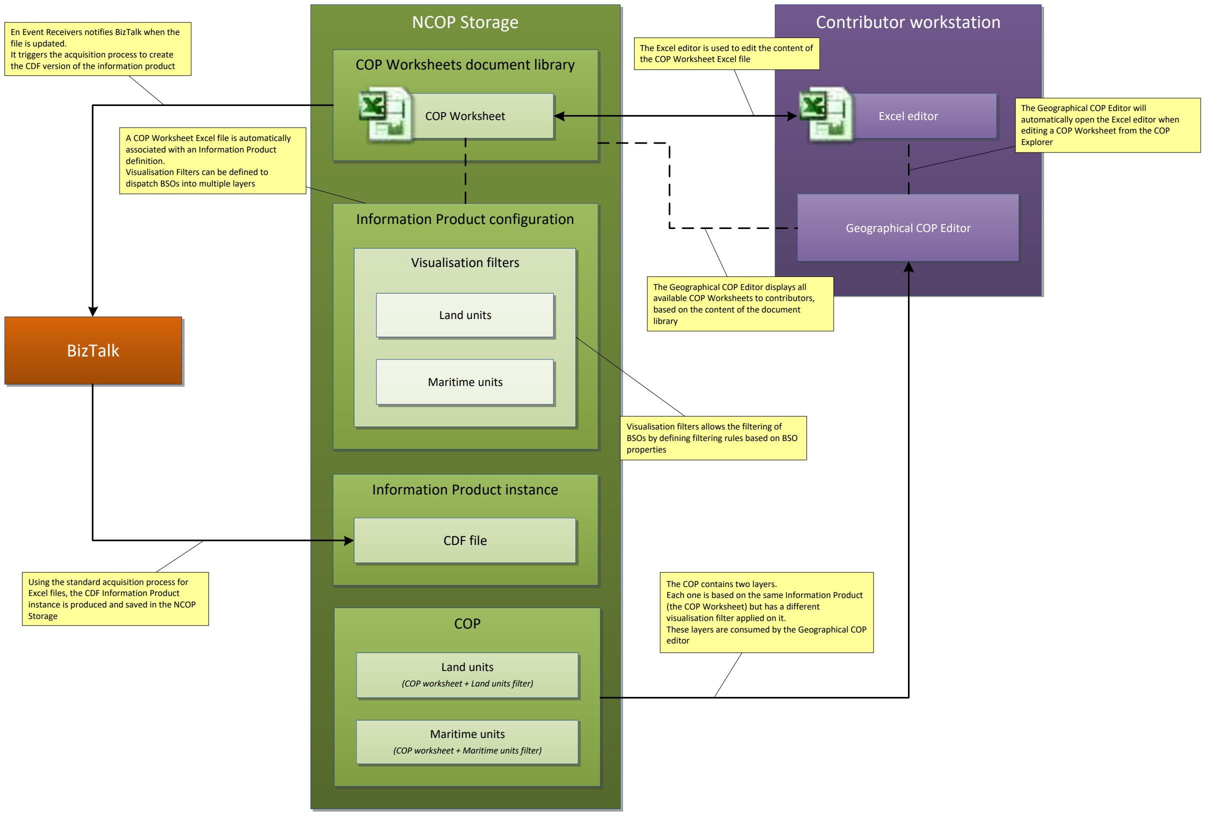
The NCOP Visualization Filter feature also allows the COP Manager to include the COP Worksheet Information Product multiple times in the COP but each time with a different visualization filter applied. This gives the illusion to COP consumers that the COP is made of different Information Products even if the data comes from a single Information Product. The UI for including an Information Product with a predefined visualization filter in a COP is described at chapter 5.3.2.2.2.2.

6.2.12.5 Event-driven processing of updates

The COP worksheet feature requires an event-driven processing in order to quickly expose changes when a contributor modifies the content of a COP Worksheet. This is implemented NCOP by the use of Event Receivers defined in the SharePoint document library that is used to store the COP Worksheet excel files. This event receiver detects file updates and notifies BizTalk so it starts processing the data immediately.

6.2.12.6 Global COP Worksheet feature implementation overview

The following figure presents the NCOP components involved in the processing of a COP Worksheet. It is based on a simple scenario where a COP Worksheet contains both land and maritime units and the COP Manager exposes 2 different layers in his COP based on this COP Worksheet.



En Event Receivers notifies BizTalk when the file is updated.
It triggers the acquisition process to create the CDF version of the information product

A COP Worksheet Excel file is automatically associated with an Information Product definition.
Visualisation Filters can be defined to dispatch BSOs into multiple layers

The Excel editor is used to edit the content of the COP Worksheet Excel file

The Geographical COP Editor will automatically open the Excel editor when editing a COP Worksheet from the COP Explorer

The Geographical COP Editor displays all available COP Worksheets to contributors, based on the content of the document library

Visualisation filters allows the filtering of BSOs by defining filtering rules based on BSO properties

Using the standard acquisition process for Excel files, the CDF Information Product instance is produced and saved in the NCOP Storage

The COP contains two layers.
Each one is based on the same Information Product (the COP Worksheet) but has a different visualisation filter applied on it.
These layers are consumed by the Geographical COP editor

Figure 6-12: COP Worksheet processing overview

6.2.13 Certificates requirements

This chapter describes the certificates that are needed when NCOP is implemented on a site. Certificates are required for:

On NCOP SQL server(s):

- 1 certificate (Single node) or 4 certificates (HA node – 1 certificate per clustered SQL Server instance) used to:
  - Encrypt SQL Server communications with SharePoint and BizTalk servers

On NCOP SharePoint server(s):

- 1 certificate used for:
  - Signing COP archives
  - Encrypting sources credentials
  - Encrypting/decrypting synchronisation credentials
- 1 certificate used for:
  - Encrypting data send by NCOP NVG Streaming connector 2.0 to NVG Streaming 2.0 provider in the case of a HTTPS exchange
- n certificates for https: one per hostheader
  - Central administration
  - NCOP Operational portal
  - NCOP Exercise portal
  - NCOP Training portal

On NCOP BizTalk server(s):

- 1 certificate used to:
  - Signing CDF files. *Optional, required when the CDF data signature is activated (cf. chapter 5.4.1.4).*
- 1 certificate used to:
  - Decrypting credentials
- n certificates for https: one per hostheader
  - BizTalk services hosted on IIS (SIFToNVG Converter, …)

On NCOP Application server(s):

- n certificates for https: one per hostheader
  - Geographicail COP Editor and Geographical COP Editor services
  - Common Services

On NCOP GeoServer server(s):

- n certificates for https: one per hostheader
  - GeoServer portal

On NVG Streaming 2.0 provider server(s):

- 1 certificate used to:
    - Decrypting data sent by NVG Streaming 2.0 provider to NCOP NVG Streaming connector 2.0 in the case of a HTTPS exchange

Certificates used for sources credentials on NCOP SharePoint server(s) and NCOP BizTalk server(s) must be the same. You can also use this certificate for signing CDF files.

Certificates used for NVG Streaming 2.0 exchanges must be different.

The following tables present the certificate properties required for the purposes listed above (subset). The complete list of certificate properties required for the purposes listed above will be defined on the INSTALLATION AND CONFIGURATION GUIDE (ICG) -ANNEX 03A Defining a custom PIE certificate.

TABLE 6-6: CERTIFICATES PROPERTIES (CDF SIGNING)

Required certificate characteristics for NCOP CDF signing	
Certificate name	ncop.cdf.sign.<site name> *(e.g. ncop.cdf.sign.jfcbs)*
Certificate Subject	cn=ncop.cdf.sign.<site name>, o=NATO *(e.g. cn= ncop.cdf.sign.jfcbs, o=NATO)*
Certificate role	Document signature
Expected format	Pfx file
Include private key	Yes
Include certification chain	Yes
Delivery on token allowed	No

TABLE 6-7: CERTIFICATES PROPERTIES (NCOP SYNCHRONIZATION)

Required certificate characteristics for NCOP synchronisation	
Certificate name	ncop.sync.crypt.<site name> *(e.g. ncop.sync.crypt.jfcbs)*
Certificate Subject	cn=ncop.sync.crypt.<site name>,o=NATO *(e.g. cn=ncop.sync.crypt.jfcbs, o= NATO)*
Certificate role	Data encryption and Document signature
Expected format	Pfx file
Include private key	Yes
Include certification chain	Yes

Delivery on token allowed	No

For all 3 certificates, the Certificate Subject properties is a proposal: properties (cn,o,c etc.) can be adjusted as required by the NPKI policy.

6.2.14 Secure communication

Secured server-server configuration is the default NCOP installation. Thus, communications between SQL and BizTalk/SharePoint server(s) are encrypted to avoid any password or data disclosure.

6.3 SUBORDINATE CONFIGURATION ITEMS

The following figure presents the decomposition of main Configuration Items into Subordinate Configuration Items (CI). Each Subordinate Configuration Item groups several Implementation Components (IC) that are themselves decomposed in software artefacts (SA) introduced in the detailed design. Mapping between subordinate CI and SA is provided in section 0 of this document as well as within the implementation model.

Note that subordinate CI cannot be considered as CSCI as defined by DoD2167A, mainly because they cannot be tested independently. However they are configuration managed (versioning, allocation of problem reports).

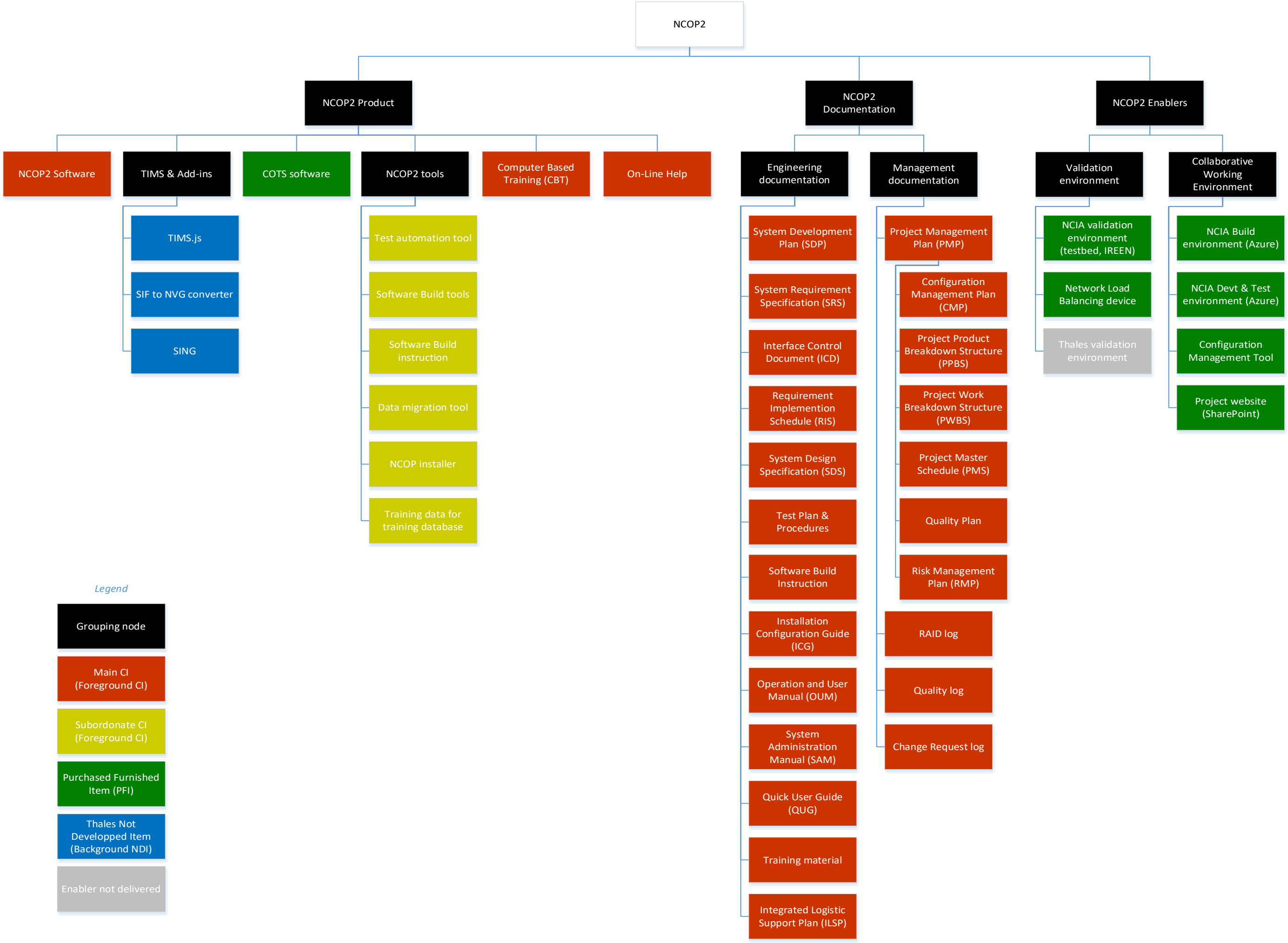

NCOP2
NCOP2 Product
NCOP2 Documentation
NCOP2 Enablers
NCOP2 Software
TIMS & Add-ins
COTS software
NCOP2 tools
Computer Based Training (CBT)
On-Line Help
TIMS.js
SIF to NVG converter
SING
Test automation tool
Software Build tools
Software Build instruction
Data migration tool
NCOP installer
Training data for training database
Engineering documentation
System Development Plan (SDP)
System Requirement Specification (SRS)
Interface Control Document (ICD)
Requirement Implemention Schedule (RIS)
System Design Specification (SDS)
Test Plan & Procedures
Software Build Instruction
Installation Configuration Guide (ICG)
Operation and User Manual (OUM)
System Administration Manual (SAM)
Quick User Guide (QUG)
Training material
Integrated Logistic Support Plan (ILSP)
Management documentation
Project Management Plan (PMP)
Configuration Management Plan (CMP)
Project Product Breakdown Structure (PPBS)
Project Work Breakdown Structure (PWBS)
Project Master Schedule (PMS)
Quality Plan
Risk Management Plan (RMP)
RAID log
Quality log
Change Request log
Validation environment
NCIA validation environment (testbed, IREEN)
Network Load Balancing device
Thales validation environment
Collaborative Working Environment
NCIA Build environment (Azure)
NCIA Devt & Test environment (Azure)
Configuration Management Tool
Project website (SharePoint)
Legend
Grouping node
Main CI (Foreground CI)
Subordonate CI (Foreground CI)
Purchased Furnished Item (PFI)
Thales Not Developped Item (Background NDI)
Enabler not delivered

Figure 6-13: NCOP System decomposition in Subordinate Configuration Items

The following table describes each subordinate Configuration Item:

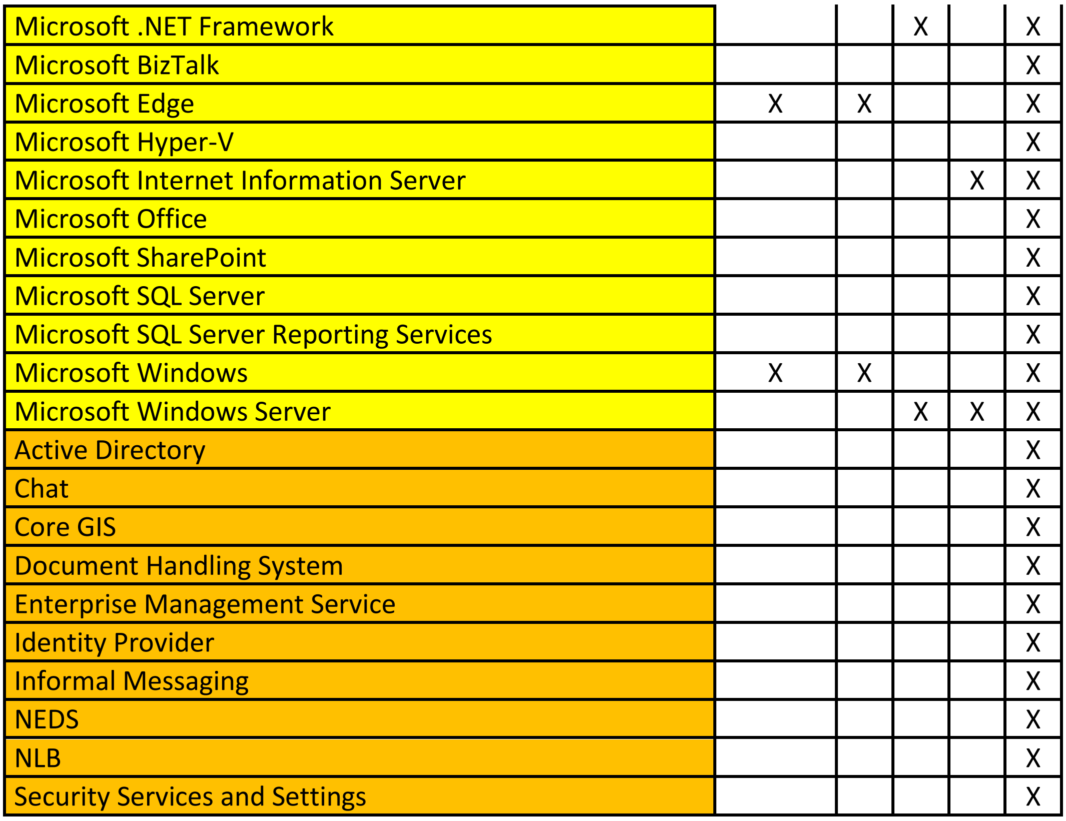
TABLE 6-8: SUBORDINATE CONFIGURATION ITEMS DESCRIPTION

Configuration Item	Subordinate configuration Item	Description
TIMS & Add-ins		
	TIMS.js	TIMS.js is a Software Development Kit (SDK) that allows developing civilian and military GIS based Web Applications.
	SIF to NVG Converter	Software component dedicated to the conversion of LC2IS SIF files into NVG. It is invoked by the NCOP interoperability subordinate configuration item
	SING	Software component dedicated to the parsing of ADatP-3 and OTH-T Gold messages. It provides a library and a user interface. The library is invoked by the NCOP interoperability subordinate configuration item. The user interface is used to edit and analyse the content of ADatP-3 and OTH-T Gold messages.
NCOP Tools		
	Test Automation Tool	
	Software Build Tools	
	Software Build Instruction	
	Data Migration Tool	
	NCOP Installer	
	Training Data for Training database	

The following table identifies any off-the-shelf and government furnished equipment (GFE) components necessary to build, deploy, or execute the identified Configuration Item.

TABLE 6-9: COTS AND GFE REGARDING CSCI

COTS\CSCI	Computer Based Training (CBT)	On-Line Help	NCOP2 Tools	TIMS & Add-ins	NCOP2 Software
Altova MapForce					X
Angular					X
Antivirus					X
GeoServer					X
Java Runtime Environment				X	X
JavaScript Libraries					X
PDF Reader					X
Vmware					X

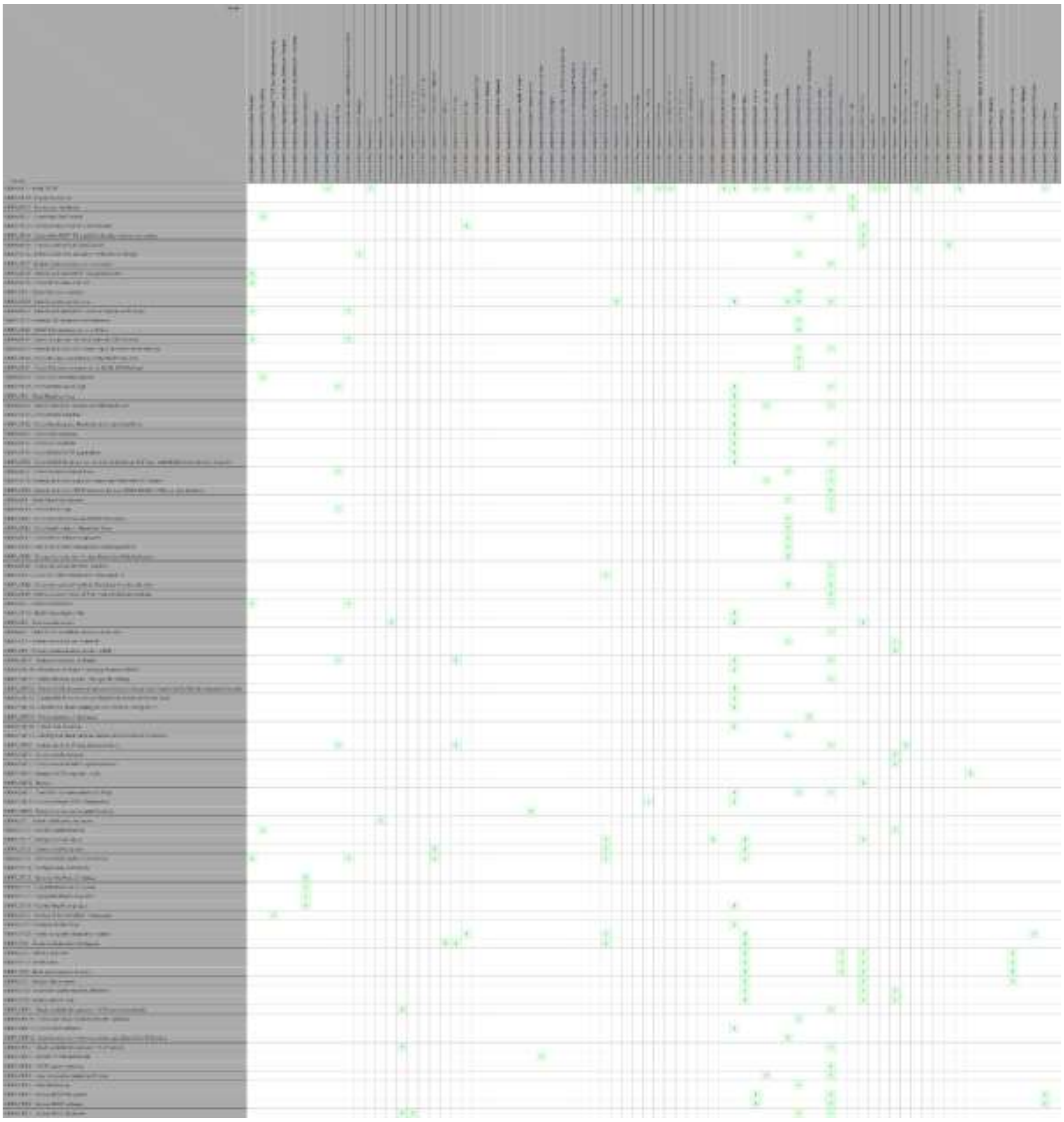


Microsoft .NET Framework			X		X
Microsoft BizTalk					X
Microsoft Edge	X	X			X
Microsoft Hyper-V					X
Microsoft Internet Information Server				X	X
Microsoft Office					X
Microsoft SharePoint					X
Microsoft SQL Server					X
Microsoft SQL Server Reporting Services					X
Microsoft Windows	X	X			X
Microsoft Windows Server			X	X	X
Active Directory					X
Chat					X
Core GIS					X
Document Handling System					X
Enterprise Management Service					X
Identity Provider					X
Informal Messaging					X
NEDS					X
NLB					X
Security Services and Settings					X

6.4 OPERATION AND MAINTENANCE TASK ANALYSIS (OMTA)

The list of all operation tasks, SM&C (Service, Management and Control) tasks, administrative tasks, corrective maintenance tasks and preventive maintenance tasks, are defined in the [ILSP] .

The following table, shows the Implementation Components associated to each OMTA Task (the complete redeable mapping is defined in the EAP file):



7 PHYSICAL VIEW

This section details the COTS software and hardware items required for NCOP Increment-2 deployments at the following NATO site types:

- XL for NATO Data Centre;
- HA for Mission Networks (e.g. MIR);
- SC for scalable but not mission critical environments;
- SN for non mission critical environments;
- AIO for testing or demonstration

7.1 NCOP DEPLOYMENTS

NCOP shall be deployed inside bunkers, offices, deployed environments, afloat and airborne platforms where the infrastructure is available to host NCOP Services. Networks include LAN and WAN (NGCS) environments.

The NCOP supporting hardware is installed and operates on Local Area Network (LAN) of a certain Security Domain (e.g. NATO SECRET, MISSION SECRET) part of each site infrastructure. This LAN is connected to the WAN through a specific NATO IP Cryptographic Equipment (NICE), allowing information exchange between these security domains through Information Exchange gateways (IEG) as appropriate;

Each site has its own technical infrastructure and that also comprises:

- Operators Workstations;
- Servers provided by the different Bi-SC AIS core services;
- Servers handling other contributing NATO systems for NCOP;
- Most sites (except training and visualization sites) will also have a Storage Area Network (SAN).

7.1.1 NCOP Nodes architecture principles

7.1.1.1 General principles

The general principles of the chosen architecture for NCOP Nodes are based on the use of dedicated virtualized servers for the most demanding Software COTS: Microsoft SharePoint, Microsoft BizTalk and Microsoft SQL Server. The number and type of servers will depend on the Node configuration.

1 or n servers dedicated to Microsoft SharePoint under load balancing;

1 or n servers dedicated to Geographical COP Editor under load balancing;

1 or n servers dedicated to NCOP services under load balancing;

Optionally: 1 or 2 servers dedicated to Dynamic IP Connectors under load balancing;

1 or 2 servers dedicated to Microsoft BizTalk under distributed installation;

1 or 2 servers in cluster hosting Microsoft SQL Server. An alternative consisting in the installation of SQL Server AlwaysOn Availability Groups is currently analysed.

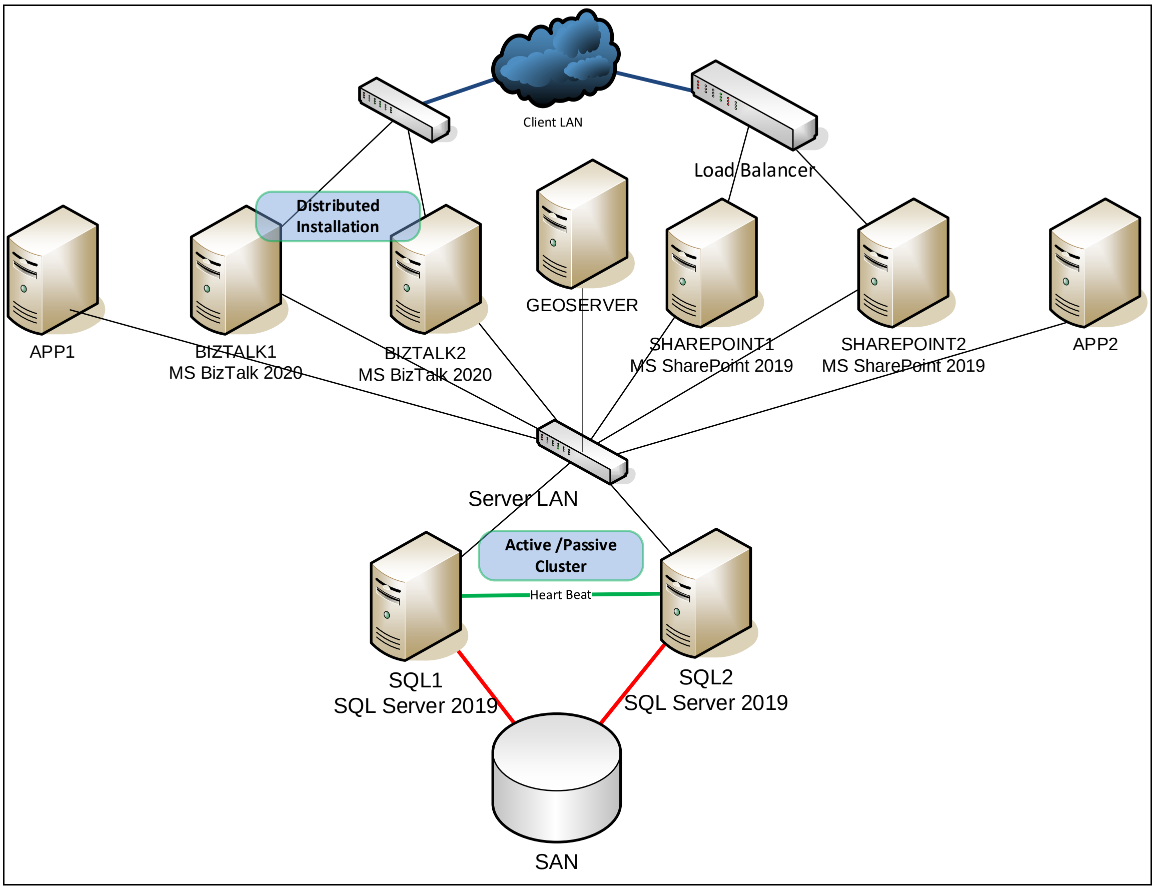


Figure 7-1: Generic NCOP Nodes Hardware Architecture Principles

All servers are hosted on Windows 2019 Server time synchronized through Network Time Protocol (NTP) in order to ensure time accuracy.

All Servers are reachable through DNS protocol.

These general principles allow NCOP system to be used for any type of activities: training, demonstration, exercise, static, deployed, mobile, civil or military locations, aircrafts or ships.

In particular, hardware and software choices made during the establishment allow the operation of NCOP system nodes in deployed sites to at least 3000 meters height above sea level.

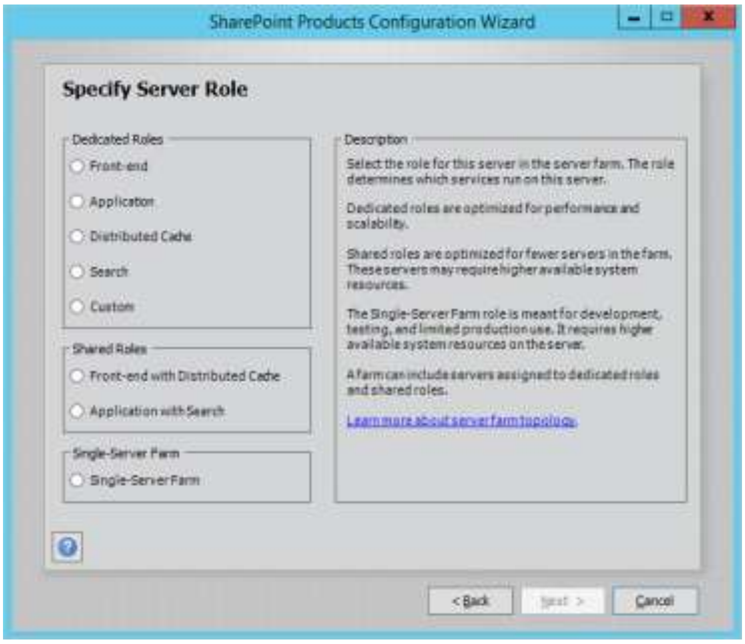
The solution maximizes Reliability, Availability and Maintainability (RAM) by the choice of redundant hardware/software servers and use Built In Test Equipment (BITE) at hardware level.

7.1.1.2 SharePoint roles

SharePoint is based on several server roles:

- Application Server
- Web Front End Server
- Search Server
- Distributed Cache
- Custom

As illustrated below, the role has to be chosen, on installation phase, in the SharePoint installation wizard:



Specify Server Role

Dedicated Roles

○ Front-end

○ Application

○ Distributed Cache

○ Search

○ Custom

Shared Roles

○ Front-end with Distributed Cache

○ Application with Search

Single-Server Farm

○ Single-Server Farm

Description

Select the role for this server in the server farm. The role determines which services run on this server.

Dedicated roles are optimized for performance and scalability.

Shared roles are optimized for fewer servers in the farm. These servers may require higher available system resources.

The Single-Server Farm role is meant for development, testing, and limited production use. It requires higher available system resources on the server.

A farm can include servers assigned to dedicated roles and shared roles.

Learn more about server farm topology.

Figure 7-2: SharePoint 2019 Server roles

In NCOP Increment-1 the deployment of SharePoint Servers was based on a Two-Tier Farm:

- Web Tier: All Web and application server roles
- Database Tier

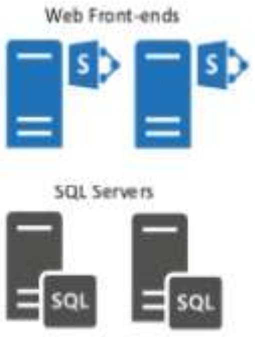


Figure 7-3: SharePoint topologies: Two-Tier Farm,

In NCOP Increment-2 the deployment of SharePoint Servers will be based on several topologies:

- A Two-Tier Farm (Limited number of users)
    - Web Tier: All Web and application server roles
    - Database Tier
- Three-Tier Farm (Large number of users)
    - Web Tier
    - Application Tier
    - Database Tier

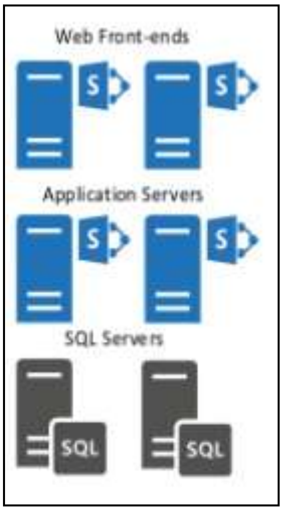


Figure 7-4: SharePoint topologies: Three-Tier Farm,

Many other topologies are permitted in SharePoint:

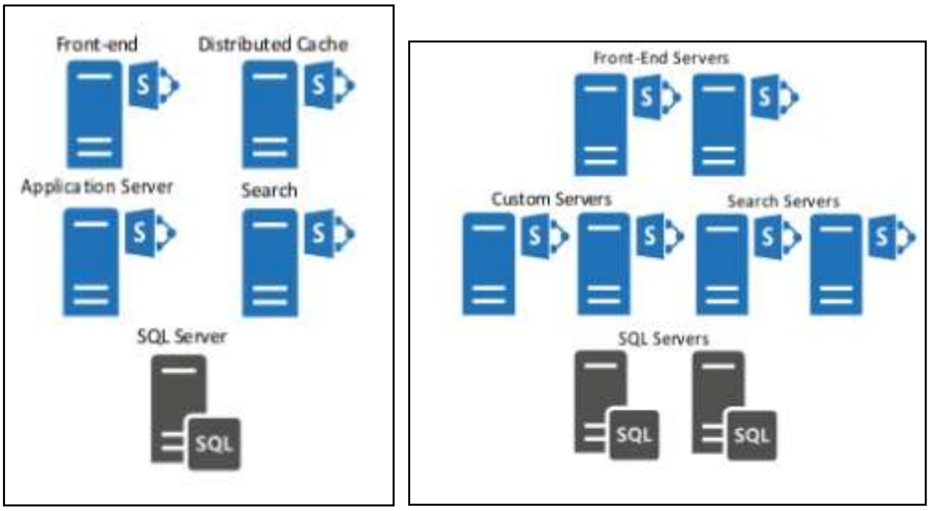


Figure 7-5: SharePoint topologies,

The main SharePoint server roles are described in the following sections.

SharePoint “Web Front End” Servers

Web Front End (WFE) servers form the connection point for clients that request content or services from SharePoint. Every request from a client is directed to a WFE server and every response to a client is sent from a WFE server. This means that all client requests place some load on WFE servers. A WFE server is responsible for:

- Processing incoming requests through IIS.
- Requesting any data from service applications and databases that are required to service the request.
- Processing the data returned by service applications and databases.
- Compiling responses as ASP.NET pages and sending the responses to the requestor.

In small farms (as in NCOP Increment-1), WFE servers often perform application roles in addition to the WFE role. WFE servers do not require large quantities of disk storage; instead, they rely heavily on processor power and memory for performance.

To improve the performance of page rendering and client access, it is necessary to add more WFE servers to the farm and implement network load balancing and request management.

SharePoint “Application” Servers

By default, the server that hosts Central Administration, in a three-tier farm (“Web Front End”, “Application” and “Database”), is an Application Server. We can add Application Servers to host services that can be deployed to a single server and used by all the servers in a farm. Services with similar usage and performance characteristics can be logically grouped on a server and if it is necessary, hosted on multiple servers if a scale out is required to respond to performance or capacity requirements.

Application Servers host service applications. We can distribute service applications among the servers in our server farm to manage load. The specific hardware demands imposed by service applications vary both by the type of service application and by how the service application is used. However, as a general rule, service applications do not require disk space on the Application Server; instead, they may impose significant processor and memory demands.

SharePoint “Search” Servers

The search service application can add significantly to the resource requirements of a SharePoint server farm. Although the components of the search service are technically the responsibility of Application Servers, many large SharePoint deployments use dedicated servers to run components of the search service. Since SharePoint 2013, the search service consists of the following major components:

- **The index component**: The search index is divided into one or more index partitions. Each partition stores part of the search index as a set of files on disk. Index partitions can be allocated (and replicated) across individual servers in a server farm. The index component writes index items received from the content processing component and issues result sets to the query processing component. The index component can place high demands on memory and disk input and output (I/O).
- **The query processing component**: The query processing component receives search requests from a WFE server. It processes the request and sends it to the index component, which returns a result set. It then processes the result set and returns it to the WFE server as search results. Typically, the query processing component places high demands on memory and processor power.
- **The search administration component**: The search administration component manages the processes and timer jobs that underpin the search service. In isolation, the search administration component does not place heavy demands on hardware.
- **The crawl component**: The crawl component browses content sources on a scheduled basis and provided crawled content, together with any associated

metadata, to the content processing Component. The crawl component places very heavy demands on the available processor power and consumes a large amount of I/O bandwidth.

- **The content processing component**: The content processing component receives content and Metadata from the crawl component. It transforms the crawled items into index-ready items, for example by parsing documents and mapping crawled properties to managed properties. Typically, the content processing component places high demands on memory and processor power.
- **The analytics component**: The analytics processing component analyzes crawled items and how the search service is used. It writes the results of this analysis to the analytics reporting database. The analytics component can place high demands on memory and processor power and it consumes significant I/O bandwidth. Each of these components can be allocated to one or more Application Servers in the server farm.

7.1.1.3 NCOP configurations

The following figure illustrates the SN configuration:

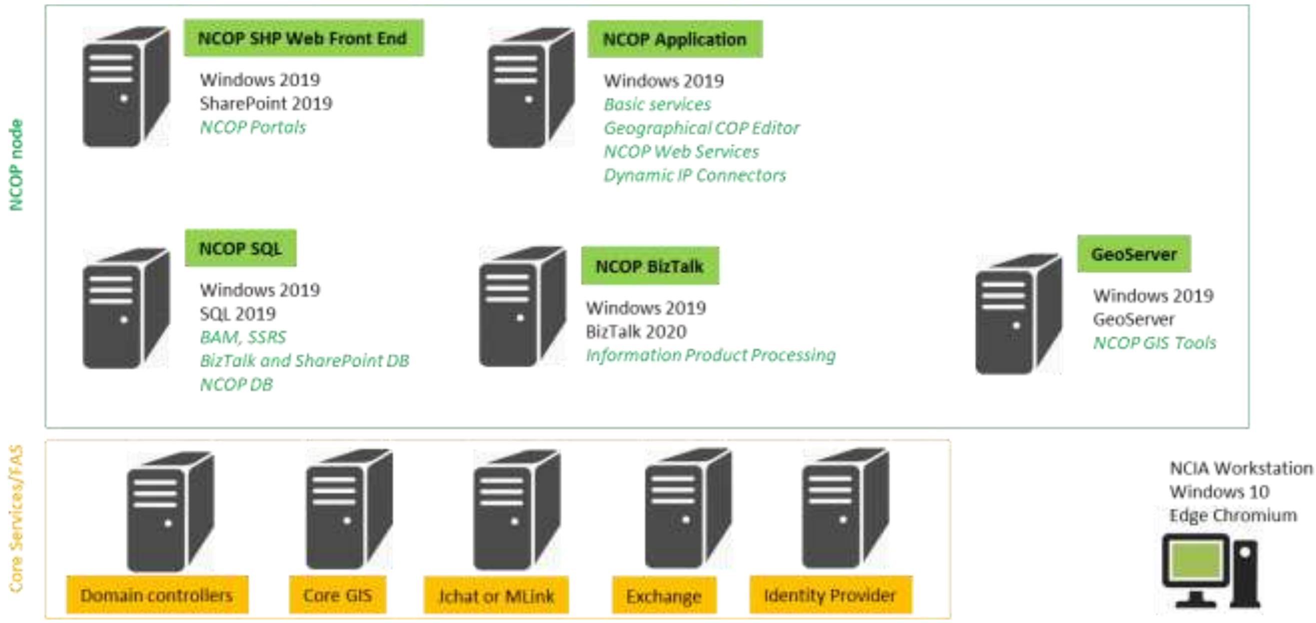


Figure 7-6: SN Configuration

The following figure illustrates the HA, SC, XL configuration:

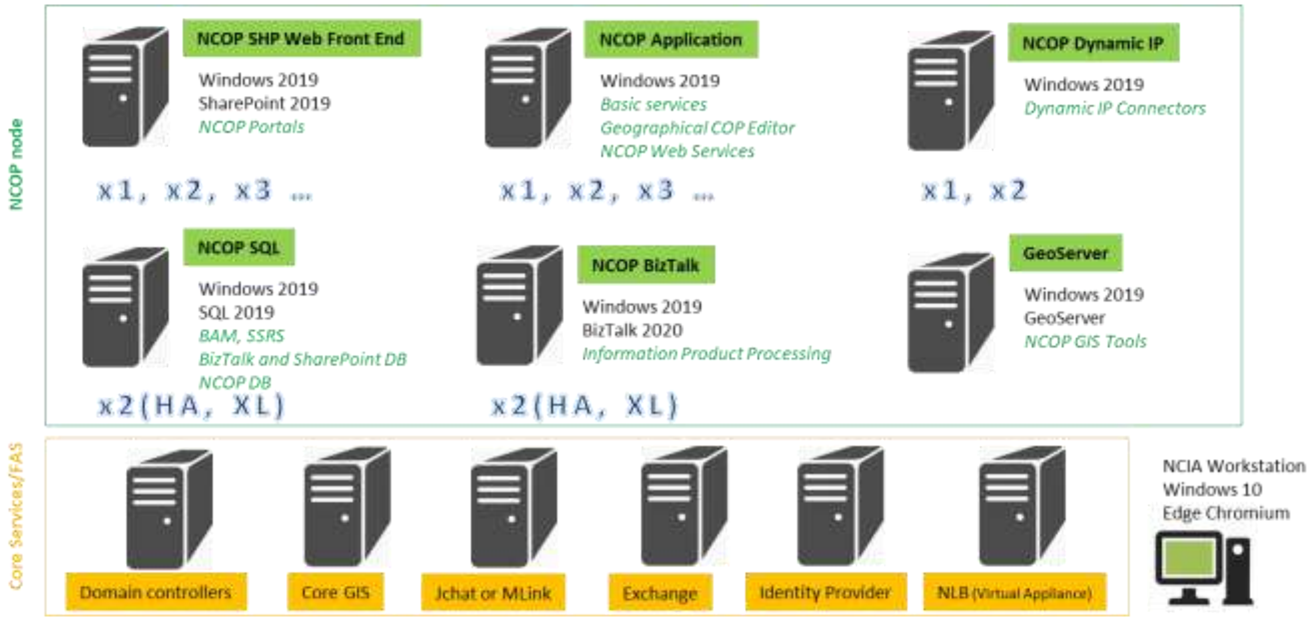


Figure 7-7: HA, SC, XL Configurations

The HA and SC are closed configurations.

The XL configuration will integrate ITM constraints that needs to be consolidated.

Based on these general principles, five main configurations have been designed for the needs of the different NCOP sites types:

Configuration XL (Extra Large): composed of a minimum of 9 virtual servers (**n** SharePoint, 2 SQL, 2 BizTalk Servers, **m** NCOP Application, 1 GeoServer); optionally, 2 other virtual servers can be dedicated to the NIRIS connector.

Configuration HA (High Availability): composed of 9 virtual servers (2 SharePoint, 2 SQL, 2 BizTalk Servers, 2 NCOP Application, 1 GeoServer); optionally, 2 other virtual servers can be dedicated to the NIRIS connector.

Configuration SC (Scalable): composed of a minimum of 7 virtual servers (**n** SharePoint, 1 SQL, 1 BizTalk Server, **m** NCOP Application, 1 GeoServer); optionally, 1 or 2 other virtual servers can be dedicated to the NIRIS connector.

Configuration SN (Single Node): composed of 5 virtual servers (1 SharePoint, 1 SQL, 1 BizTalk Server, 1 NCOP Application, 1 GeoServer); optionally, 1 other virtual server can be dedicated to the NIRIS connector.

Configuration SCC (SCC Node): composed of 1 virtual server (1 NCOP Application);

Configuration All-In-One (All-In-One Node): composed of 1 virtual server; It includes SharePoint, SQL, BizTalk Server, NCOP Application, GeoServer in a same VM. This configuration is not intended to be used in an operational site.

Hardware and software licences provided within these different configurations allow the use of NCOP system in any NATO context: exercise, mission, static and deployable commands, NATO Response Force (NRF).. All software licences are not restricted in terms of volume users (whatever the type of Configuration Node as detailed in section 7.1.2), information elements stored or exchanged nor limited in terms of time, duration and location of usage.

The architecture of NCOP is flexible enough to allow the deployment on limited hardware configurations. For example if NCOP must be installed on a site where few users will connect and with a limited number of COPs and information products, it is possible to deploy NCOP on a single server (physical or virtual). However, precautions must be taken during the installation to ensure that different network ports will be used by each component.

Note that Hardware and Software are designed to be installed and run by NATO resource only (access rights).

7.1.1.4 Virtualization

The NCOP architecture allows installing a NCOP Node on physical servers or virtualized servers.

NCOP technical solution is compatible with NATO’s main virtualisation solution based on VMware ESX and is also compatible with the Microsoft Hyper-V solution.

The following figure illustrates the NCOP virtual servers hosted by Hyper-V and stored into the SAN as files.

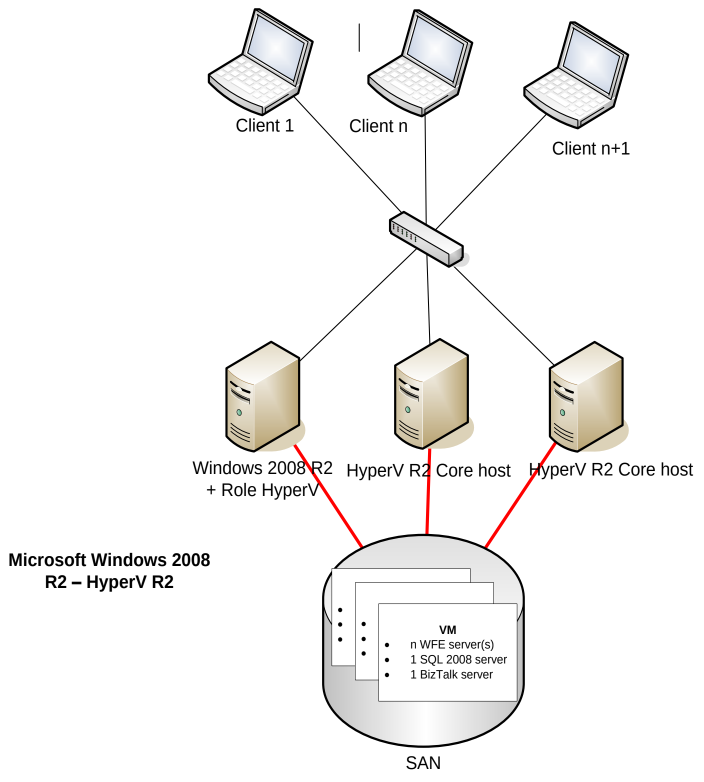


Figure 7-8: Virtualized NCOP Nodes Hardware Architecture

This solution features interesting points such as:

- Small footprint and minimal overhead on servers;
- Easy migrations through Live/Quick Migration features;
- Easy integration in the designed target architecture.

The software / hardware redundancy of NCOP infrastructure services (Microsoft BizTalk ESB, Microsoft SharePoint EDMS and Microsoft SQL Server RDBMS) together with SAN persistency also allows smooth and seamless integration update of any software / hardware component for maintenance or upgrade purposes.

Furthermore, the choice of COTS and technologies made when establishing the NCOP system software architecture solution ensures:

Restart and full recovery from hardware and / or software failure within 3 minutes;

Reconfiguration to follow changes in mission architecture in-near-real-time;

A level of repair for NCOP system hardware in the limits of the NATO Line-Replaceable Unit (LRU);

Virtualisation infrastructure can also provide natively failover and load balancing capabilities. This can be an alternate failover/load balancing solution that could possibly be used if the deployment site offers the appropriate infrastructure.

7.1.2 Recommended Hardware configurations

Not applicable

7.1.3 Recommended virtual server configurations

The following table presents the recommended technical requirements for NCOP hosting servers deployed as virtual machines:

TABLE 7-1: RECOMMENDED TECHNICAL REQUIREMENTS FOR NCOP SERVERS

Server name	Operating system	vCPU	RAM
SharePoint-WFE	Windows 2019 Standard	8	16 GB
BizTalk Server	Windows 2019 Standard	4	8 GB
SQL Server	Windows 2019 Standard	8	32 GB
Application Server	Windows 2019 Standard	4	16 GB
GeoServer	Windows 2019 Standard	4	8 GB

These recommendations are based on the various platform configurations that have been used during NCOP development and integration phases.

For all servers, more vCPU and memory may be required depending on the number of Sources and Information Products to be acquired (impacting BizTalk, SQL and SharePoint) and also depending on the number of NCOP users (impacting SharePoint SQL servers).

7.1.4 Recommended storage configuration

7.1.4.1 Storage sizing

The following table presents the recommended storage configuration for each server:

TABLE 7-2: RECOMMENDED STORAGE CONFIGURATION FOR NCOP SERVERS

Server name	Storage requirements	Content
SharePoint-WFE	260 GB	• COTS installation • Log files • Temporary data (including COP archives)
BizTalk Server	240 GB	• COTS installation • Log files • Temporary data
SQL Server	The minimum required disk size is 1.6 TB split as follow: • C: System 80 GB • D: Data 80 GB • E : Logs 80 GB • F: Biztalk_Data 300 GB • G: Biztalk_Logs 80 GB • H: Biztalk_Temp 10 GB • I: Sharepoint_Data 300 GB • J: Sharepoint_Logs 80 GB • K: Sharepoint_Temp 10 GB • L: Common_Data 300 GB • M: Common_Logs 80 GB • N: Common_Temp 10 GB • O: **History_Data *** • P: History_Logs 80 GB • Q : History_Temp 10 GB • R BizTalk Maintenance 100 GB	• COTS installation • Log files • Data ○ SharePoint data, ○ BSO Search, ○ BSO History
GeoServer	200 GB	• COTS installation • Log files • Map data

* The **History_Data** storage size depends on, the number of connected sources (external interfaces), the frequency of data update and the duration of archiving as explained below.

The storage requirements for SQL Server are the result of an analysis based on the following hypotheses:

First of all, the storage required for NCOP depends on the number of Sources and Information Products being declared on an NCOP node.

Three different configurations are being considered:

- Small: About 5 connected sources or 30 Information Products (the number of BSO is less than 10.000 ; equivalent to a training configuration)
- Medium : About 15 connected sources or 75 Information products (the number of BSO is less than 40.000 ; equivalent to the Representative COP content as described in the SRS)
- Large : About 40 connected sources or 150 Information Products (the number of BSO is less than 100.000 ; equivalent to the actual ISAF COPs configuration)

The second parameter to be taken into account is the Information Product update frequency set by the COP Manager for each Information Product For our calculation, we evaluate the average update frequency as: every 10 minutes.

The third parameter to be taken into account is the persistence archiving duration parameter value set by the COP Manager when the BSO history feature has been activated by the COP Manager.

The average weight of a BSO in terms of storage in the NCOP infrastructure has been estimated to:

- 14 kB for each BSO in CDF format Information Product storage (7 kB) and original format Information Product storage (7kB)
- 15 kB for each BSO in the BSO Search storage
- 8 kB for each BSO in the BSO History storage

Considering the parameters described above, the following estimations can be proposed for the CDF format Information Product storage, original format storage and BSO Search:

Configuration	**Maximum BSO SharePoint Storage** = BSOs weight * BSOs number *100	**BSO Search Storage** =BSOs weight * BSOs number
Small	**14 GB**	**150 MB**
Medium	**56 GB**	**600 MB**
Large	**140 GB**	**1.5 TB**

Note that the storage volume remains constant across time because:

- NCOP proposes to limit the number of successive versions stored in SharePoint to 100 (one hundred),
- The BSO Search database only contains the latest version of each BSO regardless of the Information Product update frequency.

Considering the parameters described above, the following estimations can be proposed for the BSO History storage:

Configuration	**Historic database size** = BSOs weight * BSOs number	**Historic database size per day** (with an update every 10 minutes) = Historic database size * 24 * 6	**Historic database size per month** **=** Historic database size * 30
Small	**80 MB**	**12 GB**	**360 Go**
Medium	**320 MB**	**44 GB**	**1.3 TB**
Large	**800 MB**	**120 GB**	**3.6 TB**

It is important to note that these estimations are for information only because they are made on the assumptions that every Information Product is configured as data-driven, with the same update frequency parameter and that BSO History has been activated for all Information Products.

7.1.4.2 SAN availability

NCOP recommends the use of a SAN infrastructure to store NCOP data. As it has been confirmed during site surveys, it may happen that the deployment site has no SAN available (no disk space left or no SAN infrastructure at all).

If no SAN is available on a site, NCOP can use local hard disk drives instead. It has been taken into account in the installation packages and documentation of NCOP. It only requires that:

- Additional local hard disk drive be provided for the hosting physical servers
- Partitions and/or logical drives be created on the hosting logical servers

It has to be noted that a SAN infrastructure usually integrates native backup solution for the stored data. If no SAN can be used, the backup method and strategy may be different.

7.1.5 NCOP network ports

NCOP requires that network ports be opened between NCOP hosting servers to allow communication between NCOP services (for example BizTalk communicating with SharePoint).

NCOP also requires that network ports be opened between NCOP hosting servers and NCOP consumers (to allow consumption of NCOP services from COP Users).

Multiple NCOP web sites are exposed to provide access to NCOP user interfaces and services. They are organized as follows:

Site URL	Port	Content description
https://[ncop-operational].domain	443	NCOP web portal for the operational environment
https://[ncop-operationalservices].domain	443	NCOP web services for the operational environment
https://[ncop-training].domain	443	NCOP web portal for the training environment
https://[ncop-trainingservices].domain	443	NCOP web services for the training environment
https://[ncop-exercise].domain	443	NCOP web portal for the exercise environment
https://[ncop-exerciseservices].domain	443	NCOP web services for the exercise environment
https://[ncop-commonservices].domain	443	NCOP common web services for the 3 environments (e.g. Dynamic Source Server)

These ports are the default configuration. They can be reconfigured manually by an authorized user at runtime if required.

The web site server name and domain is dependant of the deployment environment.

The list of required ports to be opened is detailed in the NCOP SSDS.

7.1.6 NCOP installation

NCOP installation process is described in full details in the NCOP Installation manual.

The sub-chapters present an overview of the following aspects:

- Main installation steps
- Installation options
- Relations between NCOP CSCIs and installation packages

7.1.6.1 Main installation steps

The main installation steps that have to be followed in order to install and configure NCOP are the following:

- Infrastructure preparation
  - Operating system installation
  - COTS installation
  - Environment preparation (services accounts, DNS entries, …)
- NCOP software installation
- NCOP software configuration
  - Roles initialization
  - Synchronization configuration
  - ….

7.1.6.2 Installation options

Provided installation packages and documentation take into account the various deployment modes that can be applied:

- Basic mode (SN node)
- Intermediate mode (SC node) (including load balancing)
- High-availability mode (HA, XL nodes) (including load balancing and failover)

The required target site configurations are taken into account:

- Basic mode (SN node): 5 servers configuration
- Intermediate mode (SC node): minimum 7 servers configuration
- High-availability (HA, XL nodes): minimum 9 servers configuration

In addition to those required target configurations, NCOP installation packages and documentation can be applied to other configurations with a different number of hosting servers: as described in chapter 5.3.5.7, a physical or virtual server can host multiple NCOP services and therefore allows NCOP to be installed on configurations with one servers: All-In One (AIO) node.

7.1.6.3 Relations between NCOP CSCIs and installation packages

The following table presents the distribution of NCOP CSCIs in the NCOP installation packages.

TABLE 7-3: NCOP CSCI DISTRIBUTION IN THE NCOP INSTALLATION PACKAGES

	NCOP-SQL-Deploy	NCOP-SHP-Deploy	NCOP-BIZ-Deploy	NCOP-Maps-Deploy	NCOP-APP-Deploy	NCOP-SCC-Deploy	NCOP-SCC-OP-Deploy	NCOP-CBT-Deploy	NCOP-OLH-Deploy	NCOP-DYN-Deploy
NCOP2 Software	x	x	x	x	x	x	x			x
On-Line Help (*)									x	
Computer Based Training (CBT) (*)								x		
NCOP2 Tools (**)										
TIMS & Add-ins					x	x	x			
COTS Software	-	-	-	-	-	-	-	-	-	-

(*) These CSCI are delivered in integrated mode (included in the corresponding installation package) and in standalone mode (delivered separately on the installation media)

(**) These CSCI are delivered in standalone mode only and are not part of an installation package (delivered separately on the installation media).

7.2 PERFORMANCES

NCOP performance will be compliant with the performance requirements described in §4.1.2 and §4.1.4 of SRS.

7.2.1 Network Consumption

NCOP architecture is designed to optimize network utilization, thereby minimizing the impact of the available bandwidth and latency of information retrieval. The minimum performance characteristics required for NCOP are as follows:

For exchange between NCOP hosting servers and other NATO servers on a local-area network: 100Mb/sec;

For LAN workstations: at least 256 Kb/sec;

For cases involving WAN connection to remote workstations: at least 512 Kb/sec and latency less than 1 second (s).

The provision of sustained high performance levels that minimizes bandwidth utilization and latency impacts has been a key driver of the design of the solution.

Main network bandwidth optimizations that are implemented for NCOP:

Favour the use of low bandwidth transport protocols such as HTTP, REST or SOAP;

Rigorously check HTML pages size during project development and ensure that average page size does not rise over 100 Kbytes;

Systemically use compression for HTML pages;

Use image titling to reduce the size of files transferred across the network;

Plan usage of WMS and WFS services in order to optimize the size of network transferred maps;

Reduce network exchange between server and browsers by developing HTML5 application running into the web browser (using AJAX-JavaScript or Angular technologies);

Reduce network exchange of large sized information elements by caching at server and workstation levels:

- Caching of JavaScript libraries, map and image tiles at workstation level;
- Web browser is configured to maintain libraries from the NCOP services in the browser cache. Libraries are loaded at the first User connection so future connections do not need to load them;
- Geographic views and image processing inside the web browser execute dedicated OpenLayers libraries that perform caching functionalities for map and

image tiles. Libraries allow caching of tiles residing on the NCOP cartographic server or core GIS server which has been requested by a User on the workstation. A subsequent request by a second User, or the same User running a second session, can access the cached title directly from the workstation without requiring a second server access;

Reduce the footprint and overhead induced by the exchange of large size information elements by encoding/compression means that can be activated in the WCF SOAP stack of .NET 4.0 Framework:

- Use of Text Encoding;
- Use of Binary Encoding;
- Use of Message Transmission Optimization Mechanism (MTOM), which is a good trade-off between the efficiency and the versatility of Text Encoding and the rapidity of the Binary Encoding;

Caching of NCOP data and preview files at server level:

- The NCOP services can maintain in cache, any NCOP data retrieved from a distant node following a request by a User on the local node. Subsequent requests for the same product by any other local User access the cached product directly without requiring a second network access;
- The NCOP services can also maintain in cache, preview files of any data (local and remote) that has been created when requested by a User. Any other User on the same local node, subsequently looking at the same product, can automatically access the cached preview and does not require new preview generation; and note that when an NCOP data is updated or removed, NCOP services automatically notify servers at other nodes to clear preview and products cache.

Optimizing network exchange mechanisms between NCOP organizational nodes and external systems:

- Administration tools allow data replication mechanisms to be configured depending on the network capabilities: authorized configurations start from replicating only metadata of a small number of data types up to replication of full range of attributes and relationships;
- External system watchers can also be configured in order to take account of the network capabilities. For instance, administrators can set the frequency of polling external system for updates;
- Provide compression services.

Reducing latency impacts:

- Careful management of timeout disconnections at server level;
- Favour development of web applications that do not require session management;
- When sessions or transactions are needed, favour use of data exchange based on standard HTTP protocol where web browser sends information into the URL and receives results inside standard HTML pages.

7.2.2 System Scalability

The Hardware architecture lies on basic principles (described in §7.1.1) allowing scalability and growth potential:

Vertical scalability, through specialized COTS S/W hosting servers, for Microsoft SharePoint (web application platform), Microsoft BizTalk (ESB) and Microsoft SQL Server (Database);

Horizontal scalability, through deployment of more than one server per capability for load balancing and scaling according to the type of node.

The choice of servers has been done on a basis of users and usage so as to support extension of the system as required in the SRS.

In NCOP, load balancing can be provided for following aspects

- Data access
- Data processing

7.2.2.1 Load balancing for data access

Regarding data access, NCOP can provide load balancing by using a network load balancing solution. This mechanism will take care of redirecting client requests to one of the servers that has been configured to be part of the network load balancing cluster. This load balancing solution applies to the NCOP portal component and to NCOP Web services. For the NCOP portal components to work with network load balancing the SharePoint servers have to be configured as a single SharePoint farm.

The network load balancing mechanism proposed by NCOP is based on PulseSecure Traffic Manager software (preferred) or the Microsoft NLB capability. This capability offers a lot of flexibility regarding how client requests will be redirected. Redirections can be configured per network port and redirection rules can be set up by declaring (automatically or manually) the overall percentage of requests that will be handled by a server. It is also possible to define an affinity between a client and a server in way that once a server received a client request, all subsequent requests will be automatically redirected to that same server.

The following figure presents a sample configuration where a weight as been manually set for each server according to their processing capabilities:

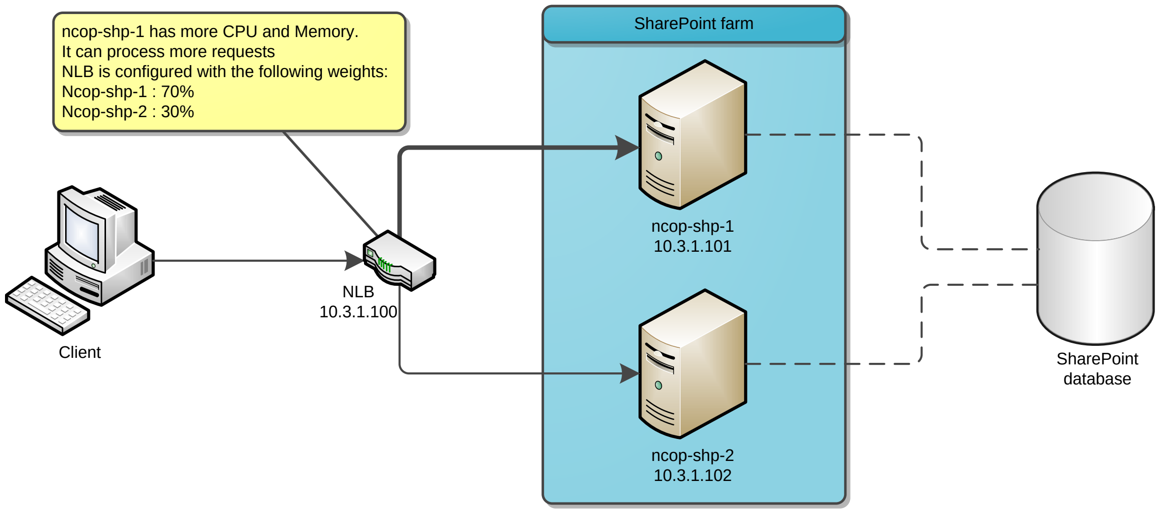


Figure 7-9: NLB deployment scenario

Another alternative for load balancing would have been the use of Round Robin DNS but the NLB solution is also able to provide a failover capability: if one NLB cluster server is down, incoming requests will be redirected to online servers only.

7.2.2.2 Load balancing for data processing

To provide load balancing for data processing, NCOP requires the use of multiple BizTalk Servers configured as part of the same BizTalk Group. This BizTalk group concept allows multiple BizTalk servers to agree together on which server will execute a certain process. It means that if an orchestration is initiated by a particular server, some steps of the orchestration can be executed by other servers. Such behaviour is possible because BizTalk servers in the same BizTalk Group share the same configuration database and messages processed are stored regularly with their associated execution context in the message box.

Before an orchestration is executed, the BizTalk Group determines the most appropriate server to execute the process, taking into account the activity and workload of all the servers in that Group.

Also, if a BizTalk server crashes during the execution of an orchestration, the BizTalk Group will ask another server to re-execute this orchestration. The chosen server will then retrieve the message that was being processed (and associated execution context) and continue the execution of the orchestration where it was stopped.

7.2.3 System availability

7.2.3.1 Hardware availability

NCOP is designed to avoid Hardware SPoF (Single Points of Failure).

NCOP software is installed, run, and managed on duplicated physical servers (see §7.1.1.1) using network balancing and clustering. Availability of NCOP services is maintained in the event that one of the physical servers fails, with no significant impact on already connected users.

In terms of SLA, the NCOP system is compliant with the requirements of the SRS (30 days availability, non-availability time and availability interruption duration).

7.2.3.2 Data availability

The data availability is secure by the usage of a Backup Agent component. This component is the COTS (latest patches) product for backup and restores data maintained in the NCOP hosting servers.

Using the component the System Administrators are able to:

Perform full and incremental backups of NCOP data and software without impacting system availability;

Backup and archiving of both complete NCOP Repository or selected entities, possibly on transportable media;

Archive data that is not currently required in order to reduce the number of records to be maintained;

Perform a full backup of all or selected NCOP data automatically at a configurable frequency (e.g. every 24 hours).

All NCOP data and configuration is stored in Microsoft SQL Server:

- BizTalk database
  - BizTalk settings,
  - BizTalk BAM configuration and storage,
  - BizTalk data flow configuration and processed data
- SharePoint database
  - SharePoint Sites configuration
  - Document libraries and lists definition and contents
    - NCOP information elements
    - User settings
    - User feedbacks
- NCOP common database
  - Users and Roles management
  - Synchronization settings
  - Events management data
  - Alert/Notification settings and data
- NCOP history database
  - BSO History data
  - BSO Search data
  - Users layers
  - Users icons

Also, the cartographic server provided with NCOP contains:

- Map data
- Map Services configuration

Therefore, in order to allow the recovery of an NCOP node, it is required that the Backup Tool backup the following elements:

- NCOP SQL Databases (NCOP Storage);
    - SharePoint Database;
    - NCOP common Database;
    - NCOP history Database;
    - BizTalk SQL Database;
- GeoDatabase hosted by NCOP GeoServer Server;

The NCOP System Administration Manual describes in more details the elements to be backed up. In addition, the system administration manual describes multiple recovery scenarios depending on the failure type.

The detailed description of the databases content is provided in Appendix M Databases Diagrams.

7.2.3.3 Network availability

NCOP Architecture is designed to maintain full system availability when network performances fall up to a bandwidth of 512 kbps and latency is up to 1100 milliseconds (ms).

In case of LAN failure, NCOP hosting servers continue to perform all non-networked functions, e.g. consistency and security checks of data stored on NCOP hosting servers. See details on §5.4.20 NCOP behaviour in degraded mode.

If WAN connectivity is unavailable, the NCOP node continues to perform all functions that do not require WAN connectivity, such as maintenance of local information, administration of local systems and local data dissemination. In particular NCOP will preserve existing data, objects and products following the loss of any components and/or services of the Bi-SC AIS on WAN level. Availability of these data, objects and products is subject to the dependency of underlying COTS to critical Bi-SC AIS Core services (e.g. Active Directory).

NCOP hosting servers automatically detect the availability and re-establishment of network connectivity and automatically continue or restart tasks that were ongoing at the time a failure occurred, and initiate subsequent tasks as though network connectivity had not been lost.

From an end-user point of view, the layered architecture solution ensures that NCOP Users experience limited and controlled interruption of services. In particular, the loose coupled and asynchronous architecture of the NCOP system detects fall or loss of connectivity, allows NCOP Users to follow on a limited set of activities when disconnected and seamlessly restart working on the full set of functionalities when full connectivity is reached again.

7.2.4 Software performances

The choices made for architecture solution guaranties the following facts:

System start-up: All NCOP system functions are available in less than 5 minutes after the Microsoft Windows Server operating system is started. This is obtained through the controlled use of Microsoft COTS (SQL Server, SharePoint, and BizTalk) and a limited number of especially developed components;

System availability: The redundancy principles of the hardware and software architecture solution (see section 7.1.1.1) ensures that there is no software SPoF at least for the following mission functions:

- Native Information Product collection and acquisition from External System Information Product Provider Source Entities;
- COP dissemination from NCOP Entities Nodes;
- NCOP Nodes synchronization in the case of NCOP entities spread over several sites.

This availability is obtained through the following capacities:

- Microsoft SharePoint Load Balancer;
- Microsoft BizTalk ESB multiples Message Box configuration for high availability;
- SQL Server in cluster mode or SQLServer AlwaysOn mechanism..

End-user interface access and interaction: All NCOP functions are available through user interface in less than 5 seconds (for local users) and 10 seconds (for remote users) after the first access to the NCOP end-user web application. This assertion is valid for both Management and end-users functions and takes into account the authentication/authorization (RBAC) delays. These delays are guaranteed through the use of SharePoint Web Portal and the controlled use of especially developed WebPorts for local access plus network optimization for remote access;

Information elements exchanges: All exchanges that occur between native Information Product Sources Entities, NCOP entities or nodes, COP Users or contributors are triggered on change event (create/update/delete) on information elements and are compliant with the zero latency requirements. In the case of NCOP nodes synchronization the frequency of the exchanges results from a trade-off treatment between changes granularity and need for near real time exchanges (limited latency) between NCOP nodes spread over several sites;

Asynchronicity and loose-coupling: On the one side (server), NCOP business or service layers components are embedded within Microsoft IIS application server of Microsoft SharePoint Portal solution or integrated through BizTalk ESB adapters. On the other side (client), user interface layers components are built using Web 2.0 and HTML5 technologies. These architectural choices ensure both decorrelation and asynchronicity between each side and within server side components. For example, this guaranties that HTML5 code executed on client side NCOP system never waits for service invocation requests that may require performing time-consuming services;

Concurrency handling: All NCOP functions are based on MT-Safe, re-entrant COTS or especially developed software component capable to handle up to 25 concurrent access as well as invocation request, update events or messages per NCOP node.

Furthermore, both selected COTS (section 7.1.1.1) and the virtualized infrastructure (section 7.1.1.4) ensures the efficiency of the NCOP system architecture solution in terms of scalability.

In particular, it allows:

Its scalability to supports the five target information volume as described in the SRS:

- “Large” information volume;
- “Standard” information volume;
- “Reference” information volume;
- “Training” information volume;
- “Visualization” information volume.

In coherence with the “Large” Hardware Node Configurations user volume, it is also able to support up to 1000 concurrent active users on the same node.

Its initial dimensioning based on the use of scalable software component allows NCOP system software architecture to support increase in user and data volume of 10% for user volume and 25 % for data volume per year during five years without any loss in performance. In coherence with this last capacity and for the same reasons, the persistence layer is capable to support a increase in space needed for persistent information elements database of 20 % per year during five years.

Note that NCOP performances assessment is to be based on the performance scenario as described in the SRS (representative COP, baseline, regular and important load).

As explained in sections §5.4.7.2 and §5.4.7.3 BSOs are stored in relational database to allow better access performances for the following features:

- COP Wide Search
- BSO History
- Alerts based on BSO properties

Some frequently used web services, such as the NCOP IPS that provides Information Products Instances, are based on a cache mechanism. It allows data to be retrieved without systematic SharePoint access and allows simultaneous access by a large number of COP consumers. This cache is only updated when data is modified.

In order to identify performance bottlenecks in NCOP applications, the Redgate ANTS Performance Profiler Pro tool is used. It is useful for the Geographical COP Editor and it allows to:

- Drill down to slow lines of code with line-level timings
- Capture outgoing web requests
- Profile asynchronous code

The .NET Memory Profiler is used to find Memory Leaks and Optimize Memory Usage in NCOP .NET Programs.

CDF Information Elements are based on XML description and stored directly in XML format into SharePoint List attributes instead of using a relational database or a SharePoint model. It allows faster object retrieval when manipulating Information Element through web services and User Interface such as the Geographic COP Editor.

As explained in section §5.3.3.3.1.1.4 BizTalk acquisition of Information Product in pull mode is based on the Nato.NCOP.Scheduler component. It is able to launch simultaneous acquisition processes (one per Information Product). The number of simultaneous processes can be tuned to adapt the BizTalk behaviour according to the hosting infrastructure capabilities (disk speed, available RAM, available CPU …).

All software performances are dependent on hardware capabilities (disk speed for system and data in particular). This is especially the case when the NCOP software is hosted on virtualized environment.

7.2.5 Performance impact analysis

By design, the usage of NCOP depends on operational needs. The way NCOP is used and configured will change depending on the deployment context and configuration. NCOP do not impose any limitation but several aspects must be taken into account to understand their impact on NCOP overall performance.

The first aspect is the number of source and of associated Information Products. The more sources and Information Products are being declared in NCOP, the more BizTalk server will have to process incoming data, having an impact on the CPU and RAM usage of this server and the SQL server where the acquired data is stored.

The second aspect is the update frequency configuration defined for Information Products. Information Products being acquired with a high frequency will also have an impact on the CPU and RAM usage of this server and the SQL server where the acquired data is stored.

The third aspect to be taken into account is the activation of the BSO history feature. This feature can be activated per Information Product and it has a strong impact on both acquisition process and storage volume. Regarding the acquisition process, as for the previous aspects, the CPU and RAM usage on the BizTalk server and SQL server will be impacted. Regarding the storage volume usage, when this BSO history feature is combined with the Information Product update frequency parameter it can significantly increase the storage volume required by the accumulation of all successive version of each BSO that has been acquired. Despite the potential impact of this functionality, it is activated by default when an information product is created. When it is activated, the user must select an expiration duration to prevent the database from growing indefinitely.

All these three aspects also have an impact on the network because data acquisition is mainly using network connections (internal and external). Also even if it designed to minimize the network bandwidth usage, the synchronisation process between NCOP nodes might require additional bandwidth depending on the number of Information Products and the associated update frequency.

Finally, the last aspect to be taken into account is the number of users that are using NCOP for consuming COPs. This parameter has a significant impact on the performance of the NCOP map server (impact limited by the using of map tiling and browser cache), and eventually on NATO map servers, because the cartographic features are base functionalities used widely by all COP Users. The number of users also has an impact on the NCOP services parameters because COP and Information Products are based on these services. However this impact is limited by the implementation of server-side caches to optimize data access.

7.3 COTS

This paragraph details the specifications of the hardware and the software items exposed in the configurations above-mentioned.

7.3.1 COTS Hardware Configuration

This paragraph details the specifications of the hardware items exposed in the configurations above-mentioned.

7.3.1.1 NLB (Network Load Balancing)

The Hardware NLB that was planned for NCOP Increment-2 is unavailable. Two software appliances are identified for the NLB expected by SC, HA and XL NCOP configurations:

- The PulseSecure Traffic Manager software. Its is the preferred solution.
- The Microsoft NLB software (already used in NCOP Increment-1) will be used in case of unavailability of the PulseSecure Traffic Manager software.

7.3.2 COTS Software Configuration

The COTS version and latest release is defined prior to the development as part of the CDR (Critical Design Review).

7.3.2.1 Servers

The following table provides the COTS software configuration for all NCOP hosting server types (standard, large, deployable, etc).

Note: The COTS required to build the NCOP release are defined in the [SBI] (Software Build Instructions) document.

TABLE 7-4: COTS SOFTWARE CONFIGURATION FOR NCOP HOSTING SERVER

COTS Software Item Name	Version	Release	Manufacturer	Manufacturer part number	Provided by Contractor	Open source	Provided by Purchaser	SharePoint server	SQL Server	BizTalk server	GeoServer	Application Server
Microsoft Windows Server	2019 Standard		Microsoft				X	X	X	X	X	X
Microsoft .NET Framework	4.7.2 4.8		Microsoft		X			X	X	X	X	X
Microsoft .NET Core	5		Microsoft		X							X
OpenJDK	17 (for some sources acquired by BizTalk) 11 (for GeoServer)		Oracle		X	X				X	X	
GeoServer	2.20				X	X						
Microsoft SQL Server	2019 Standard / Enterprise (SQL-Server AlwaysOn)		Microsoft	7NQ-01599			X		X			
Microsoft SharePoint	2019		Microsoft	76P-02014			X	X				
Microsoft BizTalk	2020 Standard / Enterprise		Microsoft	D75-02484			X			X		

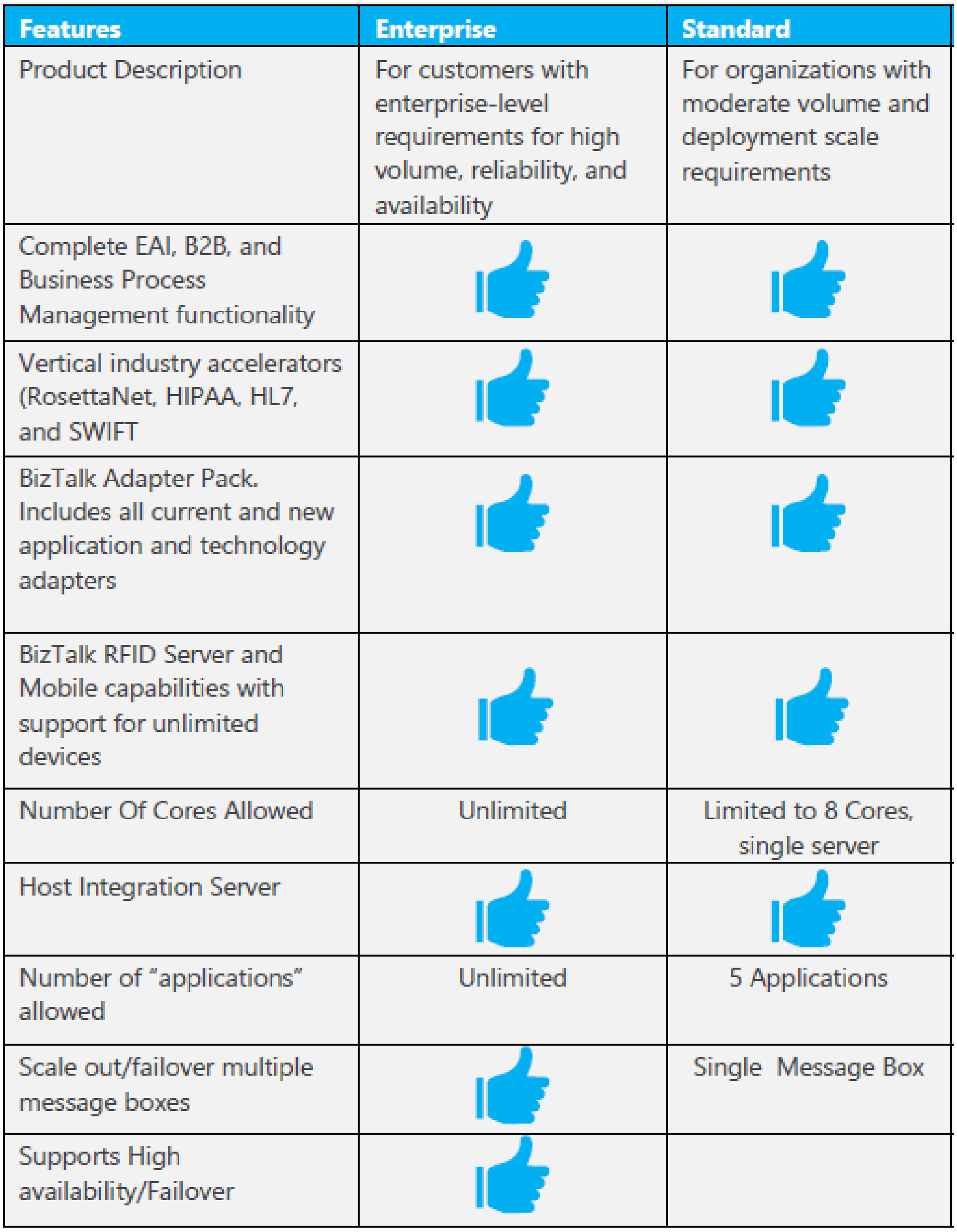
COTS Software Item Name	Version	Release	Manufacturer	Manufacturer part number	Provided by Contractor	Open source	Provided by Purchaser	SharePoint server	SQL Server	BizTalk server	GeoServer	Application Server
XMPP Adapter for BizTalk	2020	Latest	/n software				X			X		
EMAIL Adapter for BizTalk	2020	Latest	/n software				X			X		
REST Adapter for BizTalk	2020	Latest	/n software				X			X		
NCIRC GPO Security	2019						X	X	X	X	X	X

Microsoft BizTalk Server 2020 offers four editions:

- Enterprise Edition for customers with enterprise level requirements for high volume, reliability and availability
- Standard Edition for organizations with moderate volume and deployment scale requirements
- Branch Edition for hub and spoke deployment scenarios
- Developer Edition for testing and development use in conjunction with any of the above three editions.

NCOP can operate with any of Enterprise or Standard editions. However, using the Standard Edition of BizTalk is only possible for deployment configuration where high-availability is not required (i.e. Single Node or All-In-One)

Hereafter is a table that compares Enterprise and Standard editions (extract from Microsoft BizTalk Server Licensing Datasheet and FAQ available on the Microsoft web site):



Features	Enterprise	Standard
Product Description	For customers with enterprise-level requirements for high volume, reliability, and availability	For organizations with moderate volume and deployment scale requirements
Complete EAI, B2B, and Business Process Management functionality	👍	👍
Vertical industry accelerators (RosettaNet, HIPAA, HL7, and SWIFT	👍	👍
BizTalk Adapter Pack. Includes all current and new application and technology adapters	👍	👍
BizTalk RFID Server and Mobile capabilities with support for unlimited devices	👍	👍
Number Of Cores Allowed	Unlimited	Limited to 8 Cores, single server
Host Integration Server	👍	👍
Number of "applications" allowed	Unlimited	5 Applications
Scale out/failover multiple message boxes	👍	Single Message Box
Supports High availability/Failover	👍	

Figure 7-10: BizTalk server editions comparison

Regarding BizTalk usage in NCOP, the only difference that has an operational impact is the fact that Standard edition doesn't support high availability and failover. It means that the standard edition of BizTalk could be used only in configurations where only one BizTalk server is deployed. The operational impact is that if the BizTalk server is down, no Information Product can be acquired.

Necessary customization (by parameterization) of the off-the-shelf packages is described in NCOP Installation and Configuration Guide.

7.3.2.2 Workstations

Minimum hardware requirements for workstations:

Memory RAM: 4GB

Processor type: Core 2 Duo

Minimum resolution: 1280 x 1024

The following table provides the COTS software configuration for operator workstations.

The contractor assumes that workstations hardware and software will be provided by the purchaser (hardware and COTS software).

TABLE 7-5: COTS SOFTWARE CONFIGURATION FOR OPERATOR WORKSTATIONS

COTS Software Item Name	Version (minimum)	Release	Manufacturer	Manufacturer part number	Provided by Contractor	Open source	Provided by Purchaser
Microsoft Windows	10	Latest	Microsoft				X
Edge Chromium	94 minimum	Latest	Microsoft			X	X
Adobe Reader	DC	Latest	Adobe				X
Microsoft Office	2016/2019	Latest	Microsoft				X
Microsoft Windows Media Player	12	Latest	Microsoft				X

APPENDIX A REQUIREMENTS TRACEABILITY MATRIX

Traceability matrix between requirements and implementation components is provided as a separated Excel file (NCOP2 RIS - RTM - VCRM - User Stories) (tab: *SRS vs IC*):

- The first four columns identify paragraph numbering and titles, requirement identification and requirement text;
- The column L indicate how traceability information can be found. It gives the reference of a section within the current document where the requirement is addressed;
- The columns AA to EW (Traceability) define the allocation to the Implementation component(s) introduced in Chapter 5.3. For each requirement, a column contains a mark when the corresponding component is involved in the requirement;

Traceability matrix between requirements and configuration items is also provided in this Excel file (tab: *SRS vs CSCI*):

- The first four columns identify paragraph numbering and titles, requirement identification and requirement text;
- The columns W to AU (Traceability) define the allocation to CSCI. For each requirement, a column contains a mark when the corresponding CSCI is involved in the requirement;

Traceability between requirements and User Stories and Test Cases is also provided in this Excel file, thanks to 2 tabs which contain an export of the current traceability defined in Azure DevOps:

- Tab *SRS to US&TC* identifies the forward traceability linking the requirements to the User Stories and the Test Cases that cover the requirement. The indentation in the columns I and J materialize the link between the work items.
- Tab *US&TC to SRS* identifies the backward traceability linking the User Stories and the Test Cases to the requirements they cover. The indentation in the columns I and J materialize the link between the work items.

The User Stories are also provided in this Excel file (tab *User Stories (Product Backlog)*), as a hierarchical backlog including the Epics and Features. The content of this tab also results from an export of the current contents of the corresponding work items in Azure DevOps.

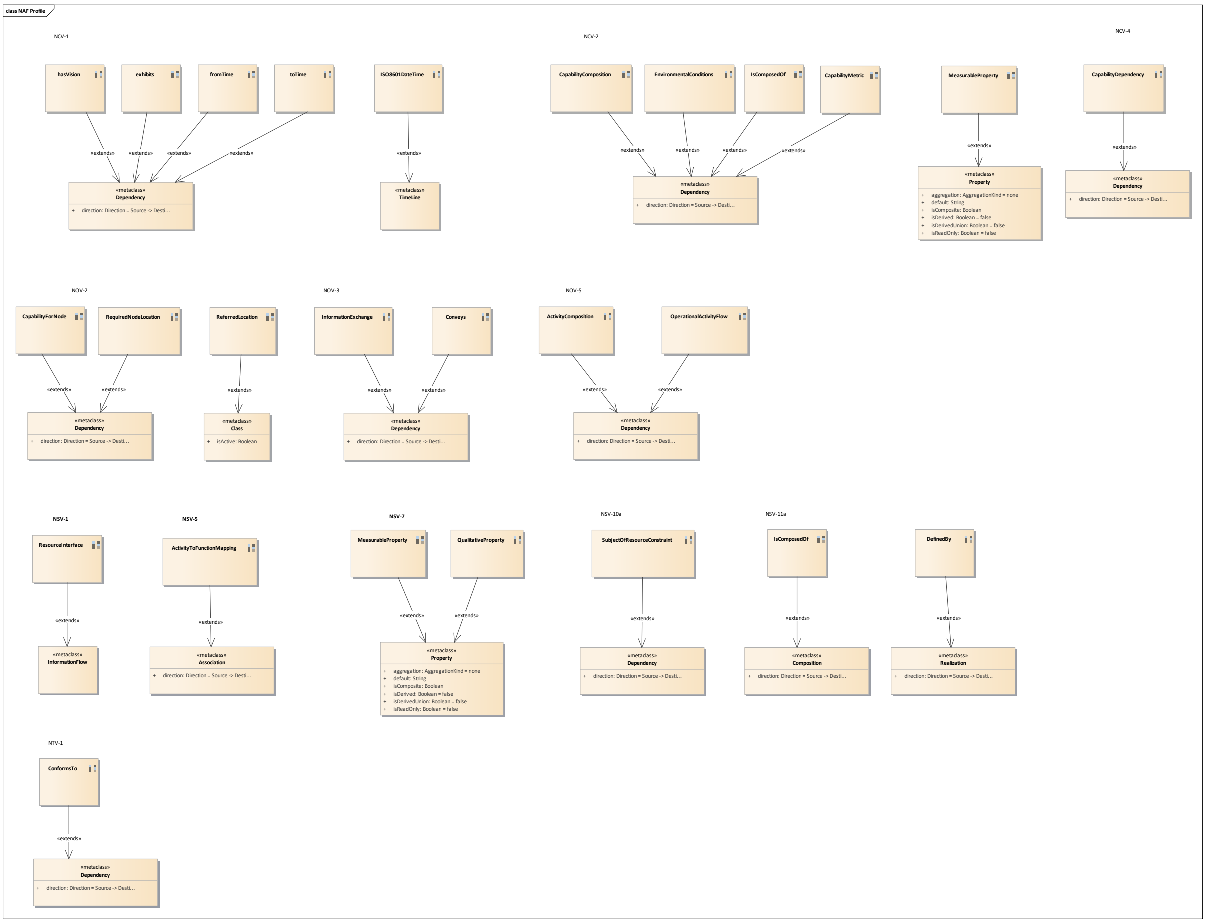
- The columns M and N respectively report the Description and the Acceptance criteria for the User Story
- The column O define the allocation of the User Story to the sprints. The value of “Product Backlog” marks unallocated User Stories.

APPENDIX B NAF V3.1 VIEWS

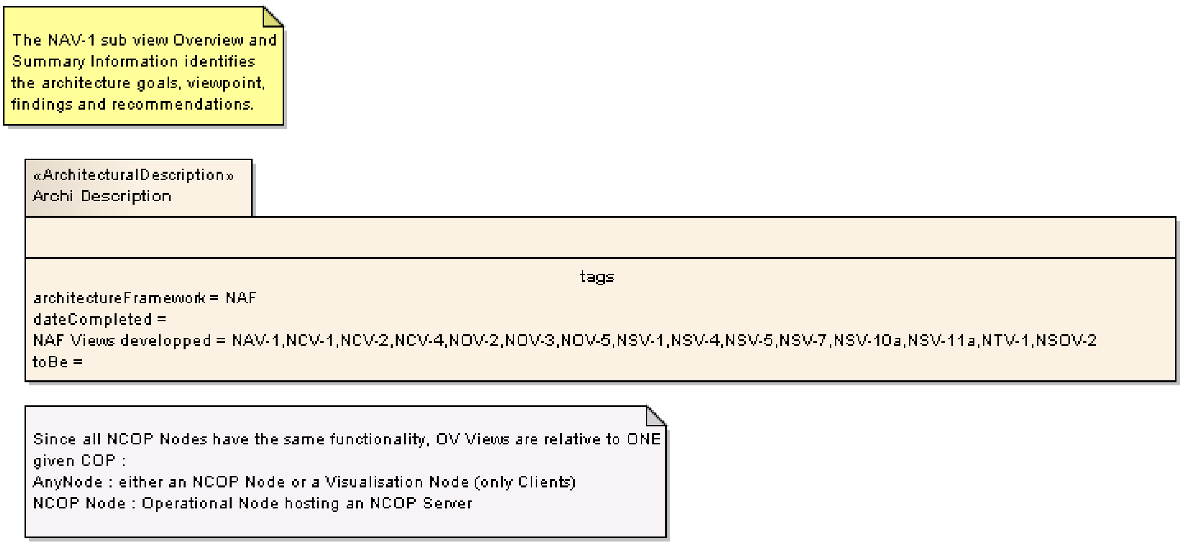
For better readability, NAF views are also provided as a separate zip file containing:

An html export of the EAP file,

Two images of matrices NOV-3 and NSV-5 (these matrices are not properly exported in html format).



B.1 NAV-1



The NAV-1 sub view Overview and Summary Information identifies the architecture goals, viewpoint, findings and recommendations.

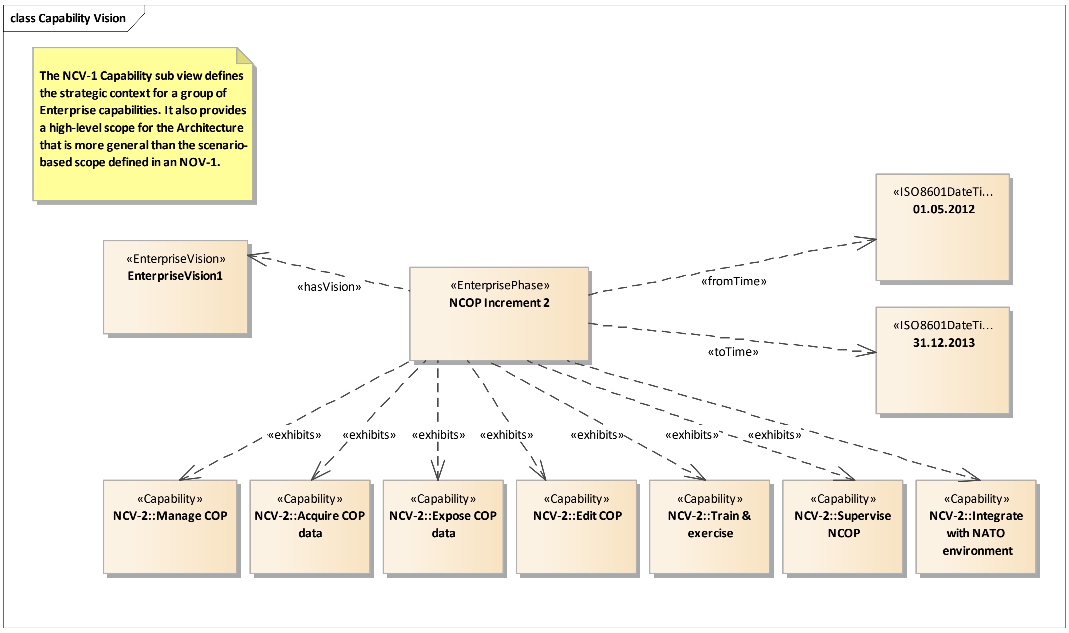
«ArchitecturalDescription»
Archi Description

tags

architectureFramework = NAF
dateCompleted =
NAF Views developped = NAV-1,NCV-1,NCV-2,NCV-4,NOV-2,NOV-3,NOV-5,NSV-1,NSV-4,NSV-5,NSV-7,NSV-10a,NSV-11a,NTV-1,NSOV-2
toBe =

Since all NCOP Nodes have the same functionality, OV Views are relative to ONE given COP :
AnyNode : either an NCOP Node or a Visualisation Node (only Clients)
NCOP Node : Operational Node hosting an NCOP Server

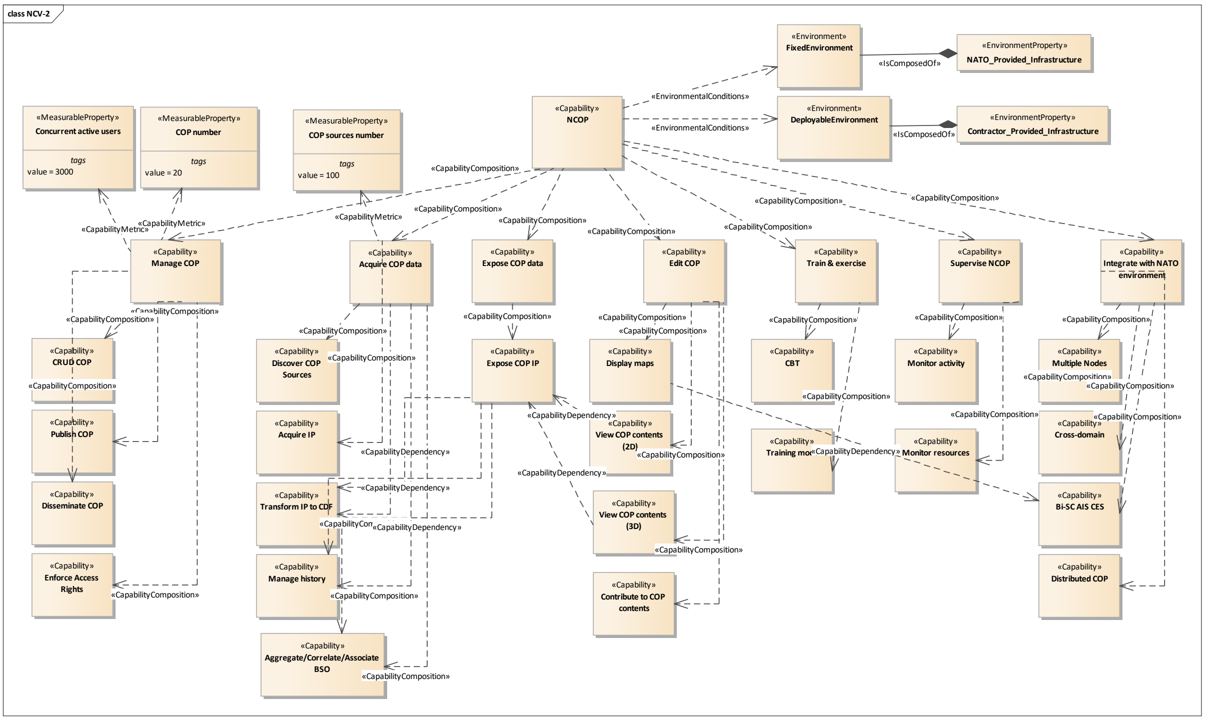
B.2 NCV-1



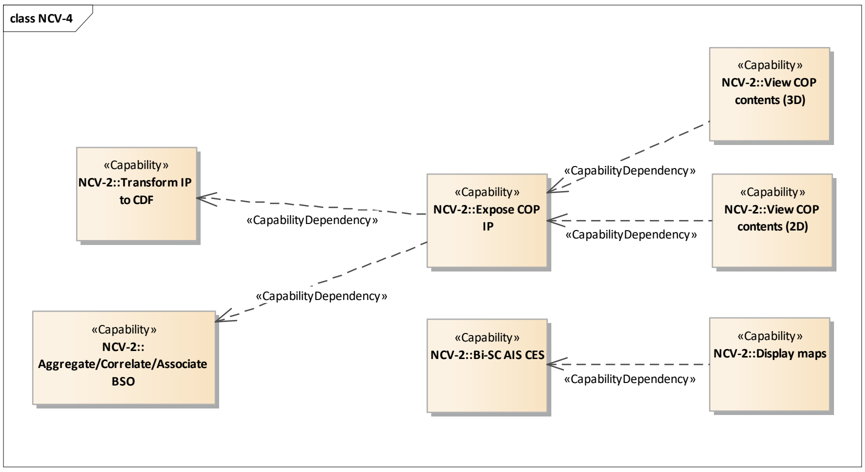
class Capability Vision

The NCV-1 Capability sub view defines the strategic context for a group of Enterprise capabilities. It also provides a high-level scope for the Architecture that is more general than the scenario-based scope defined in an NOV-1.

B.3 NCV-2

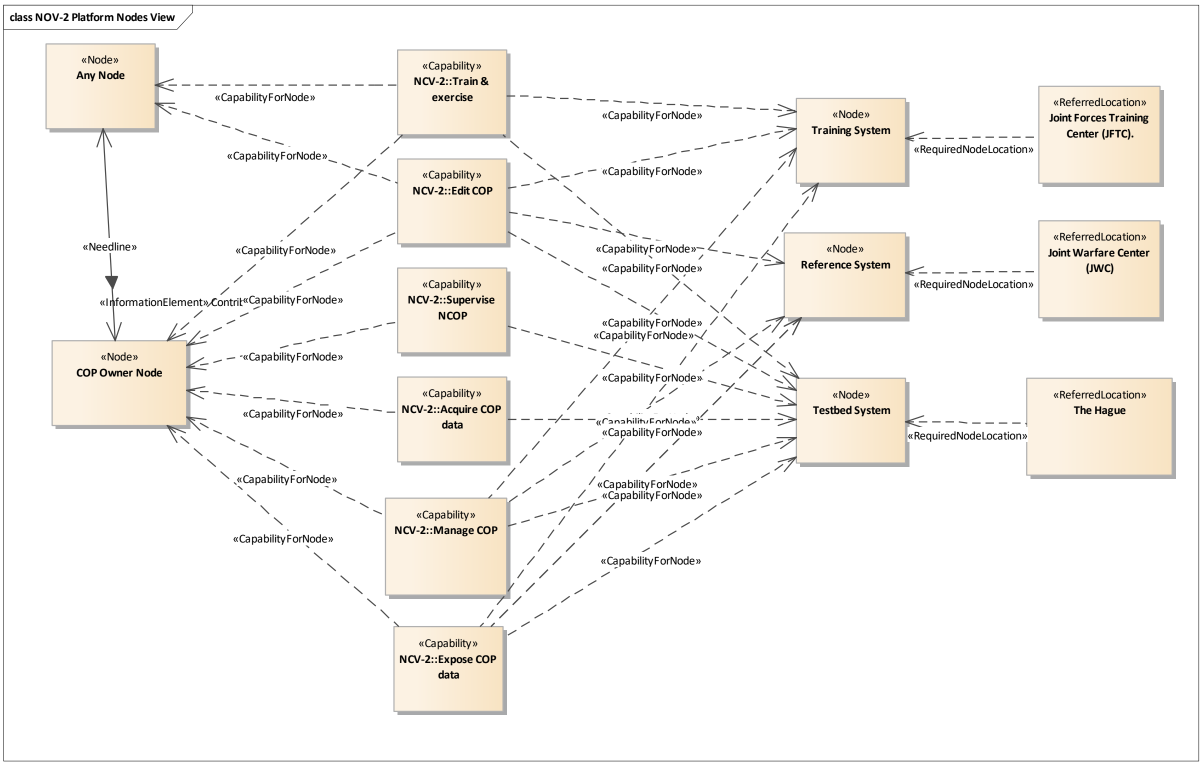

class NCV-2
«MeasurableProperty» Concurrent active users
tags
value = 3000
«MeasurableProperty» COP number
tags
value = 20
«MeasurableProperty» COP sources number
tags
value = 100
«Capability» NCOP
«Environment» FixedEnvironment
«EnvironmentProperty» NATO_Provided_Infrastructure
«Environment» DeployableEnvironment
«EnvironmentProperty» Contractor_Provided_Infrastructure
«EnvironmentalConditions»
«IsComposedOf»
«CapabilityMetric»
«CapabilityComposition»
«CapabilityDependency»
«Capability» Manage COP
«Capability» Acquire COP data
«Capability» Expose COP data
«Capability» Edit COP
«Capability» Train & exercise
«Capability» Supervise NCOP
«Capability» Integrate with NATO environment
«Capability» CRUD COP
«Capability» Publish COP
«Capability» Disseminate COP
«Capability» Enforce Access Rights
«Capability» Discover COP Sources
«Capability» Acquire IP
«Capability» Transform IP to CDF
«Capability» Manage history
«Capability» Aggregate/Correlate/Associate BSO
«Capability» Expose COP IP
«Capability» Display maps
«Capability» View COP contents (2D)
«Capability» View COP contents (3D)
«Capability» Contribute to COP contents
«Capability» CBT
«Capability» Training mo
«Capability» Monitor activity
«Capability» Monitor resources
«Capability» Multiple Nodes
«Capability» Cross-domain
«Capability» Bi-SC AIS CES
«Capability» Distributed COP

B.4 NCV-4

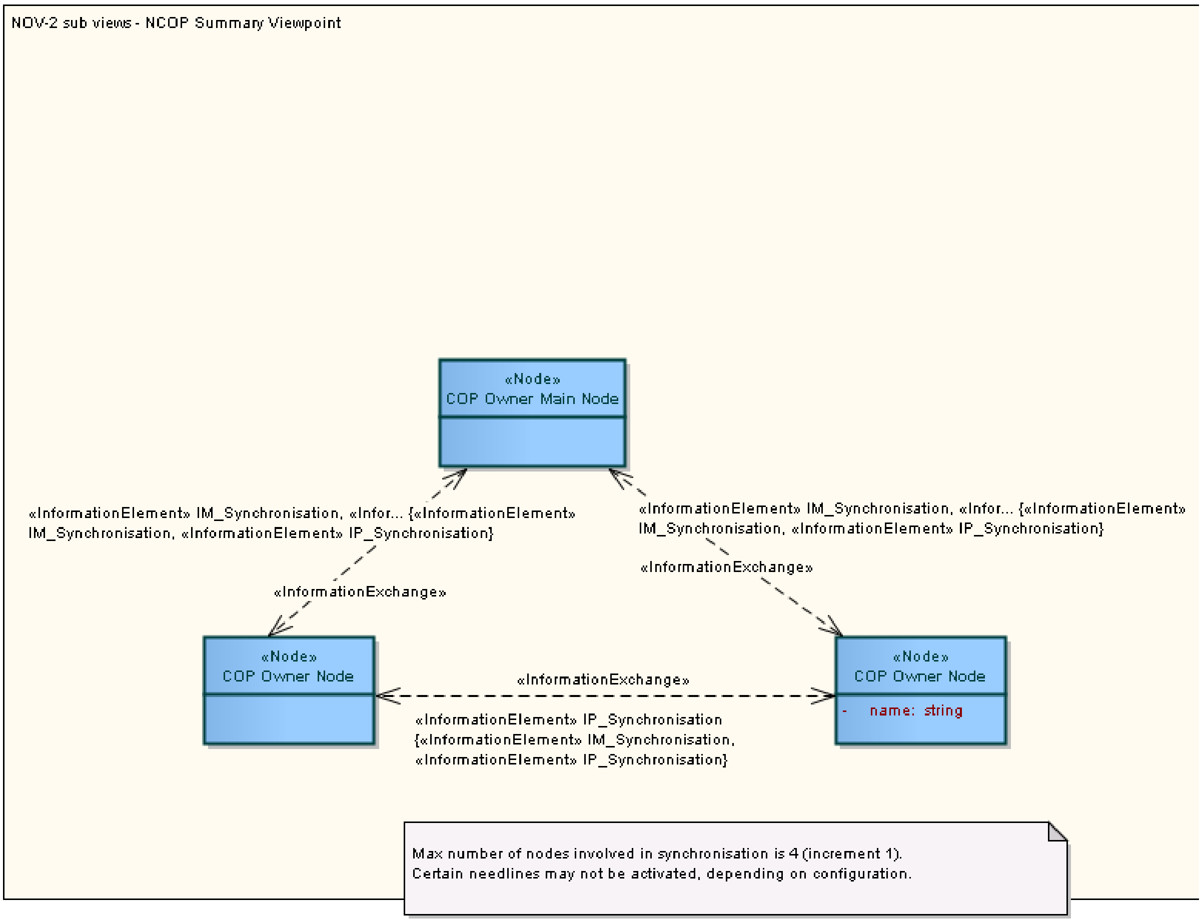

class NCV-4
«Capability» NCV-2::Transform IP to CDF
«Capability» NCV-2::Expose COP IP
«Capability» NCV-2::View COP contents (3D)
«Capability» NCV-2::View COP contents (2D)
«Capability» NCV-2:: Aggregate/Correlate/Associate BSO
«Capability» NCV-2::Bi-SC AIS CES
«Capability» NCV-2::Display maps
«CapabilityDependency»
«CapabilityDependency»
«CapabilityDependency»
«CapabilityDependency»
«CapabilityDependency»

B.5 NOV-2 CONNECTIVITY DESCRIPTION

B.5.1 NCOP Platform nodes view

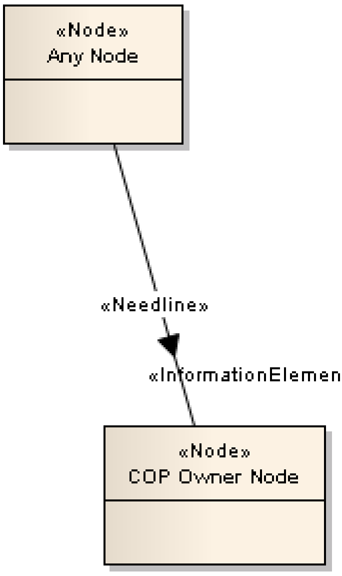


B.5.2 NCOP Synchronisation needlines

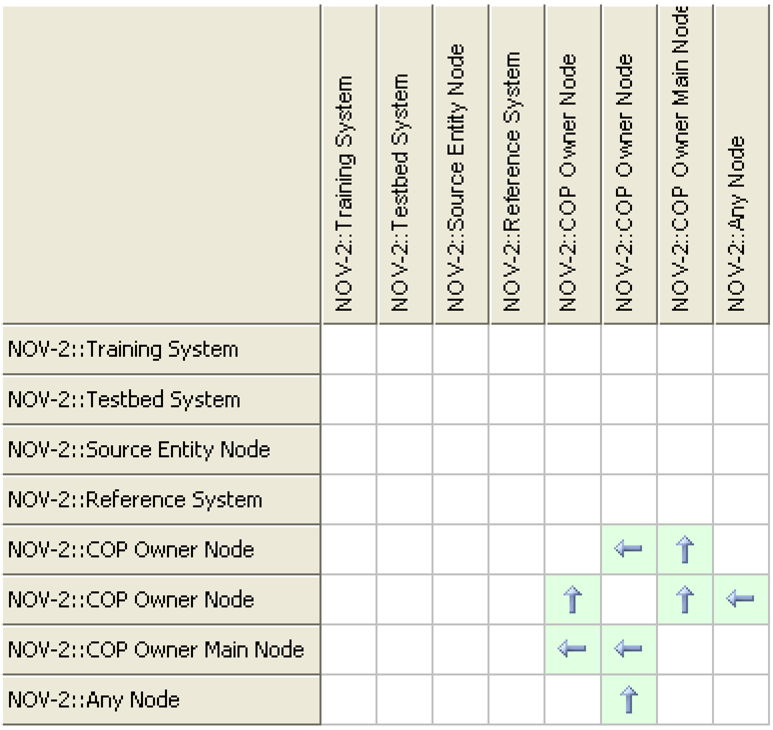

NOV-2 sub views - NCOP Summary Viewpoint
«Node»
COP Owner Main Node
«InformationElement» IM_Synchronisation, «Infor... {«InformationElement» IM_Synchronisation, «InformationElement» IP_Synchronisation}
«InformationExchange»
«InformationElement» IM_Synchronisation, «Infor... {«InformationElement» IM_Synchronisation, «InformationElement» IP_Synchronisation}
«InformationExchange»
«Node»
COP Owner Node
«InformationExchange»
«InformationElement» IP_Synchronisation {«InformationElement» IM_Synchronisation, «InformationElement» IP_Synchronisation}
«Node»
COP Owner Node
- name: string

Max number of nodes involved in synchronisation is 4 (increment 1).
Certain needlines may not be activated, depending on configuration.

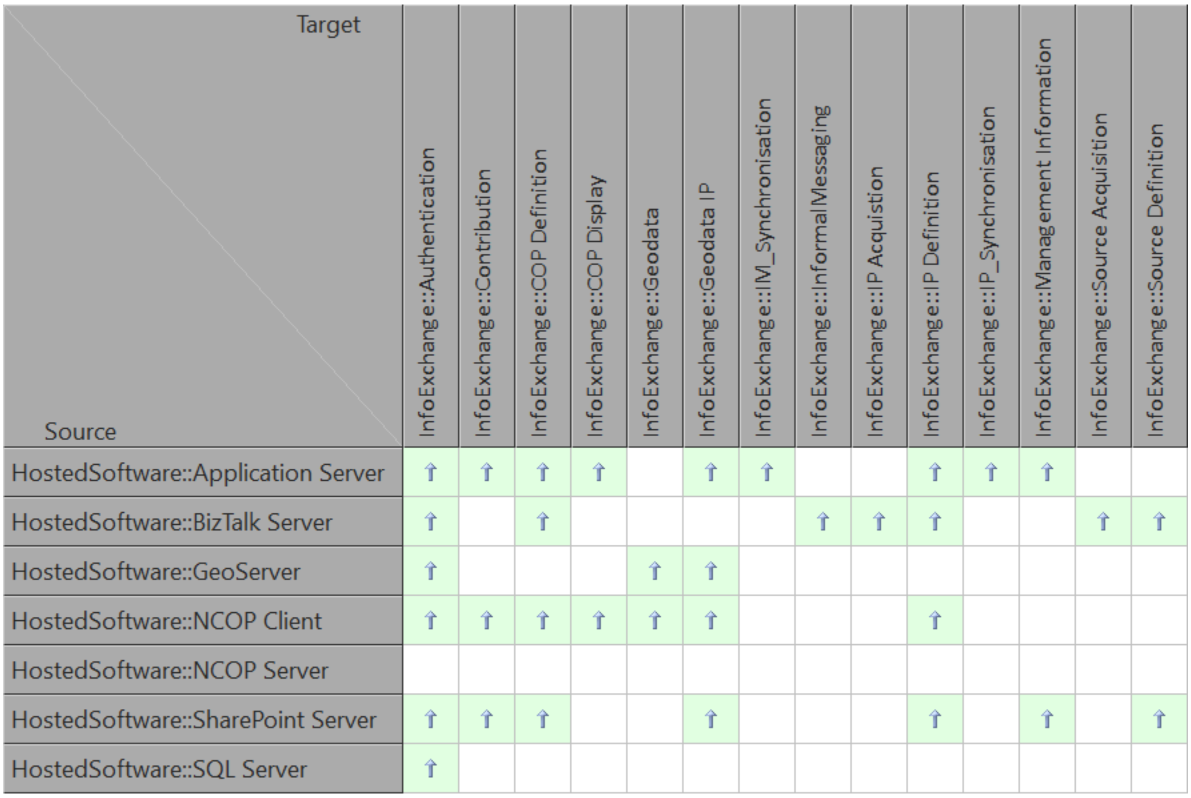
B.5.3 Viewpoint 2: COP Contribution needlines



B.6 NOV-3

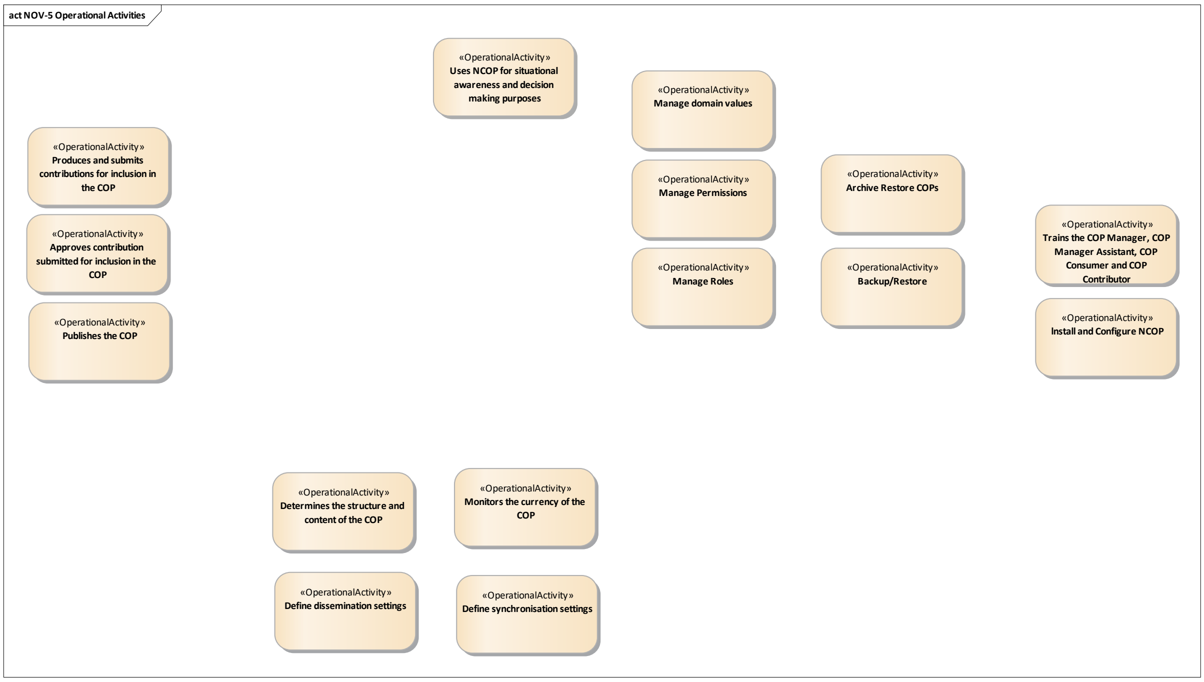


	NOV-2::Training System	NOV-2::Testbed System	NOV-2::Source Entity Node	NOV-2::Reference System	NOV-2::COP Owner Node	NOV-2::COP Owner Node	NOV-2::COP Owner Main Node	NOV-2::Any Node
NOV-2::Training System								
NOV-2::Testbed System								
NOV-2::Source Entity Node								
NOV-2::Reference System								
NOV-2::COP Owner Node						←	↑	
NOV-2::COP Owner Node					↑		↑	←
NOV-2::COP Owner Main Node					←	←		
NOV-2::Any Node						↑		



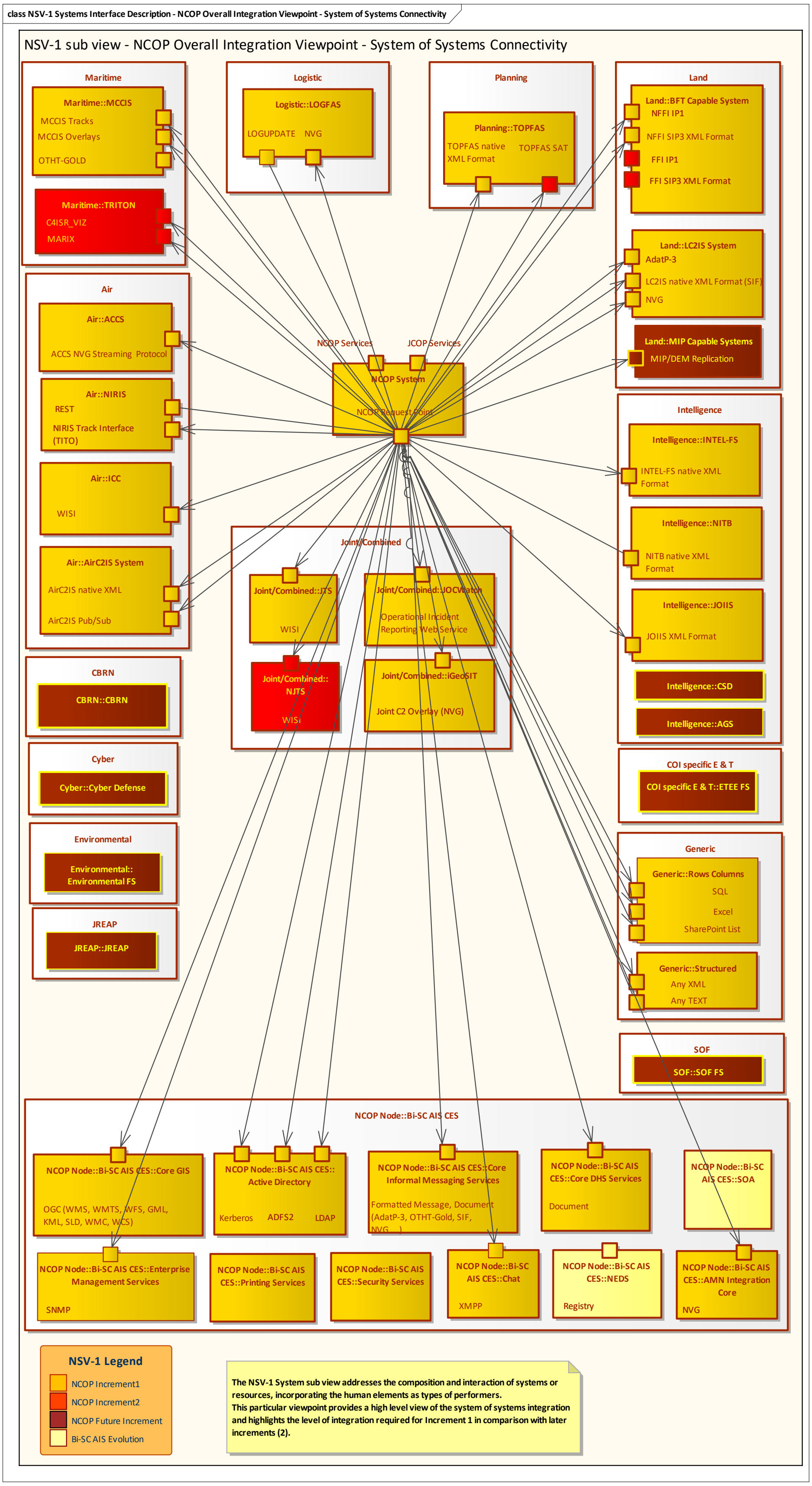
Target Source	InfoExchange::Authentication	InfoExchange::Contribution	InfoExchange::COP Definition	InfoExchange::COP Display	InfoExchange::Geodata	InfoExchange::Geodata IP	InfoExchange::IM_Synchronisation	InfoExchange::InformalMessaging	InfoExchange::IP Acquistion	InfoExchange::IP Definition	InfoExchange::IP_Synchronisation	InfoExchange::Management Information	InfoExchange::Source Acquisition	InfoExchange::Source Definition
HostedSoftware::Application Server	↑	↑	↑	↑		↑	↑			↑	↑	↑		
HostedSoftware::BizTalk Server	↑		↑					↑	↑	↑			↑	↑
HostedSoftware::GeoServer	↑				↑	↑								
HostedSoftware::NCOP Client	↑	↑	↑	↑	↑	↑				↑				
HostedSoftware::NCOP Server														
HostedSoftware::SharePoint Server	↑	↑	↑			↑				↑		↑		↑
HostedSoftware::SQL Server	↑													

B.7 NOV-5


act NOV-5 Operational Activities
«OperationalActivity» Uses NCOP for situational awareness and decision making purposes
«OperationalActivity» Manage domain values
«OperationalActivity» Produces and submits contributions for inclusion in the COP
«OperationalActivity» Manage Permissions
«OperationalActivity» Archive Restore COPs
«OperationalActivity» Trains the COP Manager, COP Manager Assistant, COP Consumer and COP Contributor
«OperationalActivity» Approves contribution submitted for inclusion in the COP
«OperationalActivity» Manage Roles
«OperationalActivity» Backup/Restore
«OperationalActivity» Publishes the COP
«OperationalActivity» Install and Configure NCOP
«OperationalActivity» Determines the structure and content of the COP
«OperationalActivity» Monitors the currency of the COP
«OperationalActivity» Define dissemination settings
«OperationalActivity» Define synchronisation settings

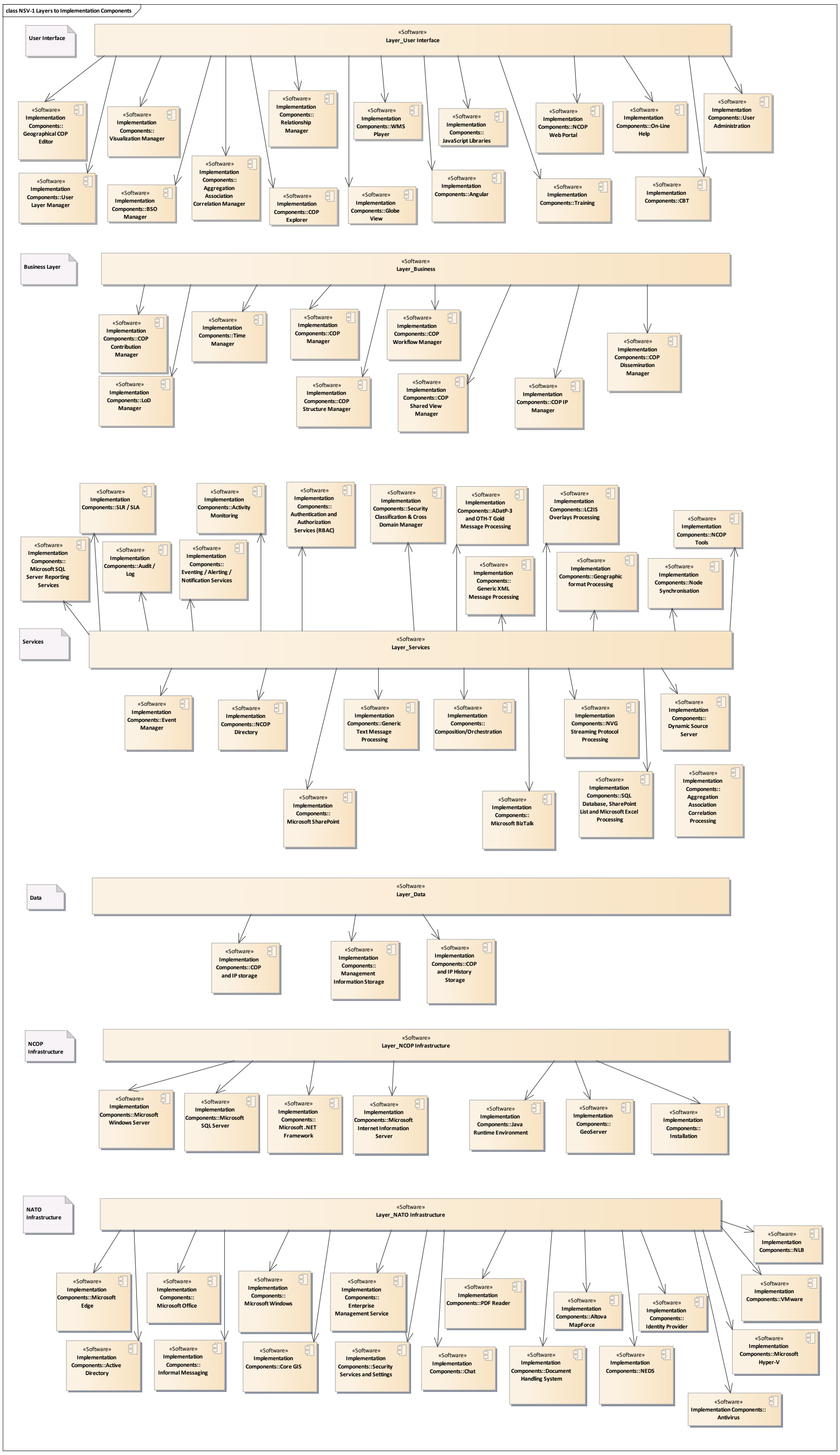
B.8 NSV-1

B.8.1 Viewpoint 1: NCOP External interfaces



The NSV-1 System sub view addresses the composition and interaction of systems or resources, incorporating the human elements as types of performers.
This particular viewpoint provides a high level view of the system of systems integration and highlights the level of integration required for Increment 1 in comparison with later increments (2).

B.8.2 Viewpoint 2: Software decomposition into Implementation Components


class NSV-1 Layers to Implementation Components
User Interface
«Software» Layer_User Interface
«Software» Implementation Components:: Geographical COP Editor
«Software» Implementation Components:: Visualization Manager
«Software» Implementation Components:: Relationship Manager
«Software» Implementation Components::WMS Player
«Software» Implementation Components:: JavaScript Libraries
«Software» Implementation Components::NCOP Web Portal
«Software» Implementation Components::On-Line Help
«Software» Implementation Components::User Administration
«Software» Implementation Components::User Layer Manager
«Software» Implementation Components::BSO Manager
«Software» Implementation Components:: Aggregation Association Correlation Manager
«Software» Implementation Components::COP Explorer
«Software» Implementation Components::Globe View
«Software» Implementation Components::Angular
«Software» Implementation Components::Training
«Software» Implementation Components::CBT
Business Layer
«Software» Layer_Business
«Software» Implementation Components::COP Contribution Manager
«Software» Implementation Components::Time Manager
«Software» Implementation Components::COP Manager
«Software» Implementation Components::COP Workflow Manager
«Software» Implementation Components::COP Dissemination Manager
«Software» Implementation Components::LoD Manager
«Software» Implementation Components::COP Structure Manager
«Software» Implementation Components::COP Shared View Manager
«Software» Implementation Components::COP IP Manager
«Software» Implementation Components::SLR / SLA
«Software» Implementation Components::Activity Monitoring
«Software» Implementation Components:: Authentication and Authorization Services (RBAC)
«Software» Implementation Components::Security Classification & Cross Domain Manager
«Software» Implementation Components::ADatP-3 and OTH-T Gold Message Processing
«Software» Implementation Components::LC2IS Overlays Processing
«Software» Implementation Components::NCOP Tools
«Software» Implementation Components:: Microsoft SQL Server Reporting Services
«Software» Implementation Components::Audit / Log
«Software» Implementation Components:: Eventing / Alerting / Notification Services
«Software» Implementation Components:: Generic XML Message Processing
«Software» Implementation Components::Geographic format Processing
«Software» Implementation Components::Node Synchronisation
Services
«Software» Layer_Services
«Software» Implementation Components::Event Manager
«Software» Implementation Components::NCOP Directory
«Software» Implementation Components::Generic Text Message Processing
«Software» Implementation Components:: Composition/Orchestration
«Software» Implementation Components::NVG Streaming Protocol Processing
«Software» Implementation Components:: Dynamic Source Server
«Software» Implementation Components:: Microsoft SharePoint
«Software» Implementation Components:: Microsoft BizTalk
«Software» Implementation Components::SQL Database, SharePoint List and Microsoft Excel Processing
«Software» Implementation Components:: Aggregation Association Correlation Processing
Data
«Software» Layer_Data
«Software» Implementation Components::COP and IP storage
«Software» Implementation Components:: Management Information Storage
«Software» Implementation Components::COP and IP History Storage
NCOP Infrastructure
«Software» Layer_NCOP Infrastructure
«Software» Implementation Components::Microsoft Windows Server
«Software» Implementation Components::Microsoft SQL Server
«Software» Implementation Components:: Microsoft .NET Framework
«Software» Implementation Components::Microsoft Internet Information Server
«Software» Implementation Components::Java Runtime Environment
«Software» Implementation Components:: GeoServer
«Software» Implementation Components:: Installation
NATO Infrastructure
«Software» Layer_NATO Infrastructure
«Software» Implementation Components::NLB
«Software» Implementation Components::Microsoft Edge
«Software» Implementation Components:: Microsoft Office
«Software» Implementation Components:: Microsoft Windows
«Software» Implementation Components:: Enterprise Management Service
«Software» Implementation Components::PDF Reader
«Software» Implementation Components::Altova MapForce
«Software» Implementation Components:: Identity Provider
«Software» Implementation Components::VMware
«Software» Implementation Components::Active Directory
«Software» Implementation Components:: Informal Messaging
«Software» Implementation Components::Core GIS
«Software» Implementation Components::Security Services and Settings
«Software» Implementation Components::Chat
«Software» Implementation Components::Document Handling System
«Software» Implementation Components::NEDS
«Software» Implementation Components::Microsoft Hyper-V
«Software» Implementation Components:: Antivirus

B.8.3 Viewpoint 2: Decomposition of Implementation Components into Software Artefacts

For readability purposes, this decomposition is provided as a textual table rather than using UML diagrams.

Implementation Component	Software Artefact	NUPKG
Active Directory	Active Directory	COTS
Activity Monitoring	Activity Monitoring UI COP Usage Reporting Services COP Usage Reporting Storage Orchestration Reporting Services Orchestration Reporting Storage Report Builder Services	bam_reports.nupkg bam_reports_data.nupkg bam_reports_synchro_role.nupkg bam_reports_synchro_type.nupkg bam_reports_synchro_type_data.nupkg
ADatP-3 and OTH-T Gold Message Processing	ADatP-3 and OTH-T Gold Message Processing Services SING	adatp-3_editor.nupkg web_services_adatp3_converter.nupkg
Aggregation Association Correlation Manager	Aggregation Association Correlation Manager UI	-
Aggregation Association Correlation Processing	Aggregation Association Correlation Processing Services	-
Altova MapForce	Altova MapForce	COTS
Angular	Angular	COTS
Antivirus	Antivirus	COTS
Audit / Log	Audit / Log UI Journal Management UI	log4net_file.nupkg temp.nupkg web_services_sharepoint.nupkg
Authentication and Authorization Services (RBAC)	Authentication and Authorization Services RBAC Services RBAC UI	users.nupkg users_type.nupkg

BSO Manager	BSO Manager UI BSO Manager Services	symbicon.nupkg symbicon_tims.nupkg symbicon_tims_public.nupkg windows_services_bso.nupkg web_services_tims.nupkg web_services_tims_public_.nupkg
CBT	CBT	CBT
Chat	Jchat	COTS
Composition/Orchestration	Composition / Orchestration Services Composition / Orchestration Storage	bam_tracking.nupkg biztalk_applications.nupkg biztalk_gac.nupkg biztalk_handlers.nupkg biztalk_hosts.nupkg biztalk_host_instances.nupkg biztalk_resources.nupkg biztalk_settings_file.nupkg biztalk_sql.nupkg biztalk_sql_bam.nupkg biztalk_swid_files.nupkg btsntsvc.nupkg helper_config_file.nupkg pipeline_components.nupkg xref.nupkg web_services_process_manager.nupkg web_services_mock.nupkg web_services_urlacl.nupkg
COP and IP History storage	BSO History Storage	databases.nupkg databases_type.nupkg jobs_index.nupkg jobs_purge.nupkg jobs_type.nupkg procedures.nupkg sql_files.nupkg

		sql_files_type.nupkg sql_swid_files.nupkg
COP and IP Storage	COP Aggregated IP Storage COP IP Instances Storage COP Manager Storage COP Shared View Storage COP Structure Storage NCOP Import Geonames Tool	sharepoint_configuration.nupkg sharepoint_data.nupkg sharepoint_help.nupkg sharepoint_swid_files.nupkg sharepoint_wsp.nupkg
COP Contribution Manager	COP Annotation Contribution UI COP Contribution Submission Services COP IP Contribution UI COP Shared View Contribution UI	web_services_user_mapping_manager.nupkg web_services_tims.nupkg
COP Dissemination Manager	COP Dissemination Rules Services COP Dissemination Rules UI	web_services_tims.nupkg web_services_tims_public_.nupkg
COP Explorer	COP Explorer UI	web_services_user_scripting.nupkg web_services_tims.nupkg web_services_tims_public_.nupkg
COP IP Manager	COP IP Manager UI	web_services_tims.nupkg
COP Manager	Archive/Restore UI Archive/Restore Services COP Manager Services COP Manager UI	web_services_tims.nupkg
COP Shared View Manager	COP Shared View Services COP Shared View UI	web_services_tims.nupkg
COP Structure Manager	COP Structure Services COP Structure UI	web_services_tims.nupkg
COP Workflow Manager	COP Annotation Workflow Manager UI COP Approval Services COP IP Workflow Manager UI COP Preview Services	web_services_tims.nupkg

	COP Shared View Workflow Manager UI COP Workflow Manager UI	
Core GIS	Core GIS Web Services	COTS
Document Handling System	Document Handling System	COTS
Dynamic Source Server	DSS	web_services_dynamic_source.nupkg
Enterprise Management Service	SNMP Services	COTS
Event Manager	Event Manager Services	web_services_eventing.nupkg
Eventing / Alerting / Notification Services	Internal pub/sub services Internal pub/sub storage External pub/sub services External pub/sub storage Alert / Notification Services Alert / Notification UI	web_services_alerting.nupkg web_services_alerting_businessrules.nupkg web_services_alerting_server.nupkg web_services_alerting_timsconnector.nupkg web_services_eventing.nupkg
Generic Text Message Processing	Generic Text Message Processing Services Generic Message Processing Storage Generic Message Processing UI	web_services_mapforce_converter.nupkg
Generic XML Message Processing	Generic XML Message Processing Services Generic XML Message Processing UI	biztalk_applications.nupkg
Geographic format Processing	Geographical format Processing services	biztalk_applications.nupkg
Geographical COP Editor	TIMS.js Geographical COP Editor UI	web_services_tims.nupkg web_services_tims_public_.nupkg
GeoServer	GeoServer Map LoD Manager UI OGC Web Services	COTS
Globe View	Globe View Services	-

	Globe View UI	
Identity Provider	Identity Provider Services Identity Provider UI	COTS
Informal Messaging	Email Services	web_services_mapi_proxy.nupkg
Installation	NCOP installer	post_install_tools.nupkg
Java Runtime Environment	OpenJDK	COTS
JavaScripts Libraries	D3.js PrimeNG	COTS
LC2IS Overlays Processing	SIF2NVG Converter	sicf.nupkg web_services_sicf_converter_.nupkg
LoD Manager	IP LoD Definition UI IP LoD Display UI IP LoD Manager Services	web_services_tims.nupkg web_services_tims_public_.nupkg
Management Information Storage	COP Dissemination Rules Storage Node synchronization Storage	sharepoint_wsp.nupkg
Microsoft .NET Framework	Microsoft .NET Framework	COTS
Microsoft BizTalk	Microsoft BizTalk Server Sources & COP IP Parameter Storage BizTalk	COTS
Microsoft Edge	Microsoft Edge Chromium	COTS
Microsoft Hyper-V	Microsoft Hyper-V	COTS
Microsoft Internet Information Server	Microsoft Internet Information Server	COTS
Microsoft Office	Microsoft Office	COTS
Microsoft SharePoint	Microsoft SharePoint Central Administration Microsoft SharePoint Server	COTS

	COP IP Parameter Storage SharePoint List Helper SharePoint Accessor Services	
Microsoft SQL Server	Microsoft SQL Server	COTS
Microsoft SQL Server Reporting Services	SQL Server Reporting Services reports	COTS
Microsoft Windows	Microsoft Windows 10	COTS
Microsoft Windows Server	Microsoft Windows Server	COTS
NCOP Directory	RBAC Storage	sql_files.nupkg
NCOP Tools	Software Build tools Software Build Instruction NCOP installer Data migration tool Training data for training database Test automation tool	
NCOP Web Portal	NCOP Web Portal Storage NCOP Web Portal UI	sharepoint_sites.nupkg web_services_sharepoint_public.nupkg web_services_sharepoint_public_ncopendpoint_aspx.nupkg
NEDS	NEDS	COTS
NLB	PulseSecure Traffic Manager	COTS
Node Synchronisation	Node Synchronisation Configuration Services Node Synchronisation UI Node Synchronisation Services	windows_services_sync.nupkg web_services_syncs_server.nupkg web_services_sync_client.nupkg web_services_sync_client_ano.nupkg web_services_sync_servert_ano.nupkg
NVG Streaming Protocol Processing	NGV Streaming Protocol Processing producer services	web_services_nvgstreaming_configurator.nupkg windows_services_nvgstreaming_15_connector.nupkg

	NVG Streaming Protocol Processing consumer services	windows_services_nvgstreaming_20_connector.nupkg
On-Line Help	On-Line Help HTML Pages	On-Line Help
PDF Reader	PDF Reader	COTS
Relationship Manager	Relationship Manager UI	web_services_tims.nupkg sharepoint_sites.nupkg
Security Classification Manager & Cross Domain Manager	Cross Domain Services Labelling Services Signature Services	
Security Services and Settings	Security Services and Settings	
SLR / SLA	Service Level Agreement Service Level Requirement	web_services_behavior_management.nupkg
SQL Database, SharePoint List and Microsoft Excel Processing	Database and Microsoft Excel Processing Services Database and Microsoft Excel Processing UI	web_services_ncopservices_sqlexcelproxy.nupkg
Time Manager	BSO History Display UI BSO Time Filter UI BSO History Services	
Training	Training UI	
User Administration	Management Information UI	
User Layer Manager	User Layer Services User Layer UI	
Visualization Manager	IP Content UI	
VMware	VMware	COTS
WMS Player	WMS Player WMS Dimension UI	

Implementation Component		Software Artefact
NFFI Interface		nffi.nupkg web_services_nffisip3_configurator.nupkg windows_services_nffisip3_connector.nupkg
AirC2IS Interface		web_services_airc2is_proxy.nupkg web_services_airc2is_receiver.nupkg
INTEL-FS Interface		web_services_intelfs_proxy.nupkg
MCCIS Interface		web_services_mccis_configurator.nupkg windows_services_mccis_connector.nupkg
NCOP Web Services Interface	JIPS JOS NCOP IPS REST API NCOP WebService Consumer Tool	web_services_ncopipsconnector.nupkg web_services_ncopservices.nupkg web_services_ncopservices_public.nupkg web_services_ips_tims_connector.nupkg web_services_ips.nupkg web_services_services.nupkg web_services_ncopservices_sharepointproxy.nupkg web_services_ncopservices_symbology.nupkg web_services_services_common.nupkg web_services_configuration_data.nupkg
NIRIS Interface		web_services_niris_configurator.nupkg windows_services_niris_38_connector.nupkg windows_services_niris_connector.nupkg
XMPP WhiteBoard Interface		web_services_ncopservices_whiteboardnotificationproxy.nupkg

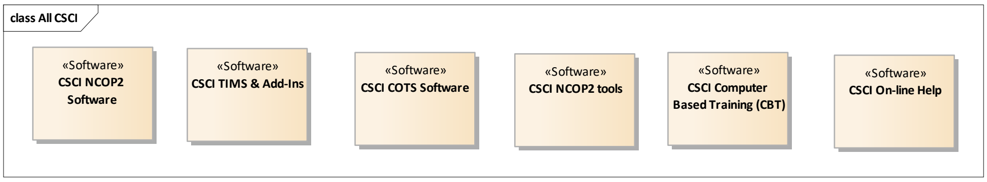
Software Artefact (nupkg)	GAC	IIS	File System	Windows Service	Registry	BizTalk	SharePoint	DB	Runtime on client workstation
adatp-3_editor.nupkg			X						
bam_reports.nupkg			X					X	
bam_reports_data.nupkg								X	
bam_reports_synchro_role.nupkg								X	
bam_reports_synchro_type.nupkg			X					X	
bam_reports_synchro_type_data.nupkg								X	
bam_tracking.nupkg			X			X			
biztalk_applications.nupkg						X			
biztalk_gac.nupkg	X								
biztalk_handlers.nupkg						X			
biztalk_hosts.nupkg						X			
biztalk_host_instances.nupkg						X			
biztalk_resources.nupkg						X			
biztalk_settings_file.nupkg			X						
biztalk_sql.nupkg			X					X	
biztalk_sql_bam.nupkg								X	
biztalk_swid_files.nupkg			X						
btsntsvc.nupkg			X						
databases.nupkg								X	
databases_type.nupkg								X	
helper_config_file.nupkg			X						
jobs_index.nupkg								X	

jobs_purge.nupkg								X	
jobs_type.nupkg								X	
log4net_file.nupkg			X						
nffi.nupkg			X						
pipeline_components.nupkg			X						
post_install_tools.nupkg			X						
procedures.nupkg								X	
sharepoint_configuration.nupkg			X						
sharepoint_data.nupkg							X		
sharepoint_help.nupkg			X						
sharepoint_sites.nupkg							X		
sharepoint_swid_files.nupkg			X						
sharepoint_wsp.nupkg							X		
sicf.nupkg					X	X			
sql_files.nupkg			X						
sql_files_type.nupkg			X						
sql_swid_files.nupkg			X						
symbicon.nupkg			X						
symbicon_tims.nupkg		X	X						
symbicon_tims_public.nupkg		X	X						
temp.nupkg			X						
users.nupkg								X	
users_type.nupkg								X	
web_services_adatp3_converter.nupkg		X	X						
web_services_airc2is_proxy.nupkg		X	X						
web_services_airc2is_receiver.nupkg		X	X						
web_services_alerting.nupkg		X	X						

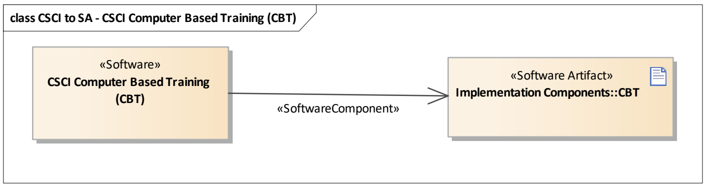
web_services_alerting_businessrules.nupkg		X	X						
web_services_alerting_server.nupkg		X	X						
web_services_alerting_timsconnector.nupkg		X	X						
web_services_behavior_management.nupkg		X	X						
web_services_configuration_data.nupkg		X	X						
web_services_dynamic_source.nupkg		X	X						
web_services_eventing.nupkg		X	X						
web_services_intelfs_proxy.nupkg		X	X						
web_services_ips.nupkg		X	X						
web_services_ips_tims_connector.nupkg			X						
web_services_mapforce_converter.nupkg		X	X						
web_services_mapi_proxy.nupkg		X	X						
web_services_mccis_configurator.nupkg		X	X						
web_services_mock.nupkg		X	X						
web_services_ncopipsconnector.nupkg		X	X						
web_services_ncopservices.nupkg		X	X						
web_services_ncopservices_public.nupkg		X	X						
web_services_ncopservices_sharepointproxy.nupkg		X	X						
web_services_ncopservices_sqlexcelproxy.nupkg		X	X						
web_services_ncopservices_symbology.nupkg		X	X						
web_services_ncopservices_whiteboardnotificationproxy.nupkg		X	X						
web_services_nffisip3_configurator.nupkg		X	X						
web_services_niris_configurator.nupkg		X	X						
web_services_nvgstreaming_configurator.nupkg		X	X						

web_services_process_manager.nupkg		X	X						
web_services_services.nupkg		X	X						
web_services_services_common.nupkg		X	X						
web_services_sharepoint.nupkg		X	X						
web_services_sharepoint_public.nupkg		X	X						
web_services_sharepoint_public_ncopendpoint_aspx.nupkg		X	X						
web_services_sicf_converter_.nupkg		X	X						
web_services_syncs_server.nupkg		X	X						
web_services_sync_client.nupkg		X	X						
web_services_sync_client_ano.nupkg		X	X						
web_services_sync_servert_ano.nupkg		X	X						
web_services_tims.nupkg		X	X						
web_services_tims_public_.nupkg		X	X						
web_services_urlacl.nupkg		X	X						
web_services_user_mapping_manager.nupkg		X	X						
web_services_user_scripting.nupkg		X	X						
windows_services_bso.nupkg			X						
windows_services_mccis_connector.nupkg			X	X					
windows_services_nffisip3_connector.nupkg			X	X					
windows_services_niris_38_connector.nupkg			X	X					
windows_services_niris_connector.nupkg			X	X					
windows_services_nvgstreaming_15_connector.nupkg			X	X					
windows_services_nvgstreaming_20_connector.nupkg			X	X					
windows_services_sync.nupkg			X	X					
xref.nupkg			X			X			

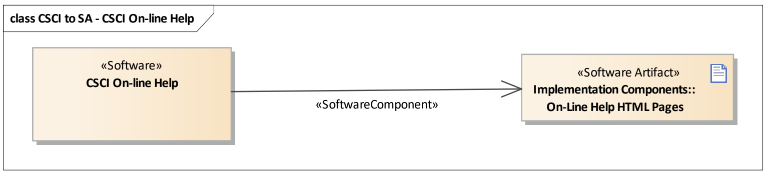
B.8.4 Viewpoint 3: Identification of CSCI



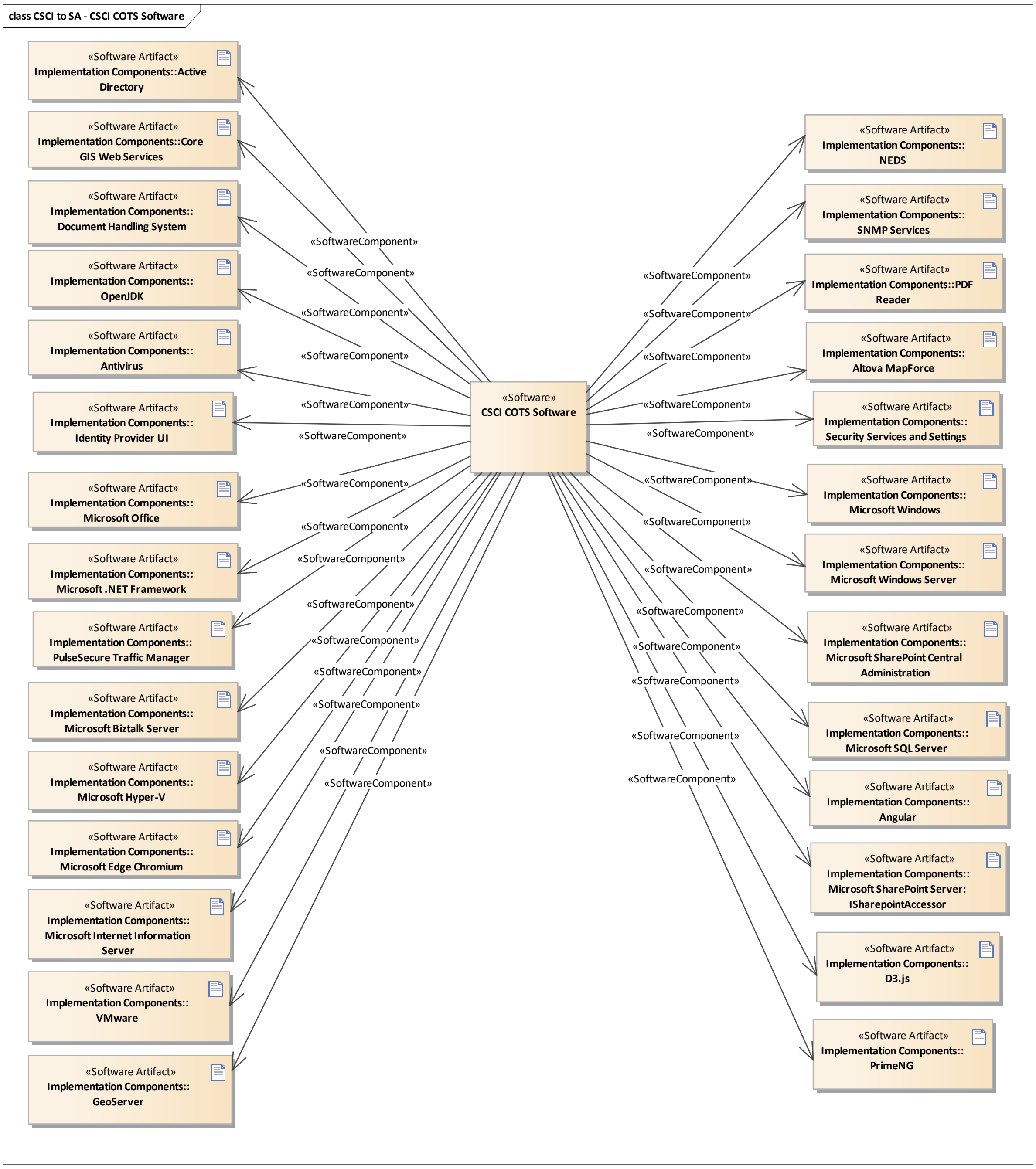
B.8.4.1 Computer Based Training (CBT)


class CSCI to SA - CSCI Computer Based Training (CBT)
«Software»
CSCI Computer Based Training (CBT)
«SoftwareComponent»
«Software Artifact»
Implementation Components::CBT

B.8.4.2 On-line Help

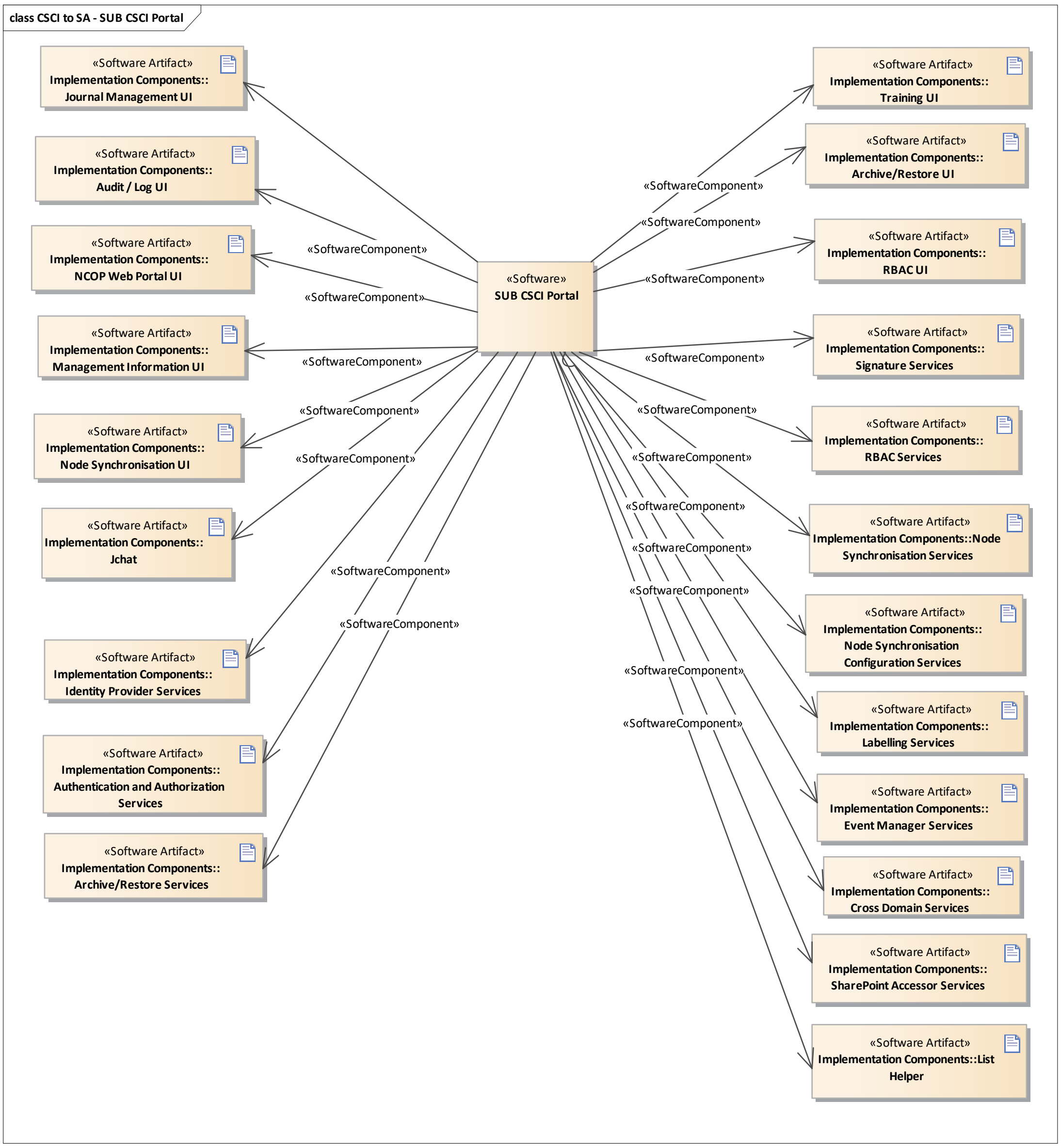


B.8.4.3 COTS Software

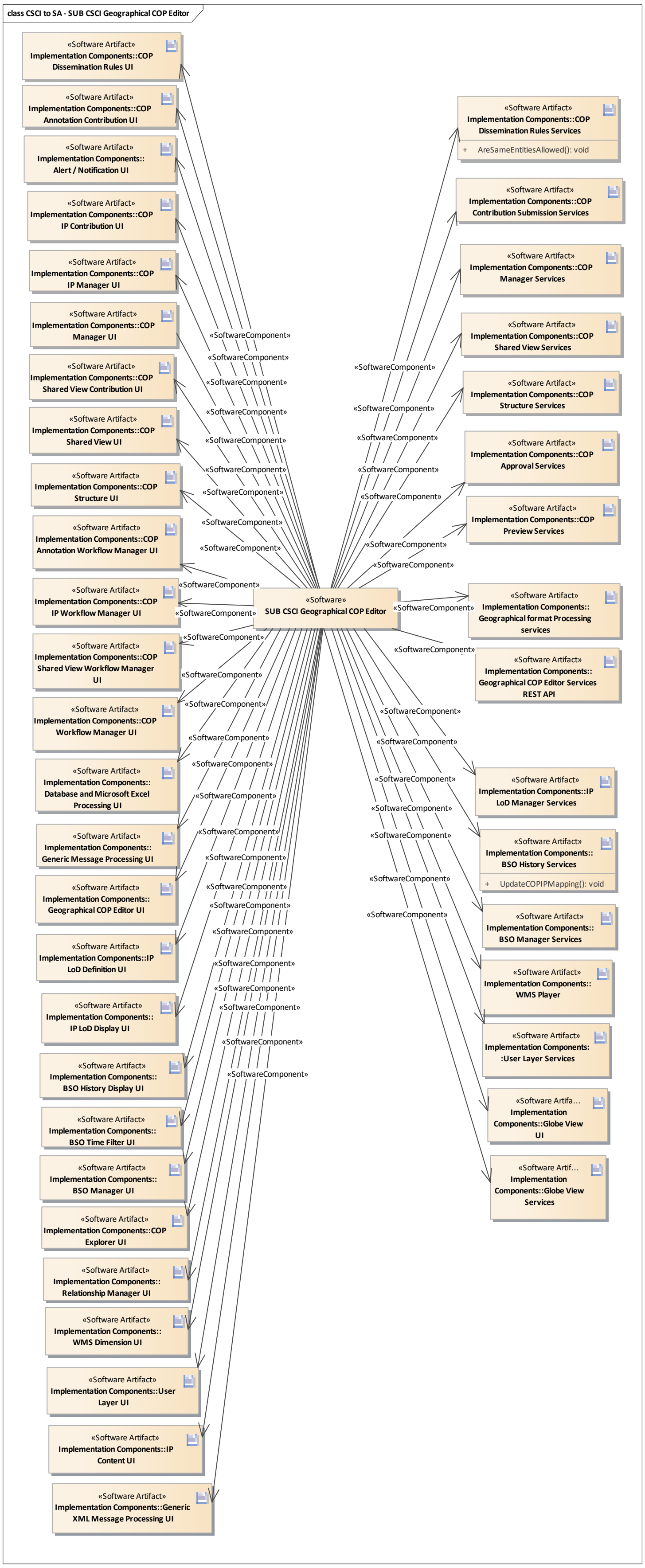

class CSCI to SA - CSCI COTS Software
«Software»
CSCI COTS Software
«Software Artifact»
Implementation Components::Active Directory
«Software Artifact»
Implementation Components::Core GIS Web Services
«Software Artifact»
Implementation Components::Document Handling System
«Software Artifact»
Implementation Components::OpenJDK
«Software Artifact»
Implementation Components::Antivirus
«Software Artifact»
Implementation Components::Identity Provider UI
«Software Artifact»
Implementation Components::Microsoft Office
«Software Artifact»
Implementation Components::Microsoft .NET Framework
«Software Artifact»
Implementation Components::PulseSecure Traffic Manager
«Software Artifact»
Implementation Components::Microsoft Biztalk Server
«Software Artifact»
Implementation Components::Microsoft Hyper-V
«Software Artifact»
Implementation Components::Microsoft Edge Chromium
«Software Artifact»
Implementation Components::Microsoft Internet Information Server
«Software Artifact»
Implementation Components::VMware
«Software Artifact»
Implementation Components::GeoServer
«Software Artifact»
Implementation Components::NEDS
«Software Artifact»
Implementation Components::SNMP Services
«Software Artifact»
Implementation Components::PDF Reader
«Software Artifact»
Implementation Components::Altova MapForce
«Software Artifact»
Implementation Components::Security Services and Settings
«Software Artifact»
Implementation Components::Microsoft Windows
«Software Artifact»
Implementation Components::Microsoft Windows Server
«Software Artifact»
Implementation Components::Microsoft SharePoint Central Administration
«Software Artifact»
Implementation Components::Microsoft SQL Server
«Software Artifact»
Implementation Components::Angular
«Software Artifact»
Implementation Components::Microsoft SharePoint Server: ISharepointAccessor
«Software Artifact»
Implementation Components::D3.js
«Software Artifact»
Implementation Components::PrimeNG
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»

B.8.4.4 NCOP2 Software

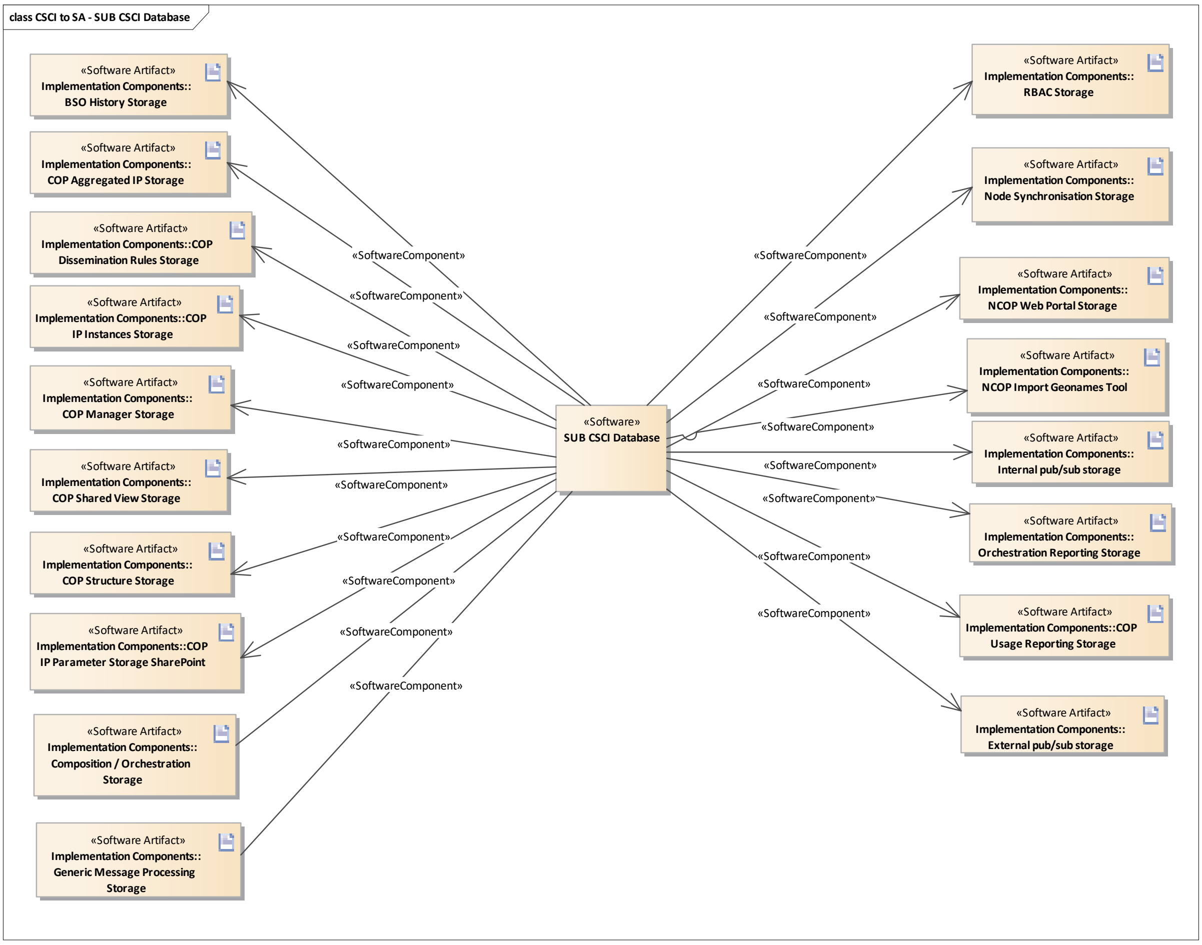
B.8.4.4.1 Portal


class CSCI to SA - SUB CSCI Portal
«Software»
SUB CSCI Portal
«Software Artifact» Implementation Components:: Journal Management UI
«Software Artifact» Implementation Components:: Audit / Log UI
«Software Artifact» Implementation Components:: NCOP Web Portal UI
«Software Artifact» Implementation Components:: Management Information UI
«Software Artifact» Implementation Components:: Node Synchronisation UI
«Software Artifact» Implementation Components:: Jchat
«Software Artifact» Implementation Components:: Identity Provider Services
«Software Artifact» Implementation Components:: Authentication and Authorization Services
«Software Artifact» Implementation Components:: Archive/Restore Services
«Software Artifact» Implementation Components:: Training UI
«Software Artifact» Implementation Components:: Archive/Restore UI
«Software Artifact» Implementation Components:: RBAC UI
«Software Artifact» Implementation Components:: Signature Services
«Software Artifact» Implementation Components:: RBAC Services
«Software Artifact» Implementation Components::Node Synchronisation Services
«Software Artifact» Implementation Components:: Node Synchronisation Configuration Services
«Software Artifact» Implementation Components:: Labelling Services
«Software Artifact» Implementation Components:: Event Manager Services
«Software Artifact» Implementation Components:: Cross Domain Services
«Software Artifact» Implementation Components:: SharePoint Accessor Services
«Software Artifact» Implementation Components::List Helper
«SoftwareComponent»

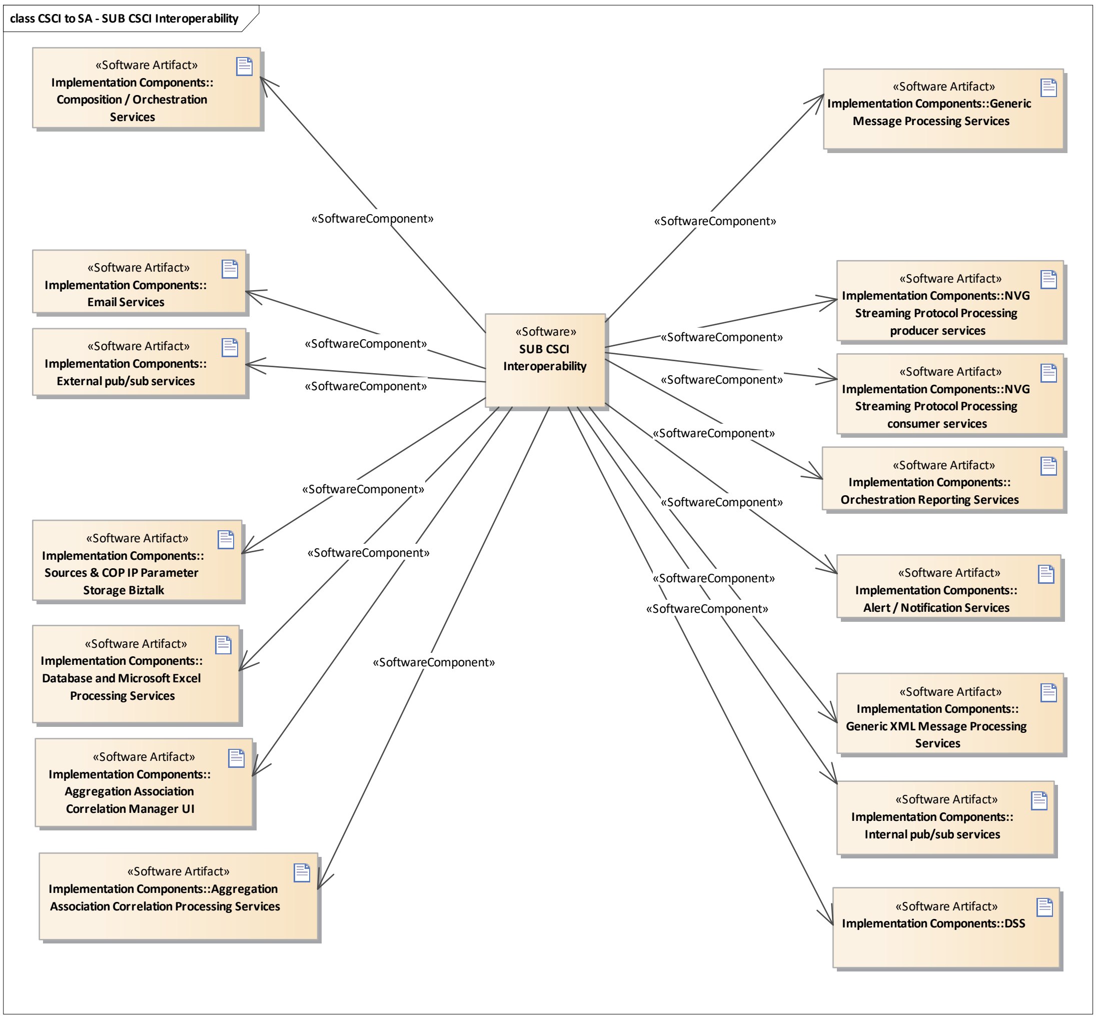
B.8.4.4.2 Geographical COP Editor


class CSCI to SA - SUB CSCI Geographical COP Editor
«Software Artifact» Implementation Components::COP Dissemination Rules UI
«Software Artifact» Implementation Components::COP Annotation Contribution UI
«Software Artifact» Implementation Components:: Alert / Notification UI
«Software Artifact» Implementation Components::COP IP Contribution UI
«Software Artifact» Implementation Components::COP IP Manager UI
«Software Artifact» Implementation Components::COP Manager UI
«Software Artifact» Implementation Components::COP Shared View Contribution UI
«Software Artifact» Implementation Components::COP Shared View UI
«Software Artifact» Implementation Components::COP Structure UI
«Software Artifact» Implementation Components::COP Annotation Workflow Manager UI
«Software Artifact» Implementation Components::COP IP Workflow Manager UI
«Software Artifact» Implementation Components::COP Shared View Workflow Manager UI
«Software Artifact» Implementation Components::COP Workflow Manager UI
«Software Artifact» Implementation Components:: Database and Microsoft Excel Processing UI
«Software Artifact» Implementation Components:: Generic Message Processing UI
«Software Artifact» Implementation Components:: Geographical COP Editor UI
«Software Artifact» Implementation Components::IP LoD Definition UI
«Software Artifact» Implementation Components:: IP LoD Display UI
«Software Artifact» Implementation Components:: BSO History Display UI
«Software Artifact» Implementation Components:: BSO Time Filter UI
«Software Artifact» Implementation Components:: BSO Manager UI
«Software Artifact» Implementation Components::COP Explorer UI
«Software Artifact» Implementation Components:: Relationship Manager UI
«Software Artifact» Implementation Components:: WMS Dimension UI
«Software Artifact» Implementation Components::User Layer UI
«Software Artifact» Implementation Components::IP Content UI
«Software Artifact» Implementation Components::Generic XML Message Processing UI
«Software» SUB CSCI Geographical COP Editor
«Software Artifact» Implementation Components::COP Dissemination Rules Services
+ AreSameEntitiesAllowed(): void
«Software Artifact» Implementation Components::COP Contribution Submission Services
«Software Artifact» Implementation Components::COP Manager Services
«Software Artifact» Implementation Components::COP Shared View Services
«Software Artifact» Implementation Components::COP Structure Services
«Software Artifact» Implementation Components::COP Approval Services
«Software Artifact» Implementation Components::COP Preview Services
«Software Artifact» Implementation Components:: Geographical format Processing services
«Software Artifact» Implementation Components:: Geographical COP Editor Services REST API
«Software Artifact» Implementation Components::IP LoD Manager Services
«Software Artifact» Implementation Components:: BSO History Services
+ UpdateCOPIPMapping(): void
«Software Artifact» Implementation Components:: BSO Manager Services
«Software Artifact» Implementation Components:: WMS Player
«Software Artifact» Implementation Components: :User Layer Services
«Software Artifa... Implementation Components::Globe View UI
«Software Artif... Implementation Components::Globe View Services
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»

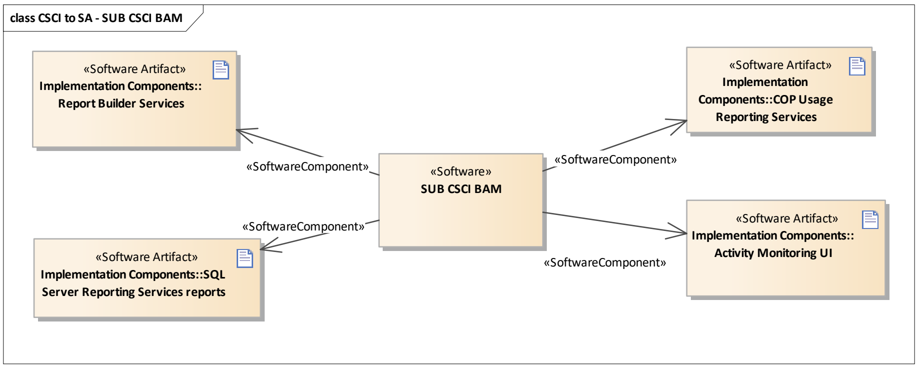
B.8.4.4.3 Database


class CSCI to SA - SUB CSCI Database
«Software»
SUB CSCI Database
«SoftwareComponent»
«Software Artifact»
Implementation Components::
BSO History Storage
«Software Artifact»
Implementation Components::
COP Aggregated IP Storage
«Software Artifact»
Implementation Components::COP
Dissemination Rules Storage
«Software Artifact»
Implementation Components::COP
IP Instances Storage
«Software Artifact»
Implementation Components::
COP Manager Storage
«Software Artifact»
Implementation Components::
COP Shared View Storage
«Software Artifact»
Implementation Components::
COP Structure Storage
«Software Artifact»
Implementation Components::COP
IP Parameter Storage SharePoint
«Software Artifact»
Implementation Components::
Composition / Orchestration
Storage
«Software Artifact»
Implementation Components::
Generic Message Processing
Storage
«Software Artifact»
Implementation Components::
RBAC Storage
«Software Artifact»
Implementation Components::
Node Synchronisation Storage
«Software Artifact»
Implementation Components::
NCOP Web Portal Storage
«Software Artifact»
Implementation Components::
NCOP Import Geonames Tool
«Software Artifact»
Implementation Components::
Internal pub/sub storage
«Software Artifact»
Implementation Components::
Orchestration Reporting Storage
«Software Artifact»
Implementation Components::COP
Usage Reporting Storage
«Software Artifact»
Implementation Components::
External pub/sub storage

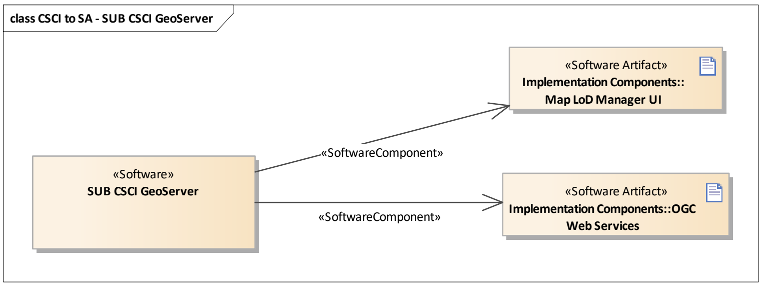
B.8.4.4.4 Interoperability


class CSCI to SA - SUB CSCI Interoperability
«Software»
SUB CSCI Interoperability
«Software Artifact»
Implementation Components:: Composition / Orchestration Services
«Software Artifact»
Implementation Components:: Email Services
«Software Artifact»
Implementation Components:: External pub/sub services
«Software Artifact»
Implementation Components:: Sources & COP IP Parameter Storage Biztalk
«Software Artifact»
Implementation Components:: Database and Microsoft Excel Processing Services
«Software Artifact»
Implementation Components:: Aggregation Association Correlation Manager UI
«Software Artifact»
Implementation Components::Aggregation Association Correlation Processing Services
«Software Artifact»
Implementation Components::Generic Message Processing Services
«Software Artifact»
Implementation Components::NVG Streaming Protocol Processing producer services
«Software Artifact»
Implementation Components::NVG Streaming Protocol Processing consumer services
«Software Artifact»
Implementation Components:: Orchestration Reporting Services
«Software Artifact»
Implementation Components:: Alert / Notification Services
«Software Artifact»
Implementation Components:: Generic XML Message Processing Services
«Software Artifact»
Implementation Components:: Internal pub/sub services
«Software Artifact»
Implementation Components::DSS
«SoftwareComponent»

B.8.4.4.5 BAM

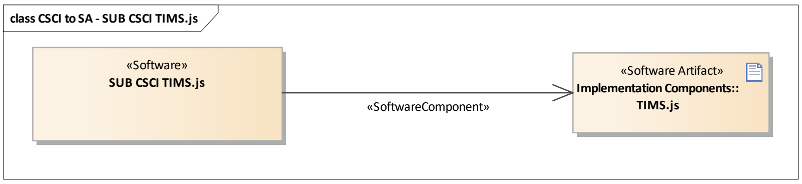

class CSCI to SA - SUB CSCI BAM
«Software»
SUB CSCI BAM
«Software Artifact»
Implementation Components:: Report Builder Services
«Software Artifact»
Implementation Components::SQL Server Reporting Services reports
«Software Artifact»
Implementation Components::COP Usage Reporting Services
«Software Artifact»
Implementation Components:: Activity Monitoring UI
«SoftwareComponent»

B.8.4.4.6 GeoServer

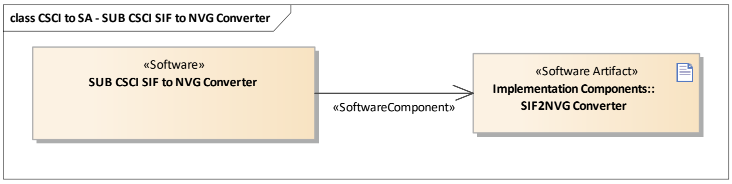


B.8.4.5 TIMS & Add-Ins

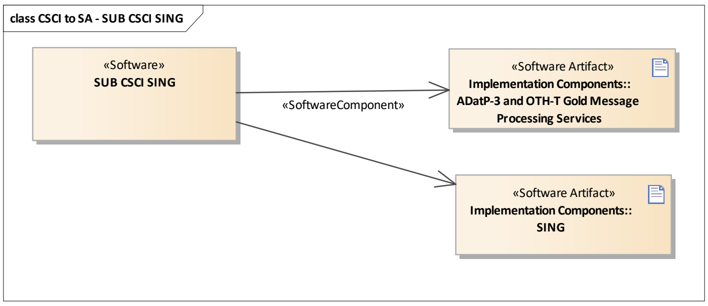
B.8.4.5.1 TIMS.js



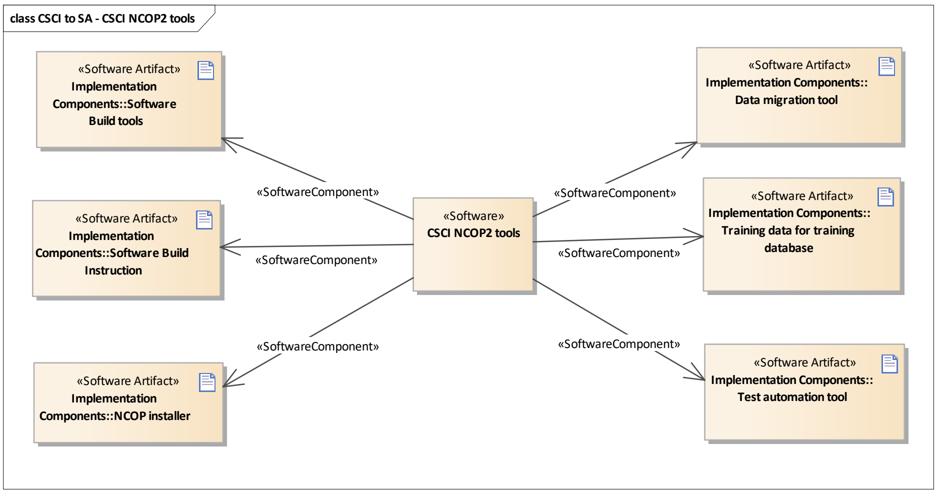
B.8.4.5.2 SIF to NVG converter


class CSCI to SA - SUB CSCI SIF to NVG Converter
«Software»
SUB CSCI SIF to NVG Converter
«SoftwareComponent»
«Software Artifact»
Implementation Components::
SIF2NVG Converter

B.8.4.5.3 SING

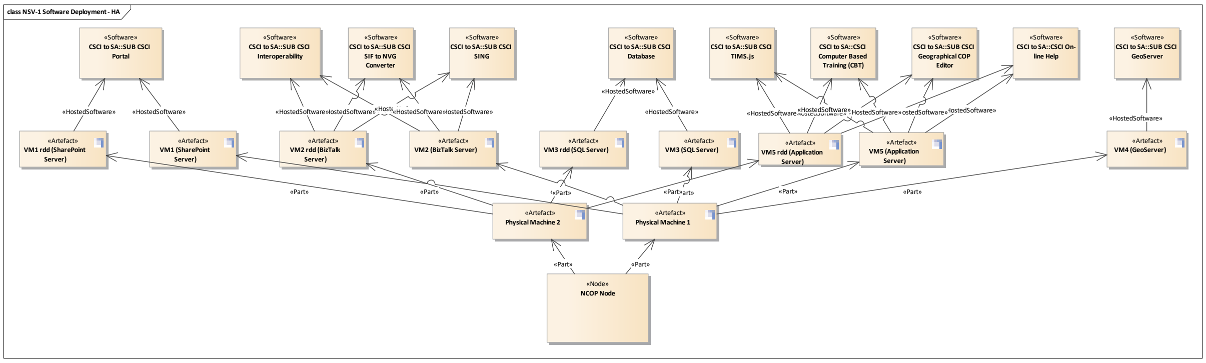

class CSCI to SA - SUB CSCI SING
«Software»
SUB CSCI SING
«SoftwareComponent»
«Software Artifact»
Implementation Components::
ADatP-3 and OTH-T Gold Message
Processing Services
«Software Artifact»
Implementation Components::
SING

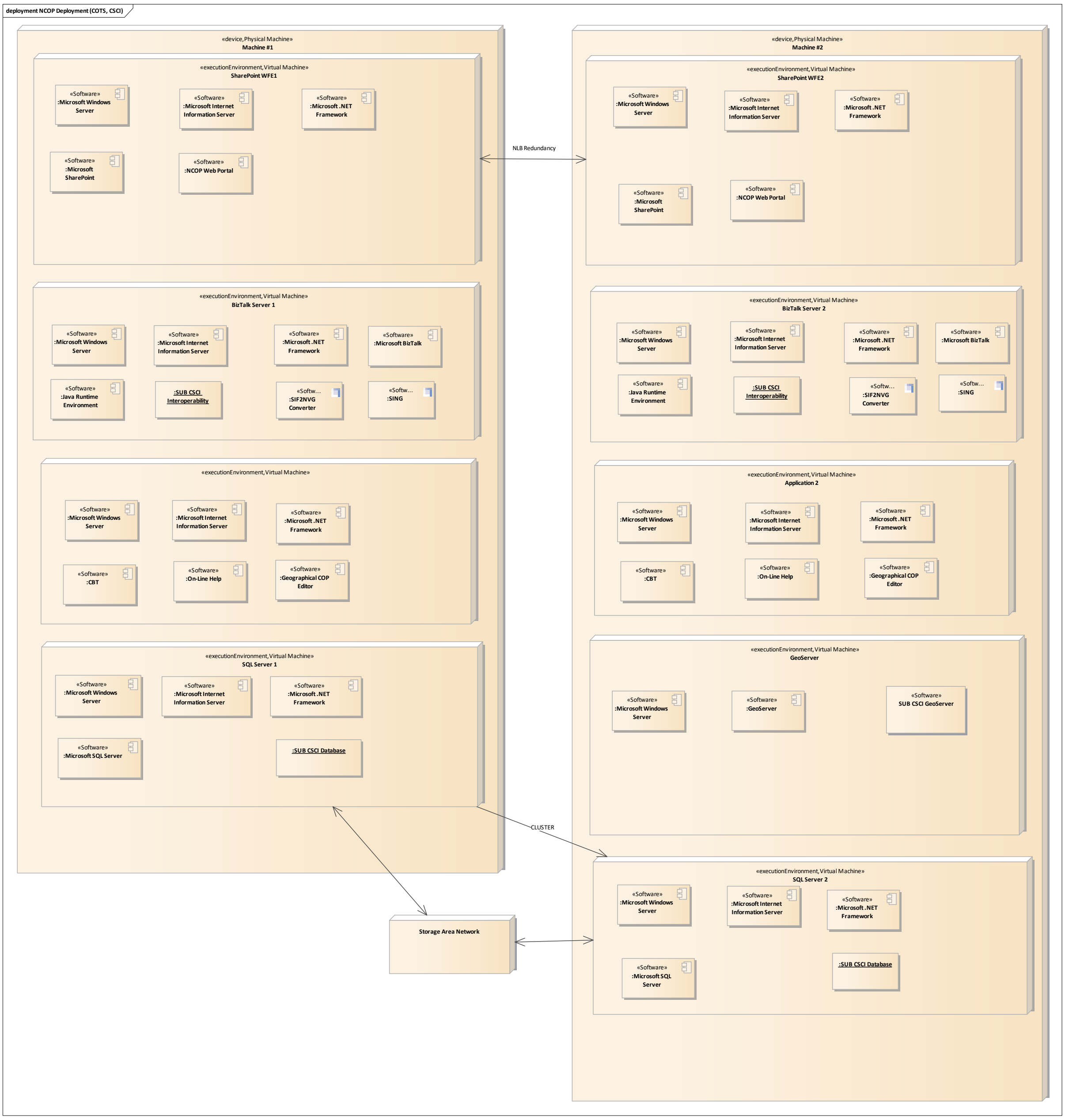
B.8.4.6 NCOP2 tools


class CSCI to SA - CSCI NCOP2 tools
«Software Artifact» Implementation Components::Software Build tools
«Software Artifact» Implementation Components::Software Build Instruction
«Software Artifact» Implementation Components::NCOP installer
«Software» CSCI NCOP2 tools
«Software Artifact» Implementation Components:: Data migration tool
«Software Artifact» Implementation Components:: Training data for training database
«Software Artifact» Implementation Components:: Test automation tool
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»
«SoftwareComponent»

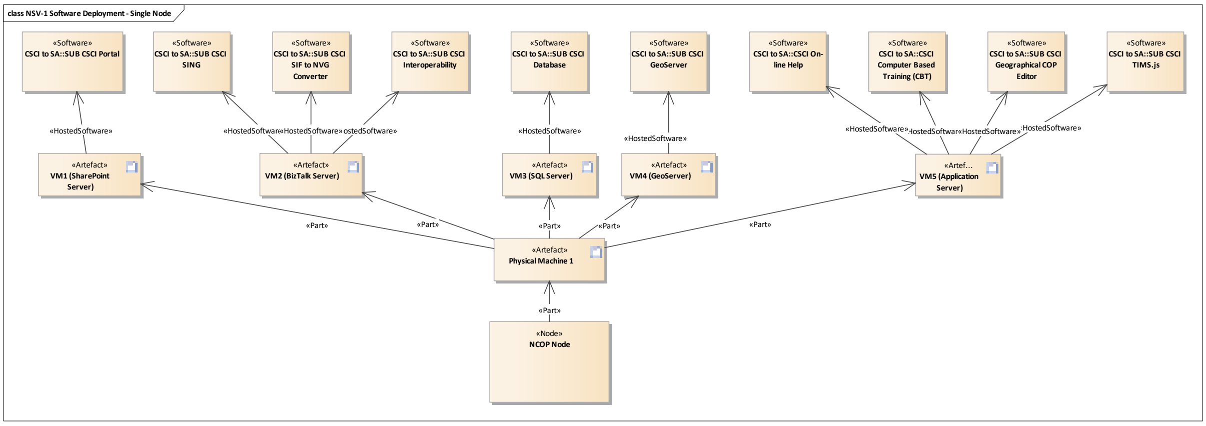
B.8.5 Software deployment

B.8.5.1 High Availability virtualised deployment

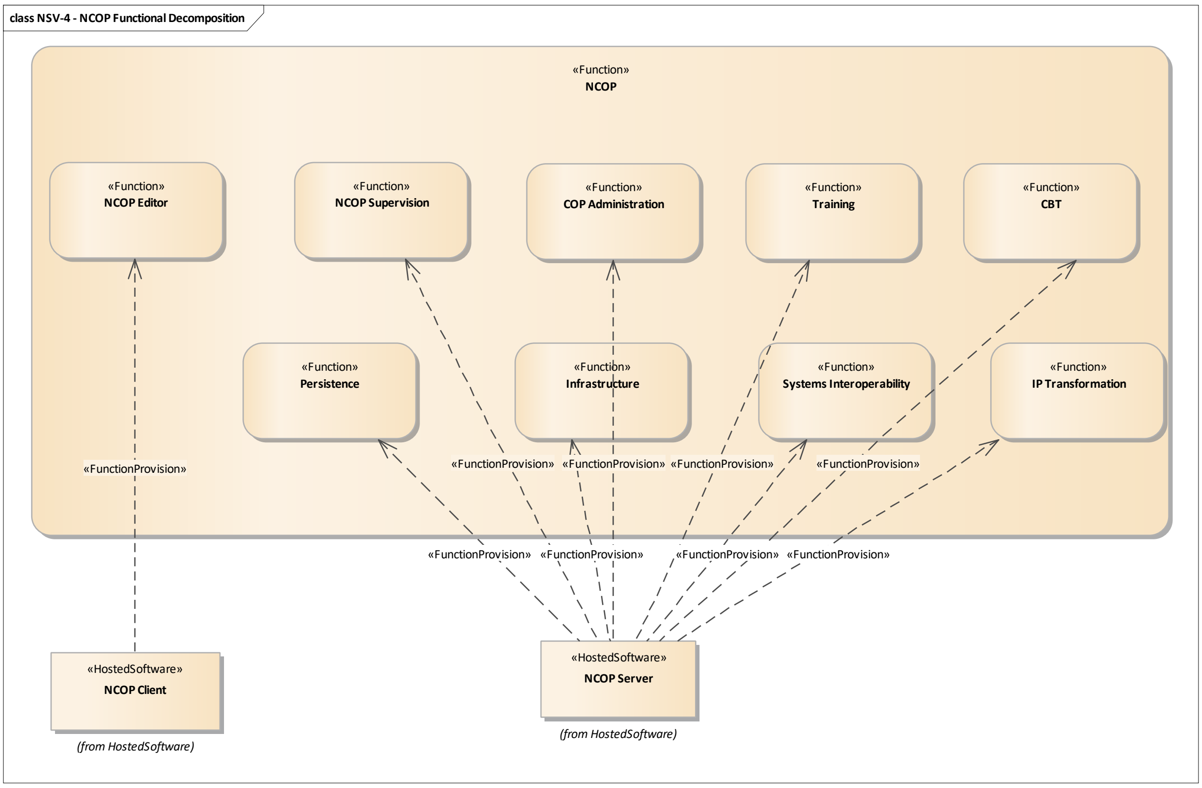

class NSV-1 Software Deployment - HA
«Software» CSCI to SA::SUB CSCI Portal
«Software» CSCI to SA::SUB CSCI Interoperability
«Software» CSCI to SA::SUB CSCI SIF to NVG Converter
«Software» CSCI to SA::SUB CSCI SING
«Software» CSCI to SA::SUB CSCI Database
«Software» CSCI to SA::SUB CSCI TIMS.js
«Software» CSCI to SA::CSCI Computer Based Training (CBT)
«Software» CSCI to SA::SUB CSCI Geographical COP Editor
«Software» CSCI to SA::CSCI On-line Help
«Software» CSCI to SA::SUB CSCI GeoServer
«HostedSoftware»
«Artefact» VM1 rdd (SharePoint Server)
«Artefact» VM1 (SharePoint Server)
«Artefact» VM2 rdd (BizTalk Server)
«Artefact» VM2 (BizTalk Server)
«Artefact» VM3 rdd (SQL Server)
«Artefact» VM3 (SQL Server)
«Artefact» VM5 rdd (Application Server)
«Artefact» VM5 (Application Server)
«Artefact» VM4 (GeoServer)
«Part»
«Artefact» Physical Machine 2
«Artefact» Physical Machine 1
«Node» NCOP Node


deployment NCOP Deployment (COTS, CSCI)
«device,Physical Machine»
Machine #1
«executionEnvironment,Virtual Machine»
SharePoint WFE1
«Software»
:Microsoft Windows Server
«Software»
:Microsoft Internet Information Server
«Software»
:Microsoft .NET Framework
«Software»
:Microsoft SharePoint
«Software»
:NCOP Web Portal
«executionEnvironment,Virtual Machine»
BizTalk Server 1
«Software»
:Microsoft Windows Server
«Software»
:Microsoft Internet Information Server
«Software»
:Microsoft .NET Framework
«Software»
:Microsoft BizTalk
«Software»
:Java Runtime Environment
:SUB CSCI Interoperability
«Softw...
:SIF2NVG Converter
«Softw...
:SING
«executionEnvironment,Virtual Machine»
«Software»
:Microsoft Windows Server
«Software»
:Microsoft Internet Information Server
«Software»
:Microsoft .NET Framework
«Software»
:CBT
«Software»
:On-Line Help
«Software»
:Geographical COP Editor
«executionEnvironment,Virtual Machine»
SQL Server 1
«Software»
:Microsoft Windows Server
«Software»
:Microsoft Internet Information Server
«Software»
:Microsoft .NET Framework
«Software»
:Microsoft SQL Server
:SUB CSCI Database
NLB Redundancy
CLUSTER
Storage Area Network
«device,Physical Machine»
Machine #2
«executionEnvironment,Virtual Machine»
SharePoint WFE2
«Software»
:Microsoft Windows Server
«Software»
:Microsoft Internet Information Server
«Software»
:Microsoft .NET Framework
«Software»
:Microsoft SharePoint
«Software»
:NCOP Web Portal
«executionEnvironment,Virtual Machine»
BizTalk Server 2
«Software»
:Microsoft Windows Server
«Software»
:Microsoft Internet Information Server
«Software»
:Microsoft .NET Framework
«Software»
:Microsoft BizTalk
«Software»
:Java Runtime Environment
:SUB CSCI Interoperability
«Softw...
:SIF2NVG Converter
«Softw...
:SING
«executionEnvironment,Virtual Machine»
Application 2
«Software»
:Microsoft Windows Server
«Software»
:Microsoft Internet Information Server
«Software»
:Microsoft .NET Framework
«Software»
:CBT
«Software»
:On-Line Help
«Software»
:Geographical COP Editor
«executionEnvironment,Virtual Machine»
GeoServer
«Software»
:Microsoft Windows Server
«Software»
:GeoServer
«Software»
SUB CSCI GeoServer
«executionEnvironment,Virtual Machine»
SQL Server 2
«Software»
:Microsoft Windows Server
«Software»
:Microsoft Internet Information Server
«Software»
:Microsoft .NET Framework
«Software»
:Microsoft SQL Server
:SUB CSCI Database

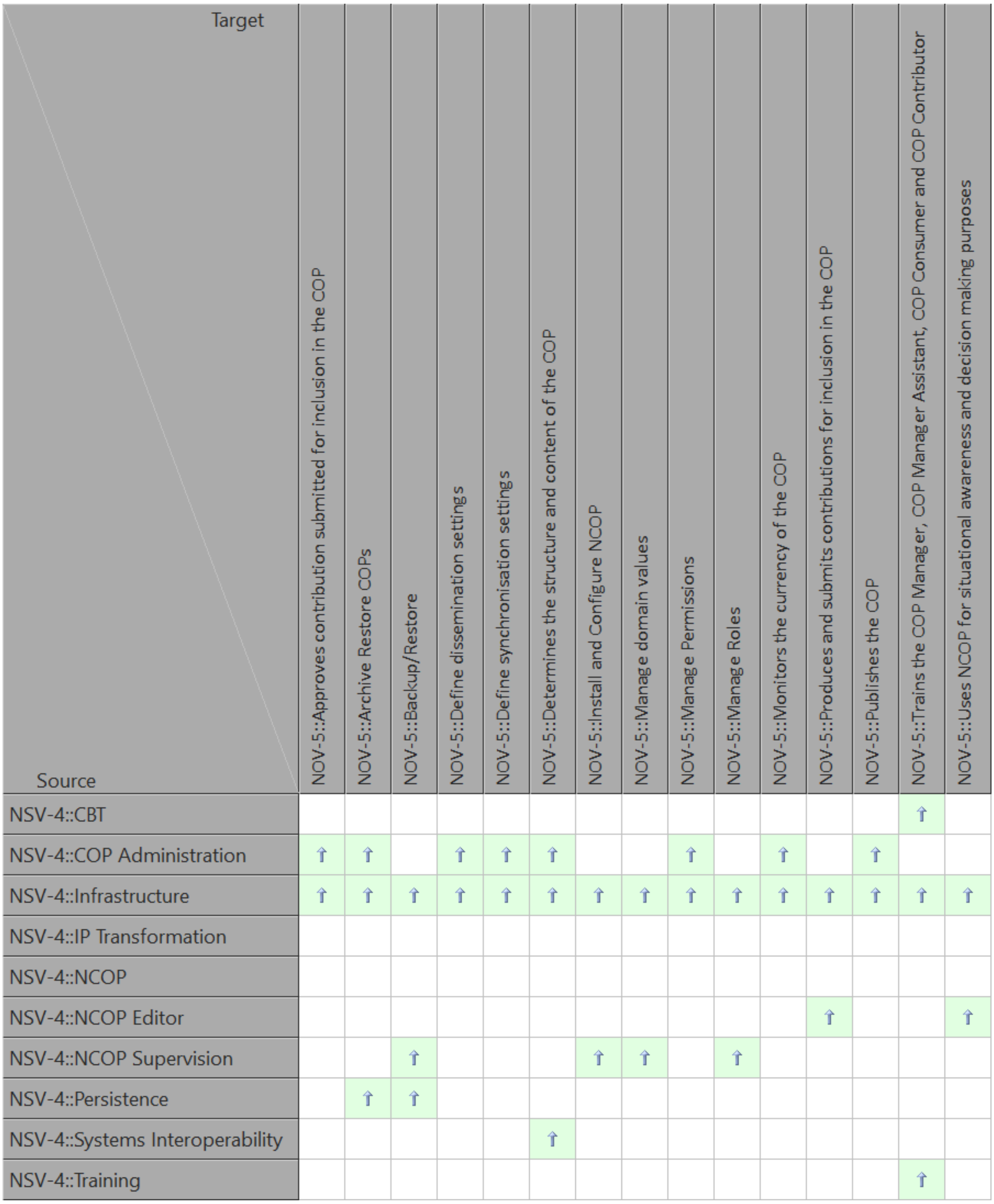
B.8.5.2 Single Node virtualised deployment


class NSV-1 Software Deployment - Single Node
«Software»
CSCI to SA::SUB CSCI Portal
«Software»
CSCI to SA::SUB CSCI SING
«Software»
CSCI to SA::SUB CSCI SIF to NVG Converter
«Software»
CSCI to SA::SUB CSCI Interoperability
«Software»
CSCI to SA::SUB CSCI Database
«Software»
CSCI to SA::SUB CSCI GeoServer
«Software»
CSCI to SA::CSCI On-line Help
«Software»
CSCI to SA::CSCI Computer Based Training (CBT)
«Software»
CSCI to SA::SUB CSCI Geographical COP Editor
«Software»
CSCI to SA::SUB CSCI TIMS.js
«HostedSoftware»
«HostedSoftwar«HostedSoftware» ostedSoftware»
«HostedSoftware»
«HostedSoftware»
«HostedSoftware»›HostedSoftwar«HostedSoftware»›HostedSoftware»
«Artefact»
VM1 (SharePoint Server)
«Artefact»
VM2 (BizTalk Server)
«Artefact»
VM3 (SQL Server)
«Artefact»
VM4 (GeoServer)
«Artef...
VM5 (Application Server)
«Part»
«Part»
«Part»
«Part»
«Part»
«Artefact»
Physical Machine 1
«Part»
«Node»
NCOP Node

B.9 NSV-4

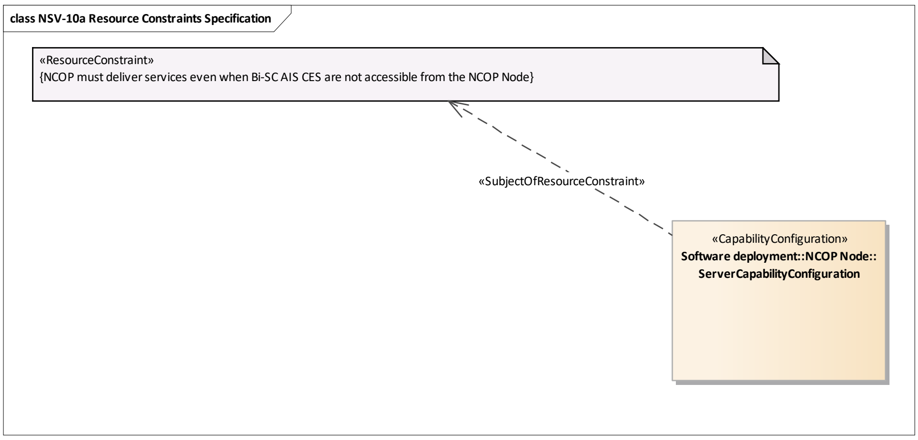

class NSV-4 - NCOP Functional Decomposition
«Function»
NCOP
«Function»
NCOP Editor
«Function»
NCOP Supervision
«Function»
COP Administration
«Function»
Training
«Function»
CBT
«Function»
Persistence
«Function»
Infrastructure
«Function»
Systems Interoperability
«Function»
IP Transformation
«FunctionProvision»
«FunctionProvision»
«FunctionProvision»
«FunctionProvision»
«FunctionProvision»
«FunctionProvision»
«FunctionProvision»
«FunctionProvision»
«FunctionProvision»
«FunctionProvision»
«HostedSoftware»
NCOP Client
(from HostedSoftware)
«HostedSoftware»
NCOP Server
(from HostedSoftware)

B.10 NSV-5



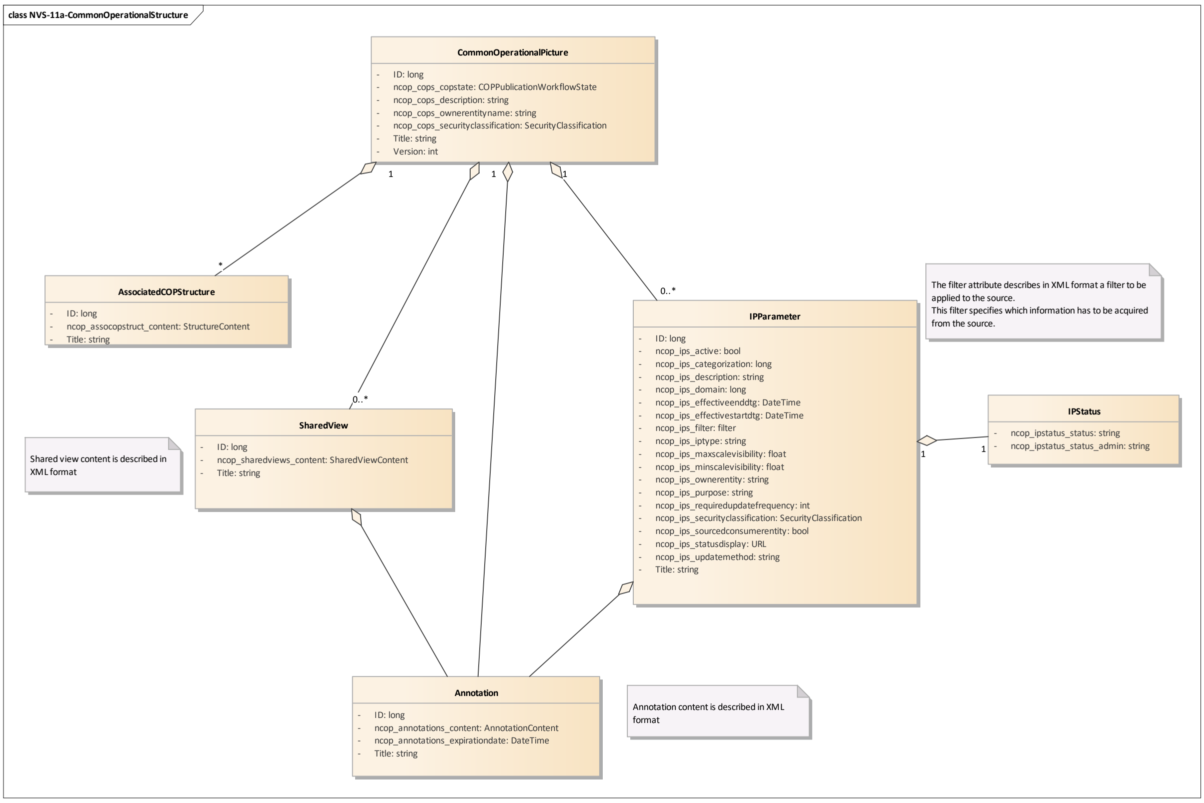
Target Source	NOV-5::Approves contribution submitted for inclusion in the COP	NOV-5::Archive Restore COPs	NOV-5::Backup/Restore	NOV-5::Define dissemination settings	NOV-5::Define synchronisation settings	NOV-5::Determines the structure and content of the COP	NOV-5::Install and Configure NCOP	NOV-5::Manage domain values	NOV-5::Manage Permissions	NOV-5::Manage Roles	NOV-5::Monitors the currency of the COP	NOV-5::Produces and submits contributions for inclusion in the COP	NOV-5::Publishes the COP	NOV-5::Trains the COP Manager, COP Manager Assistant, COP Consumer and COP Contributor	NOV-5::Uses NCOP for situational awareness and decision making purposes
NSV-4::CBT														↑	
NSV-4::COP Administration	↑	↑		↑	↑	↑			↑		↑		↑		
NSV-4::Infrastructure	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
NSV-4::IP Transformation															
NSV-4::NCOP															
NSV-4::NCOP Editor												↑			↑
NSV-4::NCOP Supervision			↑				↑	↑		↑					
NSV-4::Persistence		↑	↑												
NSV-4::Systems Interoperability						↑									
NSV-4::Training														↑	

B.11 NSV-10A

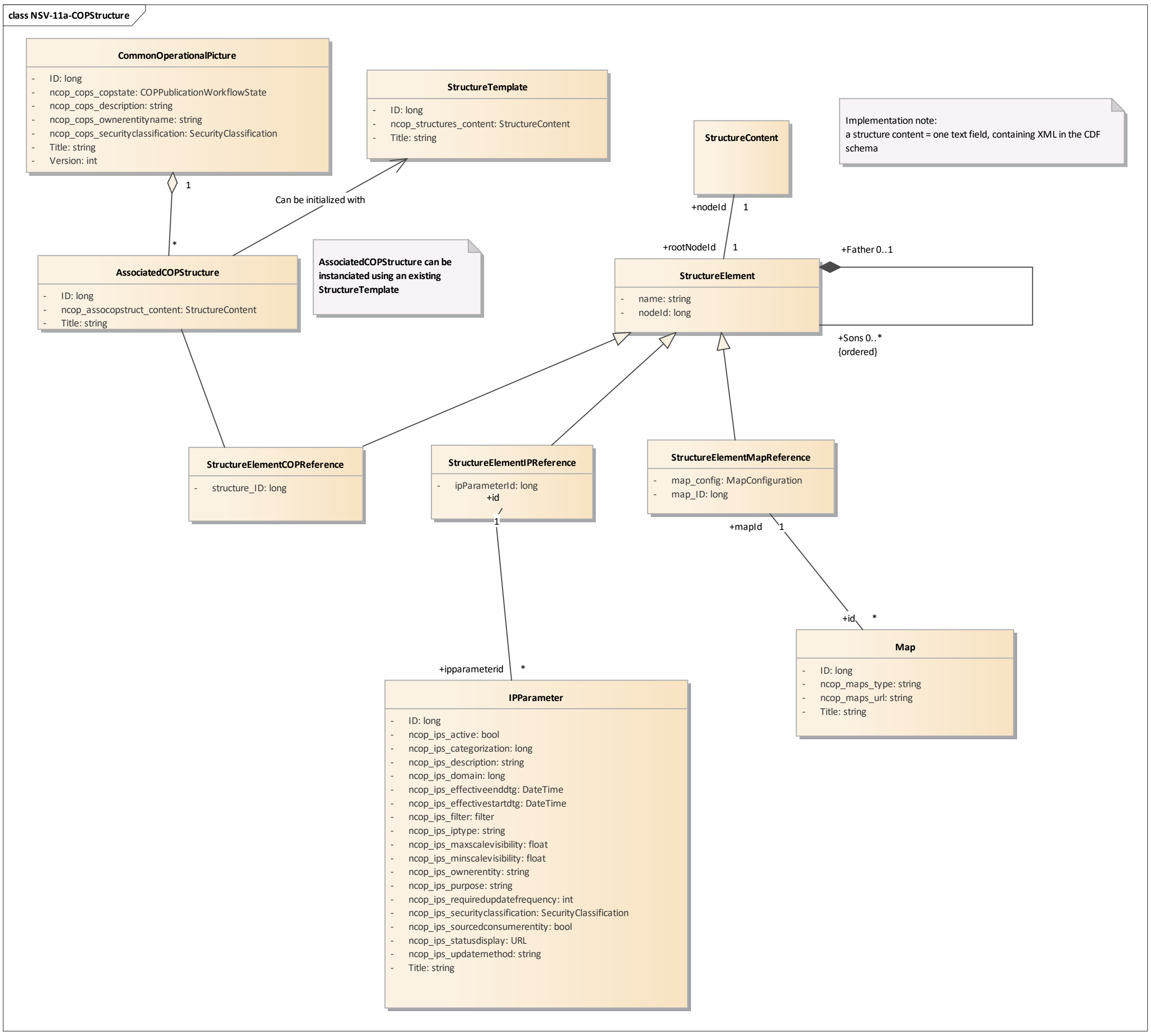

class NSV-10a Resource Constraints Specification
«ResourceConstraint»
{NCOP must deliver services even when Bi-SC AIS CES are not accessible from the NCOP Node}
«SubjectOfResourceConstraint»
«CapabilityConfiguration»
Software deployment::NCOP Node::
ServerCapabilityConfiguration

B.12 NSV-11A

B.12.1 Common Operational Picture


class NVS-11a-CommonOperationalStructure
CommonOperationalPicture
- ID: long
- ncop_cops_copstate: COPPublicationWorkflowState
- ncop_cops_description: string
- ncop_cops_ownerentityname: string
- ncop_cops_securityclassification: SecurityClassification
- Title: string
- Version: int
1
1
1
*
AssociatedCOPStructure
- ID: long
- ncop_assocopstruct_content: StructureContent
- Title: string
0..*
SharedView
- ID: long
- ncop_sharedviews_content: SharedViewContent
- Title: string
Shared view content is described in XML format
0..*
IPParameter
- ID: long
- ncop_ips_active: bool
- ncop_ips_categorization: long
- ncop_ips_description: string
- ncop_ips_domain: long
- ncop_ips_effectiveenddtg: DateTime
- ncop_ips_effectivestartdtg: DateTime
- ncop_ips_filter: filter
- ncop_ips_iptype: string
- ncop_ips_maxscalevisibility: float
- ncop_ips_minscalevisibility: float
- ncop_ips_ownerentity: string
- ncop_ips_purpose: string
- ncop_ips_requiredupdatefrequency: int
- ncop_ips_securityclassification: SecurityClassification
- ncop_ips_sourcedconsumerentity: bool
- ncop_ips_statusdisplay: URL
- ncop_ips_updatemethod: string
- Title: string
The filter attribute describes in XML format a filter to be applied to the source.
This filter specifies which information has to be acquired from the source.
1
1
IPStatus
- ncop_ipstatus_status: string
- ncop_ipstatus_status_admin: string
Annotation
- ID: long
- ncop_annotations_content: AnnotationContent
- ncop_annotations_expirationdate: DateTime
- Title: string
Annotation content is described in XML format

B.12.2 COP Structure


class NSV-11a-COPStructure
CommonOperationalPicture
- ID: long
- ncop_cops_copstate: COPPublicationWorkflowState
- ncop_cops_description: string
- ncop_cops_ownerentityname: string
- ncop_cops_securityclassification: SecurityClassification
- Title: string
- Version: int
StructureTemplate
- ID: long
- ncop_structures_content: StructureContent
- Title: string
StructureContent
1
Can be initialized with
*
AssociatedCOPStructure
- ID: long
- ncop_assocopstruct_content: StructureContent
- Title: string
+nodeId
1
+rootNodeId
1
+Father 0..1
StructureElement
- name: string
- nodeId: long
+Sons 0..*
{ordered}
StructureElementCOPReference
- structure_ID: long
StructureElementIPReference
- ipParameterId: long
+id
1
StructureElementMapReference
- map_config: MapConfiguration
- map_ID: long
+mapId
1
+id
*
Map
- ID: long
- ncop_maps_type: string
- ncop_maps_url: string
- Title: string
+ipparameterid
*
IPParameter
- ID: long
- ncop_ips_active: bool
- ncop_ips_categorization: long
- ncop_ips_description: string
- ncop_ips_domain: long
- ncop_ips_effectiveenddtg: DateTime
- ncop_ips_effectivestartdtg: DateTime
- ncop_ips_filter: filter
- ncop_ips_iptype: string
- ncop_ips_maxscalevisibility: float
- ncop_ips_minscalevisibility: float
- ncop_ips_ownerentity: string
- ncop_ips_purpose: string
- ncop_ips_requiredupdatefrequency: int
- ncop_ips_securityclassification: SecurityClassification
- ncop_ips_sourcedconsumerentity: bool
- ncop_ips_statusdisplay: URL
- ncop_ips_updatemethod: string
- Title: string

Implementation note:
a structure content = one text field, containing XML in the CDF schema

AssociatedCOPStructure can be instanciated using an existing StructureTemplate

B.12.3 BSO

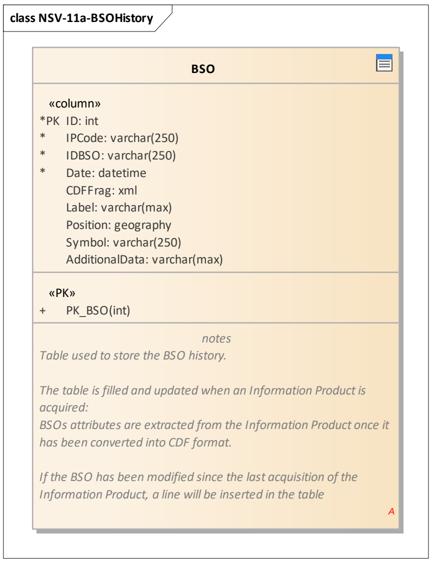
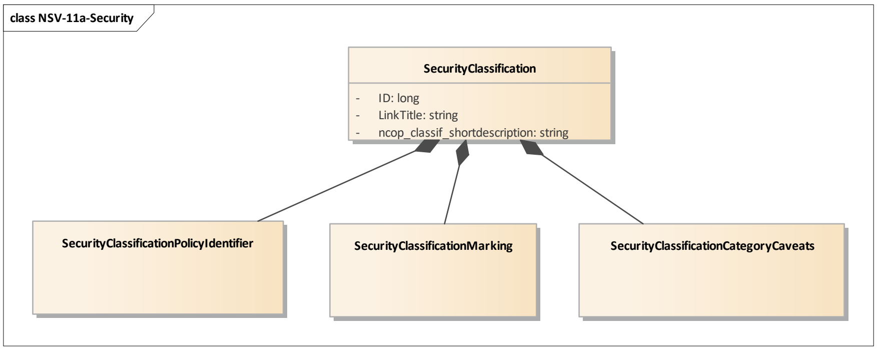


Table used to store the BSO history.

The table is filled and updated when an Information Product is acquired:
BSOs attributes are extracted from the Information Product once it has been converted into CDF format.

If the BSO has been modified since the last acquisition of the Information Product, a line will be inserted in the table

B.12.4 Security


class NSV-11a-Security
SecurityClassification
- ID: long
- LinkTitle: string
- ncop_classif_shortdescription: string
SecurityClassificationPolicyIdentifier
SecurityClassificationMarking
SecurityClassificationCategoryCaveats

B.13 NTV-1

This view corresponds to the “Standard -> CI & Sub CI” tab of the Requirements Traceability Matrix embedded in Appendix A.

B.14 NSOV-2

This view is not provided in accordance with a VTC held between Thales and NCIA on 22 November 2012.

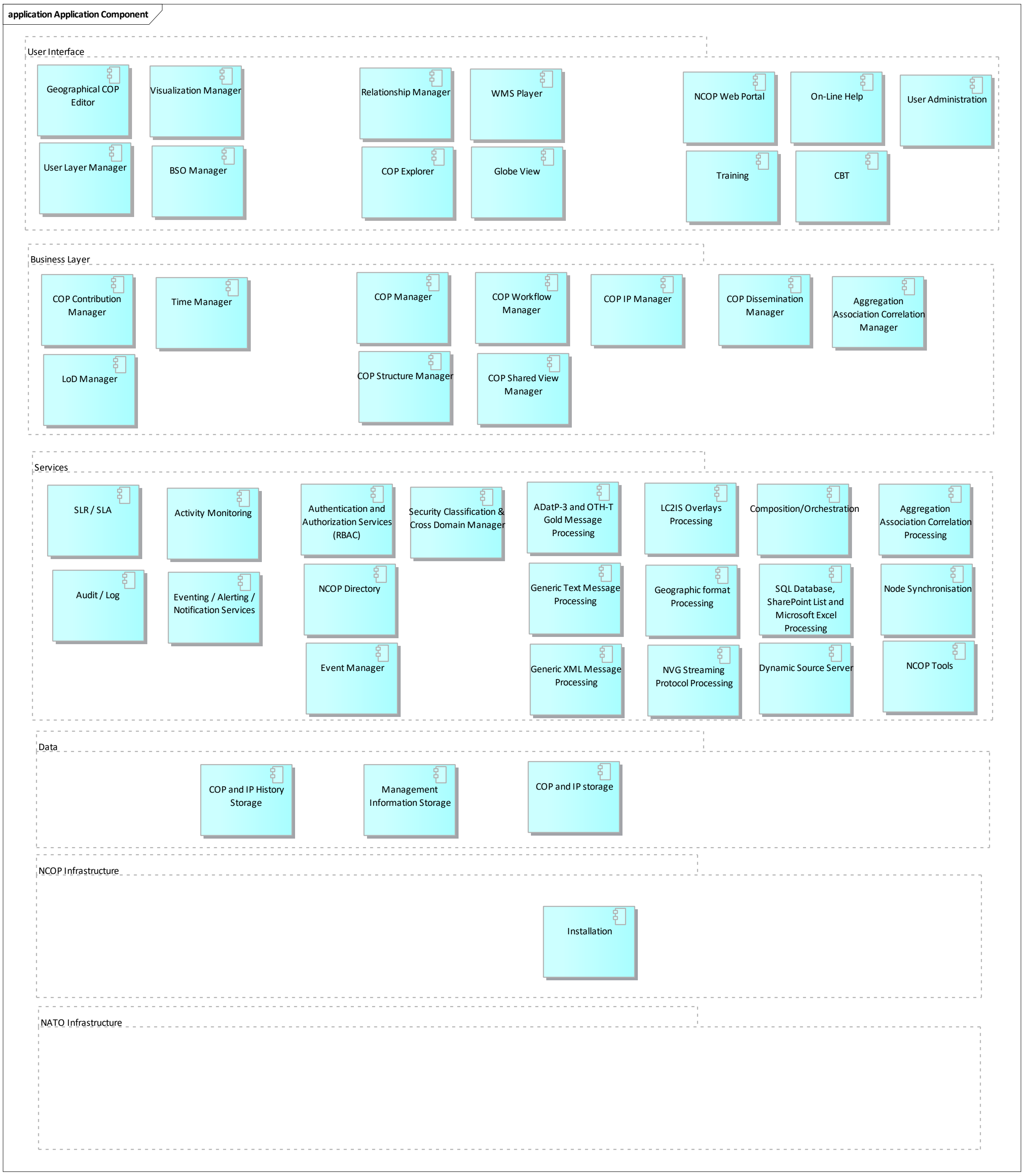
APPENDIX C ARCHIMATE VIEWS

Regarding the Archimate Views concepts, the following definitions have been identified:

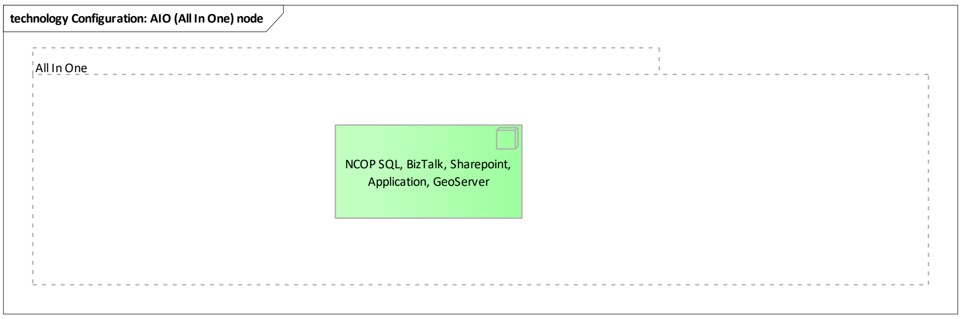
- Application Component: “IS” and “I” green Implementation Components
- System Software: “TI” COTS (yellow) and NATO Infra (orange) Implementation Components
- Node: Virtual Machines
- Application Interface: External Interfaces (sources consumed by NCOP and web services exposed by NCOP)
- Technology Interface: 53 technical interfaces defined in the [SOW]
- Business Process: Standards / Standard profiles (ADatP-3, …)
- Business Role: NISP standard profiles (833)
- Constraint: Availability, Reliability, …

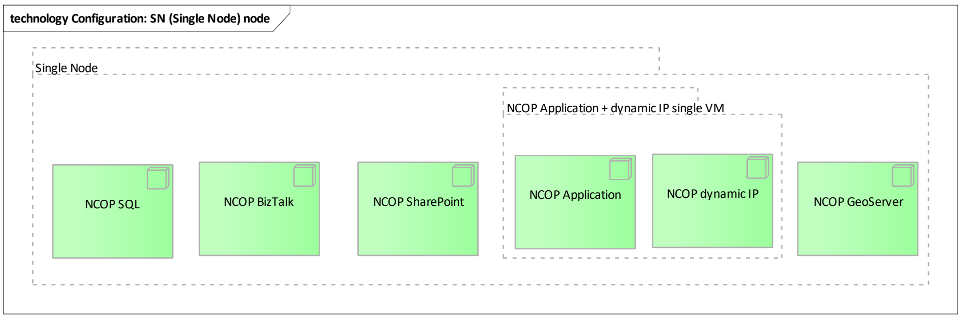
C.1 P1 – RESOURCE TYPES

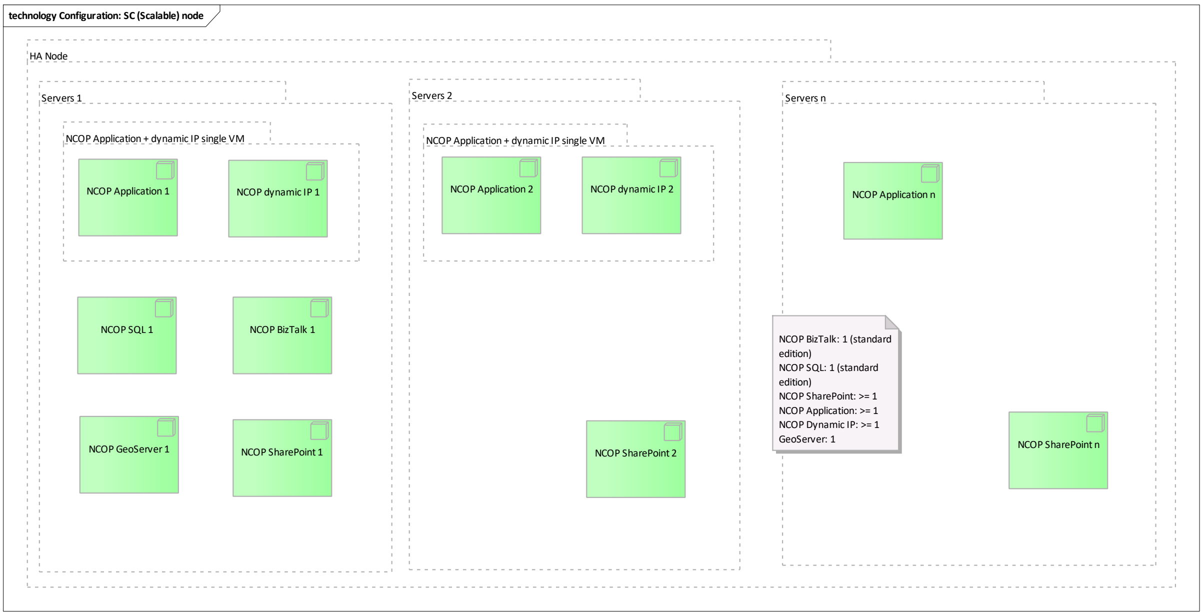
C.1.1 Application Component


application Application Component
User Interface
Geographical COP Editor
Visualization Manager
Relationship Manager
WMS Player
NCOP Web Portal
On-Line Help
User Administration
User Layer Manager
BSO Manager
COP Explorer
Globe View
Training
CBT
Business Layer
COP Contribution Manager
Time Manager
COP Manager
COP Workflow Manager
COP IP Manager
COP Dissemination Manager
Aggregation Association Correlation Manager
LoD Manager
COP Structure Manager
COP Shared View Manager
Services
SLR / SLA
Activity Monitoring
Authentication and Authorization Services (RBAC)
Security Classification & Cross Domain Manager
ADatP-3 and OTH-T Gold Message Processing
LC2IS Overlays Processing
Composition/Orchestration
Aggregation Association Correlation Processing
Audit / Log
Eventing / Alerting / Notification Services
NCOP Directory
Generic Text Message Processing
Geographic format Processing
SQL Database, SharePoint List and Microsoft Excel Processing
Node Synchronisation
Event Manager
Generic XML Message Processing
NVG Streaming Protocol Processing
Dynamic Source Server
NCOP Tools
Data
COP and IP History Storage
Management Information Storage
COP and IP storage
NCOP Infrastructure
Installation
NATO Infrastructure

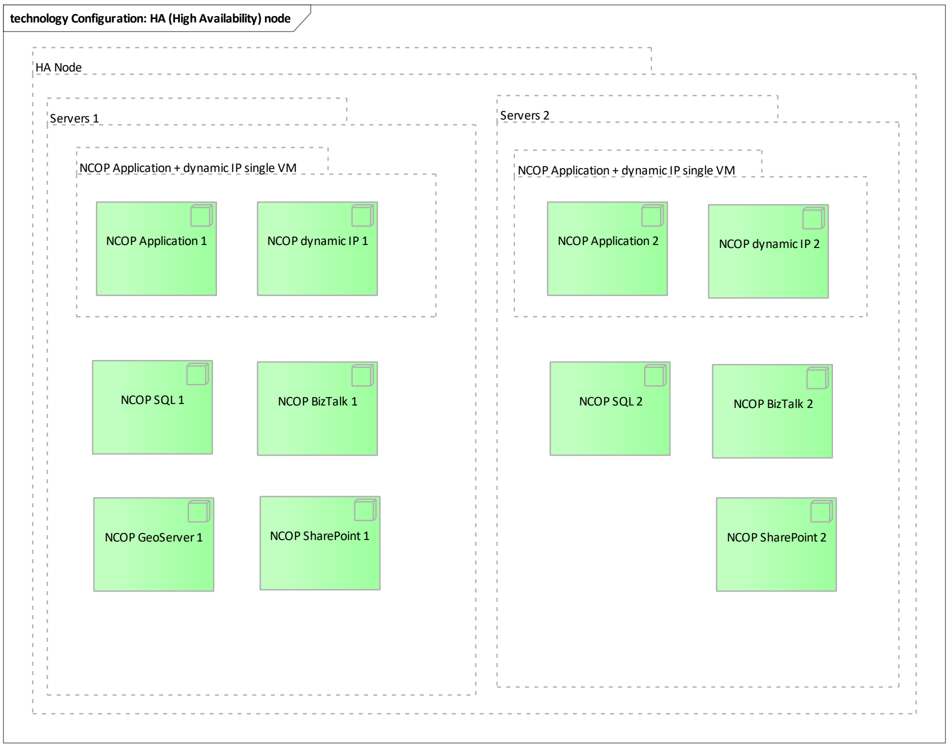
C.1.2 Node

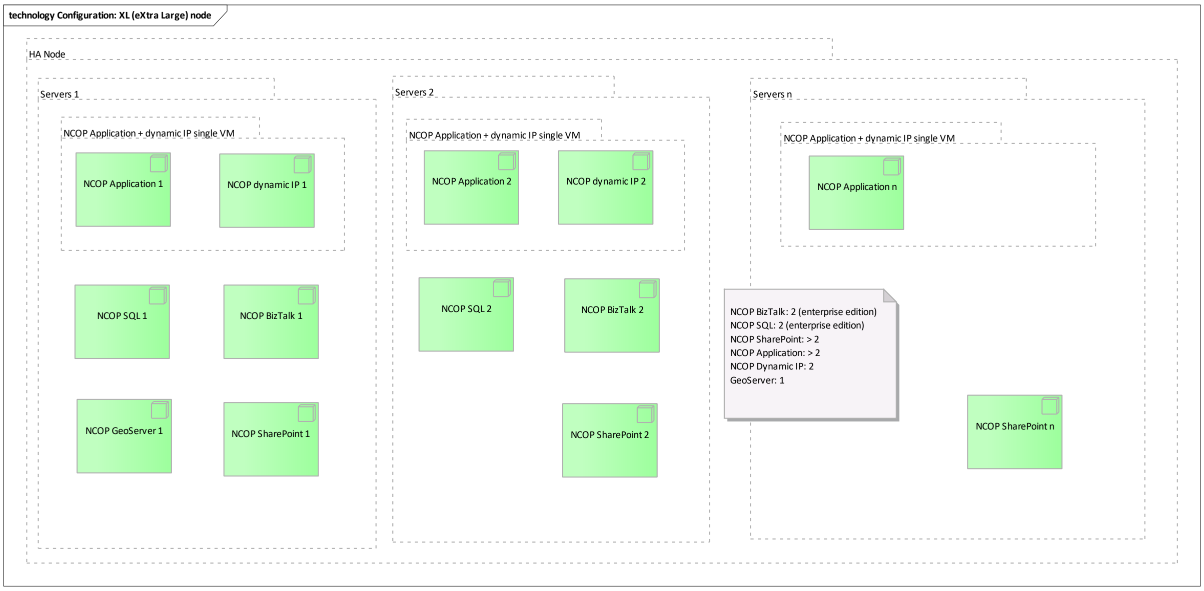

technology Configuration: AIO (All In One) node
All In One
NCOP SQL, BizTalk, Sharepoint, Application, GeoServer





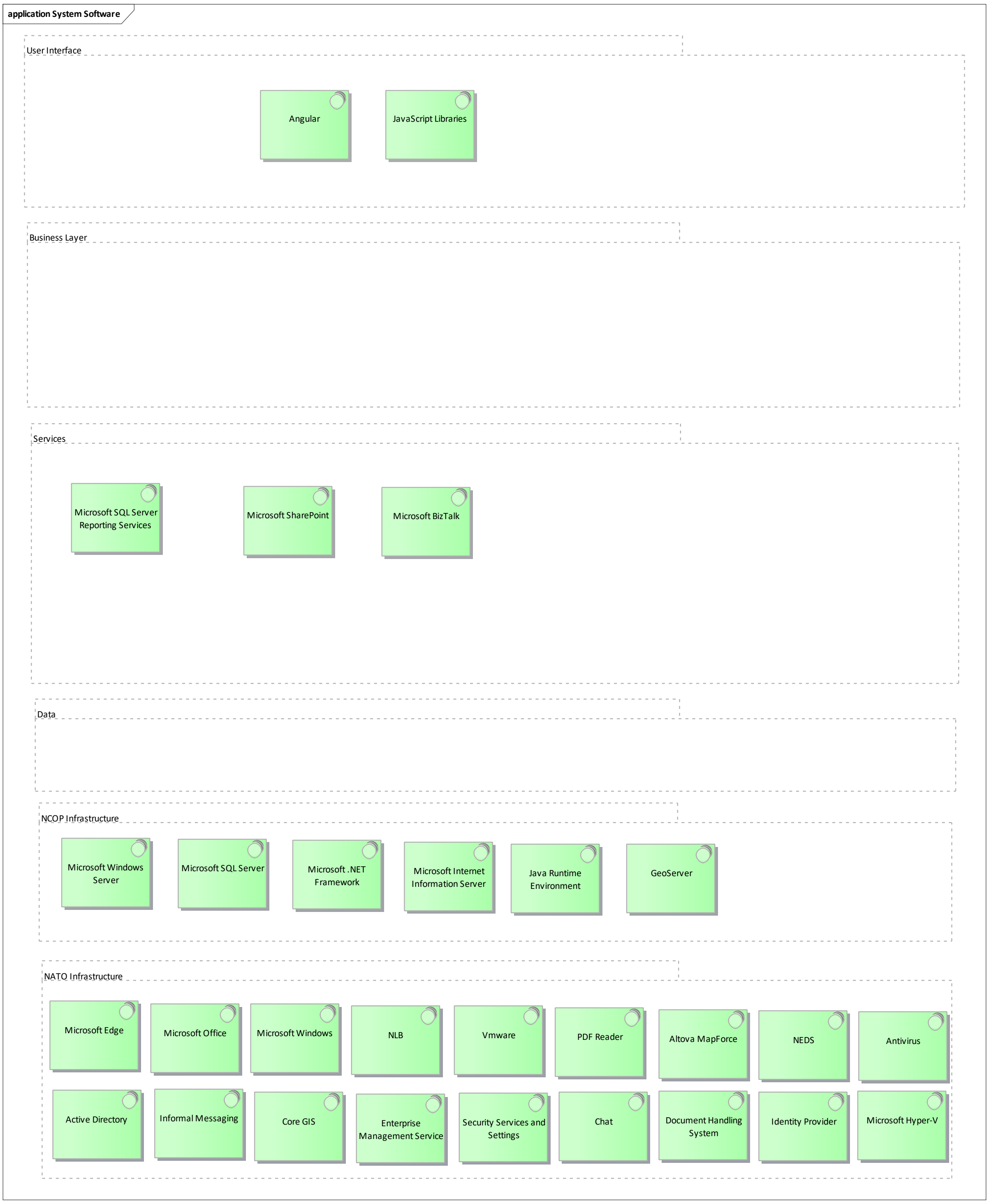
NCOP BizTalk: 1 (standard edition)
NCOP SQL: 1 (standard edition)
NCOP SharePoint: >= 1
NCOP Application: >= 1
NCOP Dynamic IP: >= 1
GeoServer: 1





NCOP BizTalk: 2 (enterprise edition)
NCOP SQL: 2 (enterprise edition)
NCOP SharePoint: > 2
NCOP Application: > 2
NCOP Dynamic IP: 2
GeoServer: 1

C.1.3 System Software



C.2 P2 – RESOURCE STRUCTURE

C.2.1 Application Component – Composition – Application Component

The P2 “Application Component – Composition – Application Component” ViewContext is illustrated by the B.8.2 Viewpoint 2: Software decomposition into Implementation Components NSV-1 NAF v3.1 view.

C.2.2 Application Component – Composition – Application Interface

The P2 “Application Component – Composition – Application Interface” ViewContext is illustrated by the B.8.1 Viewpoint 1: NCOP External interfaces NSV-1 NAF v3.1 view.

C.2.3 Node – Composition – System Software

The P2 “Node – Composition – System Software” ViewContext is illustrated by the B.8.5 Software deployment NSV-1 NAF v3.1 view.

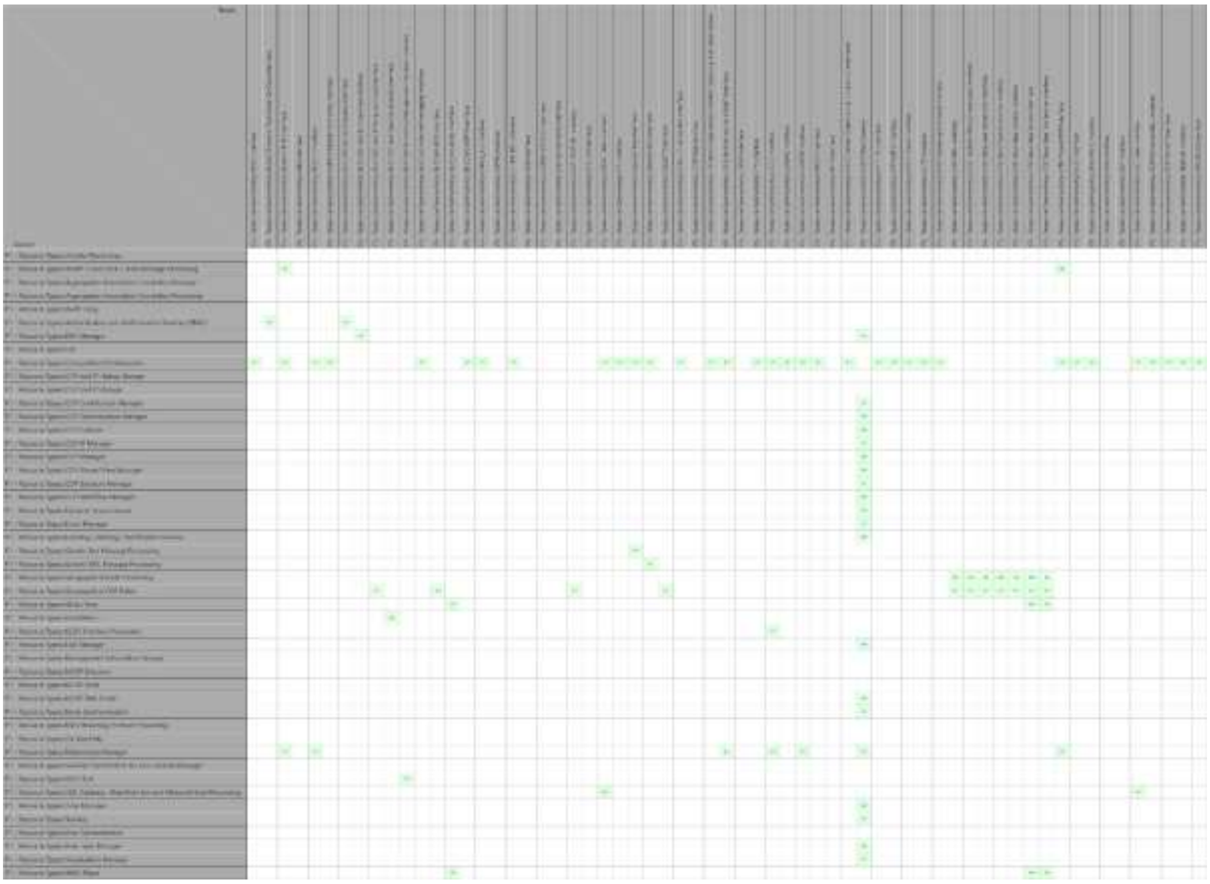
C.2.4 System Software – Composition – Technology Interface

The P2 “System Software – Composition – Technology Interface” ViewContext is illustrated by the B.8.4.3 COTS Software NSV-1 NAF v3.1 view.

C.3 P3 – RESOURCE CONNECTIVITY

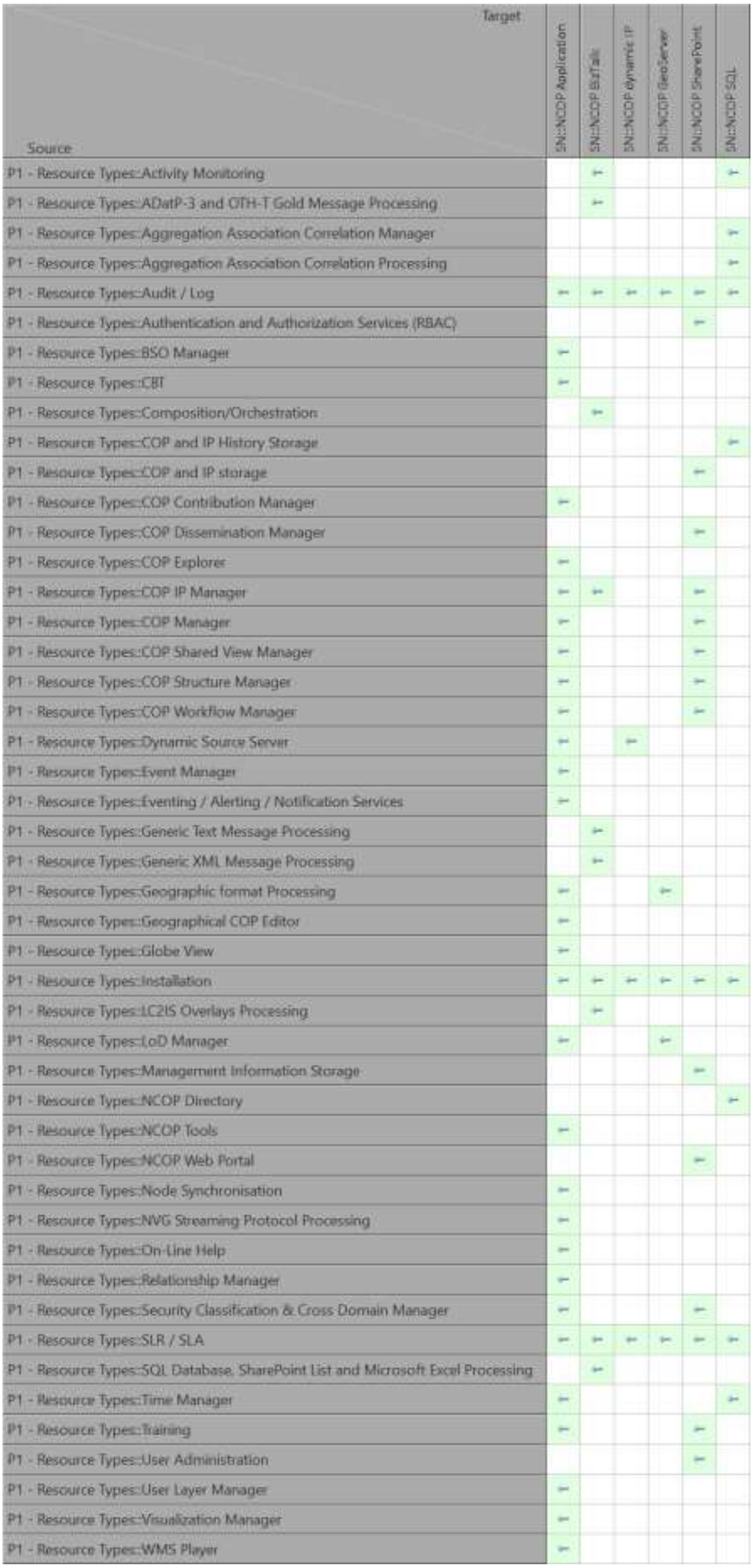
C.3.1 Application Interface – Serving – Application Component

The complete “Application Interface – Serving – Application Component” is defined in the Entreprise Architect file, in the section “P3 – Resource Connectivity” as illustrated below:



C.3.2 Node – Serving – Application Component

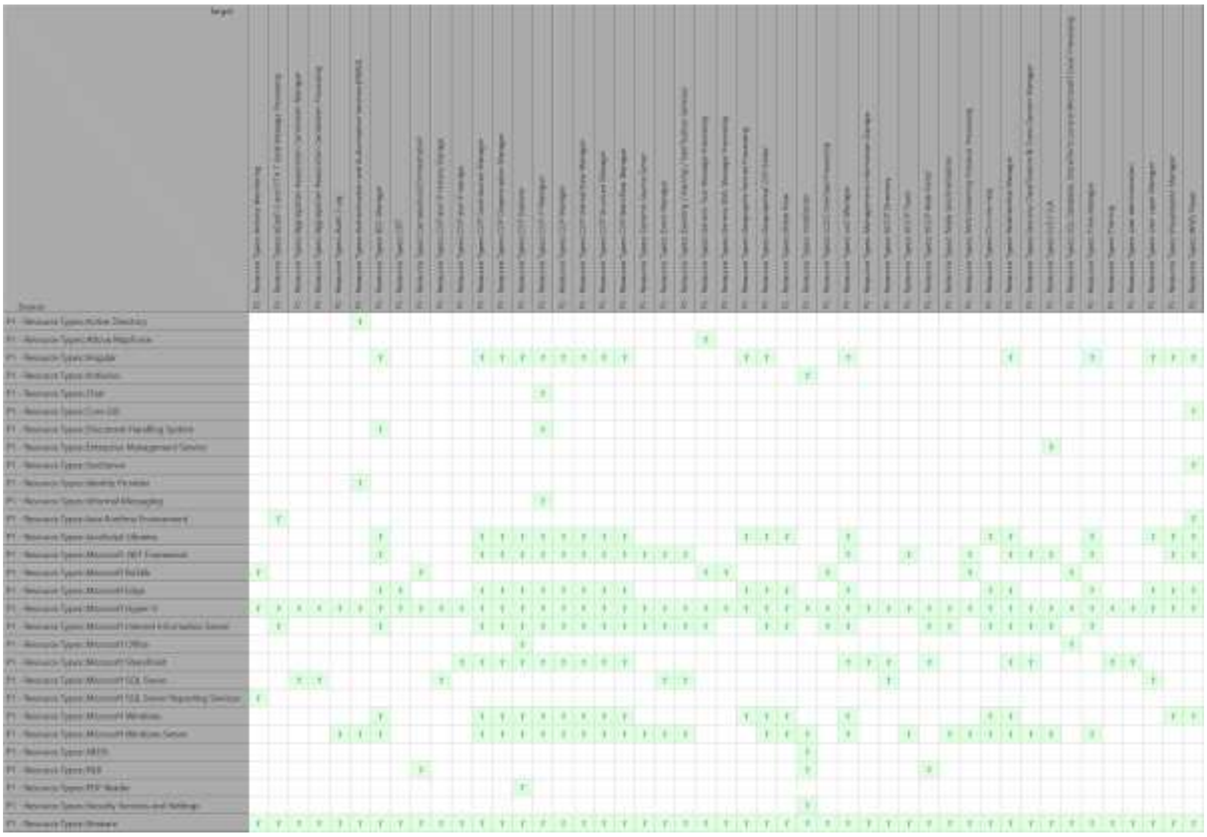
The complete “Node – Serving – Application Component” is defined in the Entreprise Architect file, in the section “P3 – Resource Connectivity” as illustrated below:



Target Source	SN::NCOP Application	SN::NCOP BizTalk	SN::NCOP dynamic IP	SN::NCOP GeoServer	SN::NCOP SharePoint	SN::NCOP SQL
P1 - Resource Types::Activity Monitoring		↤				↤
P1 - Resource Types::ADatP-3 and OTH-T Gold Message Processing		↤				
P1 - Resource Types::Aggregation Association Correlation Manager						↤
P1 - Resource Types::Aggregation Association Correlation Processing						↤
P1 - Resource Types::Audit / Log	↤	↤	↤	↤	↤	↤
P1 - Resource Types::Authentication and Authorization Services (RBAC)					↤	
P1 - Resource Types::BSO Manager	↤					
P1 - Resource Types::CBT	↤					
P1 - Resource Types::Composition/Orchestration		↤				
P1 - Resource Types::COP and IP History Storage						↤
P1 - Resource Types::COP and IP storage					↤	
P1 - Resource Types::COP Contribution Manager	↤					
P1 - Resource Types::COP Dissemination Manager					↤	
P1 - Resource Types::COP Explorer	↤					
P1 - Resource Types::COP IP Manager	↤	↤			↤	
P1 - Resource Types::COP Manager	↤				↤	
P1 - Resource Types::COP Shared View Manager	↤				↤	
P1 - Resource Types::COP Structure Manager	↤				↤	
P1 - Resource Types::COP Workflow Manager	↤				↤	
P1 - Resource Types::Dynamic Source Server	↤		↤			
P1 - Resource Types::Event Manager	↤					
P1 - Resource Types::Eventing / Alerting / Notification Services	↤					
P1 - Resource Types::Generic Text Message Processing		↤				
P1 - Resource Types::Generic XML Message Processing		↤				
P1 - Resource Types::Geographic format Processing	↤			↤		
P1 - Resource Types::Geographical COP Editor	↤					
P1 - Resource Types::Globe View	↤					
P1 - Resource Types::Installation	↤	↤	↤	↤	↤	↤
P1 - Resource Types::LC2IS Overlays Processing		↤				
P1 - Resource Types::LoD Manager	↤			↤		
P1 - Resource Types::Management Information Storage					↤	
P1 - Resource Types::NCOP Directory						↤
P1 - Resource Types::NCOP Tools	↤					
P1 - Resource Types::NCOP Web Portal					↤	
P1 - Resource Types::Node Synchronisation	↤					
P1 - Resource Types::NVG Streaming Protocol Processing	↤					
P1 - Resource Types::On-Line Help	↤					
P1 - Resource Types::Relationship Manager	↤					
P1 - Resource Types::Security Classification & Cross Domain Manager	↤				↤	
P1 - Resource Types::SLR / SLA	↤	↤	↤	↤	↤	↤
P1 - Resource Types::SQL Database, SharePoint List and Microsoft Excel Processing		↤				
P1 - Resource Types::Time Manager	↤					↤
P1 - Resource Types::Training	↤				↤	
P1 - Resource Types::User Administration					↤	
P1 - Resource Types::User Layer Manager	↤					
P1 - Resource Types::Visualization Manager	↤					
P1 - Resource Types::WMS Player	↤					

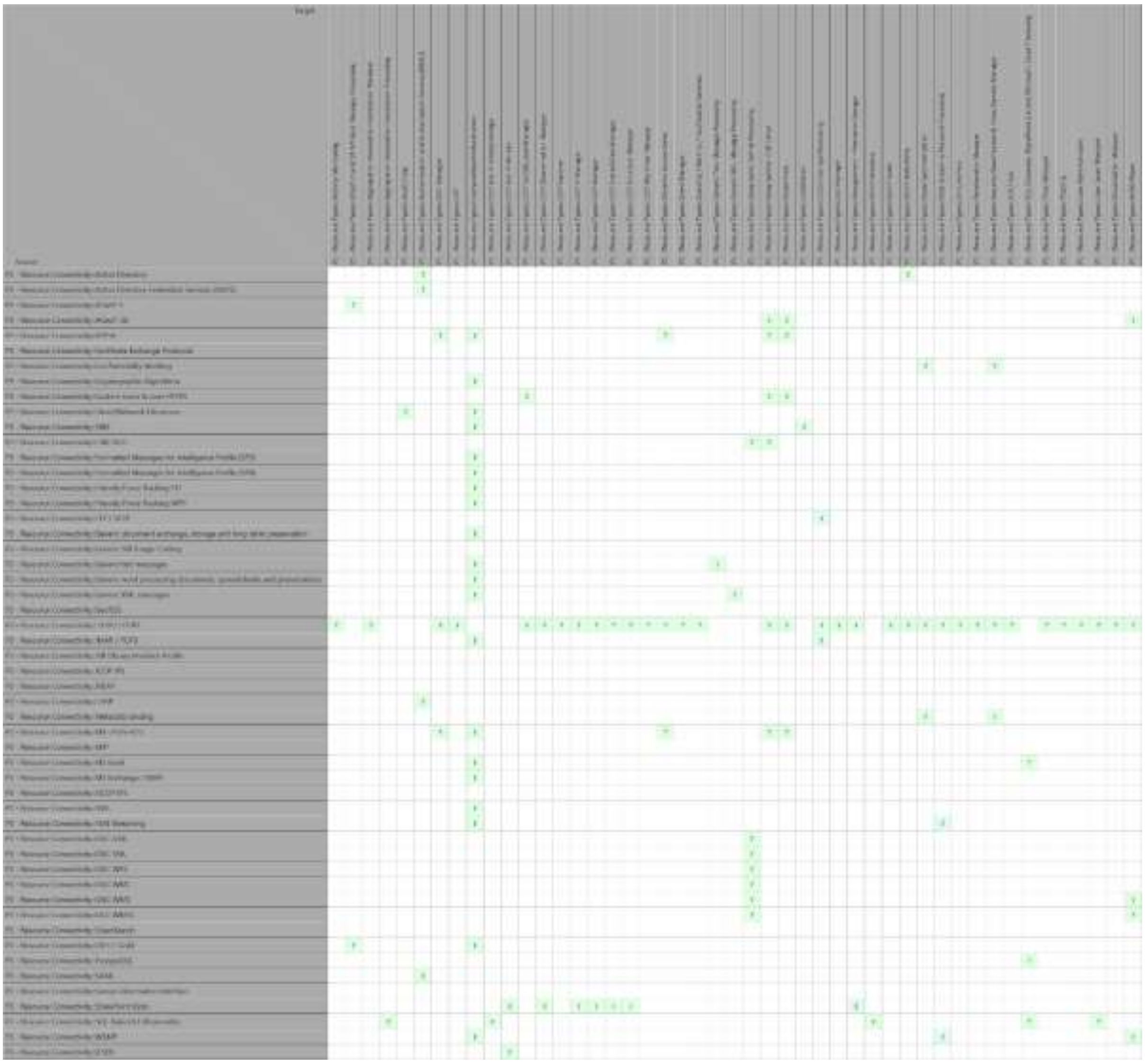
C.3.3 System Software – Serving – Application Component

The complete “System Software – Serving – Application Component” is defined in the Entreprise Architect file, in the section “P3 – Resource Connectivity” as illustrated below:



C.3.4 Technology Interface – Serving – Application Component

The complete “Technology Interface – Serving – Application Component” is defined in the Entreprise Architect file, in the section “P3 – Resource Connectivity” as illustrated below:



C.4 P4 – RESOURCE FUNCTIONS

C.4.1 Application Component – Assignment - Application Service

The P4 ViewContext is illustrated by the B.9 NSV-4 NAF v3.1 view.

C.5 L4-P4

C.5.1 Application Service - Serving - Business Process

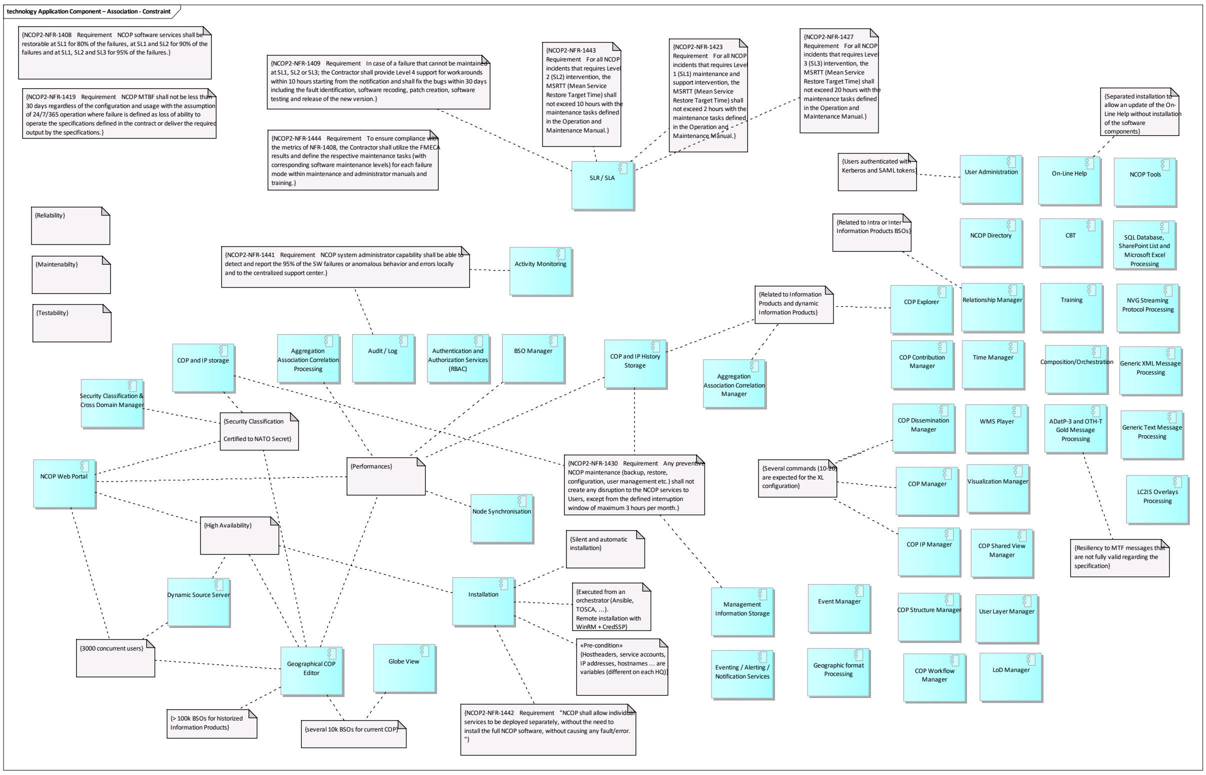
The L4-P4 ViewContext is illustrated by the B.10 NSV-5 NAF v3.1 view.

C.5.2 Application Service – Serving – Business Role

The L4-P4 ViewContext is illustrated by the B.10 NSV-5 NAF v3.1 view.

C.6 P8 – RESOURCE CONSTRAINTS

C.6.1 Application Component – Association – Constraint


technology Application Component – Association - Constraint
SLR / SLA
User Administration
On-Line Help
NCOP Tools
NCOP Directory
CBT
SQL Database, SharePoint List and Microsoft Excel Processing
Activity Monitoring
COP Explorer
Relationship Manager
Training
NVG Streaming Protocol Processing
COP and IP storage
Aggregation Association Correlation Processing
Audit / Log
Authentication and Authorization Services (RBAC)
BSO Manager
COP and IP History Storage
Aggregation Association Correlation Manager
COP Contribution Manager
Time Manager
Composition/Orchestration
Generic XML Message Processing
Security Classification & Cross Domain Manager
COP Dissemination Manager
WMS Player
ADatP-3 and OTH-T Gold Message Processing
Generic Text Message Processing
NCOP Web Portal
COP Manager
Visualization Manager
LC2IS Overlays Processing
Node Synchronisation
COP IP Manager
COP Shared View Manager
Dynamic Source Server
Installation
Management Information Storage
Event Manager
COP Structure Manager
User Layer Manager
Geographical COP Editor
Globe View
Eventing / Alerting / Notification Services
Geographic format Processing
COP Workflow Manager
LoD Manager

{NCOP2-NFR-1408 Requirement NCOP software services shall be restorable at SL1 for 80% of the failures, at SL1 and SL2 for 90% of the failures and at SL1, SL2 and SL3 for 95% of the failures.}

{NCOP2-NFR-1419 Requirement NCOP MTBF shall not be less than 30 days regardless of the configuration and usage with the assumption of 24/7/365 operation where failure is defined as loss of ability to operate the specifications defined in the contract or deliver the required output by the specifications.}

{NCOP2-NFR-1409 Requirement In case of a failure that cannot be maintained at SL1, SL2 or SL3; the Contractor shall provide Level 4 support for workarounds within 10 hours starting from the notification and shall fix the bugs within 30 days including the fault identification, software recoding, patch creation, software testing and release of the new version.}

{NCOP2-NFR-1444 Requirement To ensure compliance with the metrics of NFR-1408, the Contractor shall utilize the FMECA results and define the respective maintenance tasks (with corresponding software maintenance levels) for each failure mode within maintenance and administrator manuals and training.}

{NCOP2-NFR-1443 Requirement For all NCOP incidents that requires Level 2 (SL2) intervention, the MSRTT (Mean Service Restore Target Time) shall not exceed 10 hours with the maintenance tasks defined in the Operation and Maintenance Manual.}

{NCOP2-NFR-1423 Requirement For all NCOP incidents that requires Level 1 (SL1) maintenance and support intervention, the MSRTT (Mean Service Restore Target Time) shall not exceed 2 hours with the maintenance tasks defined in the Operation and Maintenance Manual.}

{NCOP2-NFR-1427 Requirement For all NCOP incidents that requires Level 3 (SL3) intervention, the MSRTT (Mean Service Restore Target Time) shall not exceed 20 hours with the maintenance tasks defined in the Operation and Maintenance Manual.}

{Separated installation to allow an update of the On-Line Help without installation of the software components}

{Users authenticated with Kerberos and SAML tokens}

{Related to Intra or Inter Information Products BSOs}

{Reliability}

{Maintenabilty}

{Testability}

{NCOP2-NFR-1441 Requirement NCOP system administrator capability shall be able to detect and report the 95% of the SW failures or anomalous behavior and errors locally and to the centralized support center.}

{Related to Information Products and dynamic Information Products}

{Security Classification

Certified to NATO Secret}

{Performances}

{NCOP2-NFR-1430 Requirement Any preventive NCOP maintenance (backup, restore, configuration, user management etc.) shall not create any disruption to the NCOP services to Users, except from the defined interruption window of maximum 3 hours per month.}

{Several commands (10-20) are expected for the XL configuration}

{High Availability}

{Silent and automatic installation}

{Resiliency to MTF messages that are not fully valid regarding the specification}

{Executed from an orchestrator (Ansible, TOSCA, ...). Remote installation with WinRM + CredSSP}

«Pre-condition» {Hostheaders, service accounts, IP addresses, hostnames ... are variables (different on each HQ)}

{3000 concurrent users}

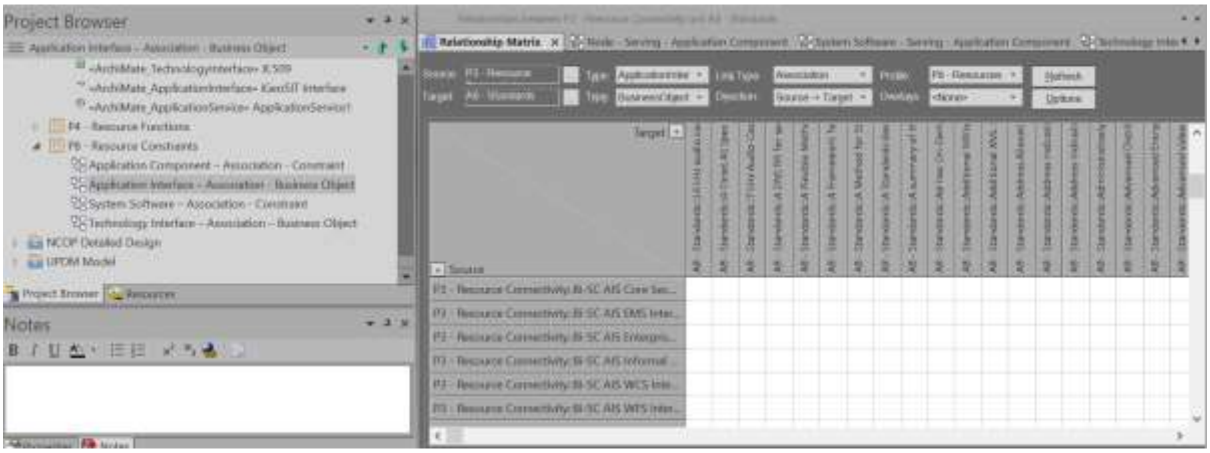
{> 100k BSOs for historized Information Products}

{several 10k BSOs for current COP}

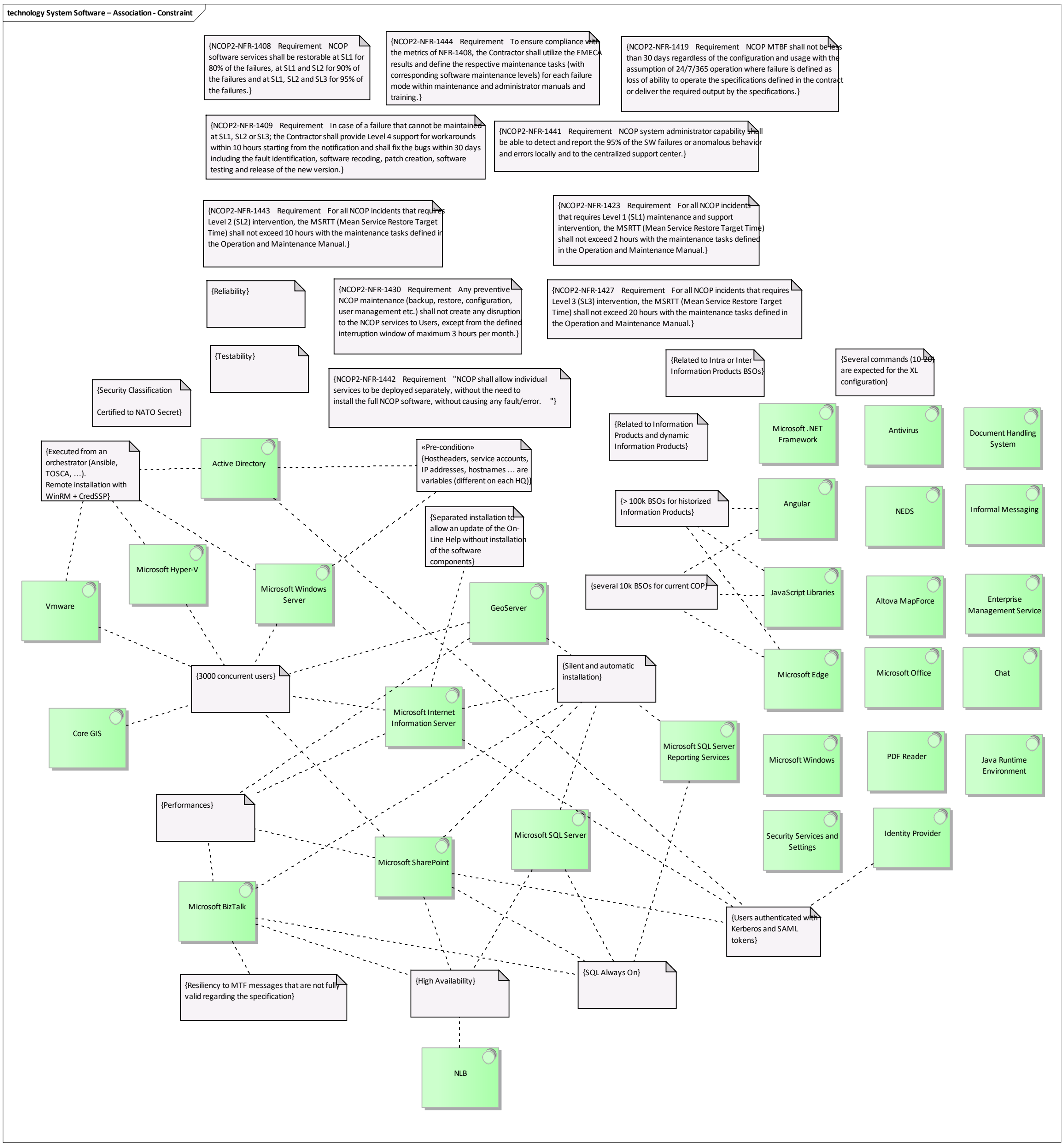
{NCOP2-NFR-1442 Requirement "NCOP shall allow individual services to be deployed separately, without the need to install the full NCOP software, without causing any fault/error. "}

C.6.2 Application Interface – Association - Business Object

The complete association between “Application Interface” and “Business Object” is defined in the Entreprise Architect file, in the section “P8 – Resources Constraints” as illustrated below:


Project Browser
Application Interface – Association – Business Object
«ArchiMate_TechnologyInterface» X.509
«ArchiMate_ApplicationInterface» [illegible] Interface
«ArchiMate_ApplicationService» ApplicationService
P4 – Resource Functions
P8 – Resource Constraints
Application Component – Association – Constraint
Application Interface – Association – Business Object
System Software – Association – Constraint
Technology Interface – Association – Business Object
NCOP Detailed Design
UPDM Model
Project Browser
Resources
Notes
Relationship Matrix
Node - Serving - Application Component
System Software - Serving - Application Component
Technology Inte
Source
Target
Type
Link Type
Association
Profile
Direction
Source -> Target
Overlays
<None>
Refresh
Options
Target
Source
P3 - Resource Connectivity: BI-SC AIS Core Ser...
P3 - Resource Connectivity: BI-SC AIS EMS Inter...
P3 - Resource Connectivity: BI-SC AIS Enterpris...
P3 - Resource Connectivity: BI-SC AIS Informal ...
P3 - Resource Connectivity: BI-SC AIS WCS Inte...
P3 - Resource Connectivity: BI-SC AIS WPS Inter...

C.6.3 System Software – Association – Constraint



technology System Software – Association - Constraint

{NCOP2-NFR-1408 Requirement NCOP software services shall be restorable at SL1 for 80% of the failures, at SL1 and SL2 for 90% of the failures and at SL1, SL2 and SL3 for 95% of the failures.}

{NCOP2-NFR-1444 Requirement To ensure compliance with the metrics of NFR-1408, the Contractor shall utilize the FMECA results and define the respective maintenance tasks (with corresponding software maintenance levels) for each failure mode within maintenance and administrator manuals and training.}

{NCOP2-NFR-1419 Requirement NCOP MTBF shall not be less than 30 days regardless of the configuration and usage with the assumption of 24/7/365 operation where failure is defined as loss of ability to operate the specifications defined in the contract or deliver the required output by the specifications.}

{NCOP2-NFR-1409 Requirement In case of a failure that cannot be maintained at SL1, SL2 or SL3; the Contractor shall provide Level 4 support for workarounds within 10 hours starting from the notification and shall fix the bugs within 30 days including the fault identification, software recoding, patch creation, software testing and release of the new version.}

{NCOP2-NFR-1441 Requirement NCOP system administrator capability shall be able to detect and report the 95% of the SW failures or anomalous behavior and errors locally and to the centralized support center.}

{NCOP2-NFR-1443 Requirement For all NCOP incidents that requires Level 2 (SL2) intervention, the MSRTT (Mean Service Restore Target Time) shall not exceed 10 hours with the maintenance tasks defined in the Operation and Maintenance Manual.}

{NCOP2-NFR-1423 Requirement For all NCOP incidents that requires Level 1 (SL1) maintenance and support intervention, the MSRTT (Mean Service Restore Target Time) shall not exceed 2 hours with the maintenance tasks defined in the Operation and Maintenance Manual.}

{NCOP2-NFR-1430 Requirement Any preventive NCOP maintenance (backup, restore, configuration, user management etc.) shall not create any disruption to the NCOP services to Users, except from the defined interruption window of maximum 3 hours per month.}

{NCOP2-NFR-1427 Requirement For all NCOP incidents that requires Level 3 (SL3) intervention, the MSRTT (Mean Service Restore Target Time) shall not exceed 20 hours with the maintenance tasks defined in the Operation and Maintenance Manual.}

{NCOP2-NFR-1442 Requirement "NCOP shall allow individual services to be deployed separately, without the need to install the full NCOP software, without causing any fault/error. "}

{Executed from an orchestrator (Ansible, TOSCA, ...). Remote installation with WinRM + CredSSP}

«Pre-condition» {Hostheaders, service accounts, IP addresses, hostnames ... are variables (different on each HQ)}

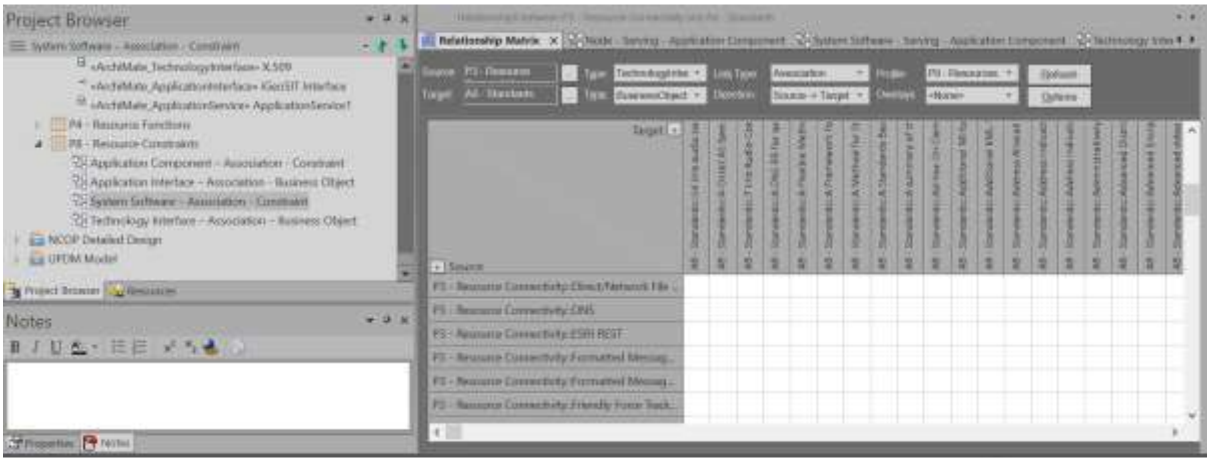
{Separated installation to allow an update of the On-Line Help without installation of the software components}

{Several commands (10-20) are expected for the XL configuration}

{Resiliency to MTF messages that are not fully valid regarding the specification}

C.6.4 Technology Interface – Association – Business Object

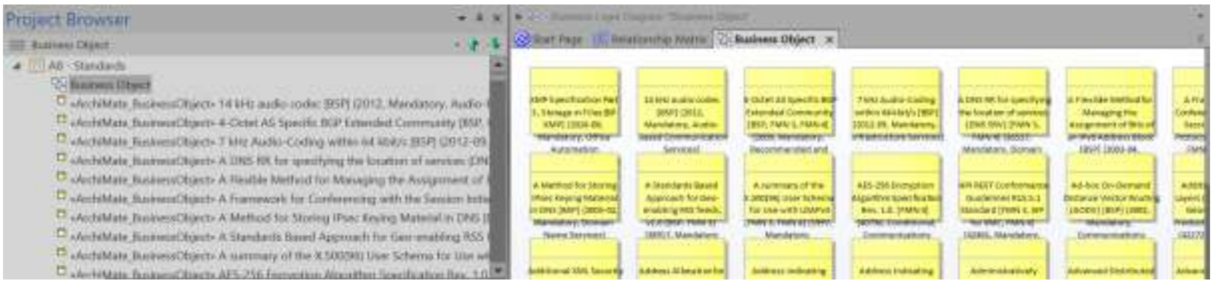
The complete association between “Technology Interface” and “Business Object” is defined in the Entreprise Architect file, in the section “P8 – Resources Constraints” as illustrated below:


Project Browser
System Software – Association – Constraint
«ArchiMate_TechnologyInterface» X.509
«ArchiMate_ApplicationInterface» IGeoSIT Interface
«ArchiMate_ApplicationService» ApplicationService1
P4 - Resource Functions
P8 - Resource Constraints
Application Component – Association – Constraint
Application Interface – Association – Business Object
System Software – Association – Constraint
Technology Interface – Association – Business Object
NCOP Detailed Design
UPDM Model
Project Browser
Resources
Notes
Properties
Notes
Relationship Matrix
Node - Serving - Application Component
System Software - Serving - Application Component
Technology Inte
Source
P3 - Resources
Target
A8 - Standards
Type
TechnologyInte
BusinessObject
Link Type
Association
Direction
Source -> Target
Profile
P3 - Resources
Overlays
<None>
Options
Target
Source
P3 - Resource Connectivity Direct/Network File ...
P3 - Resource Connectivity DNS
P3 - Resource Connectivity ESRI REST
P3 - Resource Connectivity Formatted Messag...
P3 - Resource Connectivity Formatted Messag...
P3 - Resource Connectivity Friendly Force Track...

C.7 A8 – STANDARDS

C.7.1 Business Object

The complete list of Business Objects (total 833) is defined in the Entreprise Architect file, in the section “A8 – Standard” as illustrated below:

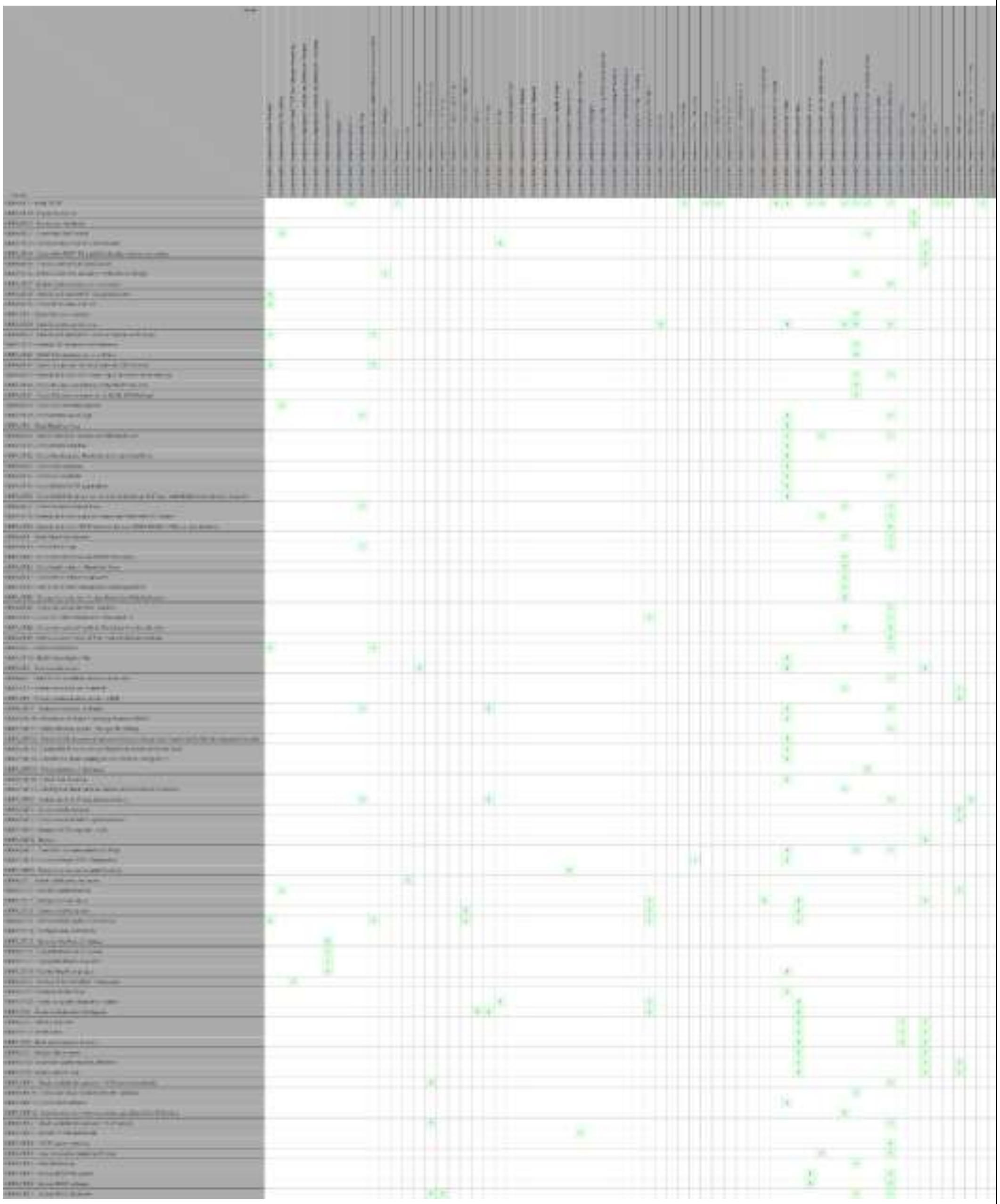

Project Browser
Business Object
A8 - Standards
Business Object
«ArchiMate_BusinessObject» 14 kHz audio codec [BSP] (2012, Mandatory, Audio-
«ArchiMate_BusinessObject» 4-Octet AS Specific BGP Extended Community [BSP,
«ArchiMate_BusinessObject» 7 kHz Audio-Coding within 64 kbit/s [BSP] (2012-09,
«ArchiMate_BusinessObject» A DNS RR for specifying the location of services (DN
«ArchiMate_BusinessObject» A Flexible Method for Managing the Assignment of
«ArchiMate_BusinessObject» A Framework for Conferencing with the Session Initi
«ArchiMate_BusinessObject» A Method for Storing IPsec Keying Material in DNS [
«ArchiMate_BusinessObject» A Standards Based Approach for Geo-enabling RSS
«ArchiMate_BusinessObject» A summary of the X.500(96) User Schema for Use wi
«ArchiMate_BusinessObject» AES-256 Encryption Algorithm Specification Rev. 1.0
Start Page
Relationship Matrix
Business Object

APPENDIX D IEEE 1016

The following table displays the traceability between IEEE 1016 ViewPoints and the corresponding section in the current SDS document:

TABLE 7-6: IEEE 1016 VIEWPOINTS VS SDS SECTIONS

IEEE 1016 ViewPoint	Section in SDS
Context viewpoint	See §2 System objective
Composition viewpoint	See §5.1.2 Implementation Components
Logical viewpoint	See §4.2.2 NCOP logical model
Dependency viewpoint	See §C.3 P3 – Resource Connectivity §B.5 NOV-2 Connectivity Description
Information viewpoint	See §3.3.4 Data Layer §5.3.4 Data
Patterns use viewpoint	See §3.1.1 Design Patterns
Interface viewpoint	See NCOP ICD [ICD] document
Structure viewpoint	See §B.8 NSV-1
Interaction viewpoint	See §4.2.2.2 Dynamic description
State dynamics viewpoint	See §4.2.2.2 Dynamic description
Algorithm viewpoint	See §4.2.2.2 Dynamic description

Resource viewpoint	See §6.4Operation and Maintenance **Task Analysis (OMTA)** The list of all operation tasks, SM&C (Service, Management and Control) tasks, administrative tasks, corrective maintenance tasks and preventive maintenance tasks, are defined in the [ILSP] . The following table, shows the Implementation Components associated to each OMTA Task (the complete redeable mapping is defined in the EAP file):  **Physical View**

APPENDIX E INTERFACES OVERVIEW

This annex lists the initial interfaces between the NCOP system and external systems. The detailed information of each interface is described in the Interface Control Document [ICD].

Identification of IC (API type)	Version	NCOP Increment
ACCS Interface		Since NCOP Increment-1
Active Directory Federation Services Interface		Increment-2
AdatP-3 MTF Interface	V11 (limited support), V12 (limited support), V13.1	Since NCOP Increment-1
AGS Interface		Future Increment
AirC2IS Interface	BL1: 4.4.0, 4.5.X BL2: 4.6.0	Since NCOP Increment-1
AMN Integration Core Interface		Since NCOP Increment-1
CBRN Interface		Future Increment
C4ISR_VIZ Interface		Increment-2
CIDNE XML Interface		Future Increment
Bi-SC AIS Active Directory Interface		Since NCOP Increment-1
Bi-SC AIS Core DHS Services Interface	DHS 2.X	Since NCOP Increment-1
Bi-SC AIS Core Printing Services Interface		Since NCOP Increment-1
Bi-SC AIS Core Security Services Interface		Since NCOP Increment-1
Bi-SC AIS Enterprise Management Services Interface	SCOM 2016 and SCOM 2019	Since NCOP Increment-1
Bi-SC AIS Informal messaging Interface	Exchange 2016 and Exchange 2019 ?	Since NCOP Increment-1
Bi-SC AIS WFS Interface	2.0.2 (from [Core GIS ICD])	Since NCOP Increment-1
Bi-SC AIS WMS Interface	1.3.0 (from [Core GIS ICD])	Since NCOP Increment-1
Bi-SC AIS XMPP Interface	RFC 3920 and RFC 3921	Since NCOP Increment-1
CSD Interface		Future Increment
CYBER DEFENSE Interface		Future Increment
ETEE FS Interface		Future Increment
Environmental FS Interface		Future Increment
ESRI REST API	ArcGIS Server 10.8.1	Since NCOP Increment-1
EXCEL Data Interface	Excel 2013, 2016 and 2019	Since NCOP Increment-1
FFI		Increment-2
Generic Text Interface		Since NCOP Increment-1
Generic XML Interface		Since NCOP Increment-1
iGeoSIT Interface		Since NCOP Increment-1
INTEL-FS native XML interface	BL1: 1.4.0, 1.4.1, 1.5.0, BL2: no update	Since NCOP Increment-1
GML	3.1.1	Since NCOP Increment-1
JCOP Web Services	0.6.1	Since NCOP Increment-1
JOCWatch Operational Incident Reporting XML Web Service		Since NCOP Increment-1
JOIIS XML format for ORBAT Interface	8.2.1	Since NCOP Increment-1
JREAP Interface		Future Increment

Identification of IC (API type)	Version	NCOP Increment
JTS Interface	BL1: 4.1.3, 4.2, 4.2.1, 4.3 BL2: 4.4	Since NCOP Increment-1
LC2IS Interface	BL1: 6.1.3, 6.1.4, 6.2	Since NCOP Increment-1
LOGFAS Interface		Since NCOP Increment-1
LOGREP Interface	6.1.5	Since NCOP Increment-1
MCCIS Interface (overlays and tracks)	MCCIS 6.3.2 and 6.4.2	Since NCOP Increment-1
MIP Interface		Future Increment
NATO Vector Graphics 1.4, 1.5 and 2.0 Interface	1.4,1.5 and 2.0	Since NCOP Increment-1
NCOP Web Services		Since NCOP Increment-1
NFFI IP1 Interface		Since NCOP Increment-1
NFFI SIP-3 Interface		Since NCOP Increment-1
NIRIS Tracks Interfaces	BL1: NIRIS 3.8 3.9, 3.10, 3.11, 4.0 BL2: 4.1 or 4.2 (Delayed CLIN)	Since NCOP Increment-1
NJTS	BL2: 0.6, 1.0 Small update (Delayed CLIN)	Increment-2
NVG Streaming Protocol Interface	1.4 and 2.0	Since NCOP Increment-1
OGC GML Interface	3.1.1	Since NCOP Increment-1
OGC Keyhole Markup Language Interface	2.2 2.3	Since NCOP Increment-1
OGC Style Layer Descriptor Interface	1.1.0	Since NCOP Increment-1
OGC Web Coverage Service Interface	1.1.2	Since NCOP Increment-1
OGC Web Feature Service Interface	1.1.0	Since NCOP Increment-1
OGC Web Map Context Interface	1.1.1	Since NCOP Increment-1
OGC Web Map Service Interface	1.3.0	Since NCOP Increment-1
OTH-T Gold MTF Interface	Rev D and 2007	Since NCOP Increment-1
REST Service		Increment-2
SharePoint Interface	SharePoint 2013, 2016 and 2019	Since NCOP Increment-1
SOA Interface		Future Increment
SOF Interface		Future Increment
SQL Data Interface		Since NCOP Increment-1
TOPFAS native XML Interface	BL1: 6.4.x BL2: 6.5.0 (Delayed CLIN) TOPFAS 7.0 ?	Since NCOP Increment-1
TOPFAS SAT Interface		Future Increment
TRITON		Increment-2
WISI (ICC) Interface	BL1: 3.4.0, 3.5.0	Since NCOP Increment-1

E.1 AIRC2IS INTERFACE

E.1.1 AirC2IS Interface Design

An NCOP internal AirC2IS Proxy is processing the AirC2IS source as follow:

- It is defined on IIS as a new web service on default IIS web site (in addition of existing proxies : Intel-FS Proxy …)
- It requests first the AirC2IS Mission List service to get the Mission Codes
- It requests the 9 AirC2IS NVG 1.5 services and the 9 AirC2IS native services:

  - ACO Service
  - Asset List Service
  - ATO Service
  - TBMD Defence Design Service
  - OPFOR TBM COA Service
  - ORBAT Service
  - RAP Service
  - Target List Service
  - TBM Picture Service
- It subscribes to the AirC2IS Pub/Sub service in order to receive AirC2IS notifications and get, in a quick way, the AirC2IS TBMD pictures

For each AirC2IS Information Product, NCOP Proxy executes the following steps:

- Gets the NVG content from the AirC2IS NVG 1.5 service
- Gets the AirC2IS XML content from the AirC2IS XML native service
- Augments the NVG with missing attributes coming from the AirC2IS XML content
- Add the units (km …)
- Add the ADEM attributes
- If defined, computes the BSO associations (Intra-IP)

When relevant, the proxy sets the <SimpleData label> in the dedicated SQL table to replace the <SimpleData key> display in the BSO List of the Geographical COP Editor.

Finally, the proxy manages the AirC2IS notifications sent by the AirC2IS Pub/Sub.

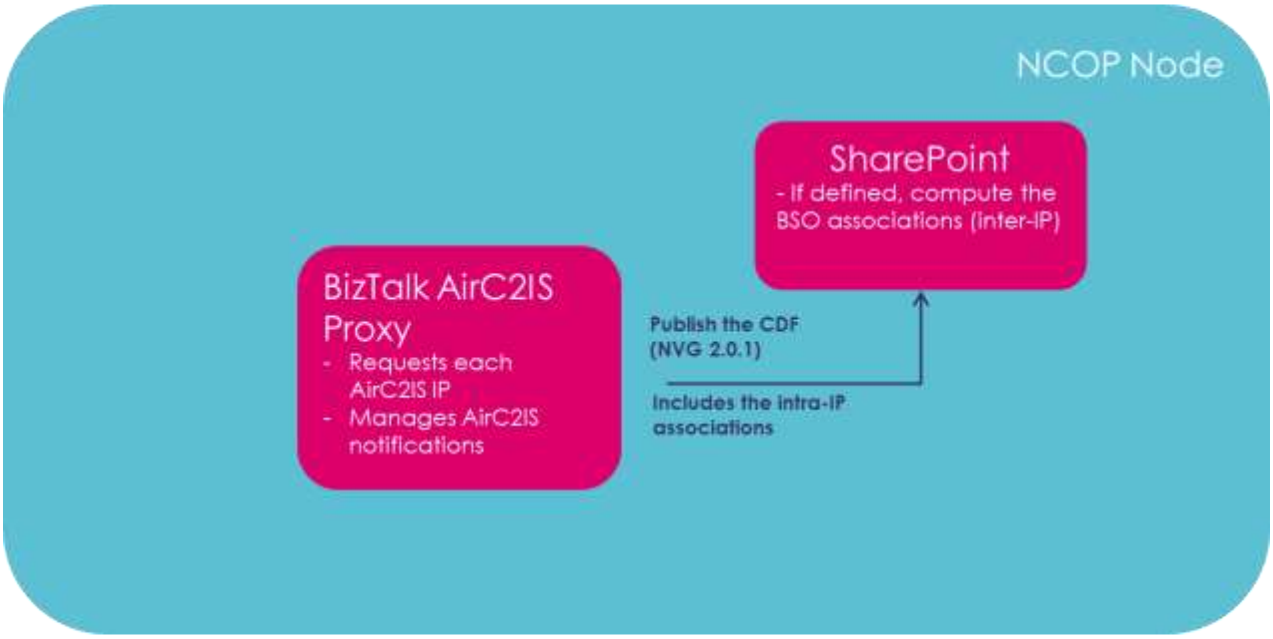

NCOP Node
SharePoint
- If defined, compute the BSO associations (inter-IP)
BizTalk AirC2IS Proxy
- Requests each AirC2IS IP
- Manages AirC2IS notifications
Publish the CDF (NVG 2.0.1)
Includes the intra-IP associations

Figure 7-11: BizTalk AirC2IS Proxy

The NCOP AirC2IS proxy is implemented as a IIS Web Service hosted on NCOP BizTalk Server.

E.1.1.1 ACO Service

The following sequence diagram shows the web service operations consumed by NCOP to get the ACO:

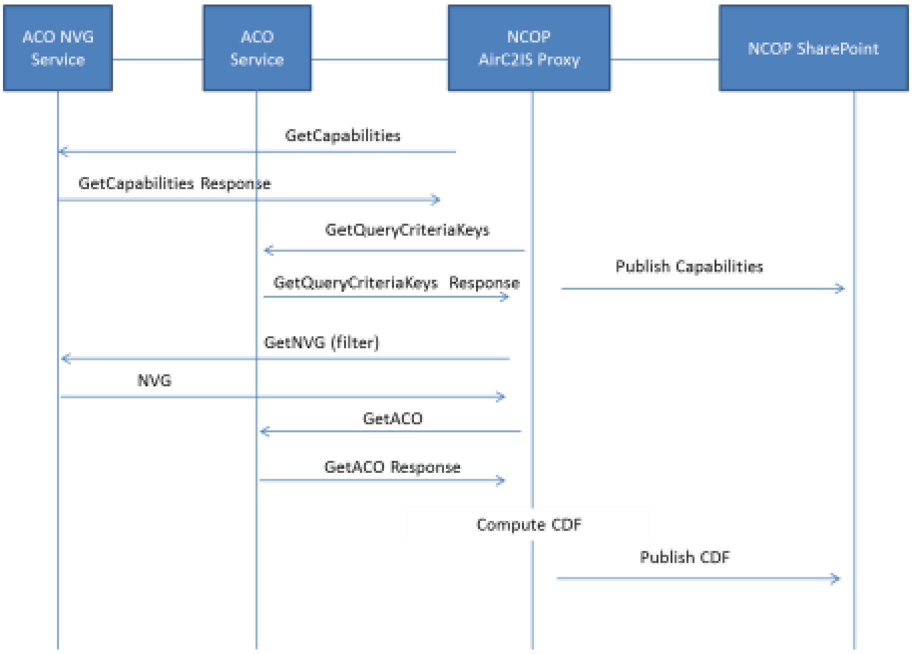
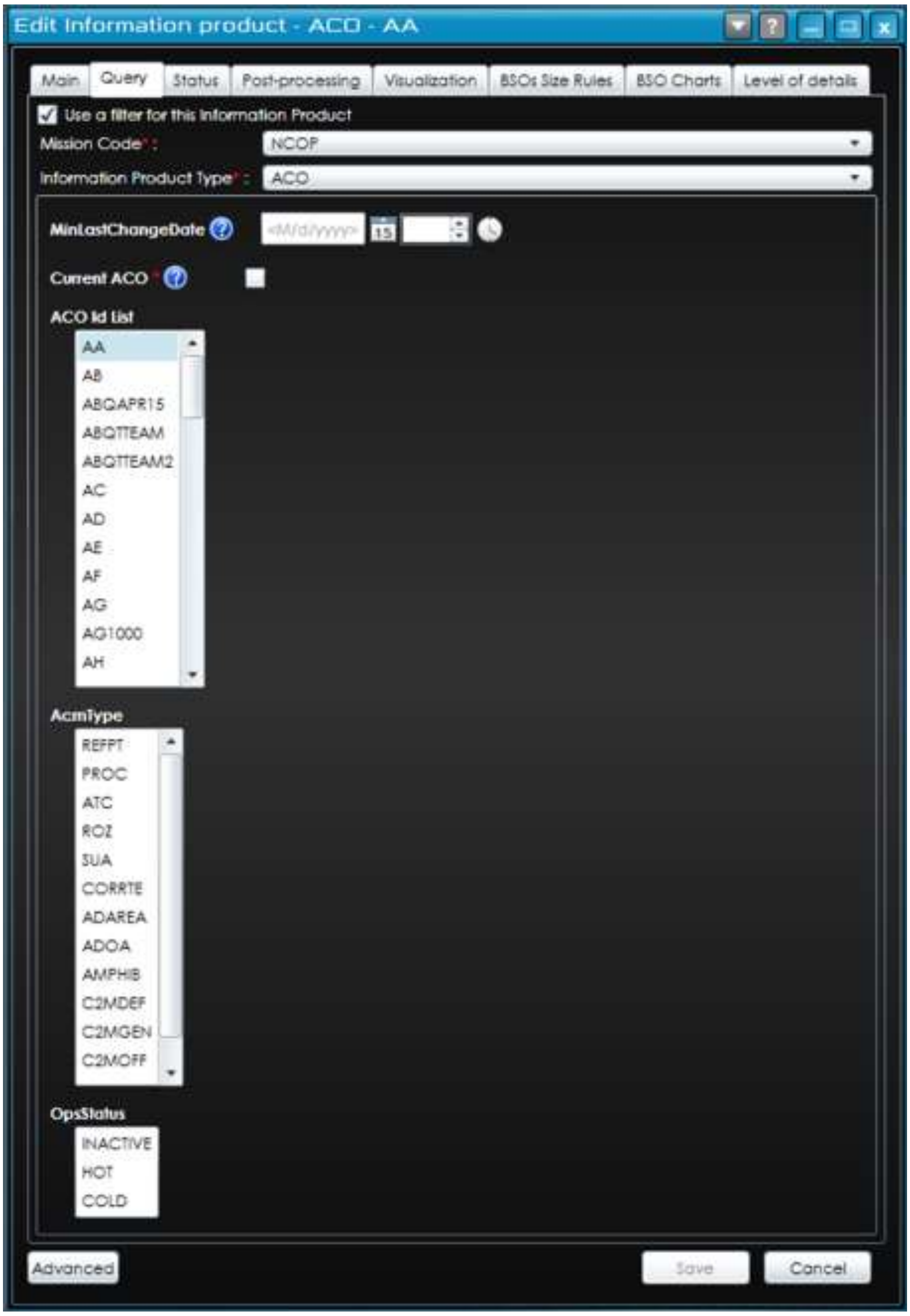


Figure 7-12: AirC2IS ACO Service sequence diagram

The following screenshot shows an overview of the AirC2IS ACO parameters that are displayed in NCOP Information Product Definition to get the ACO:



Edit Information product - ACO - AA

☑ Use a filter for this Information Product

Mission Code*: NCOP

Information Product Type*: ACO

MinLastChangeDate: <M/d/yyyy>

Current ACO*: □

Figure 7-13: AirC2IS ACO Information Product creation

The mandatory attributes are:

- The Mission Code
- The Information Product Type

The main optional attributes are:

- The ACO Id

The following screenshot shows an overview of the AirC2IS ACO displayed in the NCOP Geographical COP Editor:

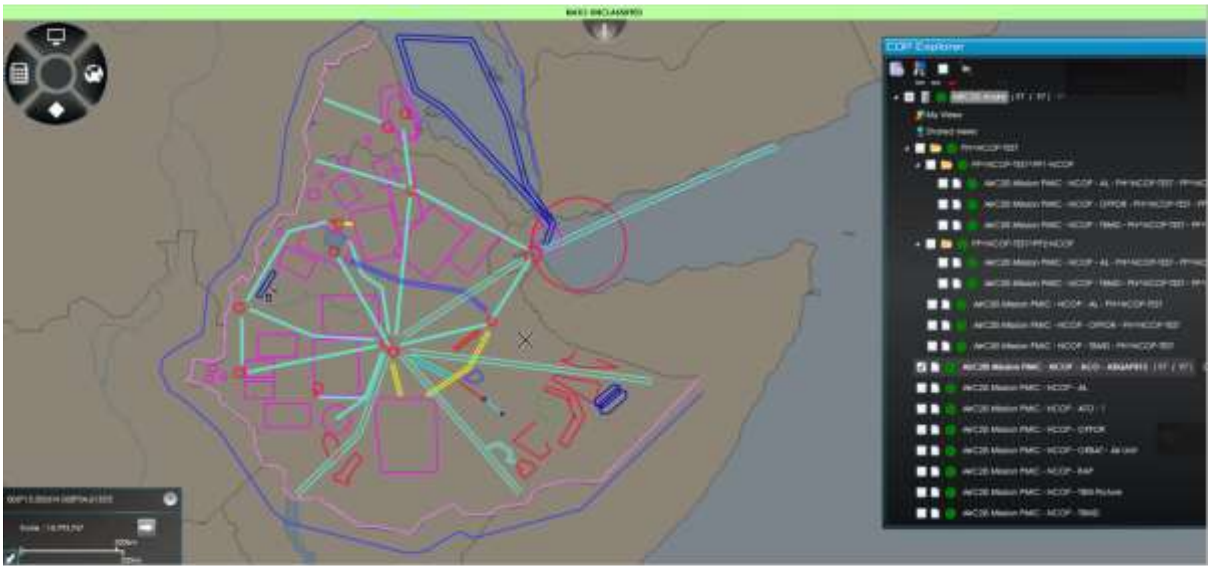


Figure 7-14: Overview of the AirC2IS ACO displayed in NCOP

E.1.1.2 Asset List Service

The following sequence diagram shows the web service operations consumed by NCOP to get the Asset List:

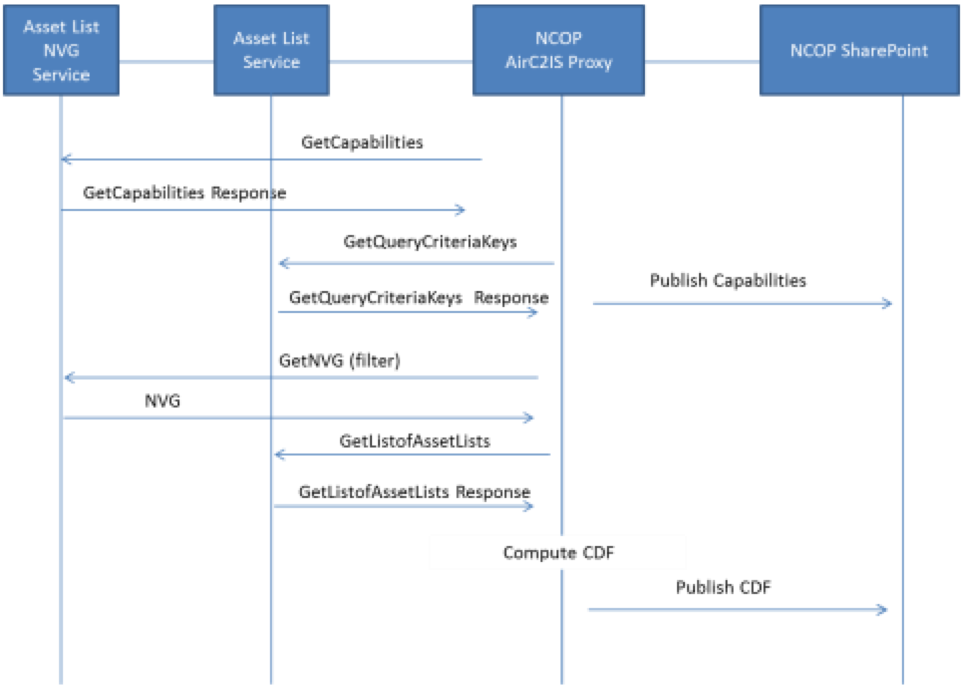
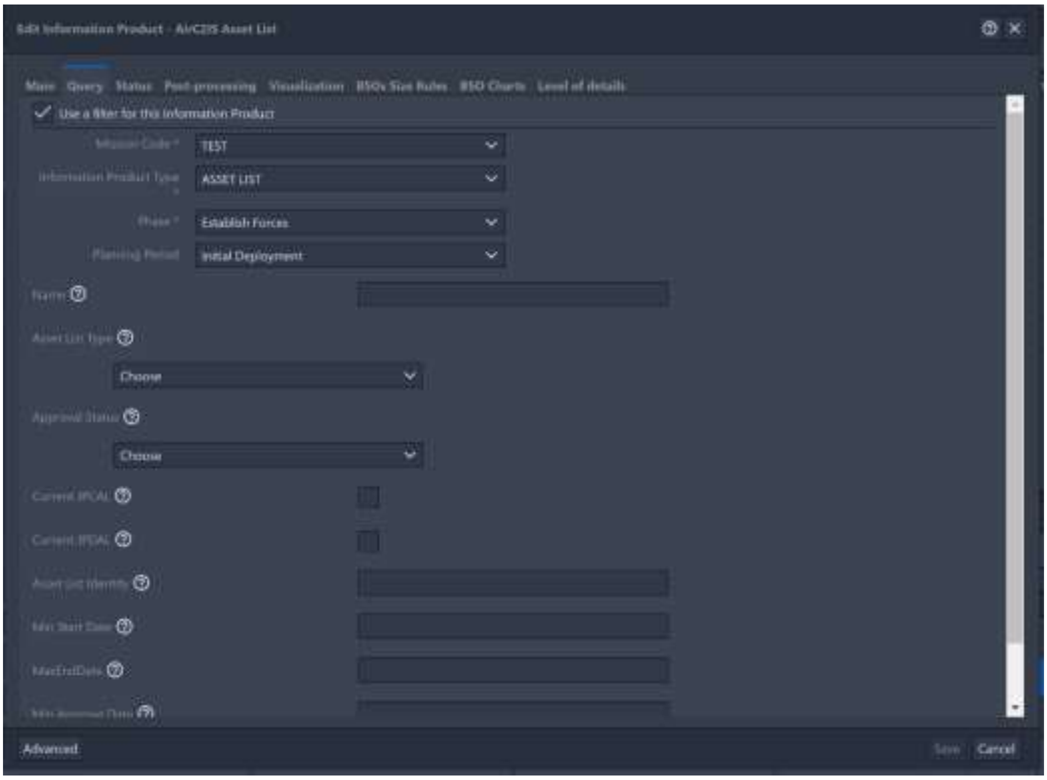


Figure 7-15: AirC2IS Asset List Service sequence diagram

The following screenshot shows an overview of the AirC2IS Asset List parameters that are displayed in NCOP Information Product Definition to get the Asset List:



✓ Use a filter for this Information Product

Mission Code * TEST

Information Product Type * ASSET LIST

Phase * Establish Forces

Planning Period Initial Deployment

Name

Asset List Type Choose

Approval Status Choose

Current IPCAL □

Current JPCAL □

Asset List Identity

Min Start Date

MaxEndDate

Min Approval Date

Figure 7-16: AirC2IS Asset List Information Product creation

The mandatory attributes are:

- The Mission Code
- The Information Product Type
- The Phase

The main optional attributes are:

- The Planning Period
- The Name

The following screenshot shows an overview of the AirC2IS Asset List displayed in the NCOP Geographical COP Editor:

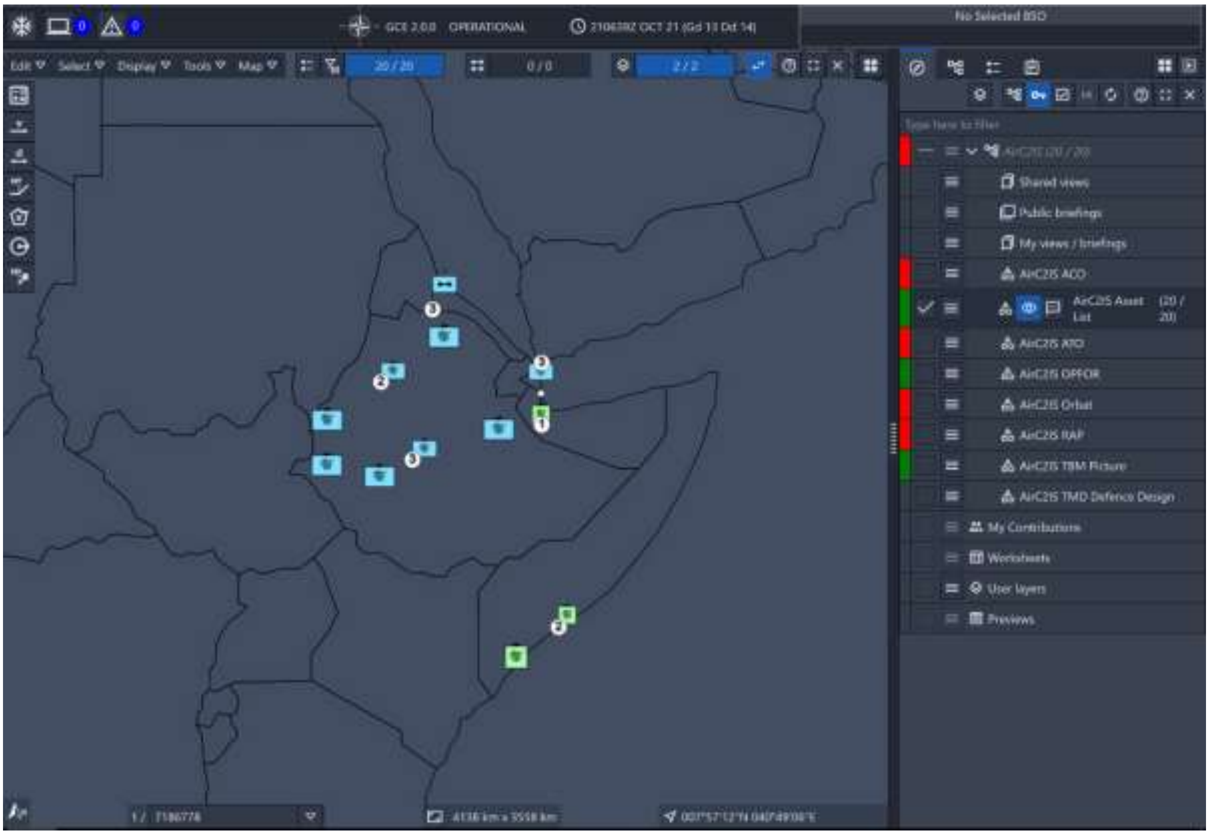


Figure 7-17: Overview of the AirC2IS Asset List displayed in NCOP

E.1.1.3 ATO Service

The following sequence diagram shows the web service operations consumed by NCOP to get the ATO:

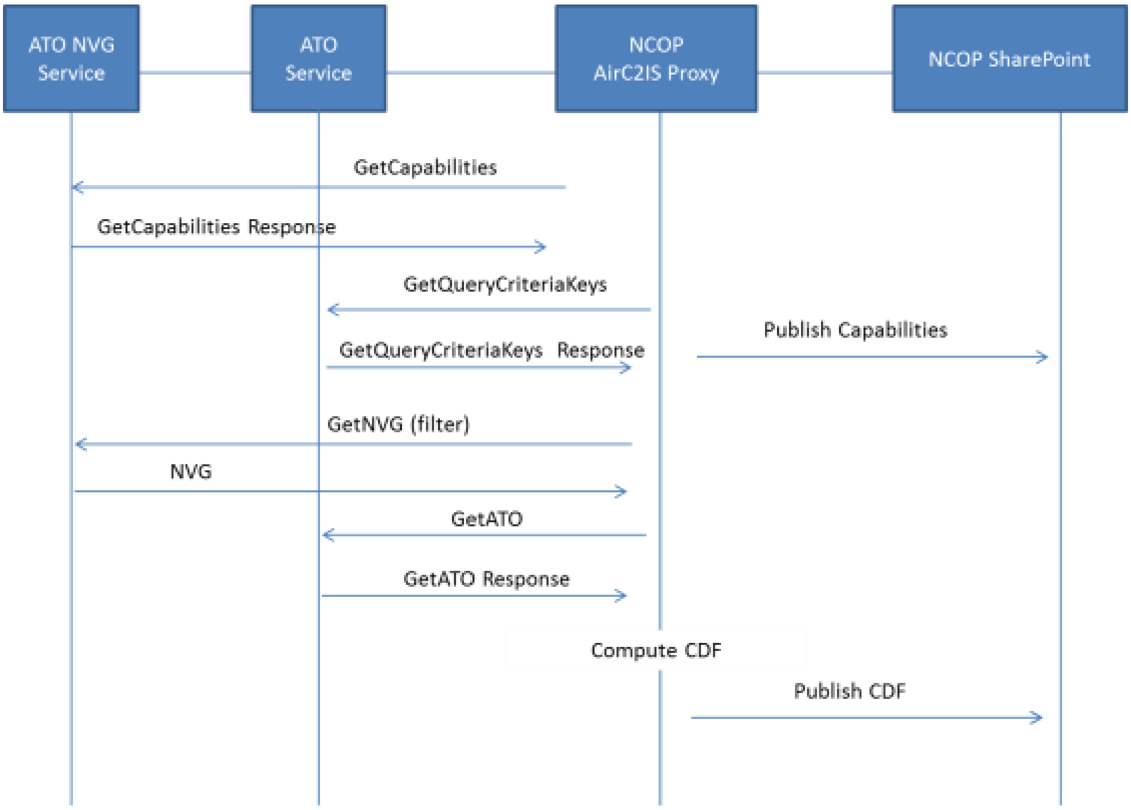
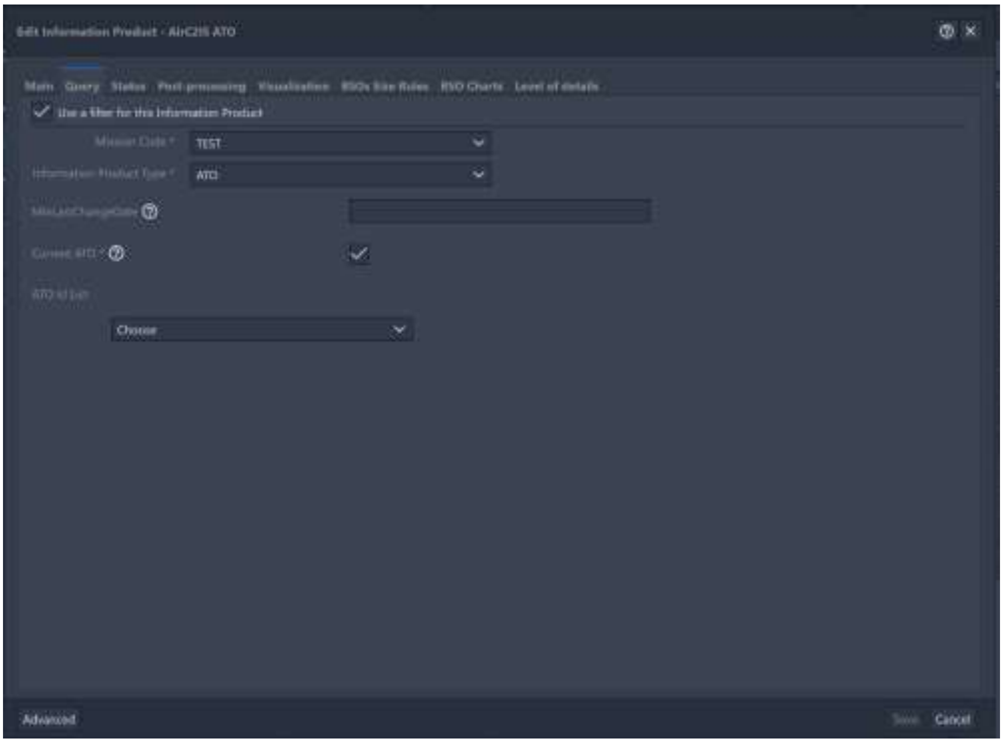


Figure 7-18: AirC2IS ATO Service sequence diagram

The following screenshot shows an overview of the AirC2IS ATO parameters that are displayed in NCOP Information Product Definition to get the ATO:



☑ Use a filter for this Information Product

Mission Code * TEST

Information Product Type * ATO

MinLastChangeDate

Current ATO * ☑

ATO Id List

Choose

Figure 7-19: AirC2IS ATO Information Product creation

The mandatory attributes are:

- The Mission Code
- The Information Product Type

The main optional attributes are:

- The ATO Id

The following screenshot shows an overview of the AirC2IS ATO displayed in the NCOP Geographical COP Editor:

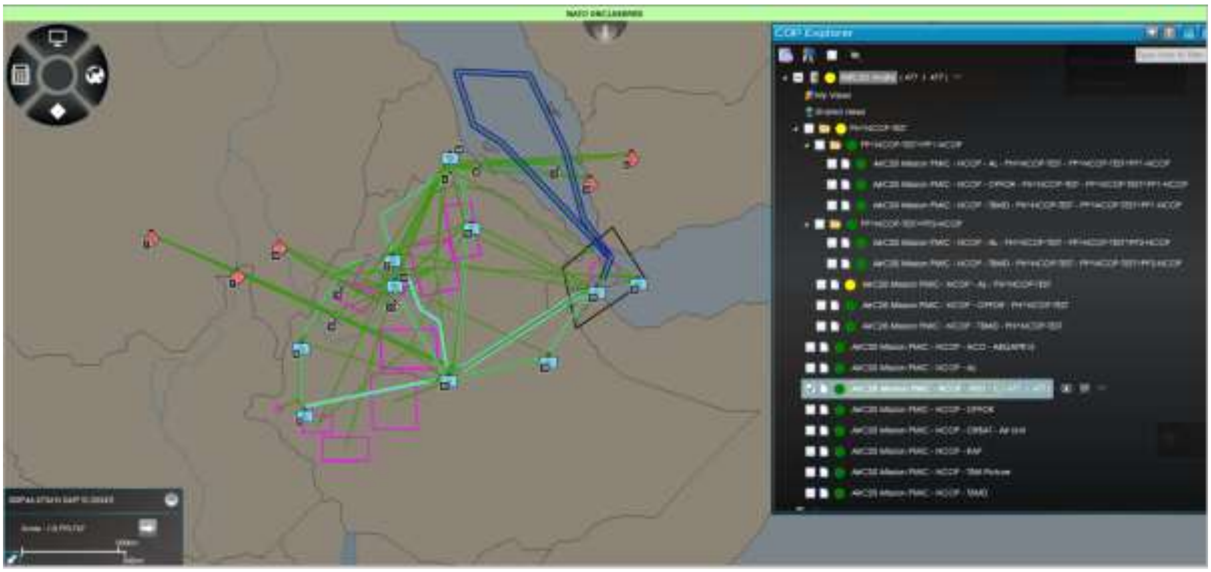


Figure 7-20: Overview of the AirC2IS ATO displayed in NCOP

E.1.1.4 TBMD Defence Design Service

The following sequence diagram shows the web service operations consumed by NCOP to get the TBM Defence Design:

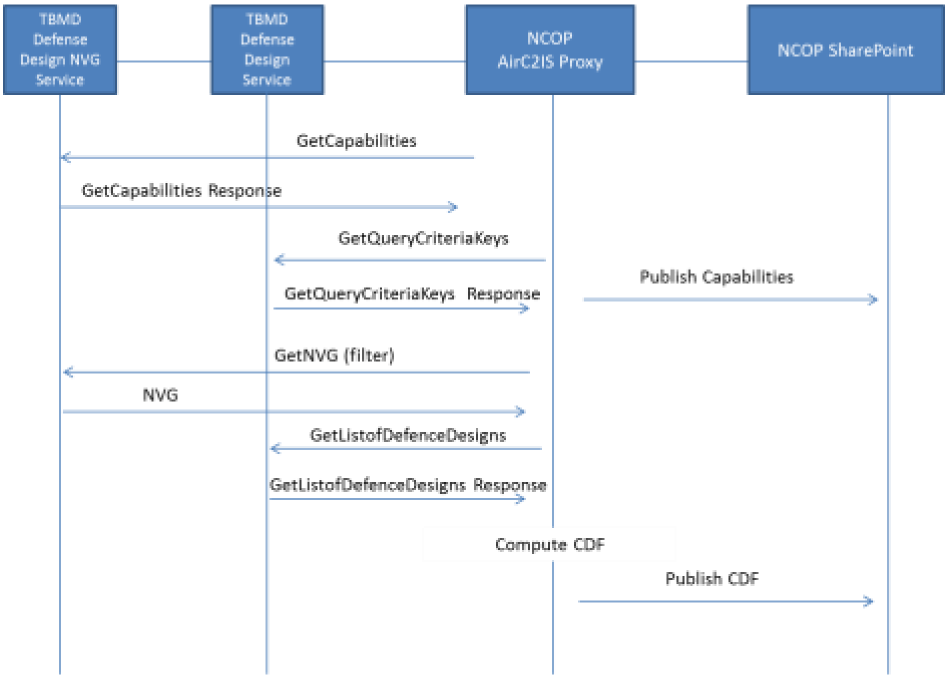
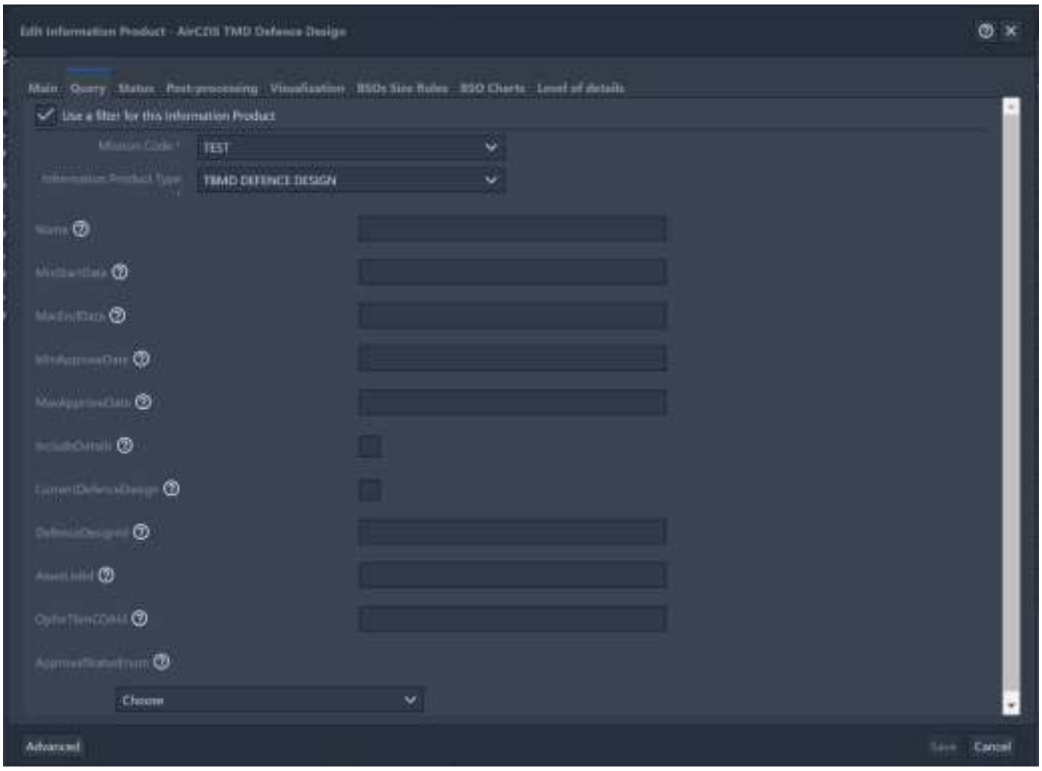


Figure 7-21: AirC2IS TBM Defence Design Service sequence diagram

The following screenshot shows an overview of the AirC2IS TBM Defence Design parameters that are displayed in NCOP Information Product Definition to get the TBM Defence Design:



☑ Use a filter for this Information Product

Mission Code * TEST

Information Product Type * TBMD DEFENCE DESIGN

Name ⓘ

MinStartDate ⓘ

MaxEndDate ⓘ

MinApproveDate ⓘ

MaxApproveDate ⓘ

IncludeDetails ⓘ □

CurrentDefenceDesign ⓘ □

DefenceDesignId ⓘ

AssetListId ⓘ

OpforTbmCOAId ⓘ

ApprovalStatusEnum ⓘ

Choose

Figure 7-22: AirC2IS TBMD Defence Design Information Product creation

The mandatory attributes are:

- The Mission Code
- The Information Product Type
- The Phase

The main optional attributes are:

- The Planning Period
- The Name

The following screenshot shows an overview of the AirC2IS TBM Defence Design displayed in the NCOP Geographical COP Editor:

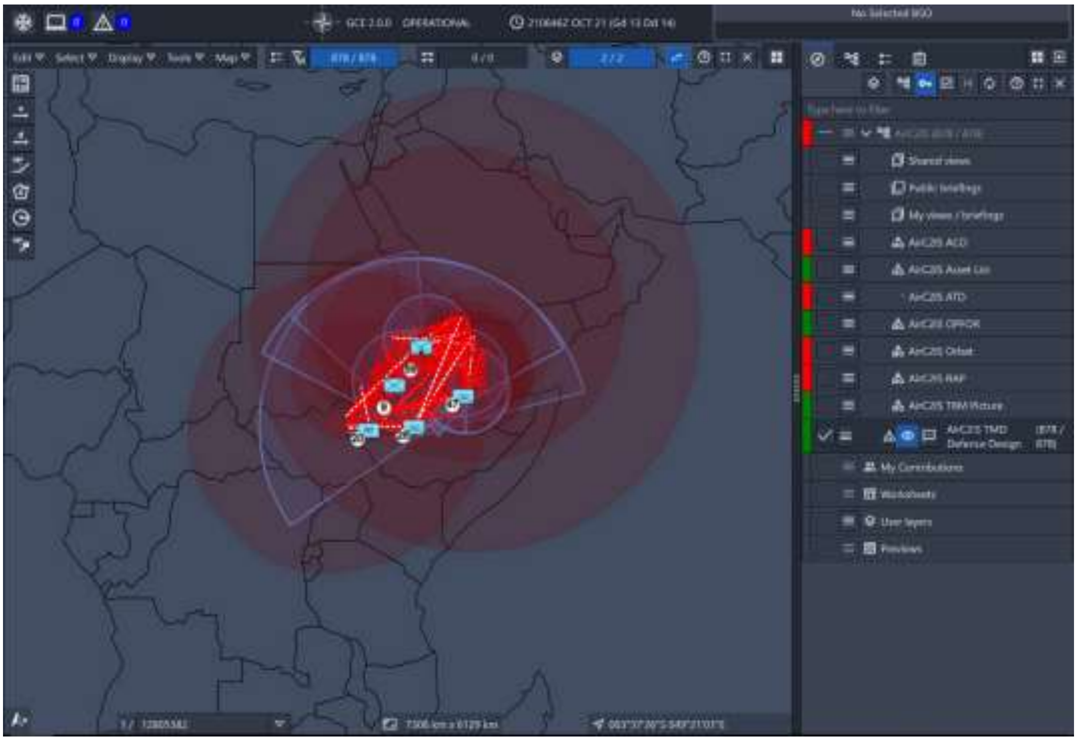


Figure 7-23: Overview of the AirC2IS TBM Defence Design displayed in NCOP

E.1.1.5 OPFOR TBM COA Service

The following sequence diagram shows the web service operations consumed by NCOP to get the OPFOR TBM COA:

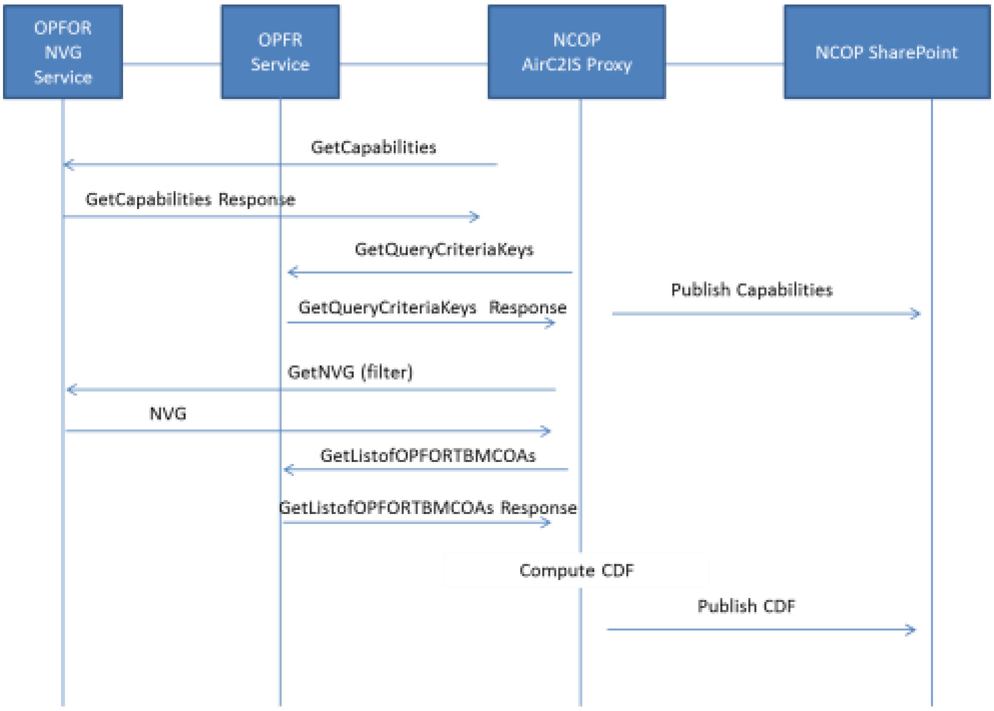
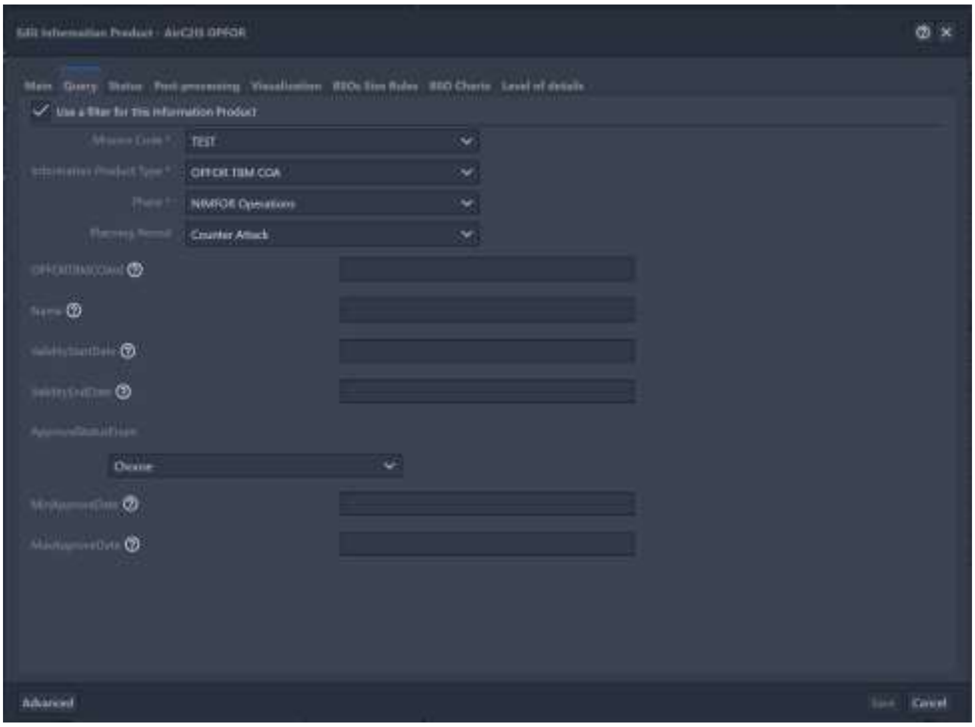


Figure 7-24: AirC2IS OPFOR TBM COA Service sequence diagram

The following screenshot shows an overview of the AirC2IS OPFOR TBM COA parameters that are displayed in NCOP Information Product Definition to get the OPFOR TBM COA:


Edit Information Product - AirC2IS OPFOR

☑ Use a filter for this Information Product

Mission Code *: TEST

Information Product Type *: OPFOR TBM COA

Phase *: NMFOR Operations

Planning Period: Counter Attack

OPFORTBMCOAId

Name

ValidityStartDate

ValidityEndDate

ApprovalStatusFrom: Choose

MinApprovalDate

MaxApprovalDate

Figure 7-25: AirC2IS OPFOR TBM COA Information Product creation

The mandatory attributes are:

- The Mission Code
- The Information Product Type
- The Phase
- The Name

The main optional attributes are:

- The Planning Period

The following screenshot shows an overview of the AirC2IS OPFOR TBM COA displayed in the NCOP Geographical COP Editor:

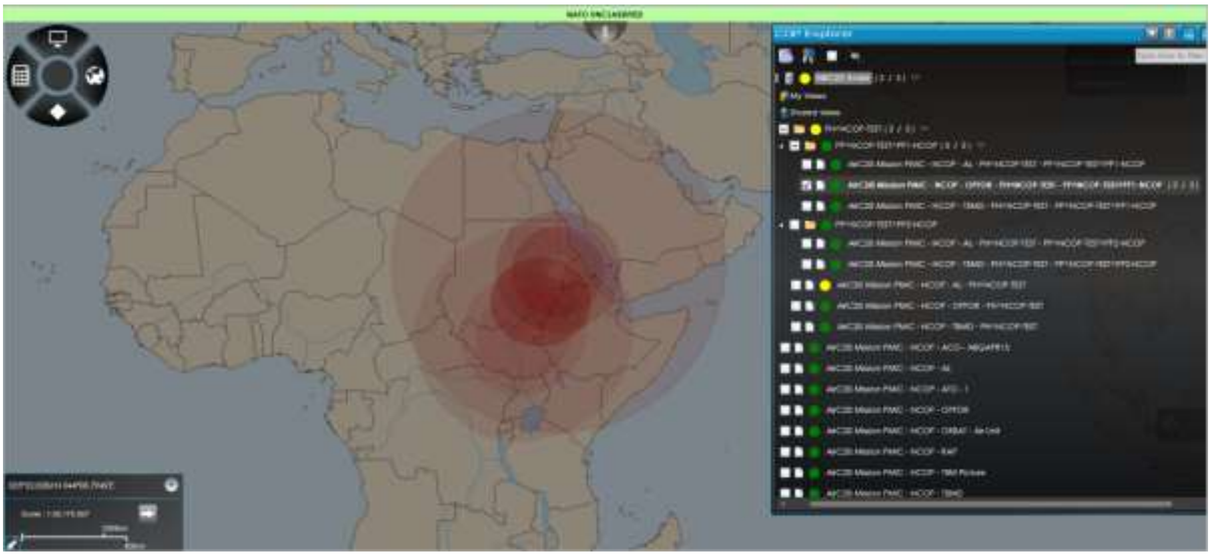

NATO UNCLASSIFIED
COP Explorer
My Views
Shared Views
AirC2IS Mission PMC - NCOP - AL
AirC2IS Mission PMC - NCOP - OPFOR
AirC2IS Mission PMC - NCOP - TBMD
AirC2IS Mission PMC - NCOP - ORBAT - Air Unit
AirC2IS Mission PMC - NCOP - TBM Picture

Figure 7-26: Overview of the AirC2IS OPFOR TBM COA displayed in NCOP

E.1.1.6 ORBAT Service

The following sequence diagram shows the web service operations consumed by NCOP to get the ORBAT:

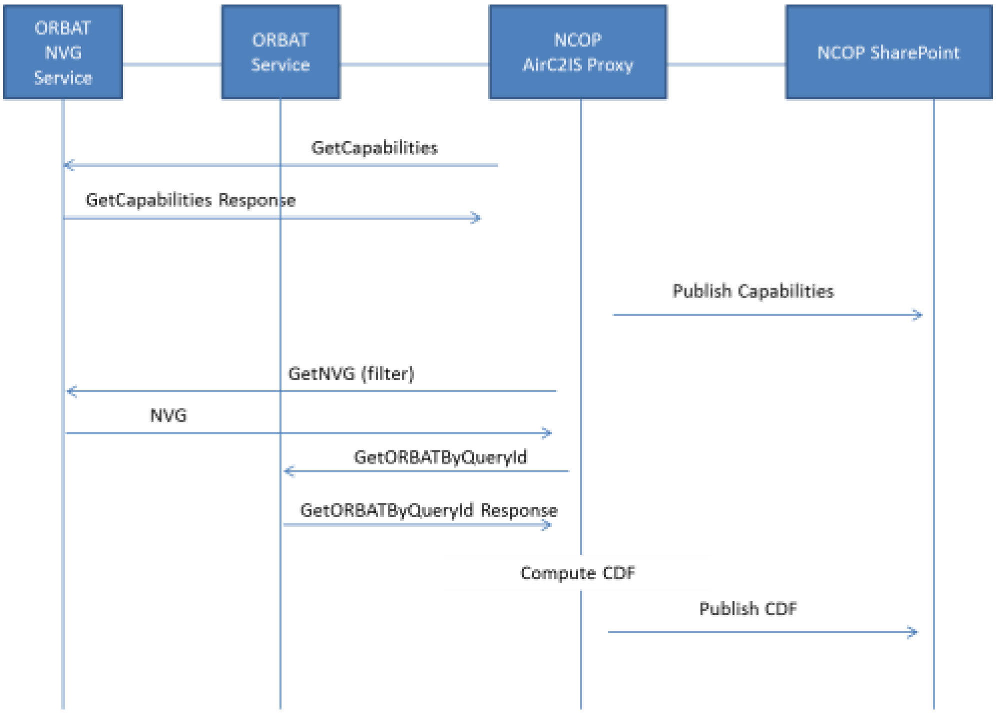
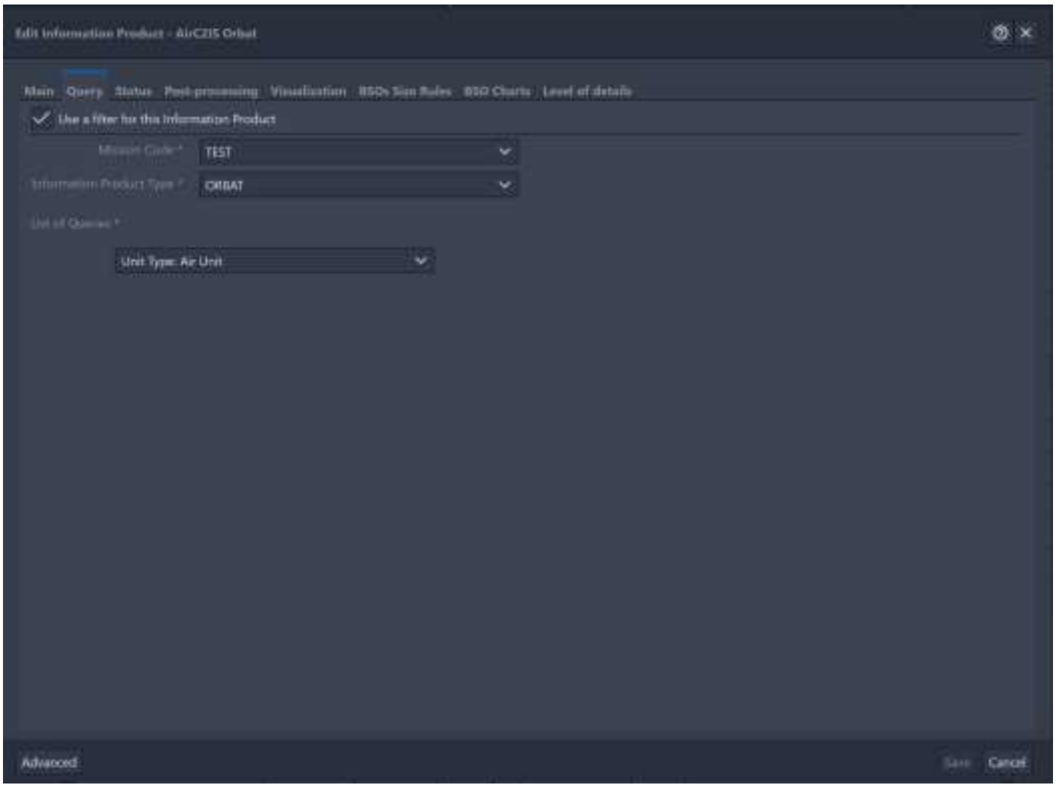


Figure 7-27: AirC2IS ORBAT Service sequence diagram

The following screenshot shows an overview of the AirC2IS ORBAT parameters that are displayed in NCOP Information Product Definition to get the ORBAT:



Edit Information Product - AirC2IS Orbat

☑ Use a filter for this Information Product

Mission Code *: TEST

Information Product Type *: ORBAT

List of Queries *

Unit Type: Air Unit

Figure 7-28: AirC2IS ORBAT Information Product creation

The mandatory attributes are:

- The Mission Code
- The Information Product Type
- The Query (examples: OPFOR BM Units, OWN Units …)

The following screenshot shows an overview of the AirC2IS ORBAT displayed in the NCOP Geographical COP Editor:

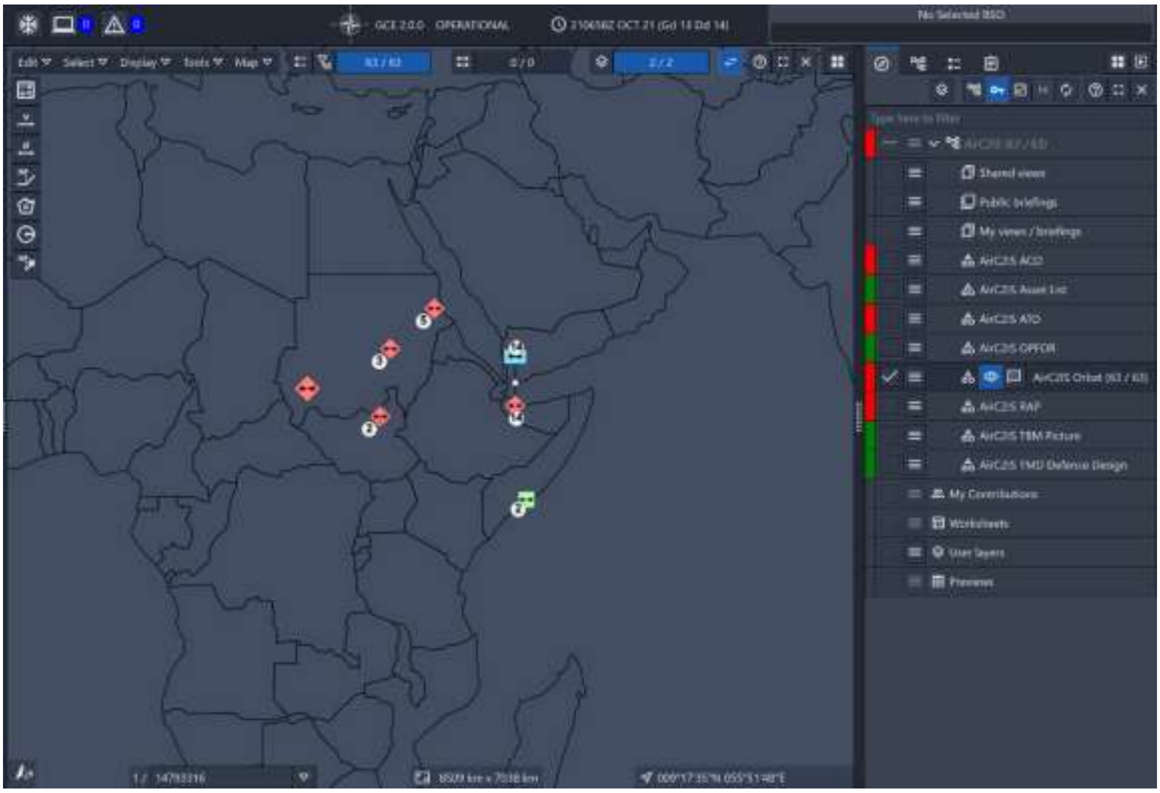


Figure 7-29: Overview of the AirC2IS ORBAT displayed in NCOP

E.1.1.7 RAP Service

The following sequence diagram shows the web service operations consumed by NCOP to get the RAP Picture:

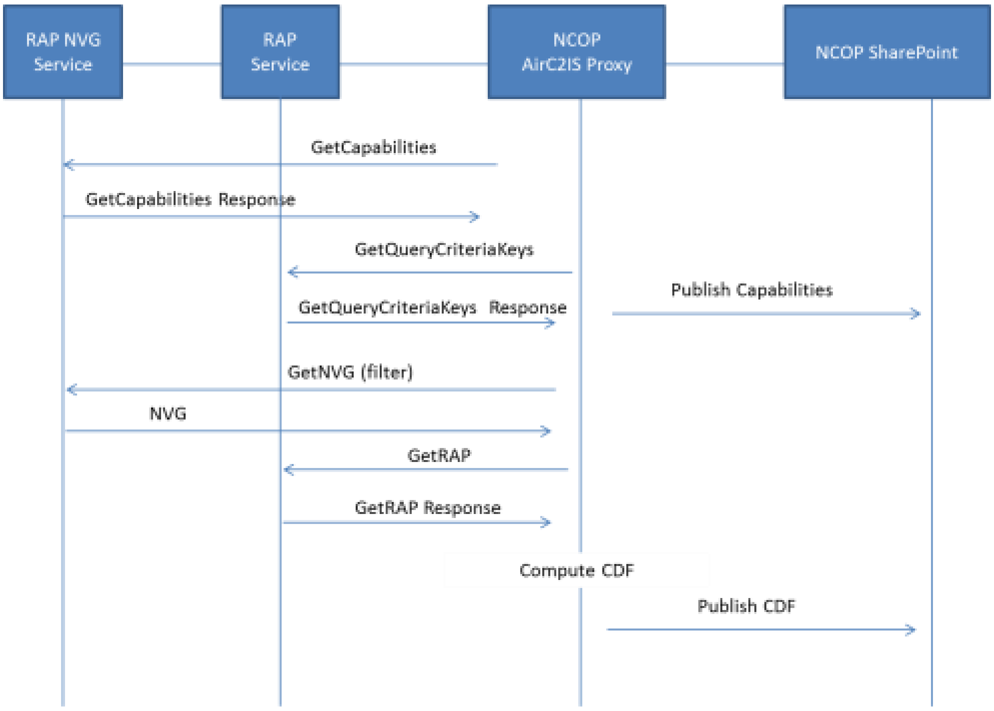
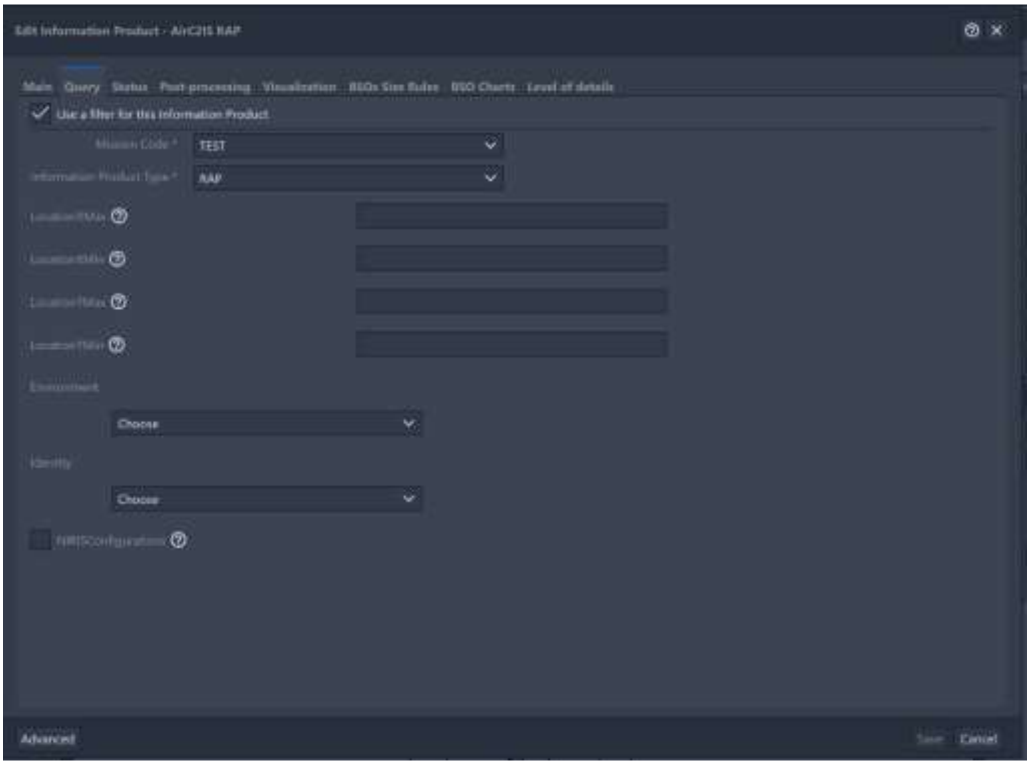


Figure 7-30: AirC2IS RAP Service sequence diagram

The following screenshot shows an overview of the AirC2IS RAP parameters that are displayed in NCOP Information Product Definition to get the RAP:



☑ Use a filter for this Information Product

Mission Code * TEST

Information Product Type * RAP

LocationEMax

LocationEMin

LocationNMax

LocationNMin

Environment

Choose

Identity

Choose

□ NIRISConfigurations

Figure 7-31: AirC2IS RAP Information Product creation

The mandatory attributes are:

- The Mission Code
- The Information Product Type

The following screenshot shows an overview of the AirC2IS RAP Picture displayed in the NCOP Geographical COP Editor:

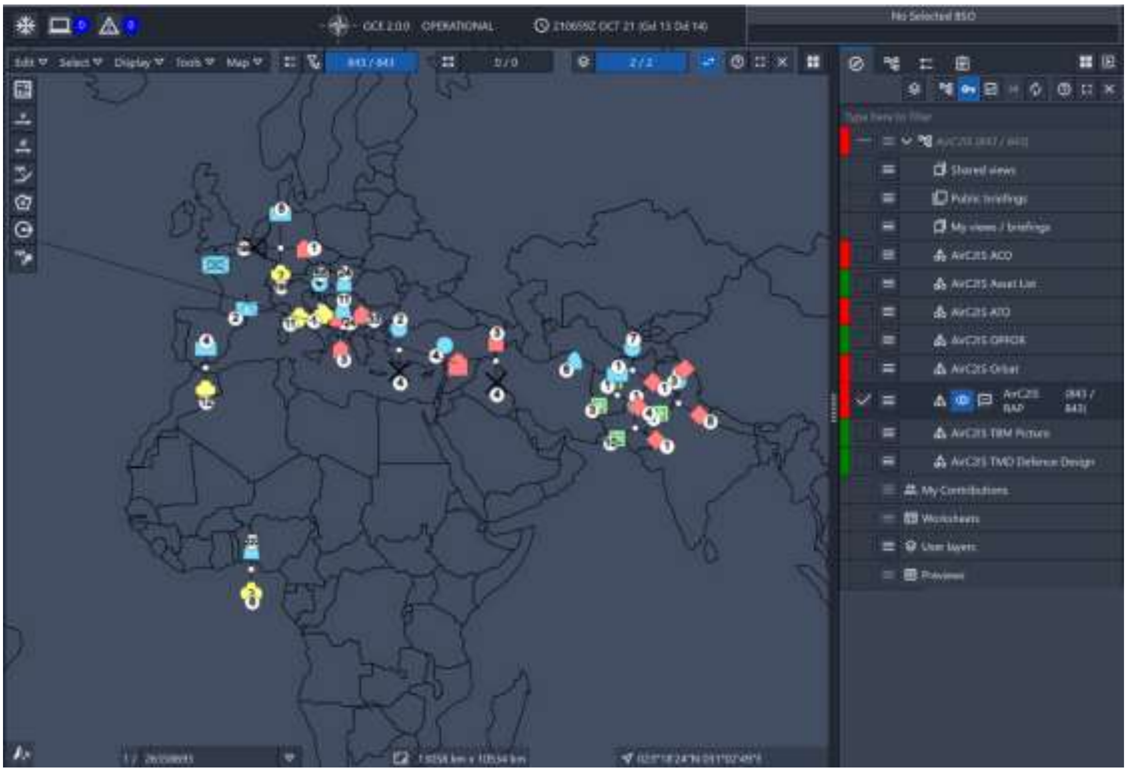


Figure 7-32: Overview of the AirC2IS RAP displayed in NCOP

E.1.1.8 Target List Service

The following sequence diagram shows the web service operations consumed by NCOP to get the Target List:

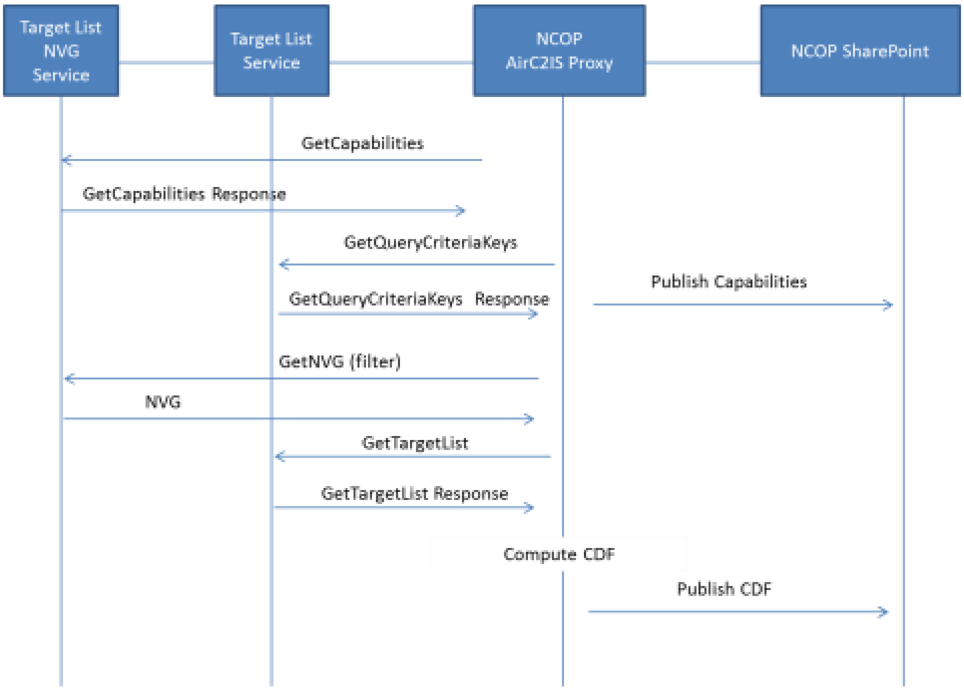
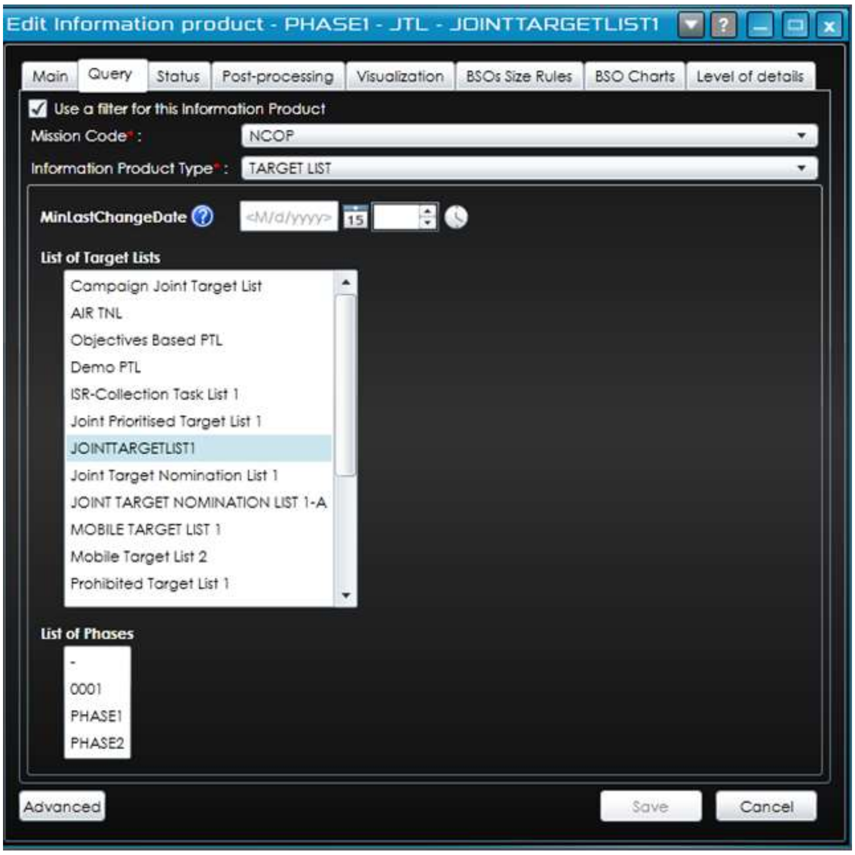


Figure 7-33: AirC2IS Target List Service sequence diagram

The following screenshot shows an overview of the AirC2IS Target List parameters that are displayed in NCOP Information Product Definition to get the Target List:



Edit Information product - PHASE1 - JTL - JOINTTARGETLIST1

☑ Use a filter for this Information Product

Mission Code* : NCOP

Information Product Type* : TARGET LIST

MinLastChangeDate <M/d/yyyy>

List of Target Lists

- Campaign Joint Target List
- AIR TNL
- Objectives Based PTL
- Demo PTL
- ISR-Collection Task List 1
- Joint Prioritised Target List 1
- JOINTTARGETLIST1
- Joint Target Nomination List 1
- JOINT TARGET NOMINATION LIST 1-A
- MOBILE TARGET LIST 1
- Mobile Target List 2
- Prohibited Target List 1

List of Phases

- -
- 0001
- PHASE1
- PHASE2

Figure 7-34: AirC2IS Target List Information Product creation

The mandatory attributes are:

- The Mission Code
- The Information Product Type

The main optional attributes are:

- The Target List Name

The following screenshot shows an overview of the AirC2IS Target List displayed in the NCOP Geographical COP Editor:

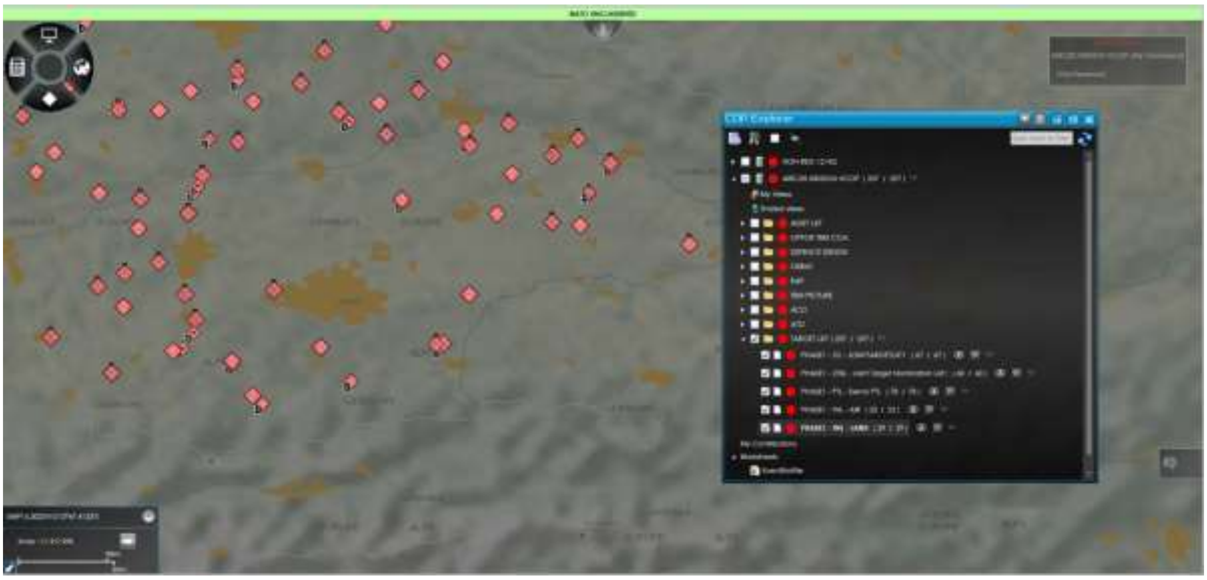


Figure 7-35: Overview of the AirC2IS Target List displayed in NCOP

E.1.1.9 TBM Picture Service

The following sequence diagram shows the web service operations consumed by NCOP to get the TBM Picture:

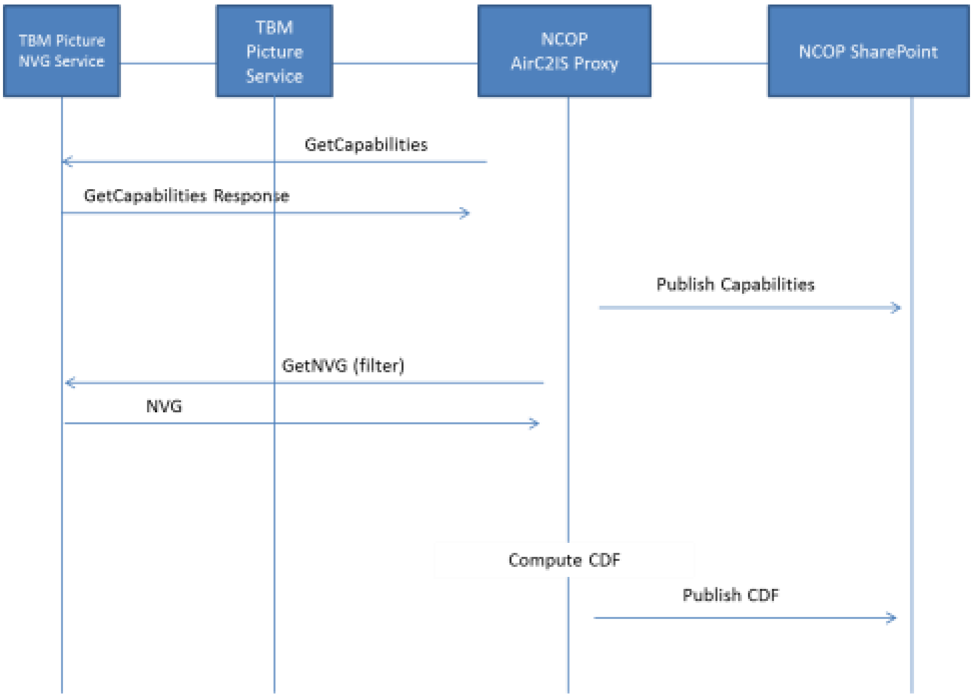
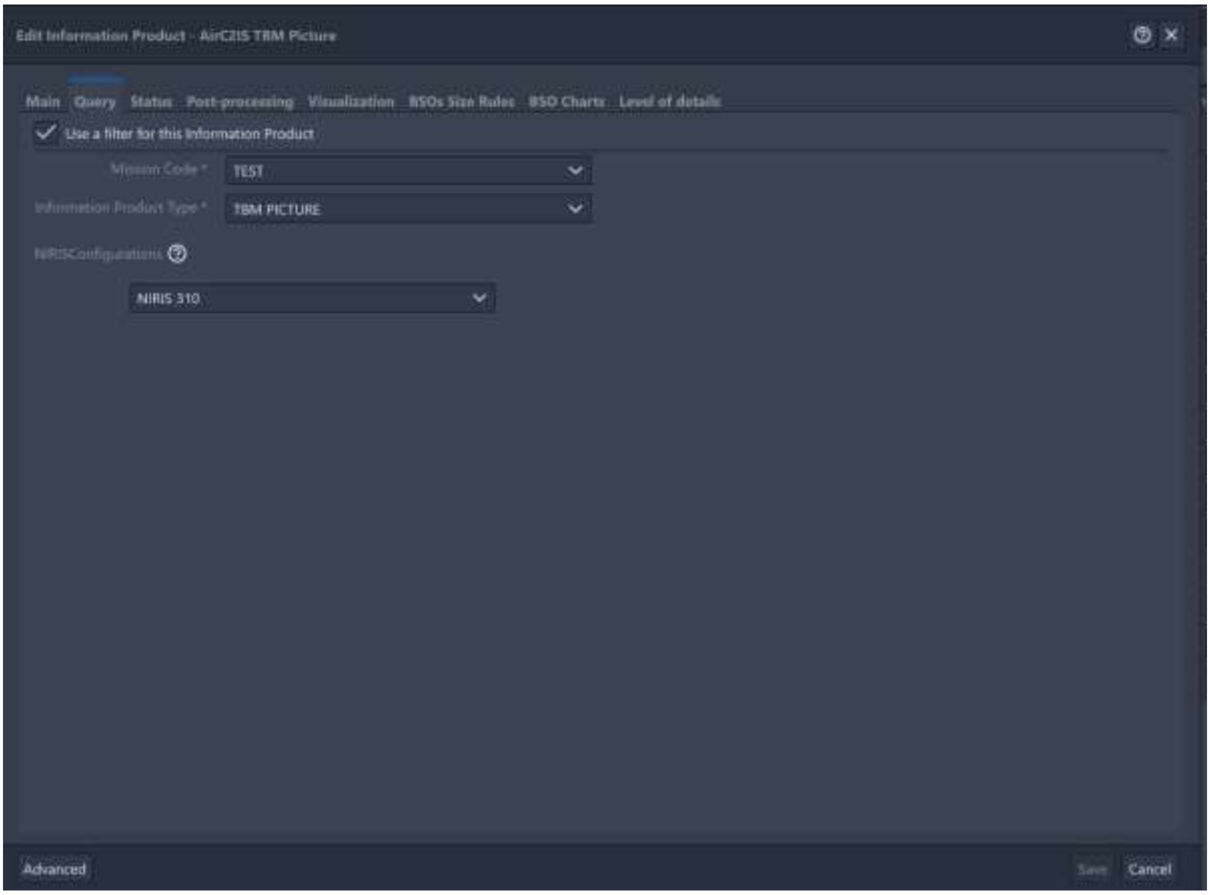


Figure 7-36: AirC2IS TBM Picture Service sequence diagram

The following screenshot shows an overview of the AirC2IS TBM Picture parameters that are displayed in NCOP Information Product Definition to get the TBM Picture:



Edit Information Product - AirC2IS TBM Picture

☑ Use a filter for this Information Product

Mission Code * TEST

Information Product Type * TBM PICTURE

NIRISConfigurations

NIRIS 310

Figure 7-37: AirC2IS TBM Picture Information Product creation

The mandatory attributes are:

- The Mission Code
- The Information Product Type

The following screenshot shows an overview of the AirC2IS TBM Picture displayed in the NCOP Geographical COP Editor:

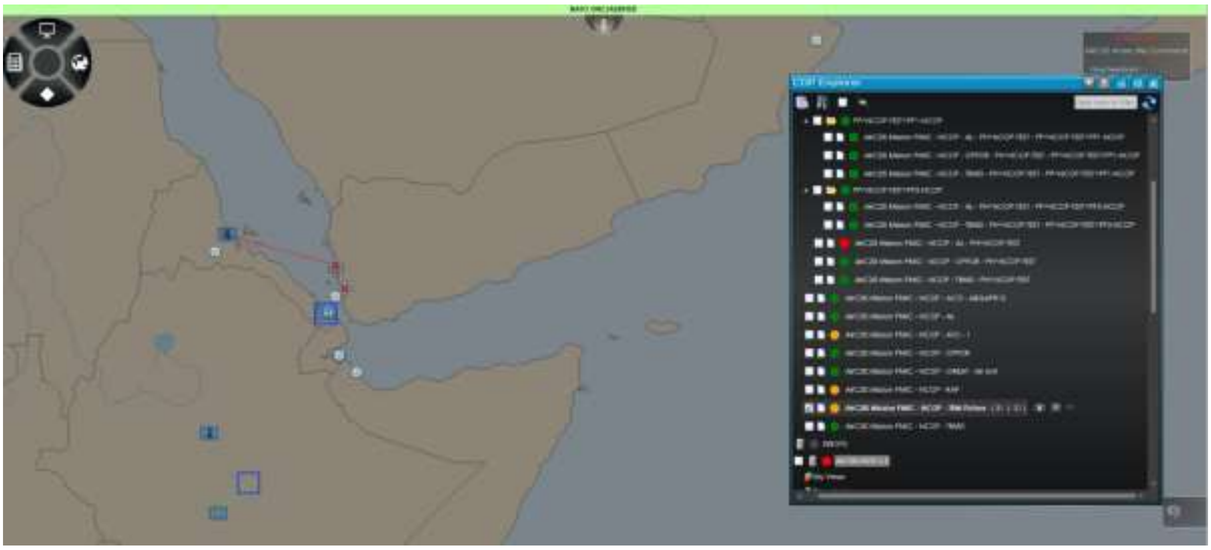


Figure 7-38: Overview of the AirC2IS TBM Picture displayed in NCOP

E.1.1.10 Pub/Sub Service

The following sequence diagram shows the main principles of the AirC2IS Pub/sub interface consumed by NCOP:

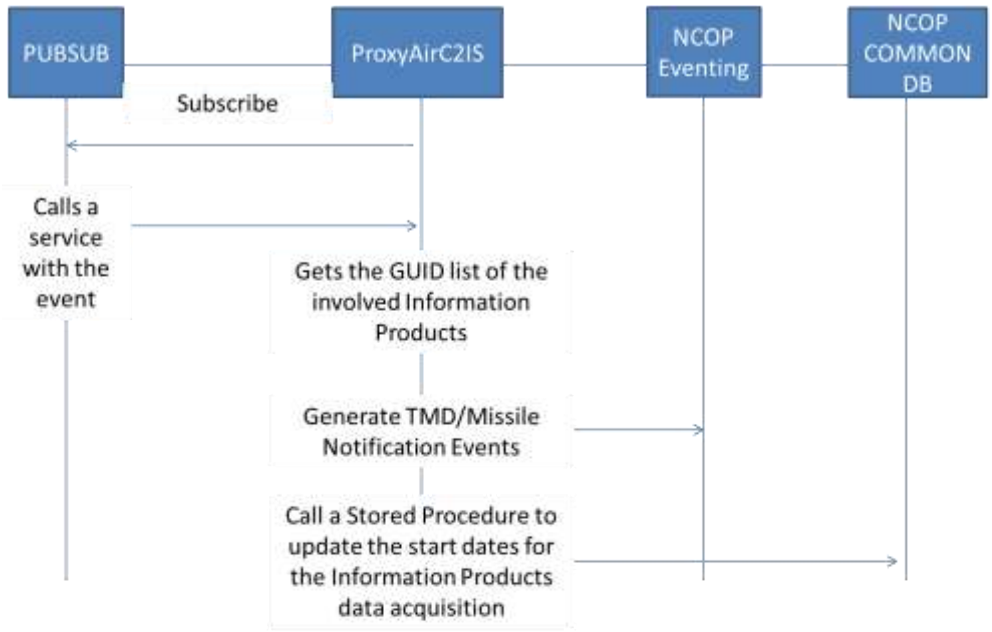
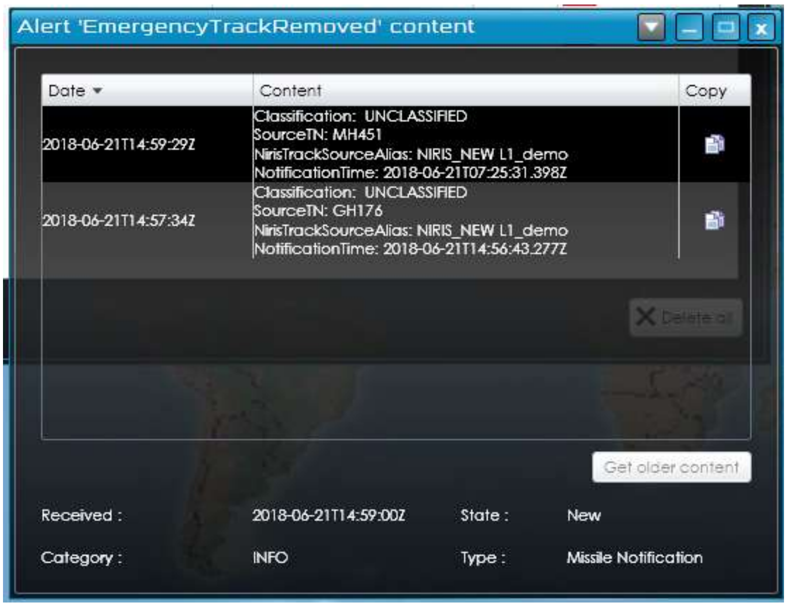

PUBSUB
ProxyAirC2IS
NCOP Eventing
NCOP COMMON DB
Subscribe
Calls a service with the event
Gets the GUID list of the involved Information Products
Generate TMD/Missile Notification Events
Call a Stored Procedure to update the start dates for the Information Products data acquisition

Figure 7-39: AirC2IS Pub/Sub Service sequence diagram

The AirC2IS PubSubService.svc is used to propagate events to the NCOP Notification Events Manager as illustrated below:


Alert 'EmergencyTrackRemoved' content

Date	Content	Copy
2018-06-21T14:59:29Z	Classification: UNCLASSIFIED SourceTN: MH451 NirisTrackSourceAlias: NIRIS_NEW L1_demo NotificationTime: 2018-06-21T07:25:31.398Z	
2018-06-21T14:57:34Z	Classification: UNCLASSIFIED SourceTN: GH176 NirisTrackSourceAlias: NIRIS_NEW L1_demo NotificationTime: 2018-06-21T14:56:43.277Z	

Received :	2018-06-21T14:59:00Z	State :	New
Category :	INFO	Type :	Missile Notification

Figure 7-40: AirC2IS Alerts displayed in NCOP Geographical COP Editor

E.1.2 AirC2IS Interface Workaround

The Excel file attached below contains the workaround that have been applied on AirC2IS Interface to bypass some AirC2IS implementation limitations or choices (described in table below):

TABLE 7-7: AIRC2IS INTERFACE WORKAROUND - SUMMARY

Service	Description
ACO	Nvg group id and label are set from native data
ALL	Replace empty labels by Uri
ALL	Replace in groups and composite empty Uri by Label
ALL	Seen on BSOs of ACO: inside a polyline somes points are repeated (2, 3, 4, etc times). Points are simplified by TIMS
ATO	Nvg group id and label are set from native data
ATO	Empty extendeddata EstSpeed because it holds a datetime
Defence Design	Replace the MOA with OPFOR elements
Defence Design	Added Native "Task" into the Nvg
Defence Design	INTRA IP creation between threat and asset through task object (threatId never exists)
OPFOR	Added Uri to composite "MOA:uri"
ORBAT	Add UIC in the non friendly units labels
ORBAT	Remove duplicated items with same uri
PICTURE	Nvg group id and label are set from extendeddata referenceTN
PICTURE	Add Uri and Label to composite : Uri=pointAmplification-trackNumberRelated-TrackNumberReference label=label of the first point in the composite
PICTURE	Add Uri to bso : Uri=type-sourceTn-trackNumberRelated
Defence Design, Asset List, OPFOR, ACO and ATO	Add segmentation concept in NCOP

Workaround.xlsx

APPENDIX F TIMS.JS TECHNICAL DETAILS

F.1 INTRODUCTION

TIMS.js is a Software Development Kit (SDK) that allows developing civilian and military GIS based Web Applications. More precisely, TIMS.js is a JavaScript library that provides Web Mapping Capabilities (WMC). TIMS.js WMC library allows building a GIS Clients that can operate with any OGC compatible GIS Server (WMS, WMTS, WCS, WFS, etc).

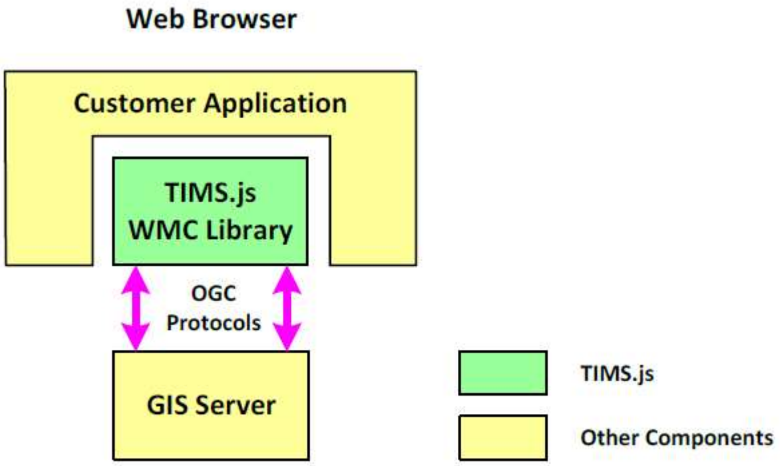


Figure 7-41: TIMS.js, Customer Application (NCOP Increment-2), and GIS Server

TIMS.js is a Thales Product developed on internal funding since 2015, based on up-to-date web technologies (HTML5, TypeScript) and Open Source Software (OpenLayers, Cesium). Thales masters the solution from “floor to ceiling” by contributing to these open source communities. Furthermore, TIMS.js provides an isolation layer around the OSS that makes it resilient to any potential future obsolescence. TIMS.js is business agnostic, it targets Thales solutions for both military and civilian domains (Business algorithms and MMI are out of the scope of TIMS.js: nevertheless, the product includes numerous extension points that allow their development and integration by the Customer Application team. For example, it allows developing business specific clustering algorithms).

F.2 MAIN CONCEPTS

The TIMS.js Web Mapping Capability library allows the Customer Application to manage the following objects:

- MMI Widgets: Viewports (2D or 3D Viewports, ie. map view UI component),
- Map Based Information: Map Grids, Raster Images and Graphics,
- Information Containers: Raster Sources, Vector Sources, Elevation Matrices, Layers and Groups of Layers,

- Geodetic Services (Geo Matrices and Computation Functions).

Viewports are the only MMI widgets that the WMC Library provides (other MMI widgets shall be implemented in the Customer Application). A Viewport is an MMI widget that allows display Map Based Information, i.e. Raster Images and Graphics, organized in Layers or in Groups of Layers. WMC provides 2 types of Viewports: 2D Viewports and 3D Viewports.

Map Based Information is provided by different Data Sources:

- Raster Data Sources,
- Image Data Sources,
- Vector-Tile Sources,
- Vector Data Sources,
- Geo Matrix Data Sources.

Each Raster Data Source corresponds to a Raster Service provided by a GIS Server through WMS or WMTS protocol. An Image Data Source is based on an image resource file (PNG, JPEG, JPEG2000 or Geotiff).

A Vector-Tile Source corresponds to a Vector-Tile Service provided by a GIS infrastructure (OpenStreetMap is a well-known “open data” vector tiles provider: http://openmaptiles.org).

Basically, a Vector-Tile Service provides tiles containing vector data (points, polylines, polygons) with meta-information through a tiled based access protocol. Vector data are rendered in 2D Viewport dedicated layers and styles may be customized using Mapbox Style.

A Vector Data Source contains a set of TIMS.js Graphics. A Graphic is a vector primitive provided by TIMS.js SDK. It is defined by a Graphic Type (geometric shape), related information (style, geolocations) and, optionally, a Symbol. When a Symbol is specified, the rendering of the Graphic is performed by the corresponding Symbology Package.

A Geo Matrix Data Source is associated to a service provided by a GIS Server. That service is in charge of providing value matrices in accordance with specific resolution and extent or in accordance with the current Viewport display extent. Geo matrices may be queried according to several standard protocols (Geotiff over WCS, PNG over WMS, etc).

WMC provides the Customer Application with Geo Matrix based Computation capabilities. To this end, it allows to attach computation and rendering functions that will work on Geo Matrix values to provide specific results and map rendering. WMC provides built-in Computation functions that are related to elevation (DTM) based Geo Matrix (viewshed, point-to-point optical inter-visibility, hypsometries, etc).

Map Based Information is organized in Layers and Layer Groups. A Layer is the representation of one given Data Source for one given Viewport. A Layer is the atomic level of information that is managed by the Viewport. The Viewport notably manages the representation of each Layer (visibility, transparency, colour palette) and the Z-Order between the different Layers (i.e. the display order of the Layers from the background to the foreground). Layers can be grouped in order to easily apply common parameters. Layer Groups are equivalent to Layers from the perspective of the Viewport.

To each Viewport are attached dedicated display parameters such as Display Name, Projection (2D viewport only), Centring Point, Camera (3D only) and Zoom Level. Multiple Viewports components can be instanced within a Customer Application and can be synchronized in order to share some of these parameters. For example, it is possible to have a shared Centring Point for a given group of Viewports: if the user changes the Centring Point in one Viewport, this change will then be propagated to each Viewport of the group.

F.3 PHYSICAL ARCHITECTURE

The TIMS.js physical architecture is described in the figure below:

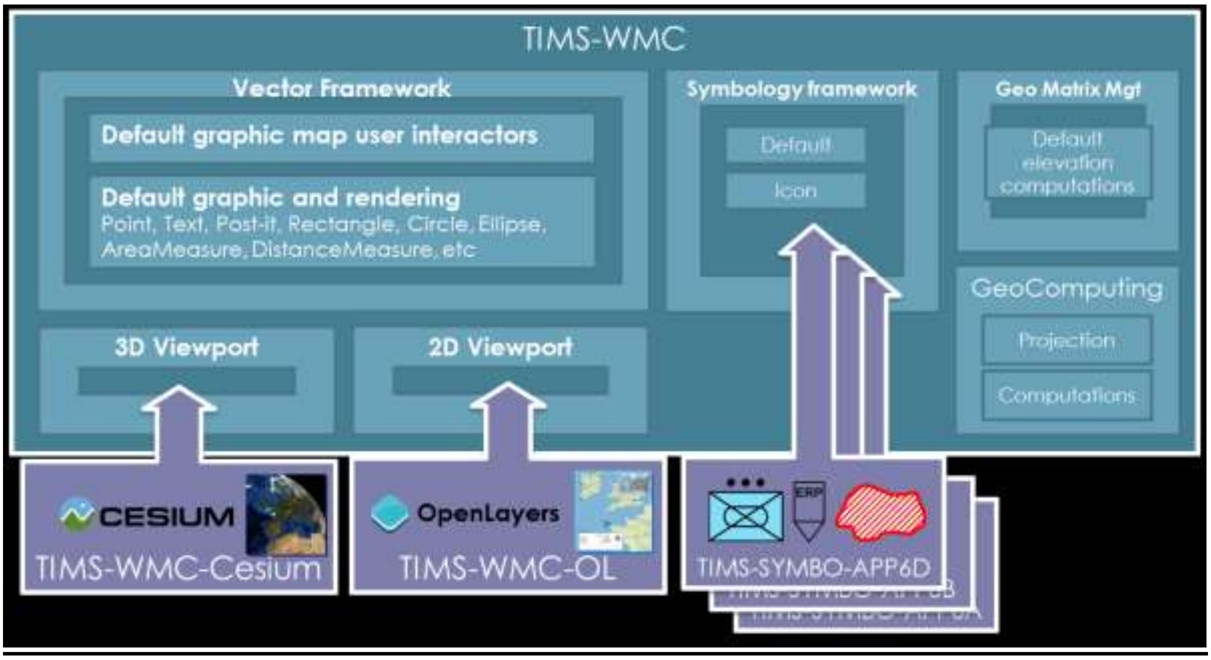


Figure 7-42: TIMS.js simplified physical architecture

The WMC library is decomposed into several modules:
□ The “Vector Framework” module contains the Graphics rendering and customization functions,

- The “Symbology Framework” module contains the Symbology Packages rendering and customization functions,

- The “2D Viewport” module implements all features associated to 2D viewports. It is currently implemented using the OpenLayers OSS. “Geo Matrix Management and Computation” module,
- “GeoComputing” module that provides common geo computing tools such as “project point” or “mid-point on segment” functions considering Spherical / Ellipsoid earth approximation models and Rhumbline / Great-circle discretization models,
- “2D Viewport” module that provides all features associated to 2D viewports. It is currently built upon OpenLayers OSS,
- “3D Viewport” module that provides all features associated to 3D viewports. It is currently built upon CESIUM.js OSS.

APPENDIX G WINDOWS REGISTRY KEYS USED BY NCOP

This section will be updated in a future version of this document.

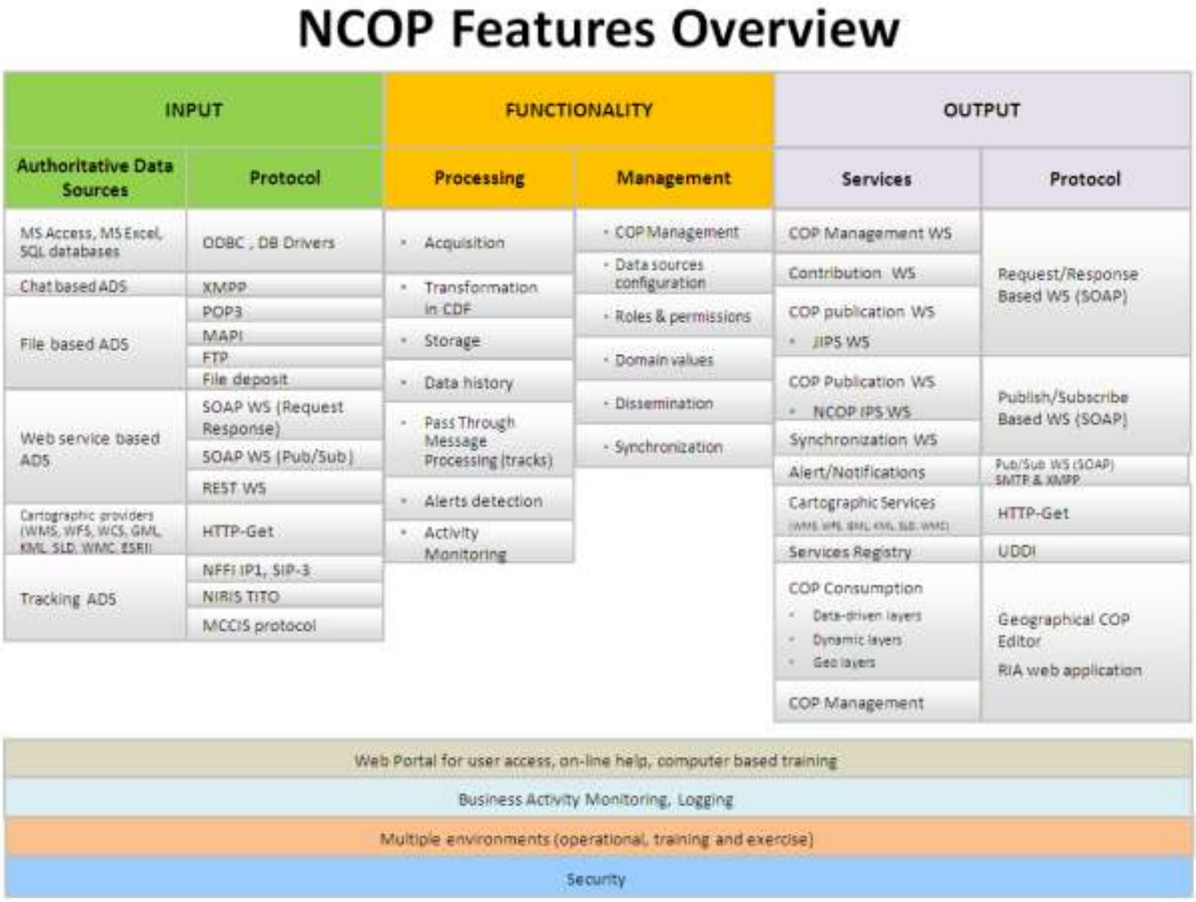
The following Windows Registry keys are set on every NCOP server:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\THALES\NCOP]

"ARCGIS_SERVER_NAME"="%ARCGIS_SERVER_NAME%"

"ARCGIS_SERVER_NAME_FULLY_QUALIFIED_DOMAIN_NAME"="%ARCGIS_SERVER_NAME%.%FULLY_QUALIFIED_DOMAIN_NAME%"

"BIZTALK_INSTANCE_NAME"="%BIZTALK_INSTANCE_NAME%"

"BIZTALK_INSTANCE_TCP_PORT"="%BIZTALK_INSTANCE_TCP_PORT%"

"BIZTALK_NLB_NAME"="%BIZTALK_NLB_NAME%"

"BIZTALK_NLB_NAME_FULLY_QUALIFIED_DOMAIN_NAME"="%BIZTALK_NLB_NAME%.%FULLY_QUALIFIED_DOMAIN_NAME%"

"BIZTALK_SQLSERVER_NAME"="%BIZTALK_SQLSERVER_NAME%"

"BIZTALK_SQLSERVER_NAME_BIZTALK_INSTANCE_NAME"="%BIZTALK_SQLSERVER_NAME%\\%BIZTALK_INSTANCE_NAME%"

"COMMON_INSTANCE_NAME"="%COMMON_INSTANCE_NAME%"

"COMMON_INSTANCE_TCP_PORT"="%COMMON_INSTANCE_TCP_PORT%"

"COMMON_SQLSERVER_NAME"="%COMMON_SQLSERVER_NAME%"

"COMMON_SQLSERVER_NAME_COMMON_INSTANCE_NAME"="%COMMON_SQLSERVER_NAME%\\%COMMON_INSTANCE_NAME%"

"DOMAIN_NETBIOS_NAME"="%DOMAIN_NETBIOS_NAME%"

"DOMAIN_NETBIOS_NAME_NCOP_BAM_PORTAL_USERS"="%DOMAIN_NETBIOS_NAME%\\%NCOP_BAM_PORTAL_USERS%"

"DOMAIN_NETBIOS_NAME_NCOP_BIZ_INSTANCE"="%DOMAIN_NETBIOS_NAME%\\%NCOP_BIZ_INSTANCE%"

"DOMAIN_NETBIOS_NAME_NCOP_BIZTALK_APPLICATION_USER_GROUP"="%DOMAIN_NETBIOS_NAME%\\%NCOP_BIZTALK_APPLICATION_USER_GROUP%"

"DOMAIN_NETBIOS_NAME_NCOP_GUEST_ACCOUNT"="%DOMAIN_NETBIOS_NAME%\\%NCOP_Guest_Account%"
```

```
"DOMAIN_NETBIOS_NAME_NCOP_WEB_SVC"="%DOMAIN_NETBIOS_NAME%\\%NCOP_WEB_SVC%"

"FULLY_QUALIFIED_DOMAIN_NAME"="%FULLY_QUALIFIED_DOMAIN_NAME%"

"HISTORY_INSTANCE_NAME"="%HISTORY_INSTANCE_NAME%"

"HISTORY_INSTANCE_TCP_PORT"="%HISTORY_INSTANCE_TCP_PORT%"

"HISTORY_SQLSERVER_NAME"="%HISTORY_SQLSERVER_NAME%"

"HISTORY_SQLSERVER_NAME_HISTORY_INSTANCE_NAME"="%HISTORY_SQLSERVER_NAME%\\%HISTORY_INSTANCE_NAME%"

"NCOP_BAM_PORTAL_USERS"="%NCOP_BAM_PORTAL_USERS%"

"NCOP_BIZ_INSTANCE"="%NCOP_BIZ_INSTANCE%"

"NCOP_BIZTALK_APPLICATION_USER_GROUP"="%NCOP_BIZTALK_APPLICATION_USER_GROUP%"

"NCOP_COMMON_SERVICES"="%NCOP_COMMON_SERVICES%"

"NCOP_COMMON_SERVICES_NCOP_HOST_HEADER_DNS_ZONE_NAME"="%NCOP_COMMON_SERVICES%.%NCOP_HOST_HEADER_DNS_ZONE_NAME%"

"NCOP_EXERCISE_WEBAPP_NAME"="%NCOP_EXERCISE_WEBAPP_NAME%"

"NCOP_GUEST_ACCOUNT"="%NCOP_Guest_Account%"

"NCOP_HOST_HEADER_DNS_ZONE_NAME"="%NCOP_HOST_HEADER_DNS_ZONE_NAME%"

"NCOP_PORTAL_WEBAPP_NAME"="%NCOP_PORTAL_WEBAPP_NAME%"

"NCOP_TRAINING_WEBAPP_NAME"="%NCOP_TRAINING_WEBAPP_NAME%"

"NCOP_WEB_SVC"="%NCOP_WEB_SVC%"

"NODE_TYPE"="HA"

"SQL_CMN_DATA_DRIVE_LETTER"="%SQL_CMN_DATA_DRIVE_LETTER%:\\"

"SQL_CMN_LOGS_DRIVE_LETTER"="%SQL_CMN_LOGS_DRIVE_LETTER%:\\"

"SQL_HIS_DATA_DRIVE_LETTER"="%SQL_HIS_DATA_DRIVE_LETTER%:\\"

"SQL_HIS_LOGS_DRIVE_LETTER"="%SQL_HIS_LOGS_DRIVE_LETTER%:\\"

"SQL_SERVER_NAME"="%SQL_SERVER_NAME_01%"
```

```
"SQL_SERVER_NAME_FULLY_QUALIFIED_DOMAIN_NAME"="%SQL_SERVER_NAME_01%.%FU
LLY_QUALIFIED_DOMAIN_NAME%"
```

APPENDIX H NCOP FEATURES OVERVIEW



NCOP Features Overview

INPUT	
Authoritative Data Sources	Protocol
MS Access, MS Excel, SQL databases	ODBC , DB Drivers
Chat based ADS	XMPP
File based ADS	POP3
	MAPI
	FTP
	File deposit
Web service based ADS	SOAP WS (Request Response)
	SOAP WS (Pub/Sub)
	REST WS
Cartographic providers (WMS, WFS, WCS, GML, KML SLD, WMC, ESRI)	HTTP-Get
Tracking ADS	NFFI IP1, SIP-3
	NIRIS TITO
	MCCIS protocol

FUNCTIONALITY	
Processing	Management
• Acquisition	• COP Management
• Transformation in CDF	• Data sources configuration
• Storage	• Roles & permissions
• Data history	• Domain values
• Pass Through Message Processing (tracks)	• Dissemination
• Alerts detection	• Synchronization
• Activity Monitoring	

OUTPUT	
Services	Protocol
COP Management WS	Request/Response Based WS (SOAP)
Contribution WS	
COP publication WS • JIPS WS	
COP Publication WS • NCOP IPS WS	Publish/Subscribe Based WS (SOAP)
Synchronization WS	
Alert/Notifications	Pub/Sub WS (SOAP) SMTP & XMPP
Cartographic Services (WMS, WFS, GML, KML, SLD, WMC)	HTTP-Get
Services Registry	UDDI
COP Consumption • Data-driven layers • Dynamic layers • Geo layers	Geographical COP Editor RIA web application
COP Management	

Web Portal for user access, on-line help, computer based training

Business Activity Monitoring, Logging

Multiple environments (operational, training and exercise)

Security

APPENDIX I IC COMPARISON BETWEEN NCOP INCREMENT-1 AND INCREMENT-2

TABLE 7-8: IC COMPARISON BETWEEN NCOP INCREMENT-1 AND INCREMENT-2

	IC (Increment-1)	IC (Increment-2)	Description of change
Bi-SC AIS Core	Core GIS	Core GIS	Update of release
	Chat	Chat	Update of release
	Informal Messaging	Informal Messaging	Update of release
	Active Directory	Active Directory	Update of release
	Enterprise Management Service	Enterprise Management Service	Update of release
	Document Handling System	Document Handling System	Update of release
	Security Services and Settings	Security Services and Settings	Update of release: NCIRC 2019
	NATO Metadata Registry and Repository	**NEDS**	IC Renamed
		Identity Provider	NEW
		NLB	Missing
NCOP COTS	PDF Reader	PDF Reader	Update of release
	Java Runtime Environment	Java Runtime Environment	Update of release
	McAfee Total Virus Defense Suite	**Antivirus**	IC Renamed
	ESRI ArcGIS Server & ArcGIS Desktop	**GeoServer**	ESRI replaced by GeoServer
	Veritas Backup Exec Agent		Deleted
	VMware	Vmware	Update of release: vSphere 6.7
		Angular	HTML5 HMI components
		Altova MapForce	Missing
		JavaScript Libraries	NEW

Microsoft COTS	Microsoft Windows XP and 7	Microsoft Windows	IC renamed. Windows 10 only for NCOP Increment-2
	Microsoft Internet Explorer	Microsoft Edge	Replacement of Microsoft Internet Explorer
	Silverlight		Deleted
	Microsoft .NET Framework	Microsoft .NET Framework	Build of code: .Net and .Net Core Update of Visual Studio solutions
	Microsoft Internet Information Server	Microsoft Internet Information Server	Update of the release
	Microsoft Windows Server	Microsoft Windows Server	Update of the Windows Server and NCIRC (2012 to 2019)
	Microsoft Office	Microsoft Office	Update of the release
	Microsoft SQL Server	Microsoft SQL Server	Update of the SQL Server (2012 to 2019)
		Microsoft SQL Server Reporting Services	Missing
	Microsoft Management Console Snap-In Tools		Deleted
	Microsoft BizTalk Services Microsoft BizTalk Administration	Microsoft BizTalk	Update of the BizTalk Server (2010 to 2020)
	Windows SharePoint Services Microsoft SharePoint Administration	Microsoft SharePoint	Update of the SharePoint Server (2010 to 2019)
	Microsoft Video Player		Deleted
	Microsoft Hyper-V	Microsoft Hyper-V	Still in the scope ?
NCOP components	Mission architecture		Deleted
	COP Manager	COP Manager	Update
	COP Structure Manager	COP Structure Manager	Update

	COP Shared View Manager	COP Shared View Manager	Update
	COP IP Manager	COP IP Manager	Update
	COP Workflow Manager	COP Workflow Manager	Update
	COP Contribution Manager	COP Contribution Manager	Update
	LoD Manager	LoD Manager	Update
	Time Manager	Time Manager	Replacement of old implementation by a complete new feature
		WMS Player	
		COP Explorer	Missing
		Relationship Manager	
		BSO Manager	
	SLR / SLA	SLR / SLA	Update
	Node Synchronisation	Node Synchronisation	Update of SOAP Headers with new STANAG 4774 and 4778 (XML Guard)
	NCOP storage	COP and IP storage	IC Renamed.
	CDF Interface		Deleted. Included in the « COP and IP storage » IC. Replacement of XML NVG 2.0.1 by NVG 2.0.2
	Management Information Storage	Management Information Storage	Update
	BSO History Manager	COP and IP History Storage	IC Renamed. Replacement of old implementation by a complete new feature
	Web Query Tool		Deleted
	NCOP Web Portal	NCOP Web Portal	Update of the SharePoint Server (2010 to 2019)
	Administration User Interface	User Administration	IC Renamed
	Geographical COP Editor	Geographical COP Editor	Replacement of TIMS.SL by TIMS.JS. Replacement of Silverlight HMI by Angular HMI. Addition of JSON services.
	Visualization Manager	Visualization Manager	Update

Role Based Access Control Manager		Deleted and content merged with Authentication and Authorization Services (RBAC)
Authentication and Authorization Manager	Authentication and Authorization Services (RBAC)	Update to allow SAML in addition of Kerberos. Migration to claims-based
COP Dissemination Manager	COP Dissemination Manager	Update
Audit / Log	Audit / Log	Update
Event Manager	Event Manager	Update
Journal Management		Deleted and content merged with Audit / Log
Activity Monitoring	Activity Monitoring	Update
Publication-Subscription		Deleted and content merged with Eventing / Alerting / Notification Services
Alert / Notification Services	Eventing / Alerting / Notification Services	Renew to reliability issues and REST API
Composition/Orchestration	Composition/Orchestration	Update
Cross Domain Manager		Deleted and content merged with Security Classification & Cross Domain Manager
Security Classification Manager	Security Classification & Cross Domain Manager	Update of SOAP Headers with new Stanag (XML Guard)
Information Panel Manager		Deleted and content splitted with COP Explorer, Relationship Manager …
User Layer Manager	User Layer Manager	Update
NCOP Directory	NCOP Directory	Update
NCOP Metadata Registry and Repository		Deleted
	Dynamic Source Server	Missing
Generic Message Processing	Generic Text Message Processing	Update
Database and Microsoft Excel Processing	SQL Database, SharePoint List and Microsoft Excel Processing	Update

	ADatP-3 Message Processing	ADatP-3 and OTH-T Gold Message Processing	Few new messages Update of Java Runtime release
	OTH-T Gold Message Processing		Deleted and content merged with ADatP-3 and OTH-T Gold Message Processing
	XML Message Processing	Generic XML Message Processing	Update
	NVG Streaming Protocol Processing	NVG Streaming Protocol Processing	Update
	Graphical symbology message Processing	LC2IS Overlays Processing	IC Renamed. Symbology processing included into the other « processing »: AdatP-3, OTHT-Gold, Generic Text, …
	Geographic format Processing	Geographic format Processing	Update
	Installation	Installation	Update
	CBT	CBT	Complete new CBT
	Training	Training	Update
	On-Line Help	On-Line Help	Update
		Aggregation Association Correlation Processing	NEW
		Aggregation Association Correlation Manager	NEW
		Globe View	Update of mapping of all sources to allow display of Z

APPENDIX J IC VS COTS DEPENDENCIES

The following table shows the dependencies between Implementation Components (type: Information System component) and the COTS.

TABLE 7-9: IC VS COTS DEPENDENCIES

IC/COTS	Activity Monitoring	ADatP-3 and OTH-T Gold Message Processing	Aggregation Association Correlation Manager	Aggregation Association Correlation Processing	Audit / Log	Authentication and Authorization Services (RBAC)	BSO Manager	CBT	Composition/Orchestration	COP and IP History Storage	COP and IP storage	COP Contribution Manager	COP Dissemination Manager	COP Explorer	COP IP Manager	COP Manager	COP Shared View Manager	COP Structure Manager	COP Workflow Manager	Dynamic Source Server	Event Manager	Eventing / Alerting / Notification Services	Generic Text Message Processing	Generic XML Message Processing	Geographic format Processing	Geographical COP Editor	Globe View	Installation	LC2IS Overlays Processing	LoD Manager	Management Information Storage	NCOP Directory	NCOP Tools	NCOP Web Portal	Node Synchronisation	NVG Streaming Protocol Processing	On-Line Help	Relationship Manager	Security Classification & Cross Domain Manager	SLR / SLA	SQL Database, SharePoint List and Microsoft Excel	Time Manager	Training	User Administration	User Layer Manager	Visualization Manager	WMS Player
Altova MapForce																							X																								
Angular							X					X	X	X	X	X	X	X	X						X	X				X								X				X			X	X	X
Antivirus																												X																			
GeoServer																																															X
Java Runtime Environment		X																																													X
JavaScript Libraries							X					X	X	X	X	X	X	X	X						X	X	X			X							X	X				X			X	X	X
PDF Reader														X																																	

IC/COTS	Activity Monitoring	ADatP-3 and OTH-T Gold Message Processing	Aggregation Association Correlation Manager	Aggregation Association Correlation Processing	Audit / Log	Authentication and Authorization Services (RBAC)	BSO Manager	CBT	Composition/Orchestration	COP and IP History Storage	COP and IP storage	COP Contribution Manager	COP Dissemination Manager	COP Explorer	COP IP Manager	COP Manager	COP Shared View Manager	COP Structure Manager	COP Workflow Manager	Dynamic Source Server	Event Manager	Eventing / Alerting / Notification Services	Generic Text Message Processing	Generic XML Message Processing	Geographic format COP Processing	Geographical COP Editor	Globe View	Installation	LC2IS Overlays Processing	LoD Manager	Management Information Storage	NCOP Directory	NCOP Tools	NCOP Web Portal	Node Synchronisation	NVG Streaming Protocol Processing	On-Line Help	Relationship Manager	Security Classification & Cross Domain Manager	SLR / SLA	SQL Database, SharePoint List and Microsoft Excel	Time Manager	Training	User Administration	User Layer Manager	Visualization Manager	WMS Player
Vmware	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Microsoft .NET Framework							X					X	X	X	X	X	X	X	X	X	X	X								X			X			X		X	X	X		X				X	X
Microsoft BizTalk	X								X														X	X					X							X					X						
Microsoft Edge							X	X				X	X	X	X	X	X	X	X						X	X	X			X							X	X				X			X	X	X
Microsoft Hyper-V	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Microsoft Internet Information Server		X					X					X	X	X	X	X	X	X	X	X	X	X	X			X	X		X	X				X	X		X	X	X	X		X					
Microsoft Office														X																											X						
Microsoft SharePoint											X	X	X	X	X	X	X	X	X											X	X	X		X				X	X				X	X			
Microsoft SQL Server			X	X						X											X	X										X													X		
Microsoft SQL Server Reporting Services	X																																														

IC/COTS	Activity Monitoring	ADatP-3 and OTH-T Gold Message Processing	Aggregation Association Correlation Manager	Aggregation Association Correlation Processing	Audit / Log	Authentication and Authorization Services (RBAC)	BSO Manager	CBT	Composition/Orchestration	COP and IP History Storage	COP and IP storage	COP Contribution Manager	COP Dissemination Manager	COP Explorer	COP IP Manager	COP Manager	COP Shared View Manager	COP Structure Manager	COP Workflow Manager	Dynamic Source Server	Event Manager	Eventing / Alerting / Notification Services	Generic Text Message Processing	Generic XML Message Processing	Geographic format Processing	Geographical COP Editor	Globe View	Installation	LC2IS Overlays Processing	LoD Manager	Management Information Storage	NCOP Directory	NCOP Tools	NCOP Web Portal	Node Synchronisation	NVG Streaming Protocol Processing	On-Line Help	Relationship Manager	Security Classification & Cross Domain Manager	SLR / SLA	SQL Database, SharePoint List and Microsoft Excel	Time Manager	Training	User Administration	User Layer Manager	Visualization Manager	WMS Player
Microsoft Windows							X					X	X	X	X	X	X	X	X						X	X	X			X							X	X									X
Microsoft Windows Server					X	X	X					X	X	X	X	X	X	X	X	X	X	X				X	X	X		X			X		X	X	X	X	X	X		X				X	
Active Directory						X																																									
Chat															X																																
Core GIS																																															X
Document Handling System							X								X																																
Enterprise Management Service																																								X							
Identity Provider						X																																									
Informal Messaging															X																																
NEDS																												X																			

IC/COTS	Activity Monitoring	ADatP-3 and OTH-T Gold Message Processing	Aggregation Association Correlation Manager	Aggregation Association Correlation Processing	Audit / Log	Authentication and Authorization Services (RBAC)	BSO Manager	CBT	Composition/Orchestration	COP and IP History Storage	COP and IP storage	COP Contribution Manager	COP Dissemination Manager	COP Explorer	COP IP Manager	COP Manager	COP Shared View Manager	COP Structure Manager	COP Workflow Manager	Dynamic Source Server	Event Manager	Eventing / Alerting / Notification Services	Generic Text Message Processing	Generic XML Message Processing	Geographic format Processing	Geographical COP Editor	Globe View	Installation	LC2IS Overlays Processing	LoD Manager	Management Information Storage	NCOP Directory	NCOP Tools	NCOP Web Portal	Node Synchronisation	NVG Streaming Protocol Processing	On-Line Help	Relationship Manager	Security Classification & Cross Domain Manager	SLR / SLA	SQL Database, SharePoint List and Microsoft Excel	Time Manager	Training	User Administration	User Layer Manager	Visualization Manager	WMS Player
NLB									X																			X						X													
Security Services and Settings																												X																			

APPENDIX K IC VS ACTORS INVOLVED

The traceability matrix between “Actors” and Implementation Components is provided as a separated Excel file (NCOP2 RIS - RTM - VCRM - User Stories) (tab: *Actors vs IC*).

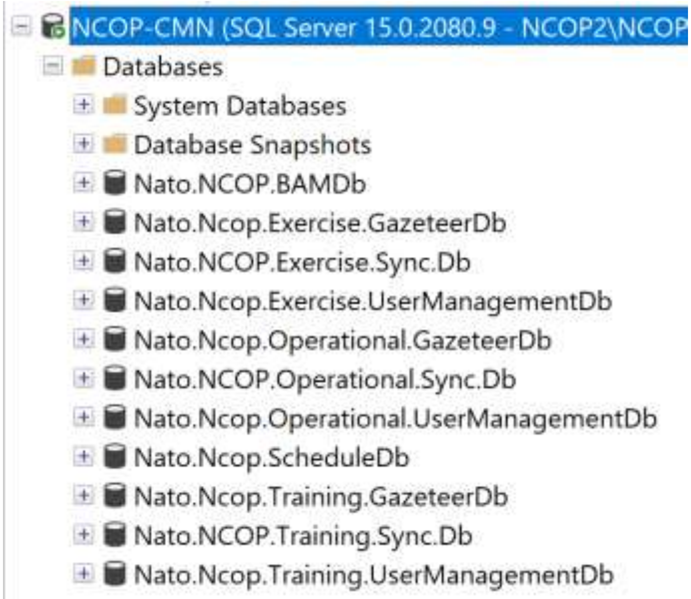
APPENDIX L IC VS OBJECTS INVOLVED

The traceability matrix between “Objects” and Implementation Components is provided as a separated Excel file (NCOP2 RIS - RTM - VCRM - User Stories) (tab: Objects vs IC).

APPENDIX M DATABASES DIAGRAMS

M.1 CMN SQL INSTANCE

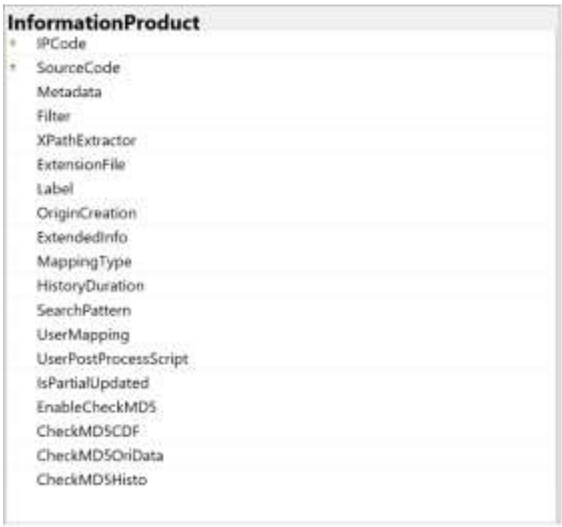
The figure below show the databases of the NCOP Common SQL instance:



```
⊟ NCOP-CMN (SQL Server 15.0.2080.9 - NCOP2\NCOP
   ⊟ Databases
      ⊞ System Databases
      ⊞ Database Snapshots
      ⊞ Nato.NCOP.BAMDb
      ⊞ Nato.Ncop.Exercise.GazeteerDb
      ⊞ Nato.NCOP.Exercise.Sync.Db
      ⊞ Nato.Ncop.Exercise.UserManagementDb
      ⊞ Nato.Ncop.Operational.GazeteerDb
      ⊞ Nato.NCOP.Operational.Sync.Db
      ⊞ Nato.Ncop.Operational.UserManagementDb
      ⊞ Nato.Ncop.ScheduleDb
      ⊞ Nato.Ncop.Training.GazeteerDb
      ⊞ Nato.NCOP.Training.Sync.Db
      ⊞ Nato.Ncop.Training.UserManagementDb
```

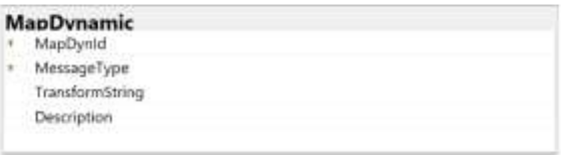
Figure 7-43: NCOP Common SQL instance databases

M.1.1.1 Nato.Ncop.ScheduleDb tables



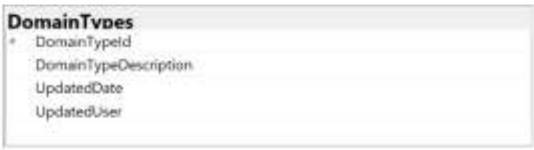
InformationProduct

- IPCode
- SourceCode
- Metadata
- Filter
- XPathExtractor
- ExtensionFile
- Label
- OriginCreation
- ExtendedInfo
- MappingType
- HistoryDuration
- SearchPattern
- UserMapping
- UserPostProcessScript
- IsPartialUpdated
- EnableCheckMD5
- CheckMD5CDF
- CheckMD5OriData
- CheckMD5Histo

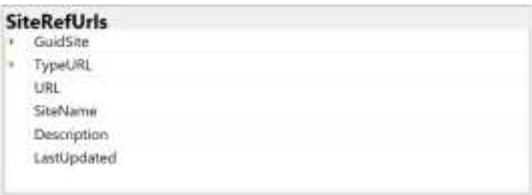


MapDynamic

- MapDynId
- MessageType
- TransformString
- Description

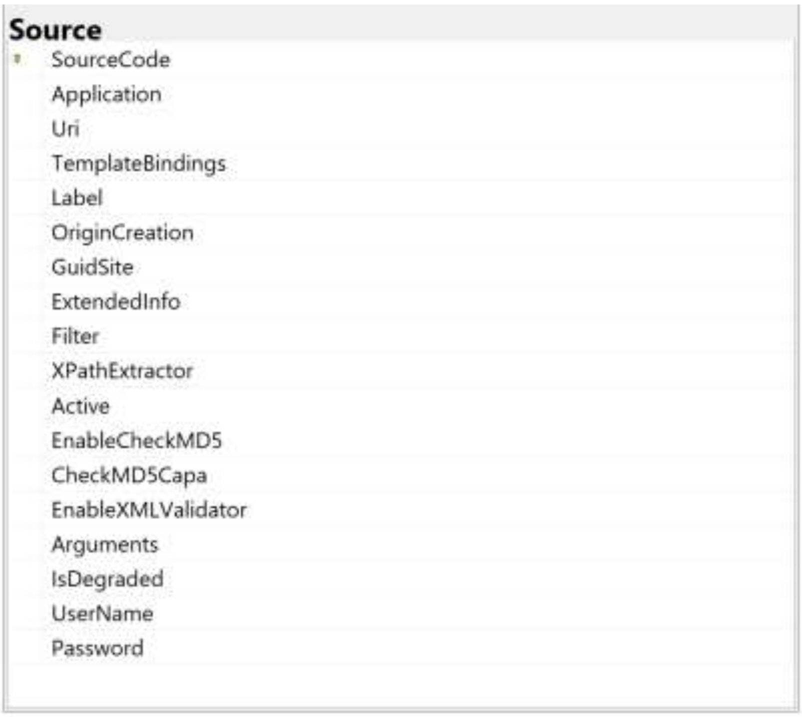


DomainTypes
DomainTypeId
DomainTypeDescription
UpdatedDate
UpdatedUser

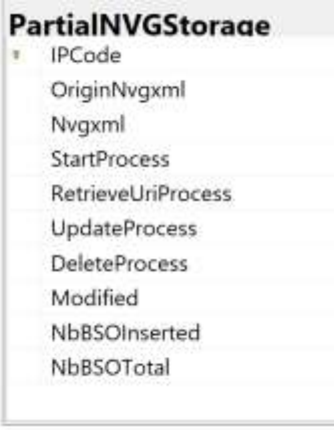


SiteRefUrls
GuidSite
TypeURL
URL
SiteName
Description
LastUpdated

P

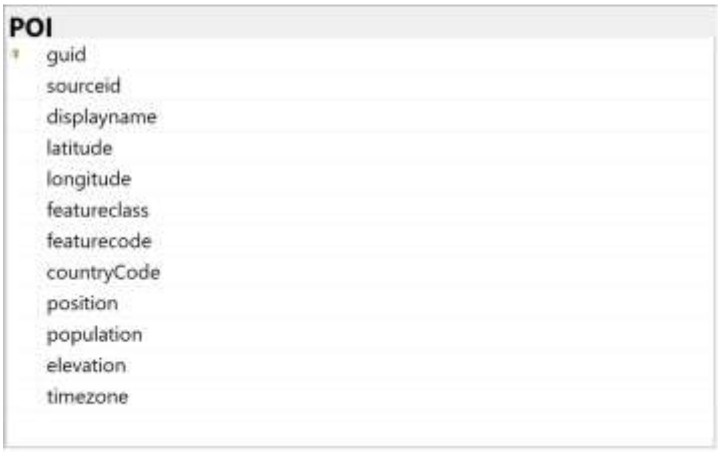


Source
SourceCode
Application
Uri
TemplateBindings
Label
OriginCreation
GuidSite
ExtendedInfo
Filter
XPathExtractor
Active
EnableCheckMD5
CheckMD5Capa
EnableXMLValidator
Arguments
IsDegraded
UserName
Password



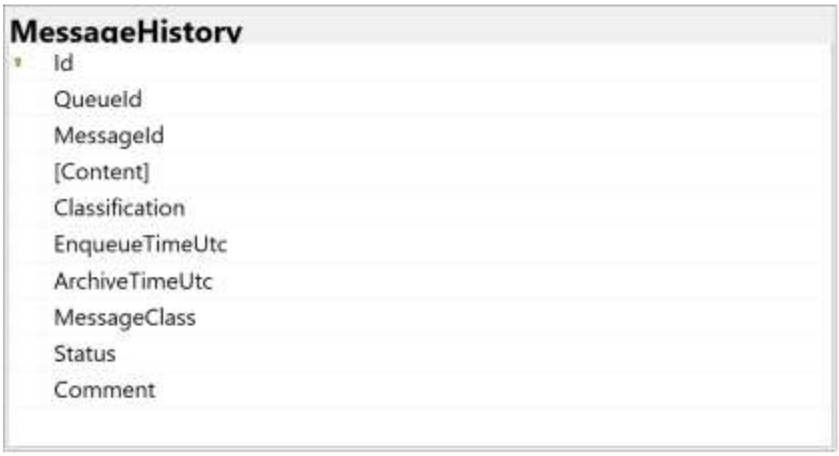
PartialNVGStorage
IPCode
OriginNvgxml
Nvgxml
StartProcess
RetrieveUriProcess
UpdateProcess
DeleteProcess
Modified
NbBSOInserted
NbBSOTotal

M.1.1.2 Nato.Ncop.OperationalGazeterDb **tables**

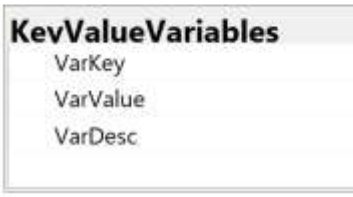


POI
guid
sourceid
displayname
latitude
longitude
featureclass
featurecode
countryCode
position
population
elevation
timezone

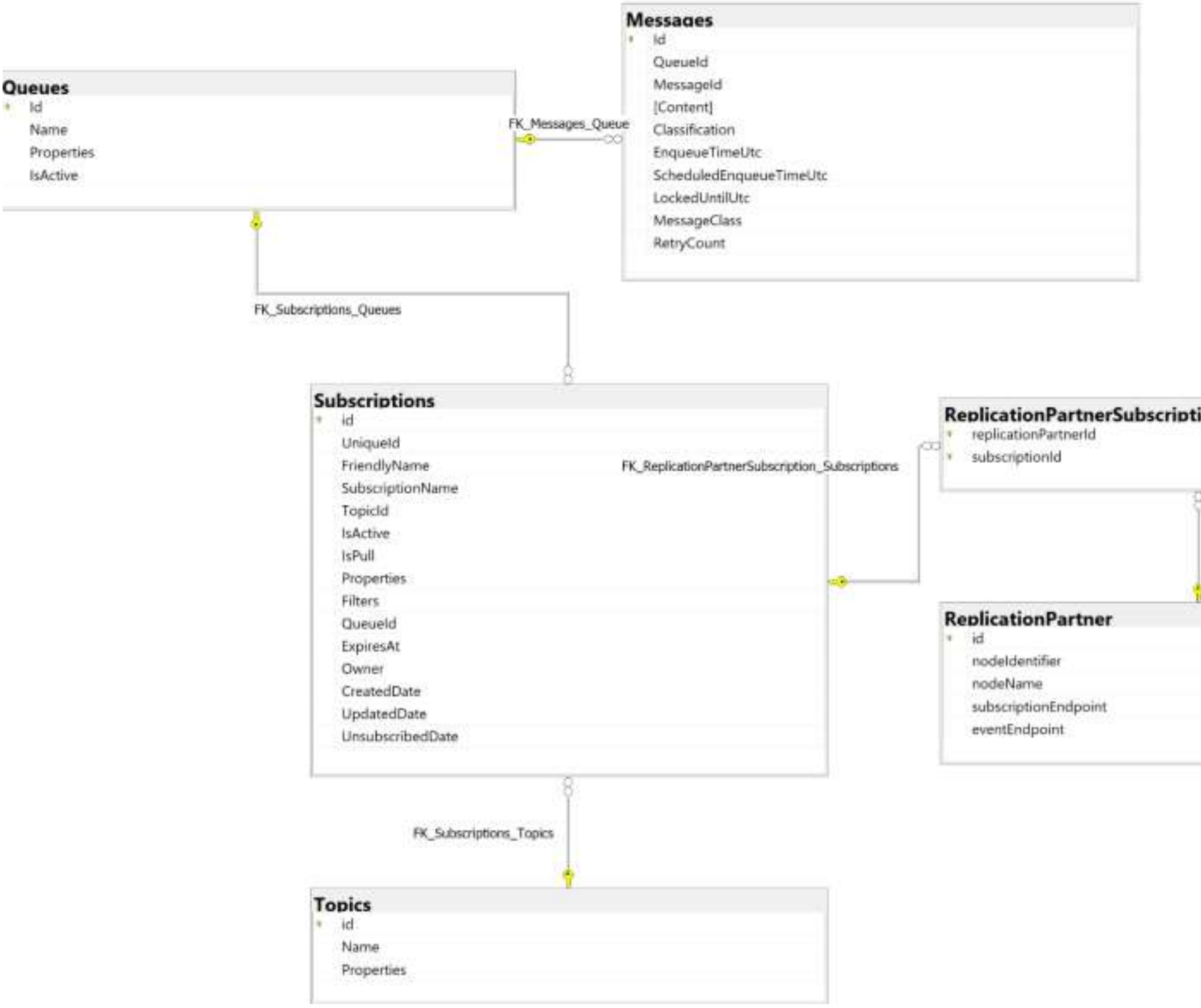
M.1.1.3 Nato.Ncop OperationalSync.Db **tables**



MessageHistory
Id
QueueId
MessageId
[Content]
Classification
EnqueueTimeUtc
ArchiveTimeUtc
MessageClass
Status
Comment



KeyValueVariables
VarKey
VarValue
VarDesc



Messages
Id
QueueId
MessageId
[Content]
Classification
EnqueueTimeUtc
ScheduledEnqueueTimeUtc
LockedUntilUtc
MessageClass
RetryCount

Queues
Id
Name
Properties
IsActive

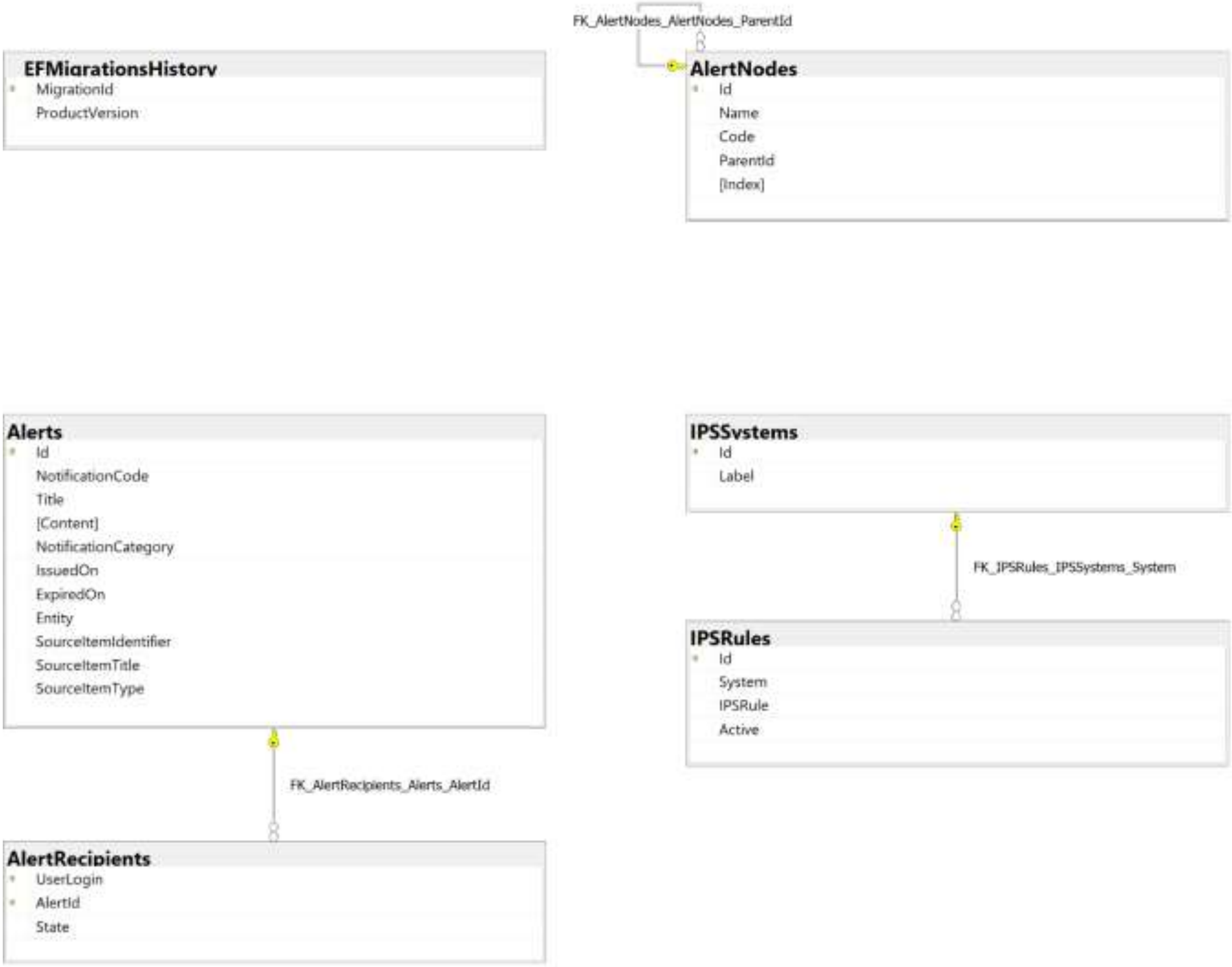
Subscriptions
id
UniqueId
FriendlyName
SubscriptionName
TopicId
IsActive
IsPull
Properties
Filters
QueueId
ExpiresAt
Owner
CreatedDate
UpdatedDate
UnsubscribedDate

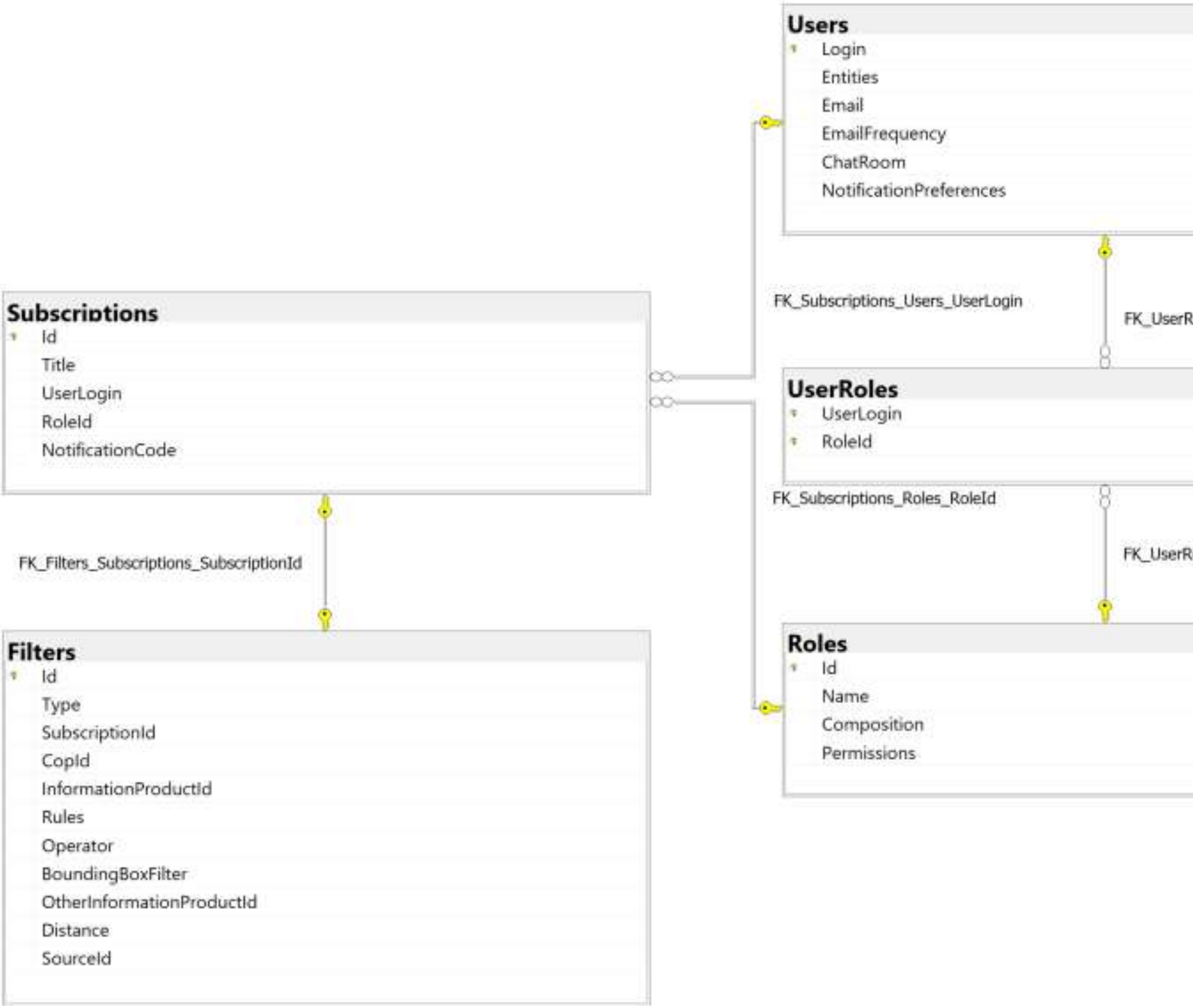
ReplicationPartnerSubscripti
replicationPartnerId
subscriptionId

ReplicationPartner
id
nodeIdentifier
nodeName
subscriptionEndpoint
eventEndpoint

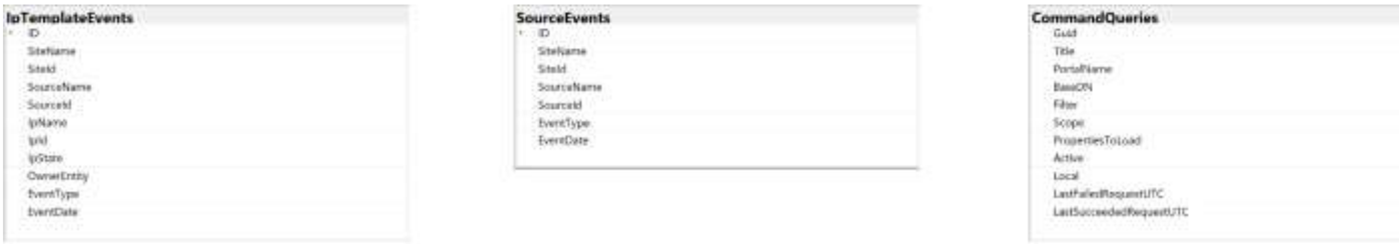
Topics
id
Name
Properties

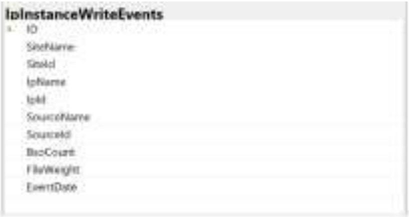
M.1.1.4 Nato.Ncop Operational.UserManagementDb **tables**



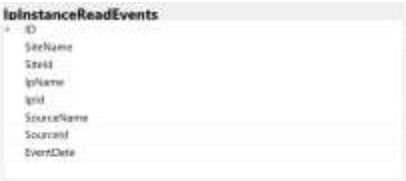


M.1.1.5 Nato.NCOP.BAMDb **tables**

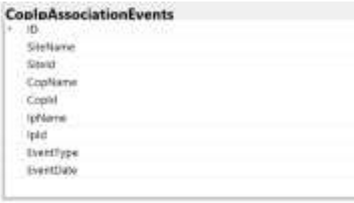




IpInstanceWriteEvents
ID
SiteName
SiteId
IpName
IpId
SourceName
SourceId
BsoCount
FileWeight
EventDate



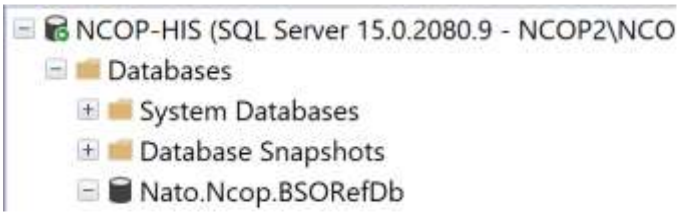
IpInstanceReadEvents
ID
SiteName
SiteId
IpName
IpId
SourceName
SourceId
EventDate



CopIpAssociationEvents
ID
SiteName
SiteId
CopName
CopId
IpName
IpId
EventType
EventDate

M.2 HIS SQL INSTANCE

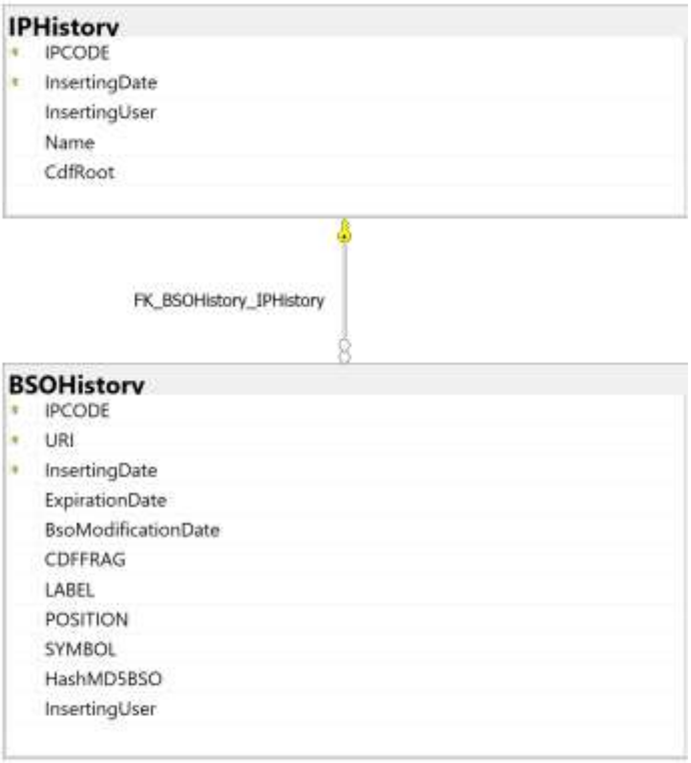
The figure below show the database of the NCOP History SQL instance:



NCOP-HIS (SQL Server 15.0.2080.9 - NCOP2\NCO
Databases
System Databases
Database Snapshots
Nato.Ncop.BSORefDb

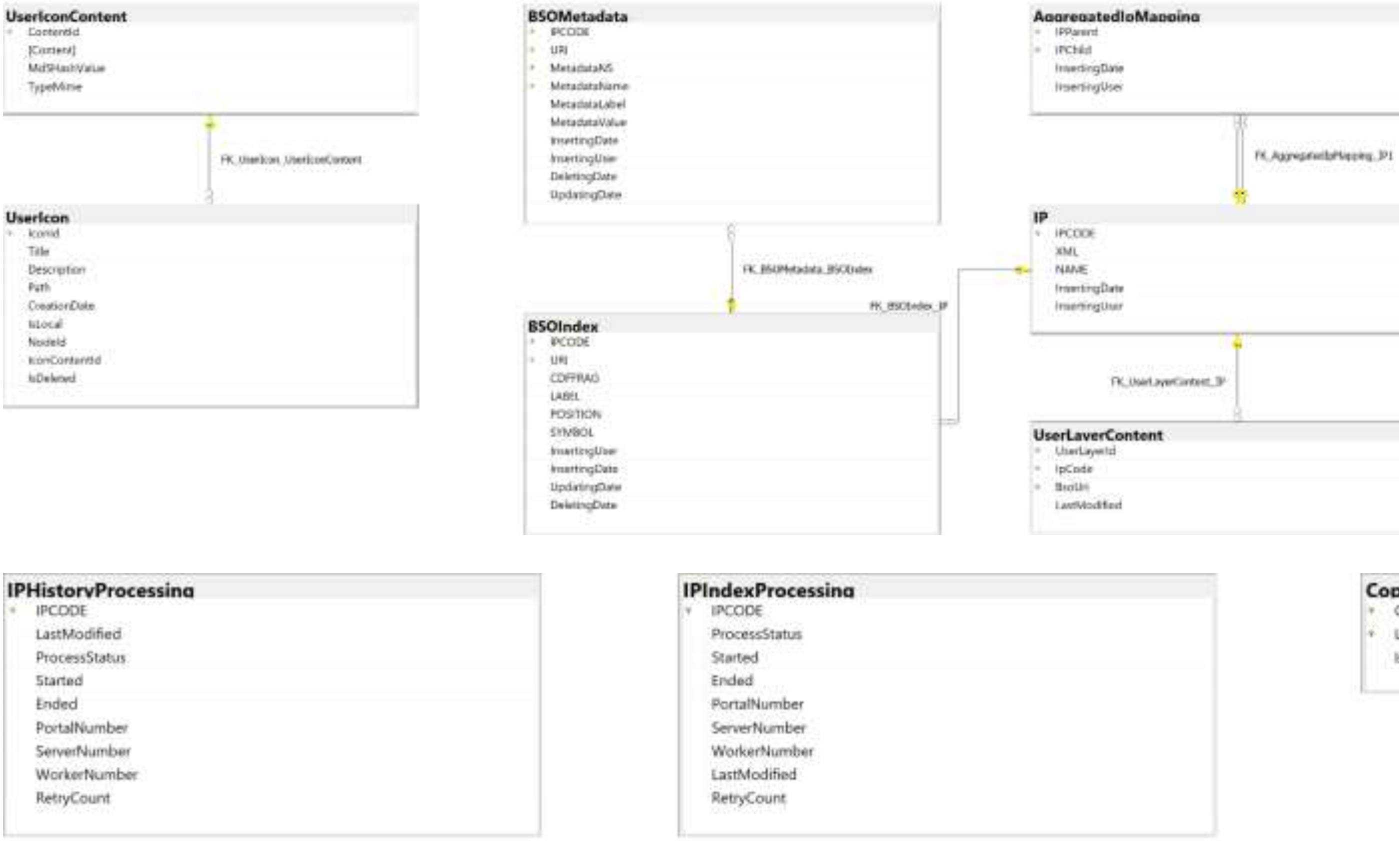
Figure 7-44: NCOP History SQL instance database

M.2.1.1 Nato.Ncop.BSORefDb **tables**



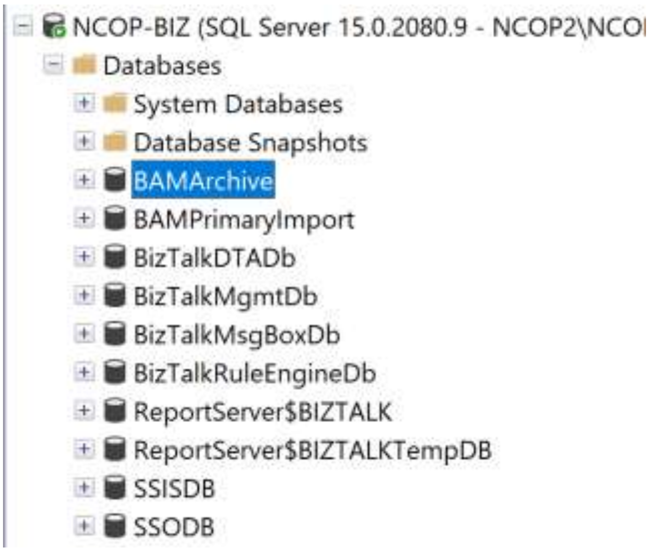
IPHistory
IPCODE
InsertingDate
InsertingUser
Name
CdfRoot

BSOHistory
IPCODE
URI
InsertingDate
ExpirationDate
BsoModificationDate
CDFFRAG
LABEL
POSITION
SYMBOL
HashMD5BSO
InsertingUser



M.3 BIZ SQL INSTANCE

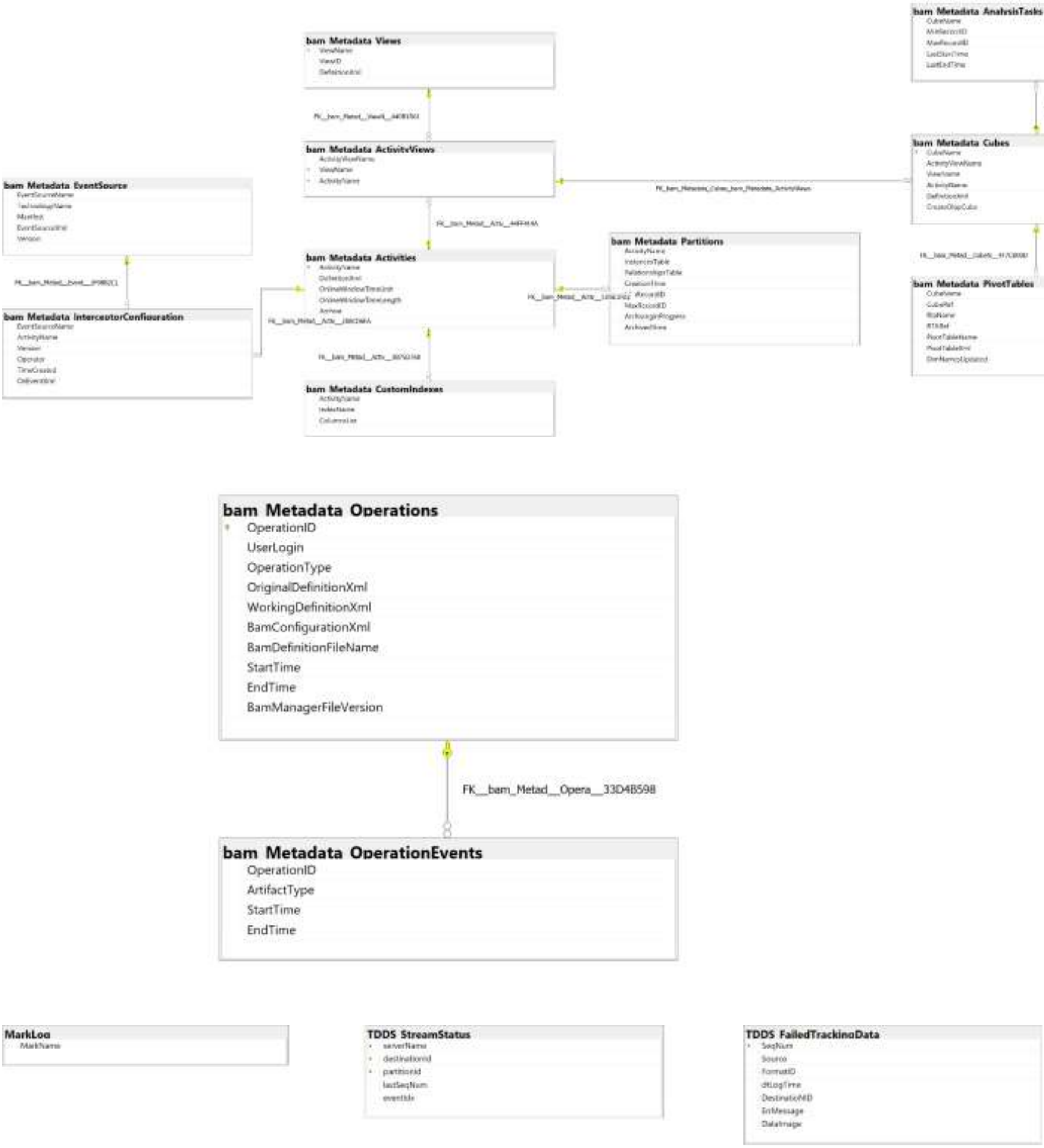
The figure below show the databases of the NCOP BizTalk SQL instance:

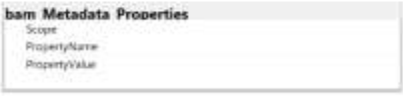


NCOP-BIZ (SQL Server 15.0.2080.9 - NCOP2\NCO
Databases
System Databases
Database Snapshots
BAMArchive
BAMPrimaryImport
BizTalkDTADb
BizTalkMgmtDb
BizTalkMsgBoxDb
BizTalkRuleEngineDb
ReportServer$BIZTALK
ReportServer$BIZTALKTempDB
SSISDB
SSODB

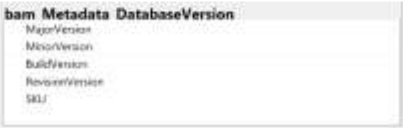
Figure 7-45: NCOP BizTalk SQL instance databases

M.3.1.1 BAMPrimaryImport tables

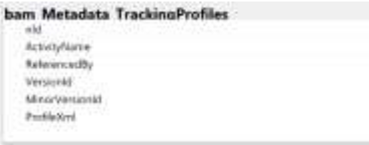




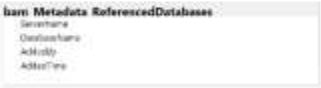
bam Metadata Properties
Scope
PropertyName
PropertyValue



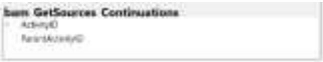
bam Metadata DatabaseVersion
MajorVersion
MinorVersion
BuildVersion
RevisionVersion
SKU



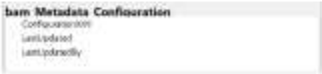
bam Metadata TrackingProfiles
nId
ActivityName
ReferencedBy
VersionId
MinorVersionId
ProfileXml



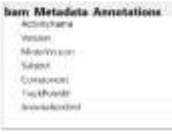
bam Metadata ReferencedDatabases
ServerName
DatabaseName
ActivityId
AddedTime



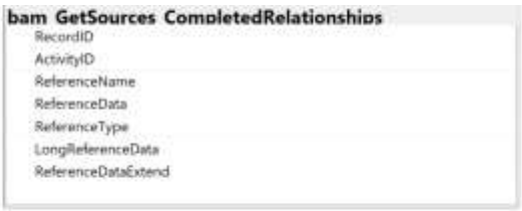
bam GetSources Continuations
ActivityID
ParentActivityID



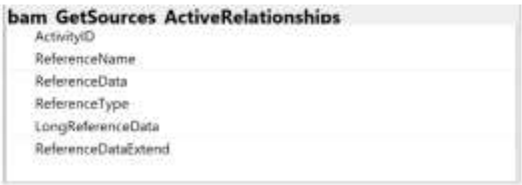
bam Metadata Configuration
ConfigurationXml
LastUpdated
LastUpdatedBy



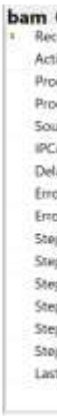
bam Metadata Annotations
ActivityName
Version
MinorVersion
Subject
ContextId
TrackPointId
AnnotationXml



bam GetSources CompletedRelationships
RecordID
ActivityID
ReferenceName
ReferenceData
ReferenceType
LongReferenceData
ReferenceDataExtend

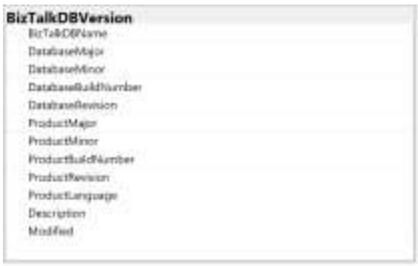


bam GetSources ActiveRelationships
ActivityID
ReferenceName
ReferenceData
ReferenceType
LongReferenceData
ReferenceDataExtend

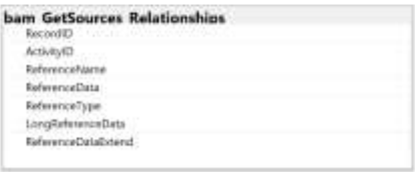


bam (
Rec
Acti
Pro
Pro
Sou
IPC
Del
Erro
Erro
Ste
Ste
Ste
Ste
Ste
Sto
Las

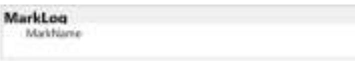
M.3.1.2 BAMArchive tables



BizTalkDBVersion
BizTalkDBName
DatabaseMajor
DatabaseMinor
DatabaseBuildNumber
DatabaseRevision
ProductMajor
ProductMinor
ProductBuildNumber
ProductRevision
ProductLanguage
Description
Modified



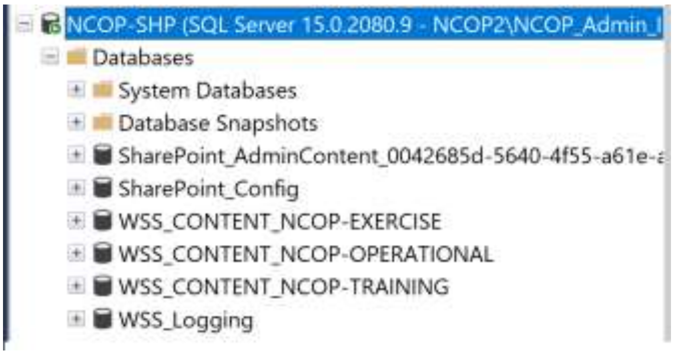
bam GetSources Relationships
RecordID
ActivityID
ReferenceName
ReferenceData
ReferenceType
LongReferenceData
ReferenceDataExtend



MarkLog
MarkName

M.4 SHP SQL INSTANCE

The figure below show the databases of the NCOP SharePoint SQL instance:



```
NCOP-SHP (SQL Server 15.0.2080.9 - NCOP2\NCOP_Admin_
  Databases
    System Databases
    Database Snapshots
    SharePoint_AdminContent_0042685d-5640-4f55-a61e-
    SharePoint_Config
    WSS_CONTENT_NCOP-EXERCISE
    WSS_CONTENT_NCOP-OPERATIONAL
    WSS_CONTENT_NCOP-TRAINING
    WSS_Logging
```

Figure 7-46: NCOP SharePoint SQL instance databases