validated, the NCOP History service returned the query result as an additional layer in the Geographical COP Editor. This layer provided the user with the successive “versions” of the selected BSOs with all properties values captured during each BSO update and with the BSO path for the selected period.

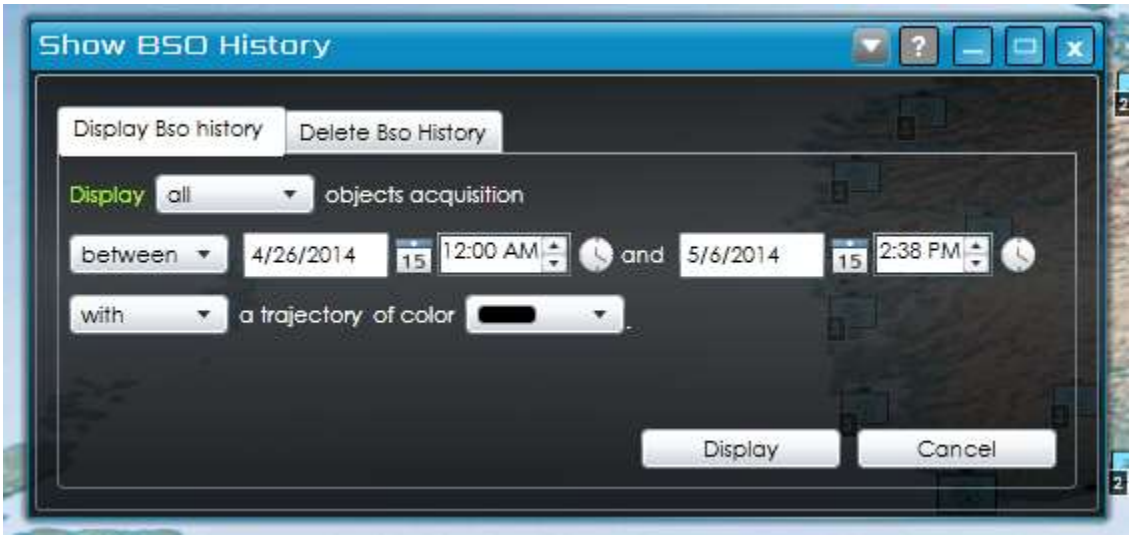


Figure 5-62: BSO history options

When the user validated his query, the Geographical COP Editor invoked the NCOP History service that will returned the information accordingly. This information was displayed as an additional layer in the Geographical COP Editor. This layer contained the successive “versions” of the BSO for which all properties values have been captured at each BSO update. The user was then able to visualize these properties as well as the path taken by the BSO during the selected period.

Figure 5-63: BSO history path display

Users having the appropriate permissions were allowed to delete the history of a specific BSO. This was done a second tab of the same BSO history visualization UI

(the tab appears only if the user is authorized to perform the action). The user had to select the timeframe for which he wanted to delete the BSO history:

Figure 5-64: BSO history deletion form

In NCOP Increment-2, the BSO history visualization UI and the path will be enhanced:

- When a path is displayed on the map, an automatic refresh of the path will be performed, each time a new update for a BSO matches the time parameters;
- The discrete BSO will be not displayed several times along the path. Its symbol will be displayed only on the last location;

5.3.2.1.3.3 Compare versions

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.

As already mentioned, each Information Product instance is stored as a CDF file in a SharePoint Document Library configured to store up to 100 versions of each CDF. These historicized CDF can be used and displayed with the “Compare versions” Panel.

As illustrated below, it displays all the previous versions of the selected Information Product.

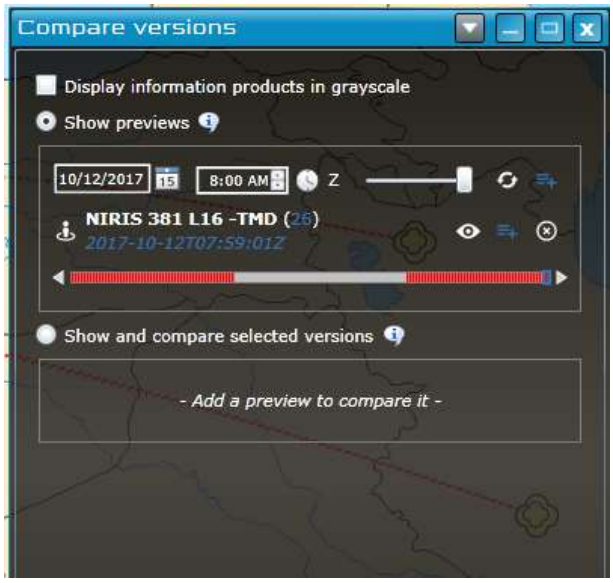


Figure 5-65: “Compare versions” panel

We can compare and monitor the selected old versions of the Information Products.

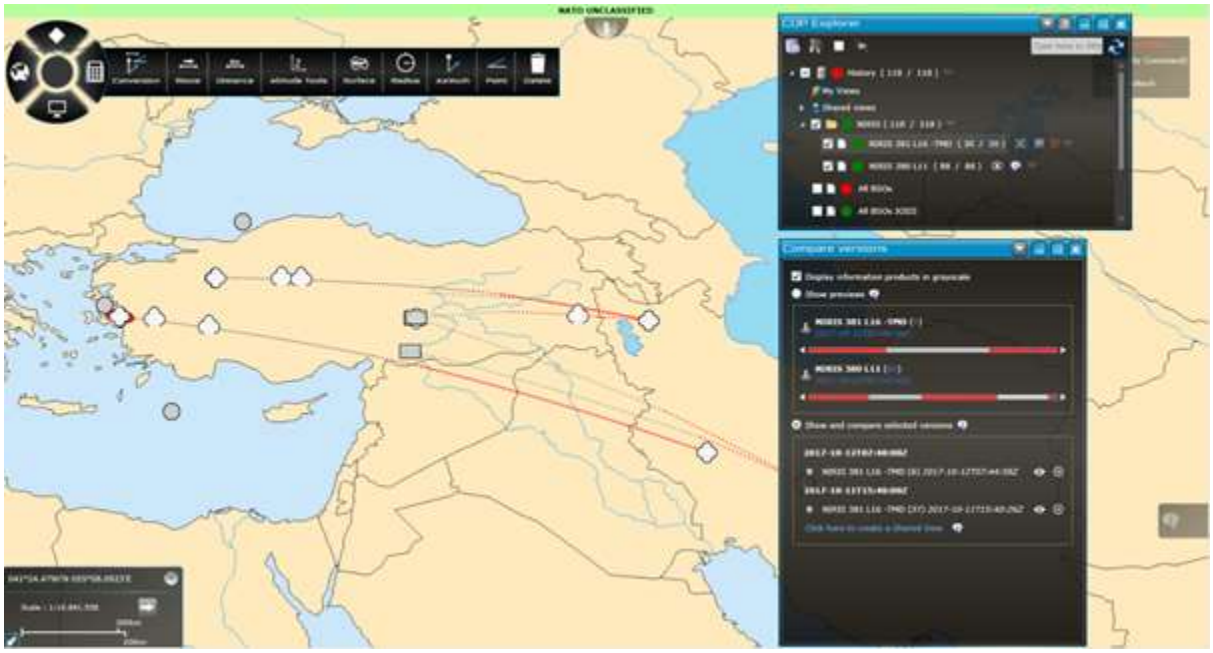


Figure 5-66: “Compare versions” applied to BSO rendering on the map background

The old versions of Information Products that have been selected can be used to create a new Shared View as shown below:

Figure 5-67: Display of 3 old versions (grayscale) and the current (colorized) of an Information Product

Figure 5-68: Shared Views based on old versions of Information Products

Finally these shared views, as any other shared view, can be added in a briefing (public or private).

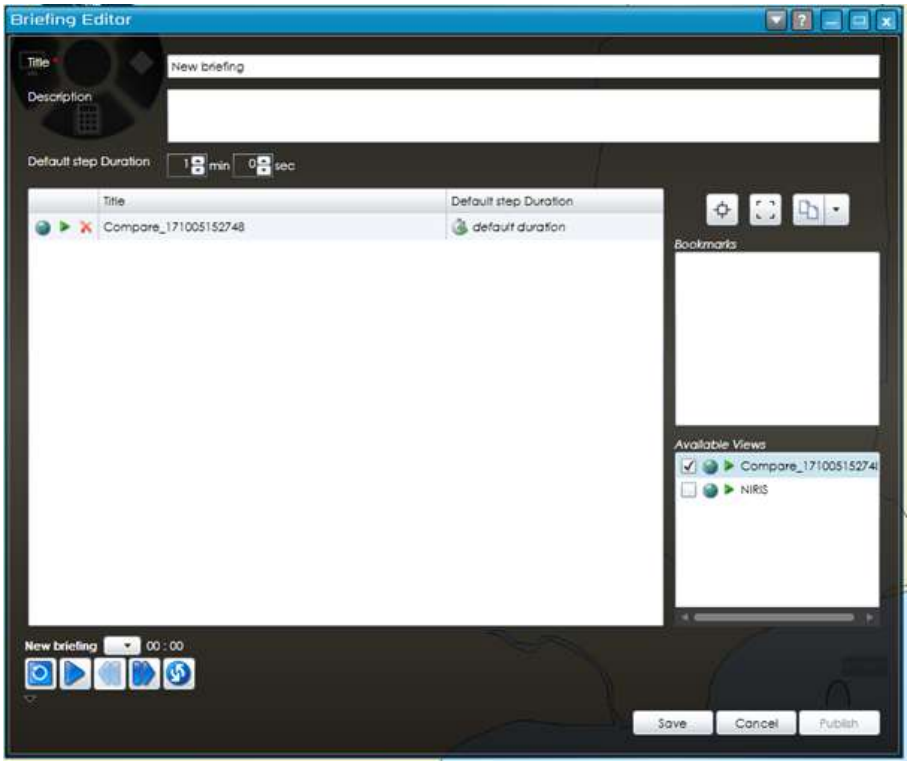


Figure 5-69: Compare_... Shared View in a briefing

5.3.2.2 COP Administration

5.3.2.2.1 COP Manager

Property Name	Description
Identification	COP Manager
Classification	IS
Behaviour	The COP Manager is a set of Web User Interfaces allowing to create and maintain a COP: It allows the COP Manager role to: save a COP as a template for defining new COPs; provide for selecting and loading a COP template for the establishment of a new COP; maintain COP definitions; transfer ownership of a COP from one Entity to another Entity with the associated transfer of privileges for maintaining the COP and all management information for that particular COP; archive a COP and retrieve an archived COP; copy a COP with all associated definitions; delete a COP.
Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved

Property Name	Description
Location (Types)	Installed on the Application Server Installed on the SharePoint Server
Interfaces	This IC interacts with back-end through the Geographical COP Editor Services REST API
Collaboration mechanism	https
Local/Configuration data	-
Operating context	TypeScript/JavaScript .NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Difficult

5.3.2.2.1.1 COP definition

The definition of a COP is performed using a dedicated web UI integrated in the Geographical COP Editor. It is only available to authorized users (‘Design COP’ permission). This UI allows the authorized user to browse, create, edit, delete and copy COPs. It is also possible to change the ownership of a COP by designating the new owner entity.

Depending on the user permissions and entity, it is possible that some functions be not accessible. For example it is not possible to modify or delete a COP that is owned by another entity.

When editing a COP the following properties can be set:

- Name
- Security classification
- Description
- Owner entity
- COP structure and content

A COP structure groups COP Information Products, COP maps, and links to other COP structures. Chapter 5.3.2.2.2 presents in more details the COP Structure Manager Implementation component dedicated to the management of COP structures.

5.3.2.2.1.2 COP-level BSO size rules

In addition to the definition of the basic COP properties, the COP Manager Implementation component allows the authorized user to define default visualization settings for the COP Information Products by defining BSO size rules. These rules will be applied by default when a COP Information Product is loaded in the Geographical OP Editor by a COP consumer. BSO size COP settings are not applied if the

Information Product has specific BSO size rules defined at the Information Product level.

The following figure presents the UI for creating BSO size rules at when editing a COP:

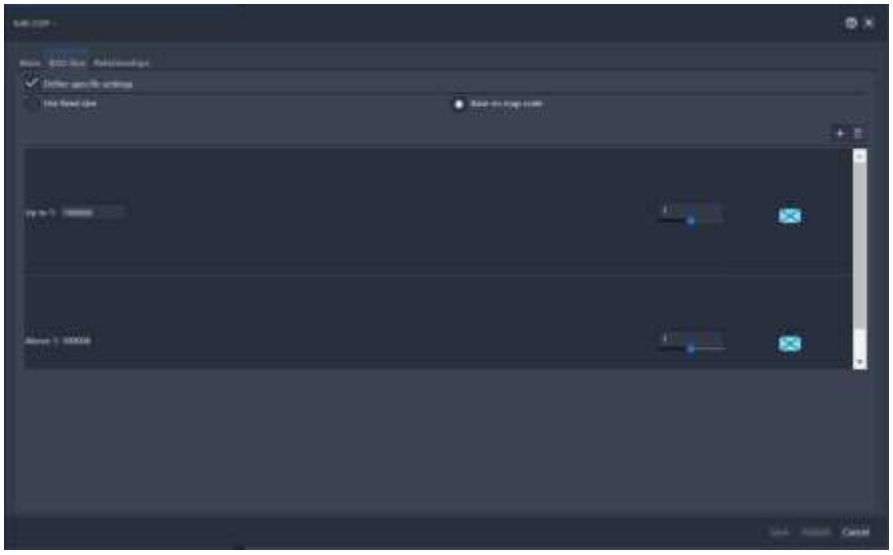


Figure 5-70: BSO size rules definition at the COP level

5.3.2.2.1.3 COP Archive management

COP archives are used to take a snapshot of a COP and all associated information elements. An archive can be reused locally to restore a previous configuration state for a COP and all associated elements (Information Products, Sources, etc.).

An archive can also be used on another NCOP node in order to quickly create a COP and all required items. In this scenario, since Sources and Information Products elements are created on a different node, it is possible that their configuration retrieved from the archive be no compliant with the node environment: for example, some sources may be unavailable or unreachable. In this case, the sources and information may require a manual adaptation (sources endpoints and credentials, and Information Product query configuration) or may need to be de-activated to avoid unnecessary acquisition errors. In any case, Information Products are restored with their data and then still allow the consumption of the COP.

The COP archive capability is available to authorized users as a web UI in the NCOP web a portal. It is available as a SharePoint custom action for each COP item in the COP list.

When a COP archive is created, the following elements are exported:

- COP
    - Definition
    - COP structure
    - IP substitution rules
- COP Information Products

    - Definition
    - CDF data
    - Original data
    - Annotations
- Sources
- Shared Views
    - Definition
    - Annotations

Regarding Information Products, the archive contains all successive versions that have been acquired (100 versions by default, can be changed by a SharePoint administrator). Both original and CDF format are exported for each version of the Information Product.

The result of the archiving process is a zip file containing all exported elements. In order to ensure data integrity, the archive contains a signature that can be used to detect any manual change in the COP archive.

The following figure presents the structure of a COP archive file.

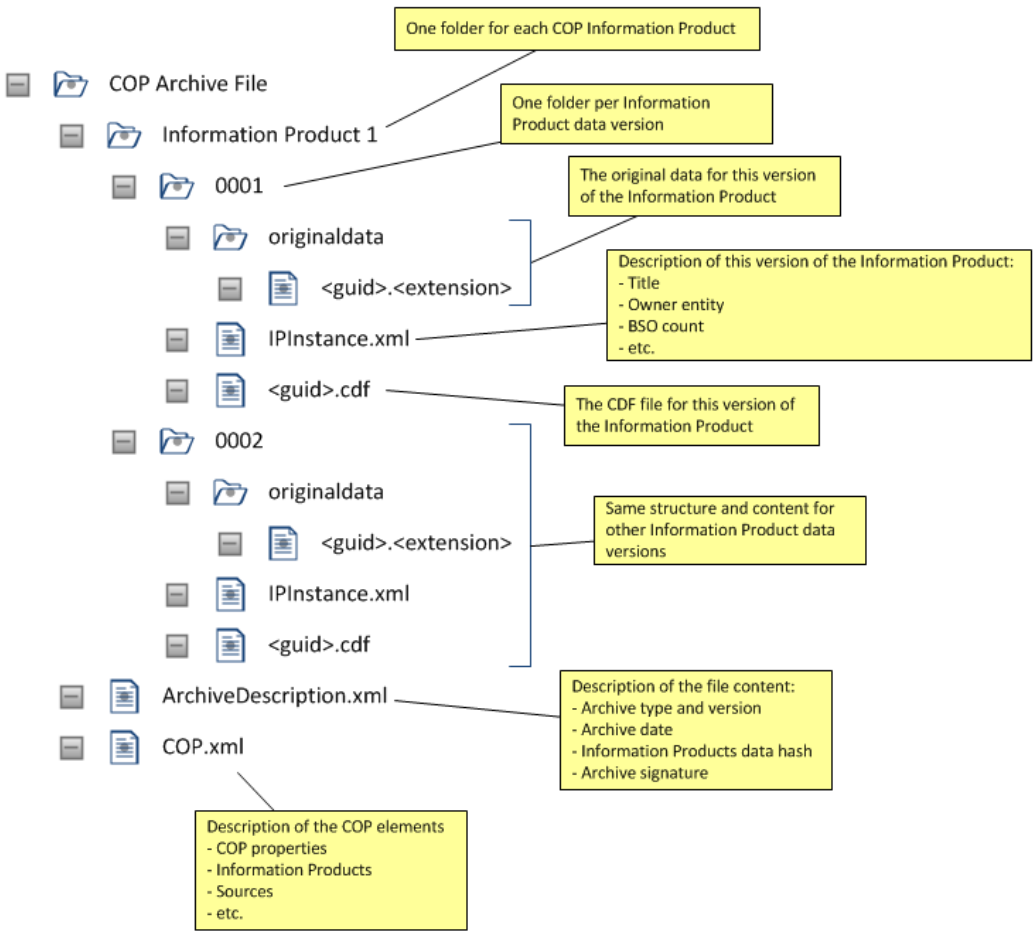


Figure 5-71: COP Archive file content description

The COP restore capability is also available in the NCOP web portal. It allows the COP manager to upload COP archive and restore its content in the NCOP storage. The following restore options are available:

- Generate new identifiers

  If no new identifiers are used, the restore process will potentially overwrite the contents of the corresponding item. This option is activated by default.

- Change owner entity

  Depending on where the archive has been created and where it is restored, it may be necessary to change the owner entity of restored elements if the COP Manager wants to be able to manage them after they are restored.

5.3.2.2.1.4 COP Templates management

The COP Templates feature is similar to the COP Archive feature. The difference is that when creating the COP template, Information Product data are not exported, neither are Source endpoints. Also when creating a COP from a template, the manager will be asked to define how sources will be restored. The manager can choose to:

- Create a new source with the same parameters as in the template
- Reuse an existing source (even if not of the same type)

If a new source is created, a manual adaptation is required to define the correct endpoint and credentials if required.

Information Products configuration may also need to be adapted, especially if a source with a different type has been reused. In this case, the configuration used to query the original source can be displayed and used as guidelines for defining a similar configuration in a format that is compliant with the reused source.

The ‘save a COP as a template’ option is available in the NCOP web portal.

The result of this action is a zip file with a structure similar to a COP archive structure but without the information product data (CDF and original). The following figure presents the structure of a COP Template file:

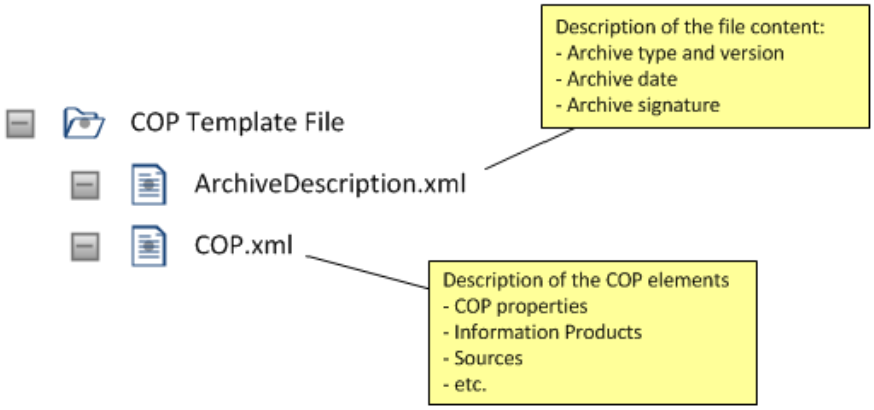


Figure 5-72: COP Template file content description

To create a COP from a template, the COP restore module is used, but during the restore process, a manual interaction is required to select the option regarding each source. Note that NCOP offers the capability to create a COP from a COP Archive file with the same options as creating a COP from a COP Template file: “Activate Source after creation ?” and “Activate Information Product after Creation ?”

Figure 5-73: COP restore options: “Restore/Import from Archive” or “Create COP from template”

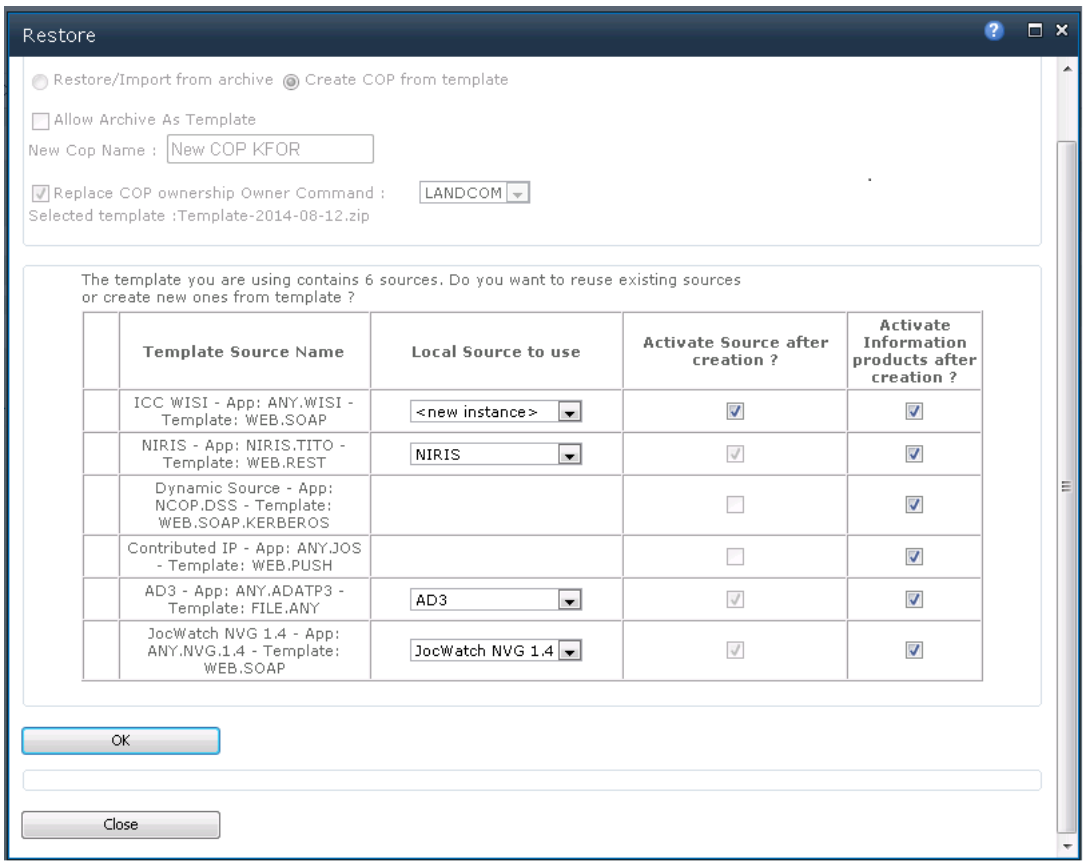


Figure 5-74: “Create COP from template” option is selected: manual source selection is required

5.3.2.2.2 COP Structure Manager

Property Name	Description
Identification	COP Structure Manager
Classification	IS
Behaviour	The COP Structure Manager is a Web User Interface allowing COP Manager role and COP Manager Assistant role to create and maintain structure for each instance of a Common Operational Picture (termed COP Structures). COP Structure defined by a name, a description and a version, is displayed as a TreeView composed of nodes and sub items containing: Link to COP Information Products (Name, Security classification and update status of Information Product are displayed) Link to COP maps; Link to COP Shared Views; Link to another COP Structure.
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 Application Server

Property Name	Description
Interfaces	This IC interacts with back-end through the Geographical COP Editor Services REST API
Collaboration mechanism	https
Local/Configuration data	-
Operating context	TypeScript/JavaScript .NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

The following UML Use Case Diagram shows the main responsibilities of the COP Manager Assistant role.

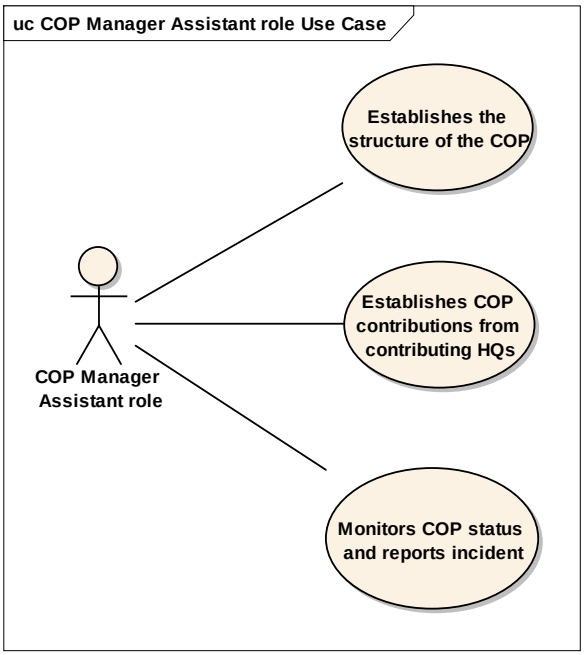


Figure 5-75: UML Use Case Diagram of COP Manager Assistant role

5.3.2.2.2.1 COP Structure basics

The UI allows the manager to perform basic operations when defining the COP structure. This UI is made 2 main panels. On the left presents the target COP structures and allows the COP Manager to design the structure by adding and organizing folders. On the right is a set of sub-panels proposing elements to be included in the COP structure:

Element	Comment
Structure template	Structure models that can be reused (fully or partially) as a basis for a new COP structure
Information Products	

➢ CDF Information Product	Based on the acquisition and conversion of data provided from Sources
➢ WMS Information Product	Based on a selection of Map Layers exposed by a WMS Map Services
➢ KML Information Product	Based on a KML file exposed by a web server
Link to other COP structure	A selection of a structure as exposed by another COP. The structure content will be resolved dynamically when consuming the COP.

This UI mainly uses the drag and drop principle to move elements from one panel to another.

The following picture presents the COP edition panel allowing the COP Manager and COP Manager Assistant to design the COP Structure:

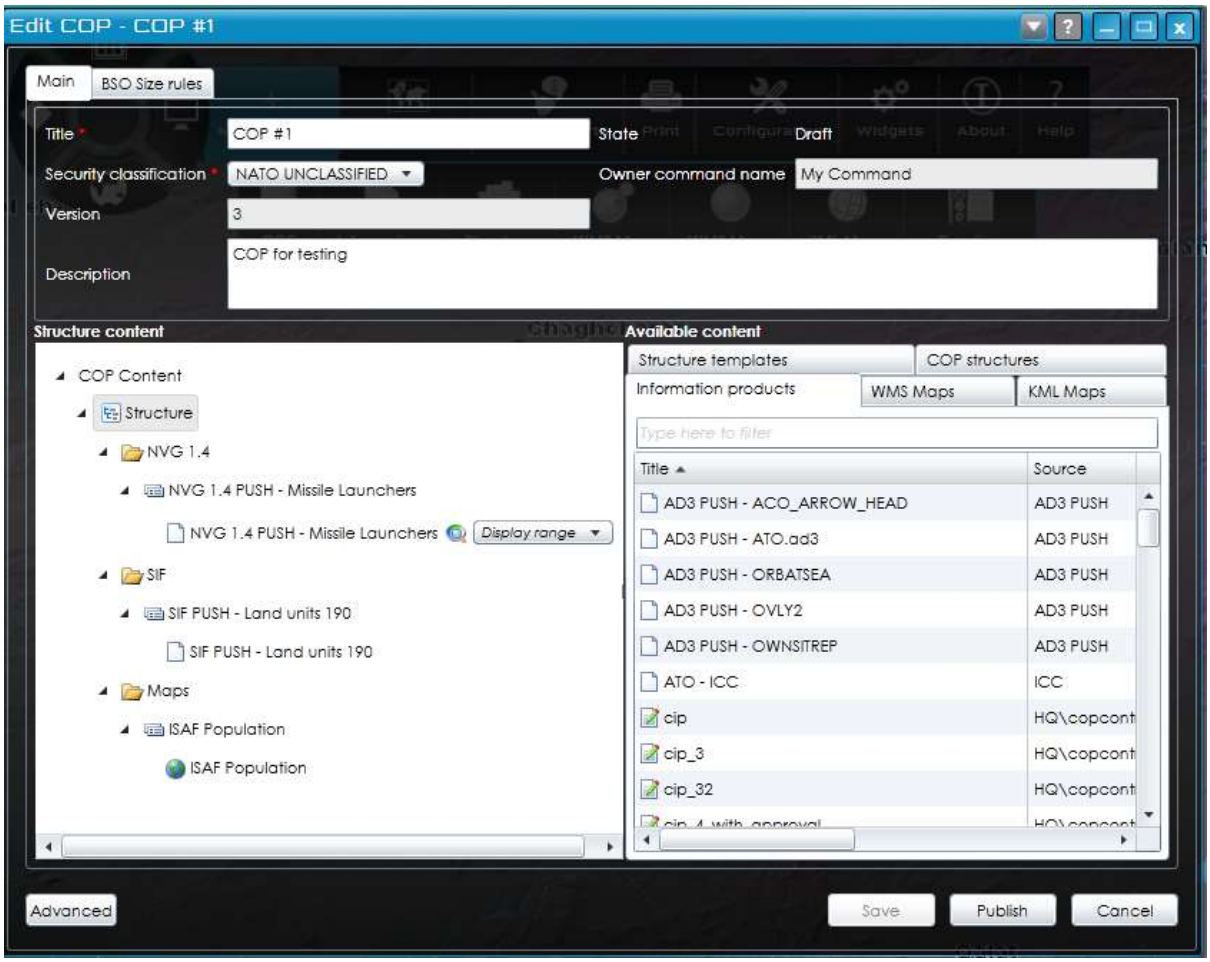


Figure 5-76: “COP Edition” Information Panel allowing COP Structures design

5.3.2.2.2.2 Pre-defined visualization filter

If a visualization filter has been defined for an Information Product, the COP Manager is allowed to use it as the default visualization mode for an Information Product: When adding an Information Product, the COP Manager is able to select from a drop down list the visualization filter to be used by default. As a result, when the COP consumers

will load the layer from the COP Explorer, the Information Product will automatically be loaded with the visualization defined by the COP Manager.

The following figure presents the visualization filter selection graphical control integrated in the COP structure edition panel:

Figure 5-77: Selection of predefined COP Information Product visualization filter

5.3.2.2.2.3 Information Product and Source substitution

NCOP proposes a feature that allows a COP Manager to replace automatically an Information Product with another based on business rules.

The typical use cases of this feature are:

- Replacing an Information Product with a more relevant data (may be required when a COP is synchronized across multiple NCOP nodes that have access to different sources that expose the same kind of information)
- Replacing an Information Product because of an acquisition problem

The substitution of an Information Product is always made in the context of a COP: it won't be applied in all COPs where the Information Product is used.

NCOP offers the following flexibility for the usage of this feature:

- Trigger selection:

  It is possible to select the event that will trigger the substitution: the substitution can be permanent or dependant of the status of the primary Information Product

- No constraint on Information Product origin or type:

  It is possible to replace an Information Product by another that is not produced by the same source. It is even possible to replace an Information Product by another that is of a different type. For example, it is possible to replace a dynamic NIRIS Information Product by a WMS Geographical Information Product.

- Substitution rule activation:

  It is possible for an authorized user to enable or disable a substitution rule. This activation/de-activation only impacts the local NCOP node.

- Synchronization of substitution rules:

  When a COP is synchronized, the associated substitution rules can be synchronized. It will be possible on the client to disable/enable the substitution rule locally or to replace it with a local substitution rule.

- Synchronization impact:

  If the primary Information Product is present on a node because of a synchronisation, it is possible to avoid the synchronization of the data updates of this Information Product if a substitution is declared.

An advanced web UI in the COP structure management panel allows the definition of rules to be used. It is presented in the figure below:

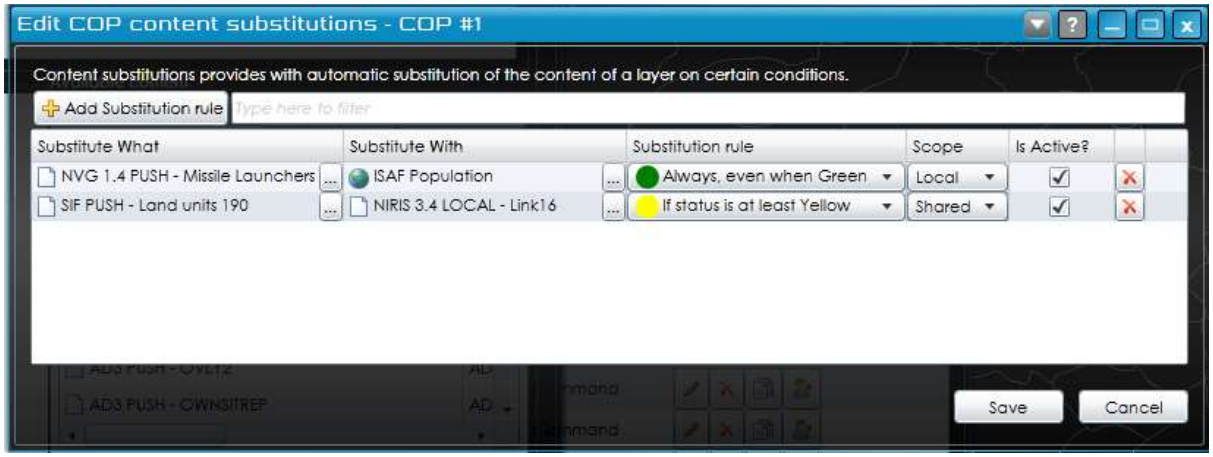


Figure 5-78: Information Product substitution rules edition panel

The substitution rules are stored using an XML representation in a dedicated SharePoint list in the NCOP storage. An Information Product substitution rule is not stored as a property of the COP:

- when substitution rules are created, deleted or modified, the COP item itself is not impacted (no version update)
- in a synchronization context, COP Managers on a client must be able to edit substitution rules for a COP they don't own

These rules are processed automatically at runtime by the NCOP IPS that will modify the reference of the underlying data when exposing the COP structure, in order to expose the appropriate Information Product properties instead of those of the primary Information Product.

The following figure presents a typical use case demonstrating the use and impacts of Information Product substitution rules on a three-node scenario:

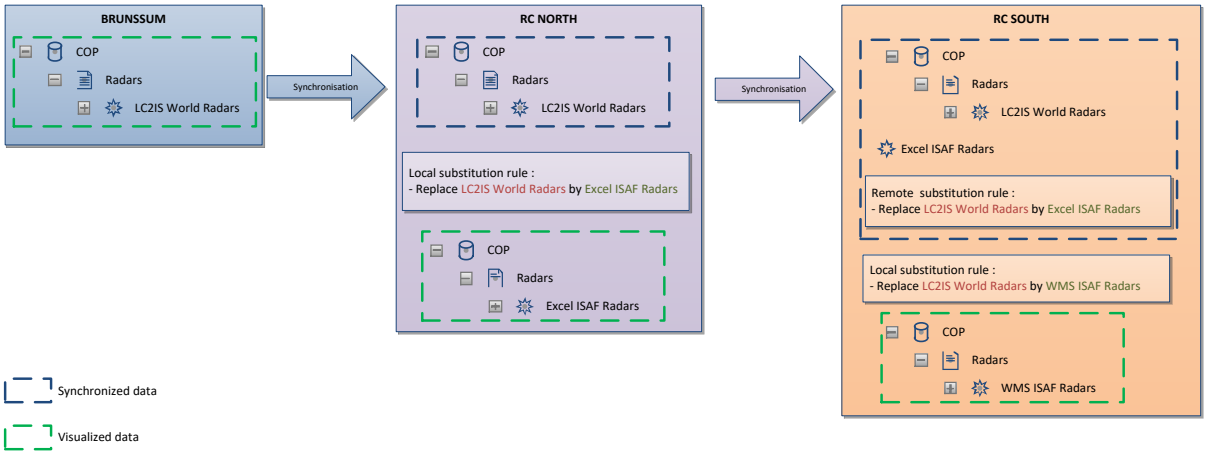


Figure 5-79: Information Product substitution use case scenario

On the Brunssum node, a COP is defined containing one ‘Radars’ layer for which the associated content is based on the contents of the ‘LC2IS World Radars’ Information Product.

On the RC North node, the COP is retrieved from Brunssum using synchronization. The COP is then visible with the same structure and the same content is supposed to be displayed. But locally a substitution rule is declared in order to replace the ‘LC2IS World Radars’ Information Product with the ‘Excel ISAF Radars’ Information Product. As a result, for the COP consumer, the COP has an unchanged structure but the data associated with the ‘Radars’ layer is the retrieved from the contents of the ‘Excel ISAF Radars’ Information Product.

On the RC South node, the COP is retrieved from RC north using synchronization. The original COP structure and content is synchronized. Because of the substitution rule declared on RC North, the Excel ISAF Radars Information Product is synchronized, and the substitution rule itself is also synchronized (but considered remote). As a result, the COP consumers on the RC south node would display the same data as on the RC North node. But locally on RC South, a substitution rule is declared to replace the ‘LC2IS World Radars’ Information Product with the ‘WMS ISAF Radars layer’. As a result, the COP consumers on the RC South can see the COP with an unchanged structure but the content of the ‘Radars’ layer is based on the ‘WMS ISAF Radars’ Information Product.

5.3.2.2.3 COP Shared View Manager

Property Name	Description
Identification	COP Shared View Manager
Classification	IS

Property Name	Description
Behaviour	The COP Shared View Manager is a Web User Interface allowing to create and maintain Views on a COP and submit them for inclusion in the COP as Shared Views. This component allows to define the following properties of a Named View: COP Information Products selected to be visible; Visualization Filter settings for visible COP Information Products; Level of Details used for COP Information Product; Geographic reference for displayed area; Geographical display scale factor; Geo data selected to be visible. After inclusion in a COP, the Named View promoted to Shared View has a new attribute: The COP it applies to.
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 Application Server
Interfaces	This IC interacts with back-end through the Geographical COP Editor Services REST API
Collaboration mechanism	https
Local/Configuration data	-
Operating context	TypeScript/JavaScript .NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

5.3.2.2.4 COP IP Manager

Property Name	Description
Identification	COP IP Manager
Classification	IS
Behaviour	The COP IP Manager is a Web User Interface allowing Organizational Node role or COP Manager role to create and maintain COP IP. The TreeView of the COP Structure can be used to browse and select a COP IP in order to: Update information of COP IP such as: o Manual setting of update status; o Forced refresh per COP IP in order to make the newest information available from the source;

Property Name	Description
	○ Manual setting of the Security Classification (overriding an existing Security Classification) Discard a COP IP when updates are missing or fails; Monitor COP IP properties such as: ○ Update status (OK/Green, Partially OK/Yellow, Almost KO/Orange, KO/Red); In addition, this Web User Interface allows: Discovering COP IP or Source capabilities that are available from COP source Entities, Presenting discovered Information Products in a list which can be ordered and filtered on one or more of the following criteria: ○ Originating system of the COP IP; ○ Information Product name; ○ Source or Source Entity. Monitoring the availability of new Information Product or evolving Source capabilities and use business rules and the Alerting Service to notify the COP Manager that an evolution has occurred in the Source Entity Combining and aggregating multiple COP IP
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 Application Server Installed on the SharePoint Server
Interfaces	This IC interacts with back-end through the Geographical COP Editor Services REST API
Collaboration mechanism	https
Local/Configuration data	-
Operating context	TypeScript/JavaScript .NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Difficult

5.3.2.2.4.1 Information Products attributes

The following table describes the physical model of the Information Product Parameter (invariant attributes after successive acquisitions of source Information Product content).

TABLE 5-3: COP IP PARAMETER PROPERTIES

Attribute name	Attribute display name	Attribute type	Attribute content	Set by
ID	ID	Counter		System
Title	Title	Text	Name of the Information Product	COP Manager
ncop_revision	Revision	Revision		System
ncop_ips_description	Description	Multiple lines of text	Description of the Information Product	COP Manager
ncop_ips_effectiveenddtg	Effective End DTG	DateTime	End date for data acquisition	COP Manager
ncop_ips_effectivestartdtg	Effective Start DTG	DateTime	Start date for data acquisition	COP Manager
ncop_ips_iptype	IP Type	Choice	Static Dynamic Technical	COP Manager
ncop_ips_maxscalevisibility	Max Scale Visibility	Text	Max geographic scale to allow the display of this Information Product on a map	COP Manager
ncop_ips_minscalevisibility	Min Scale Visibility	Text	Min geographic scale to allow the display of this Information Product on a map	COP Manager
ncop_ips_ownerentity	Owner Command	Text	Name of the Command	System
ncop_ips_purpose	Purpose	Text	Short text describing the purpose of this Information Product	COP Manager
ncop_ips_requiredupdatefrequency	Required Update Frequency	Integer	For pulled Ips : interval between 2 fetches For pushed Ips : theorical interval between 2 updates from the source	COP Manager
ncop_ips_sourcedconsumerentity	Sourced at Consumer Entity	Boolean	yes/no : indicates, if this Information Product is to be replicated, that the COP Manager of a replicated will be able to override the source of this Information Product to select a local one.	COP Manager
ncop_ips_updatemethod	Update Method	Text	Push or Pull, this option is linked to the source that provides the Information Product	COP Manager
ncop_ips_filter	Filter	Multiple lines of text (XML)	NVG source: (Optional: linked to the use of a NVG WebService compliant source.) Will hold the COP manager filter values to be applied when the	COP Manager

Attribute name	Attribute display name	Attribute type	Attribute content	Set by
			GetNvg method will be called. Other sources (SQL, WISI, AirC2IS …): Will hold the COP manager filter values to be applied when the IP Content acquisition method will be called	
ncop_ips_categorization	Categorization	Text	Categorization of the Information Product (Exercise, Simulated, Real, Training)	COP Manager
ncop_ips_domain	Domain	Text	Domain of the Information Product contents (air, land, medical, etc.)	COP Manager
ncop_ips_securityclassification	Security Classification	Lookup	Default Security classification to be set if the fetched Information Product contains no classification information	COP Manager
ncop_ips_source	Source	Lookup	reference to the associated source	COP Manager
ncop_ips_active	Active	Boolean	no indicates that the schedule of the acquisition of the Information Product is not effective	COP Manager
ncop_ips_statusdisplay	Status display	URL (Image)	Image showing the status of the information product (OK/Green, Partially OK/Yellow, Almost KO/Orange, KO/Red.)	BizTalk
ncop_guid	GUID	Text		System
ncop_ips_state	State	Choice	Draft Pending Published Used only for Contributed IP	System
ncop_ips_parentip	Parent IP	Text		System
ncop_ips_version	Version	Integer		System
ncop_ips_identificationpattern	Identification Pattern	Multiple lines of text (XML)	Identification Pattern for IP without Query. For example the Information Products that are based on file	COP Manager

Attribute name	Attribute display name	Attribute type	Attribute content	Set by
			deposit, the Identification Pattern contains the Filename.	
ncop_ips_historyduration	History Duration	Integer	BSO History Duration expressed in days	COP Manager
ncop_ips_poc	PoC	Text	Point of Contact Used only for Contributed IP	COP Contributor
ncop_ips_suggestediplocation	Suggested Ip Location	Multiple lines of text	Suggested Contributed IP Location in the COP structure Used only for Contributed IP	COP Contributor
ncop_ips_nextupdate	Next Update	DateTime		
ncop_ips_pincode	PIN Code	Text	PIN Code of the Contributed IP Used only for Contributed IP	COP Contributor
ncop_ips_format	Format	Choice	Usual Contributed Aggregate Document Worksheet Collaborative	System
ncop_ips_ipaggregated	IP Aggregated	Multiple lines of text	List of Guid of the Information Products that are aggregated. Used for aggregated Information Product only	COP Manager
ncop_ips_updatetype	Update Type	Choice	Partial Full	COP Manager
ncop_ips_statusrules	Status Rules	Multiple lines of text (XML)	Rules used to compute the status of the Information Product	COP Manager

Attribute name	Attribute display name	Attribute type	Attribute content	Set by
ncop_ips_automatictimestamping	Automatic time stamping	Boolean		COP Manager
ncop_ips_maintainer	Maintainer	Multiple lines of text	Maintainer/POC	COP Manager
ncop_ips_bsorelationrules	BSO Relation Rules	Multiple lines of text (XML)	BSO Relation Rules definition. Used for aggregated Information Product only	COP Manager
ncop_ips_ipref	IP Ref	Text	Reference to the GUID of the Technical IP instance. Used for dynamic IP only	System
ncop_ips_visualizationfilters	Visualization Filters	Multiple lines of text (XML)	Visualization Filter definition	COP Manager
ncop_ips_postprocessingscript	Post Processing Script	Multiple lines of text (XML)	Post-Processing definition	COP Manager
ncop_ips_bsosizerules	BSOs Size Rules	Multiple lines of text (XML)	BSO size rules	COP Manager
ncop_ips_areaofinterest	Area Of Interest	Multiple lines of text (XML)	Area of Interest used by the autofit when the Information Product is loaded and the user double click on the IP	COP Manager
ncop_ips_bsochartsdefinitions	BSO Charts Definition	Multiple lines of text (XML)		COP Manager
ncop_ips_originalsourceapp	Original Source Application	Text		System
ncop_ips_originalsourcetemplate	Original Source Template	Text		System
ncop_ips_originalsourceupdate	Original Source Update Method	Text		System
ncop_ips_originalsourcecapability	Original Source Capability	Multiple lines of text (XML)		System
ncop_ips_originalfilter	Original Filter	Multiple lines of text		System
ncop_ips_appereancemetadata	Appearance Date Metadata	Text		COP Manager
ncop_ips_appearancemetadataformat	Appearance Date Metadata Format	Text		COP Manager
ncop_ips_disappereancemetadata	Disappearance Date Metadata	Text		COP Manager
ncop_ips_disappearancemetadataformat	Disappearance Date Metadata Format	Text		COP Manager
ncop_ips_levelofdetail	Level Of Detail	Multiple lines of text (XML)	LoD Definition	COP Manager
ncop_ips_zordercategory	Z Order Category	Text		COP Manager

Attribute name	Attribute display name	Attribute type	Attribute content	Set by
ncop_pendingchanges	Pending Changes	Multiple lines of text		
ncop_ips_dissemination	Disseminated to	Dissemination		COP Manager
ncop_ips_display_relationsonmap	Display Relations On Map	Boolean		COP Manager
ncop_ips_segmentationcriteria	Segmentation Criteria	Integer	0: no segmentation 1: Segmentation based on NVG “Group”	COP Manager
ncop_ips_supportsmultiplesegmentations	Supports Multiple Segmentations	Boolean		COP Manager
ncop_ips_segmentationmaximumdepth	Segmentation Maximum Depth	Integer		COP Manager
	Created By	Person or Group		System
	Modified By	Person or Group		System

The following table describes the physical model of the Information Product Instance (variant attributes based on the acquired Information Product content)

TABLE 5-4: COP IP INSTANCE PROPERTIES

Attribute name	Attribute display name	Attribute type	Attribute content	Set by
ID	ID	Counter		System
Title	Title	Text		BizTalk
ncop_revision	Revision	Revision		System
EncodedAbsUrl	EncodedAbsUrl	Text	Url to CDF file in SP	System
ncop_informationproductsdoclib_description	Description	Multiple lines of text		BizTalk
ncop_informationproductsdoclib_effectiveenddtg	Effective End DTG	DateTime		BizTalk
ncop_informationproductsdoclib_effectivestartdtg	Effective Start DTG	DateTime		BizTalk
ncop_informationproductsdoclib_iptype	IP Type	Text		BizTalk
ncop_informationproductsdoclib_maxscalevisibility	Max Scale Visibility	Text		BizTalk
ncop_informationproductsdoclib_minscalevisibility	Min Scale Visibility	Text		BizTalk
ncop_informationproductsdoclib_ownerentity	Owner Command	Text		BizTalk
ncop_informationproductsdoclib_purpose	Purpose	Text		BizTalk
ncop_informationproductsdoclib_requiredupdatefrequency	Required Update Frequency	Text		BizTalk
ncop_informationproductsdoclib_sourcedconsumerentity	Sourced at Consumer Entity	Text		BizTalk
ncop_informationproductsdoclib_updatemethod	Update Method	Text		BizTalk
ncop_informationproductsdoclib_categorization	Categorization	Text		BizTalk
ncop_informationproductsdoclib_domain	Domain	Text		BizTalk
ncop_informationproductsdoclib_classification	Security classification	Text		BizTalk
ncop_informationproductsdoclib_classification_admin	Manual security classification	Text		COP Manager

Attribute name	Attribute display name	Attribute type	Attribute content	Set by
ncop_informationproductsdoclib_source	Source	Text	Name of the associated source	BizTalk
ncop_informationproductsdoclib_report	Report	URL		BizTalk
ncop_informationproductsdoclib_availability	Availability	Text		BizTalk
ncop_informationproductsdoclib_originaldata	Original Data	URL	Link to original source file	BizTalk
ncop_informationproductsdoclib_iptemplate	IP Template	Text		BizTalk
ncop_informationproductsdoclib_bsocount	BSO Count	Number		BizTalk
ncop_informationproductsdoclib_fileweight	File Weight	Text		BizTalk
ncop_informationproductsdoclib_statusDisplay	Status Display	URL		BizTalk
ncop_informationproductsdoclib_informativeclassification	Informative Classification	Text	Security Classification computed from the BSO Security Classification	BizTalk
ncop_informationproductsdoclib_sourceclassification	Source Classification	Text	Security Classification found in the Original Data of the Information Product	BizTalk
ncop_informationproductsdoclib_poc	PoC	Text		BizTalk
ncop_informationproductsdoclib_suggestediplocation	Suggested Ip Location	Multiple lines of text	Suggested Contributed IP Location in the COP structure Used only for Contributed IP	BizTalk
ncop_informationproductsdoclib_nextupdate	Next Update	DateTime		BizTalk
ncop_informationproductsdoclib_pincode	PIN Code	Text	PIN Code of the Contributed IP Used only for Contributed IP	BizTalk
ncop_informationproductsdoclib_format	Format	Text		BizTalk
ncop_informationproductsdoclib_filehash				BizTalk
ncop_guid	GUID	Text		System

Attribute name	Attribute display name	Attribute type	Attribute content	Set by
	Created By	Person or Group		System
	Modified By	Person or Group		System
	Check Out To	Person or Group		System

5.3.2.2.4.2 Source discovery

The COP IP Manager Information Panels display the capabilities sources as illustrated in the following figures.

The Figure 5-80: NVG Source Discovery displays a generic HMI according to the NVG capabilities of the source allowing the definition of the Information Product parameter.

Figure 5-80: NVG Source Discovery

The Figure 5-81: SQL and Excel Source discovery displays a preview of the SQL/Excel table data content allowing the definition of the Information Product parameter by designing the mapping to CDF attributes.

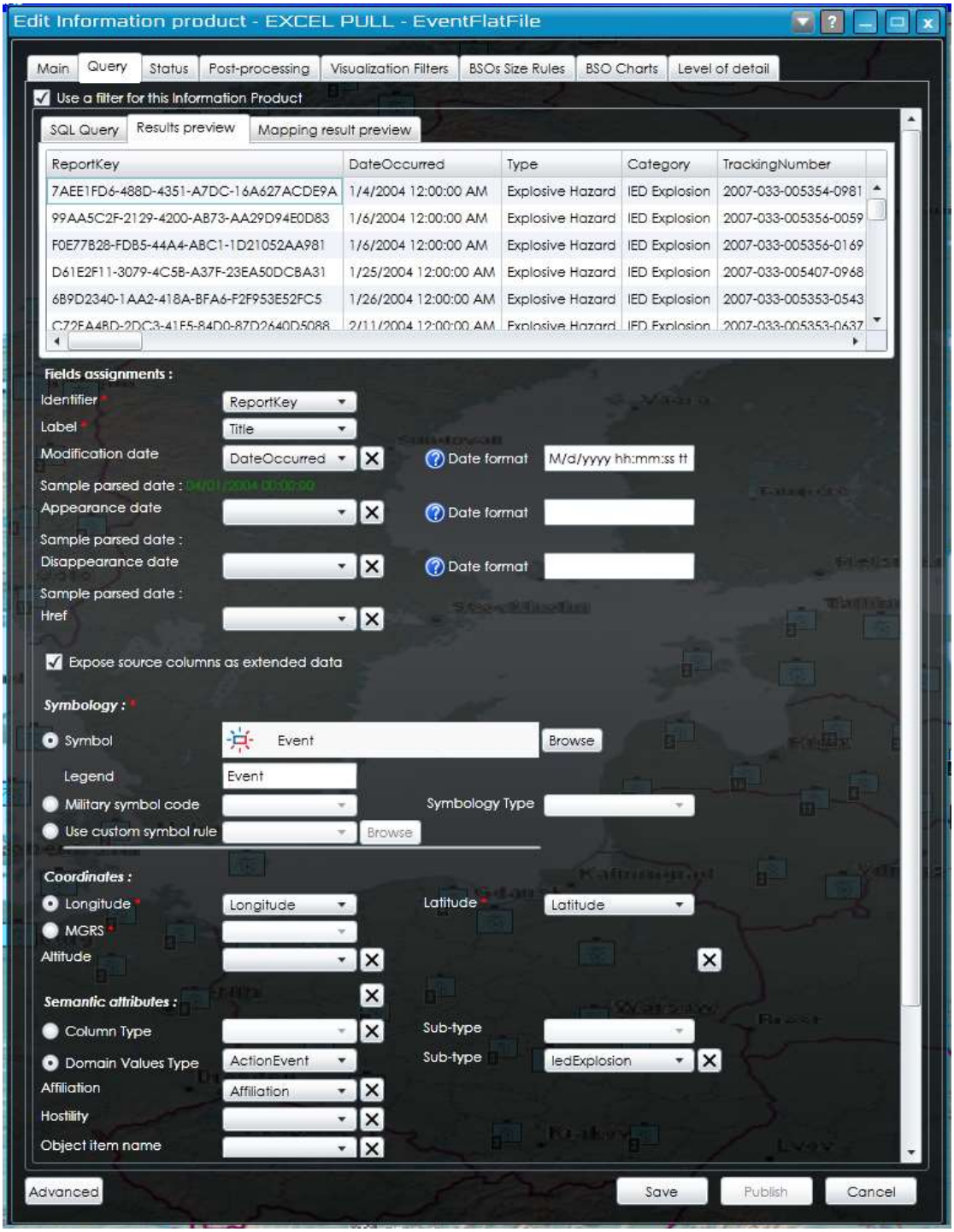


Figure 5-81: SQL and Excel Source discovery

When defining an SQL, SharePoint List or Excel-based information product, the COP manager has the capability to have a table preview to check if the columns and rules that have been used are processed correctly. This table preview can indicate:

- Missing mappings for required CDF attributes
- Incorrect values for coordinates
- No symbol applicable because of incorrect or incomplete symbol mapping rules

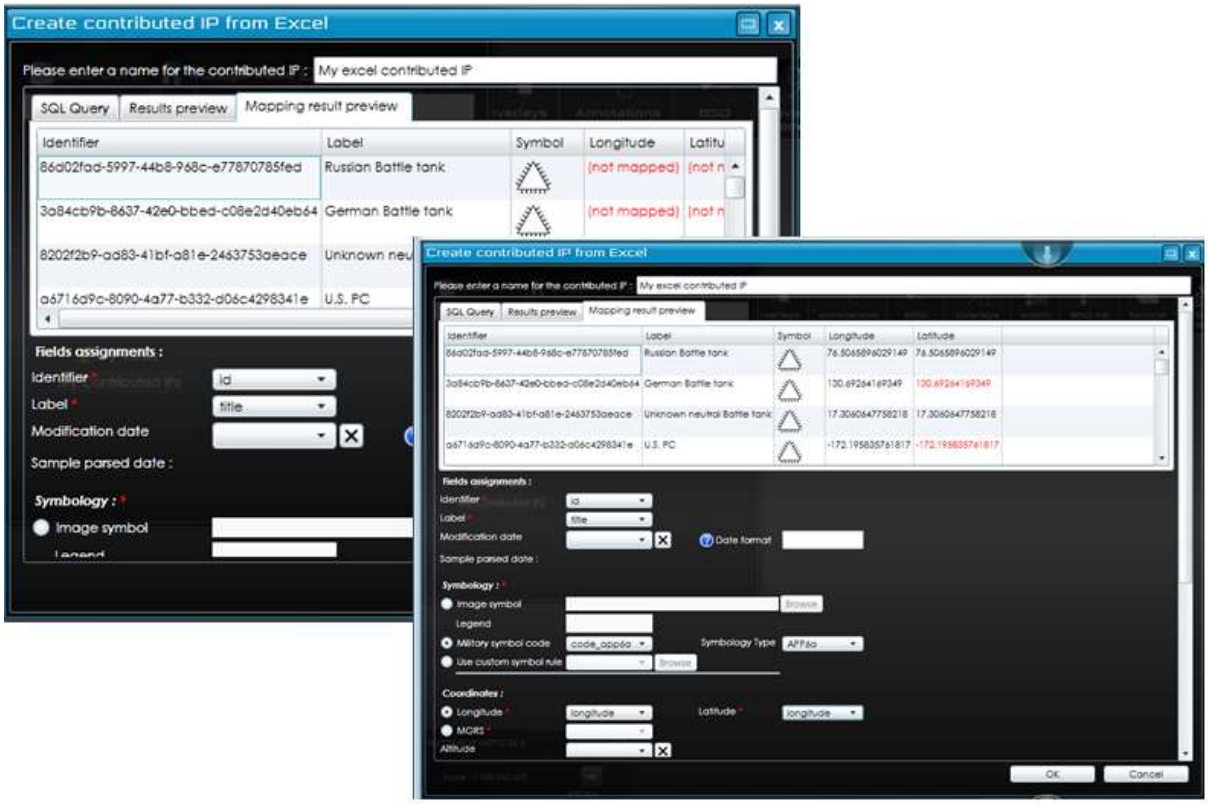


Figure 5-82: Mapping results table preview

5.3.2.2.4.3 Information Product post-processing

When defining an Information Product, the COP Manager has the capability to define post-processing rules to adjust the content of the CDF data before storing it in the NCOP portal.

The definition of these rules can be done in a dedicated tab in the Information Product edition panel.

Information Product post-processing principles and implementation are described in more details in the chapter 5.4.15.3.

5.3.2.2.4.4 Information Product visualization filters

When defining an Information Product, the COP Manager has the capability to define multiple visualization modes in order to allow a COP consumer to display the

Information Product in a specific way fulfilling an operational need. A visualization filter can filter or enhance the information displayed.

The definition of these visualization rules can be done in a dedicated tab in the Information Product edition panel.

Information Product visualization filters principles and implementation are described in more details in the chapter 5.4.15.4.

5.3.2.2.4.5 Information Product level of details

When defining an Information Product, the COP Manager has the capability to define multiple levels of details in order to adapt the visualization of the data for a particular usage according to the consumer operational objectives (may vary depending on the consumer entity) and also depending on its visualization context (current map zoom scale).

The definition of these levels of details rules can be done in a dedicated tab in the Information Product edition panel.

Information Product level of details principles and implementation are described in more details in the chapter 5.4.15.5.

5.3.2.2.4.6 BSO size rules

When defining an Information Product, the COP Manager has the capability to define specific BSO size rules. When a COP consumer loads the Information Product using the geographical COP Editor, these rules will apply and BSOs symbols will be displayed on the map with the correct size. The symbol size can be:

- Fixed
- Variable, depending on the current zoom scale

The following picture presents the corresponding UI integrated in the Information Product edition panel:

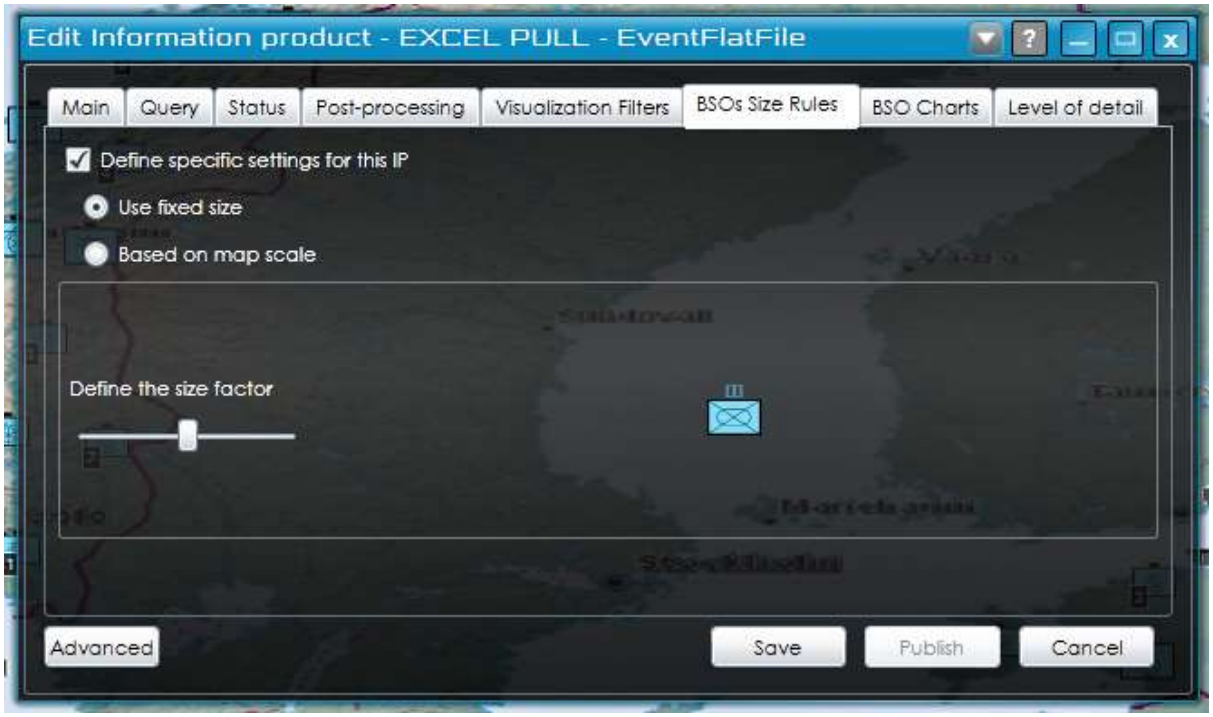


Figure 5-83: BSO size configuration at the Information Product level

5.3.2.2.4.7 BSO charts

When defining an Information Product, the COP Manager has the capability to define BSO charts. This capability will allow COP consumers to display BSO properties using a diagram representation.

A BSO chart is defined by selecting the following

- Diagram type

  Horizontal histogram, Vertical histogram, Pie chart or Radar chart

- List of properties to be displayed in the diagram
  - Property value

    BSO extended-data or constant value that represents the value to be displayed

  - Property maximum value

    BSO extended-data or constant value that represents the value to be displayed

- Additional diagram display settings

  Diagram title, Display values, Display maximum values

The COP Manager can define multiple charts for a same Information Product.

The following figure presents the configuration UI for defining BSO charts:

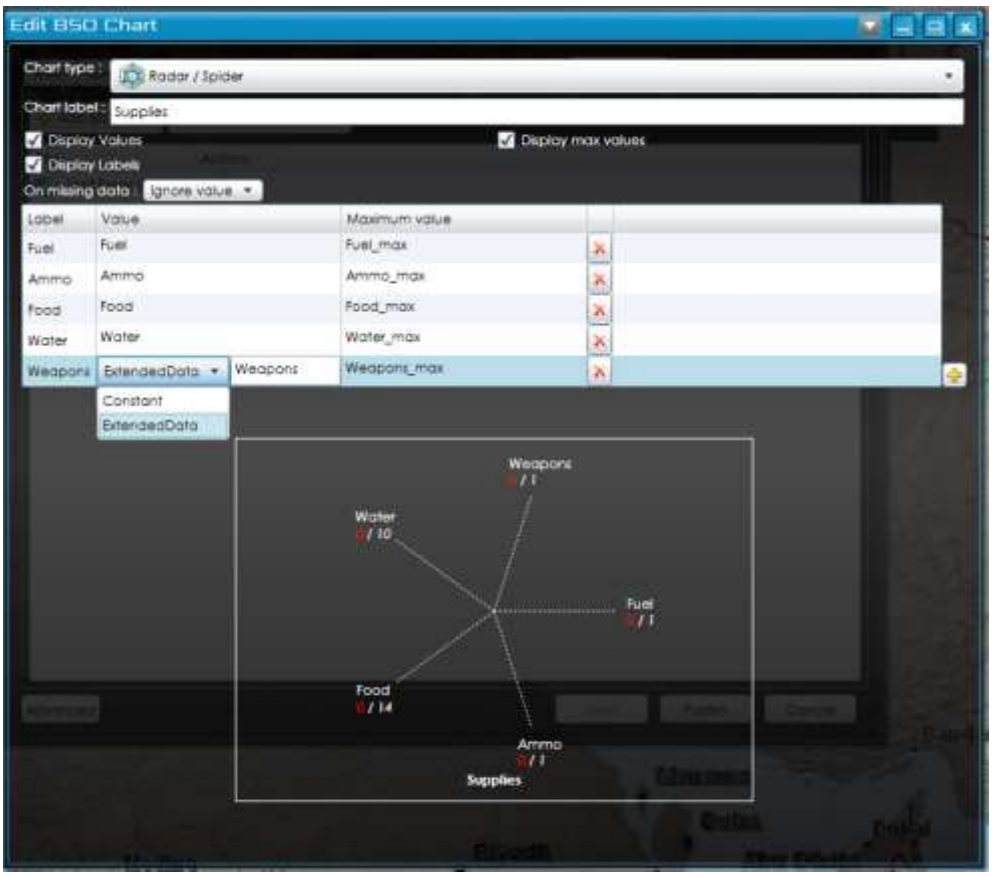


Figure 5-84: BSO chart definition UI

The definitions of BSO charts are stored in an XML document, attached as a property of the Information Product.

The following is a sample of a BSO chart definition for an Information Product:

```
<ChartsDefinition xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Pie label="Staff Breakdown" missingDataStrategy="IgnoreValue" type="Pie"
displayLabels="true" displayValues="true" displayPrecents="true">
    <Part label="United States">
      <Value>
        <ExtendedData key="Staff_US" />
      </Value>
    </Part>
    <Part label="France">
      <Value>
        <ExtendedData key="Staff_FR" />
      </Value>
    </Part>
    <Part label="United Kingdom">
      <Value>
        <ExtendedData key="Staff_UK" />
      </Value>
    </Part>
```

```
    <TotalValue>
      <ExtendedData key="Staff_total" />
    </TotalValue>
  </Pie>
</ChartsDefinition>
```

This XML representation is used at runtime when the Information Product is loaded. It is used to build the Chart display panel. Chapter 5.3.1.1.9.4 describes how BSO charts are visualised by COP Consumers.

5.3.2.2.5 COP Workflow Manager

Property Name	Description
Identification	COP Workflow Manager
Classification	IS
Behaviour	The COP Workflow Manager is a Web User Interface allowing Organizational Node Administrator role or COP Manager role to approve/reject submitted contributions of Named Views, IPs or Annotations and finally COP. Before approval or rejection, the Organizational Node Administrator role is able to preview the requested contribution or COP.
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 Application Server
Interfaces	This IC interacts with back-end through the Geographical COP Editor Services REST API
Collaboration mechanism	This IC interacts with the SQLback-end natively (SharePoint mechanism)
Local/Configuration data	-
Operating context	TypeScript/JavaScript .NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

5.3.2.2.5.1 Workflow configuration

NCOP offers the possibility to activate the approval workflow or not. The configuration is done per entity and is accessible from the Entity configuration panel in the NCOP Portal. The Information Elements for which the configuration is possible are the following:

- COP
- Shared View
- Contributed Information Product

If approval is not required, an Information Element (COP, Shared View, and Contributed Information Product) will be created automatically in the “published” state when submitted by a user.

The following figure presents the entity edition UI where the configuration must be done:

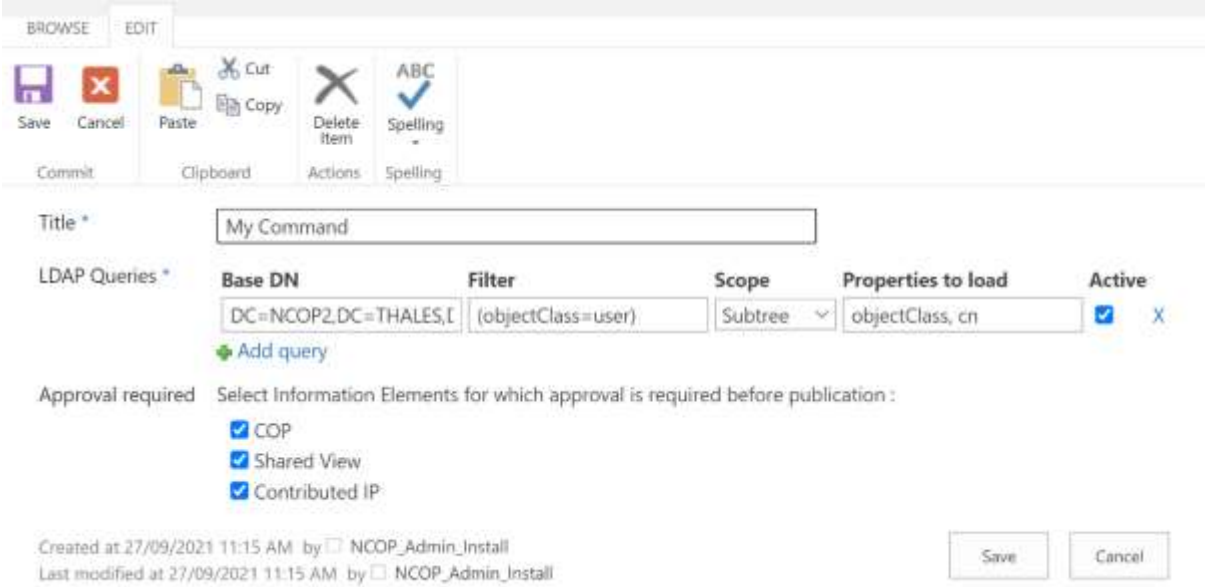


Figure 5-85: Workflow configuration UI (per Entity)

5.3.2.2.5.2 Contributions approval

In order to visualize pending contributions, a dedicated panel is available in the Geographical COP Editor. It is accessible to users with the ‘Approve contributions’ permission or the ‘Publish COP’ permission.

The ‘Publish COP’ permission gives access to the following elements:

- COPs pending for approval
- Information Products pending for approval

The ‘Approve contributions’ permission gives access to the following elements:

- Annotations pending for approval
- Shared Views pending for approval
- Contributed Information Products pending for approval

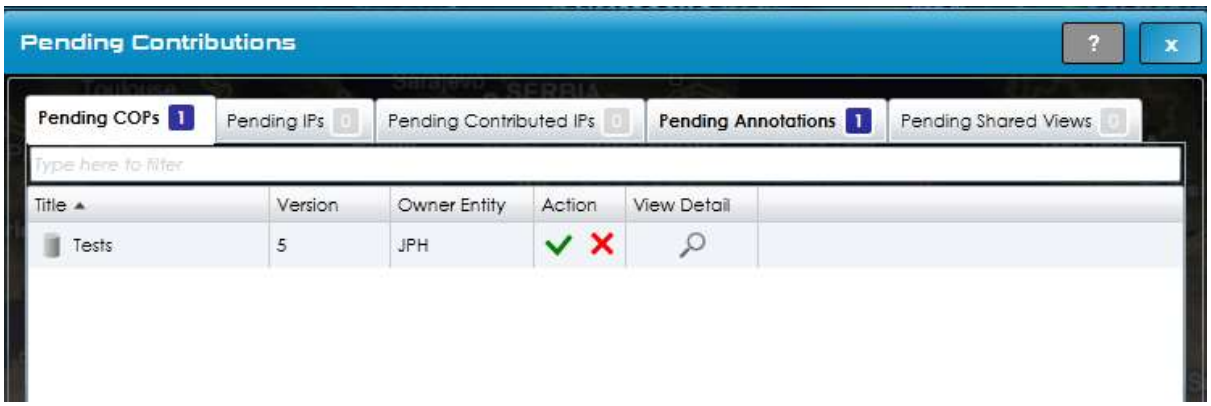


Figure 5-86: Pending contributions management panel

5.3.2.2.6 COP Dissemination Manager

Property Name	Description
Identification	COP Dissemination Manager
Classification	IS
Behaviour	The COP Dissemination Manager is a Web User Interface allowing Enterprise Administrator role or COP Manager role to set the dissemination rules of IPs. The TreeView of the COP Structure can be used to browse and select an Entity in order to: Allow an Owner Entity to enable/disable dissemination to an individual Consumer Entity; Allow a Consumer Entity to enable/disable dissemination of a COP from the Owner Entity; Discover Consumer Entities for the purpose of disseminating a COP to them; Display COPs that it subscribes to (gets disseminated) and the associated Owner Entities; Display COP Information Products subscribed to within a COP and dissemination status; In addition, COP Dissemination Manager allows selecting COP IPs within a COP to be disseminated to the individual consumer Entity.
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 Application Server
Interfaces	This IC interacts with back-end through the Geographical COP Editor Services REST API
Collaboration mechanism	https
Local/Configuration data	-
Operating context	TypeScript/JavaScript .NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

5.3.3 Services

5.3.3.1 Supervision

5.3.3.1.1 SLR / SLA

Property Name	Description
Identification	SLR / SLA
Classification	IS
Behaviour	Service Level Requirements (SLR) are the primary tools to manage SLAs (Service Level Agreement). The SLR / SLA component allow to: Define Service Levels (SLs) related to the hosting infrastructure and to the communication infrastructure; Create, update and delete SLR and SLA; Create and attach SLR for each element or task performed in NCOP; Derive SLR from any Information Element defined in NCOP; Present the complete set of SLRs and SLAs; Associate and correlate SLAs and SLRs.
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 Application Server Installed on the SharePoint Server
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

5.3.3.1.1.1 Service Level Agreement

NCOP Service Level Agreement is provided as an external document [SLA]. This document contains technical information allowing the support of the NCOP service. It covers both availability and performances aspects.

5.3.3.1.1.2 Service Level Requirements

Service Level Requirements are described in more details in the chapter 6.4 which describes the physical implementation of NCOP, focusing on:

- The various deployment configurations (physical and virtual, high availability or not, etc.)
- The performances aspect (scalability options, network usage, etc.)
- COTS requirements

5.3.3.1.1.3 NCOP behaviour management service

The purpose of this service is to provide a way to temporarily modify the behaviour of NCOP to take into account possible infrastructure limitations.

The typical use case where this service would be used is when the supervision system (operated by administrators external to the NCOP administration team) detects a temporary limitation due to unusual CPU usage or Memory consumption on the hosting infrastructure of NCOP or any other FAS to which NCOP is connected. In such a scenario, to avoid things from getting worse it is possible to ask the NCOP system to run in degraded mode by modifying temporarily its acquisition process frequency. To provide flexibility, this service proposes method to enable the degraded mode for all NCOP sources or individually.

Modifying the acquisition frequency for a specific has an impact on the following:

- NCOP CPU usage
  - BizTalk processes less information
  - Less events are generated, impacting :
    - NCOP alerting,
    - NCOP IPS,
    - NCOP synchronization.
- External FAS CPU usage
  - The FAS processes less requests coming from NCOP
- Network consumption
  - Between NCOP and the external FAS
  - Between NCOP nodes (synchronization)
  - Between NCOP and clients (NCOP IPS and Alerting notifications)

The following figure presents how supervision administrators can enable the degraded mode for NCOP and the impacted resources:

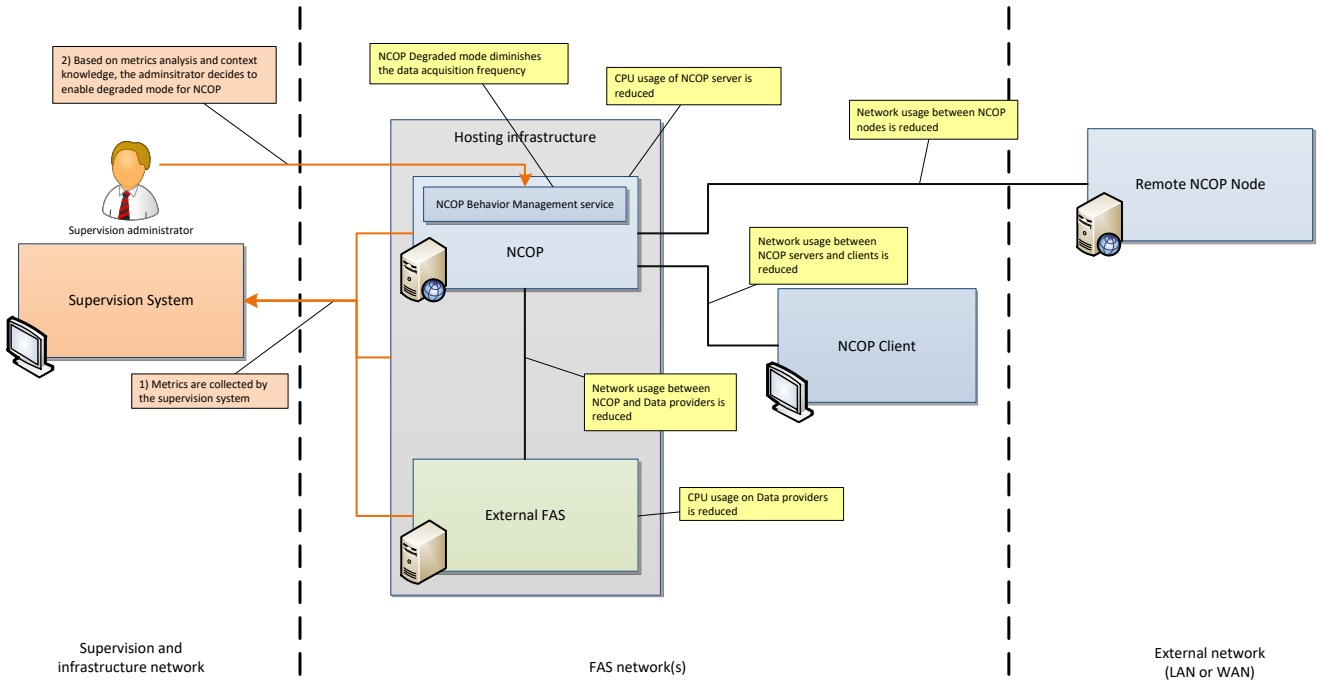


Figure 5-87: NCOP behaviour management service usage and impacts

The NCOP behaviour management web service is described in more details in the NCOP [ICD].

In addition to this externally available web service, it is possible to adjust the settings manually by modifying the attributes of the Source in the NCOP portal.

5.3.3.1.2 Activity Monitoring

Property Name	Description
Identification	Activity Monitoring
Classification	IS
Behaviour	The Activity Monitoring component is based on the Microsoft SQL Server Reporting Services feature for the presentation layer, on the BAM capabilities of Microsoft BizTalk and additional BAM capabilities developed for NCOP purpose. The Activity Monitoring component is able to: Integrate the Rights management service with the activity monitoring to record activity and propagate notifications; Allow service to create report on any activity performed; Create activity reports for any Information Product received from a Source; Create activity reports for any COP or COP IP sent to consumers; Provide customizable activity views detailing activity report and allow Enterprise Administrator role or Organizational Node Administrator role to create their own or modify existing ones;
Actors involved	See details in Appendix K IC vs Actors Involved

Property Name	Description
	IC: Microsoft BizTalk.
Objects involved	See details in Appendix L IC vs Objects Involved
Location (Types)	Installed on the BizTalk Server
Interfaces	This IC interacts with SQL Server Databases and SQL Server Reporting Services
Collaboration mechanism	https
Local/Configuration data	-
Operating context	.NET Framework SQL
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

NCOP will be deployed with the following preconfigured reports:

- Data acquisition monitoring
  - Information Products acquisition details
  - Information Products acquisition statistics

- NCOP usage monitoring
  - NCOP usage
  - NCOP statistics

The Activity Monitoring is implemented throughout the solution with two technologies:

Data acquisition BAM: this is a capability provided with the BizTalk tool. It allows the design and description of a “Functional Activity” view that is then mapped to the technical parts that compose the Information Product BizTalk flow solution.

NCOP usage BAM solution: this is a BAM capability that is built around SharePoint, and NCOP services raised event and custom SQL tables.

The two solutions are described below:

5.3.3.1.2.1 Data acquisition BAM

Data acquisition BAM is provided out of the box with the BizTalk product. It is used in NCOP for the provision of the Information Product Instance BizTalk flow Activity Monitoring.

The BAM Activity that is created is implemented with the following attributes:

Activity Name: GetSources (“NCOP-BIZ\BAMPrimaryImport\bam_GetSource_Active” table).

Property Name	Type	Description
ProcessCode	Attribute:Text	Internal code for BizTalk to identify the type of system/protocol that is used by the source
SourceCode	Attribute:Text	Code of the Information Product Source
IPCode	Attribute:Text	Code of the Information Product Parameter
Delay	Attribute:Text	Delay between each data pull attempts
ErrorCode	Attribute:Text	Error code in case of failure
ErrorDescription	Attribute:Text	Description of the error in case of failure
StepPullRequest	Milestone:Datetime	Date and time start of the data BizTalk flow process
StepGetSourceRequest	Milestone:Datetime	Date and time of the request to the source
StepGetSourceResponse	Milestone:Datetime	Date and time of the response from the source
StepArchive	Milestone:Datetime	Date and time of the archive step
StepPublishToSharePoint	Milestone:Datetime	Date and time of the publication to SharePoint
StepErrorOccured	Milestone:Datetime	Date and time of the error occurrence in case of failure

This Bam Activity is used for 2 reports:

“Information Product BizTalk flow Statistics”

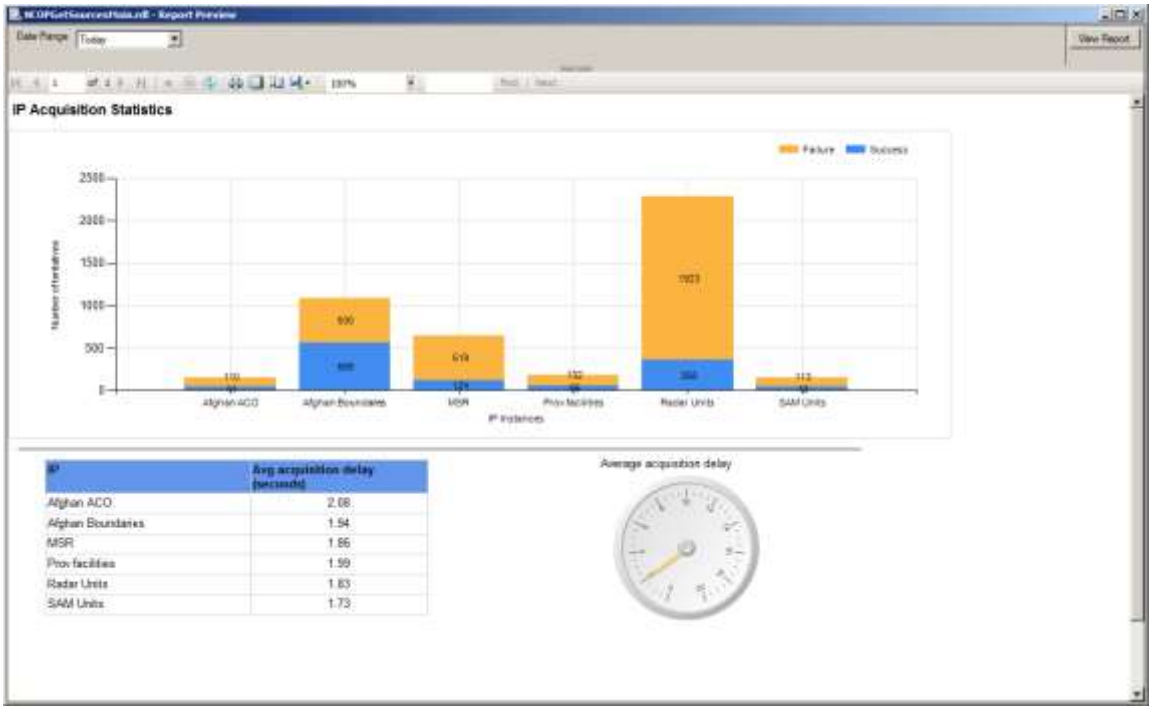


Figure 5-88: BAM activity : “Information Product BizTalk flow Statistics”

This report displays the number of success and failures of the data BizTalk flow process for each Information Product Instance over a period of time. It also provides the average delay for getting the data from the source (difference between the milestones StepGetSourceRequest and StepGetSourceResponse).

“Information Product Instance Get Sources”

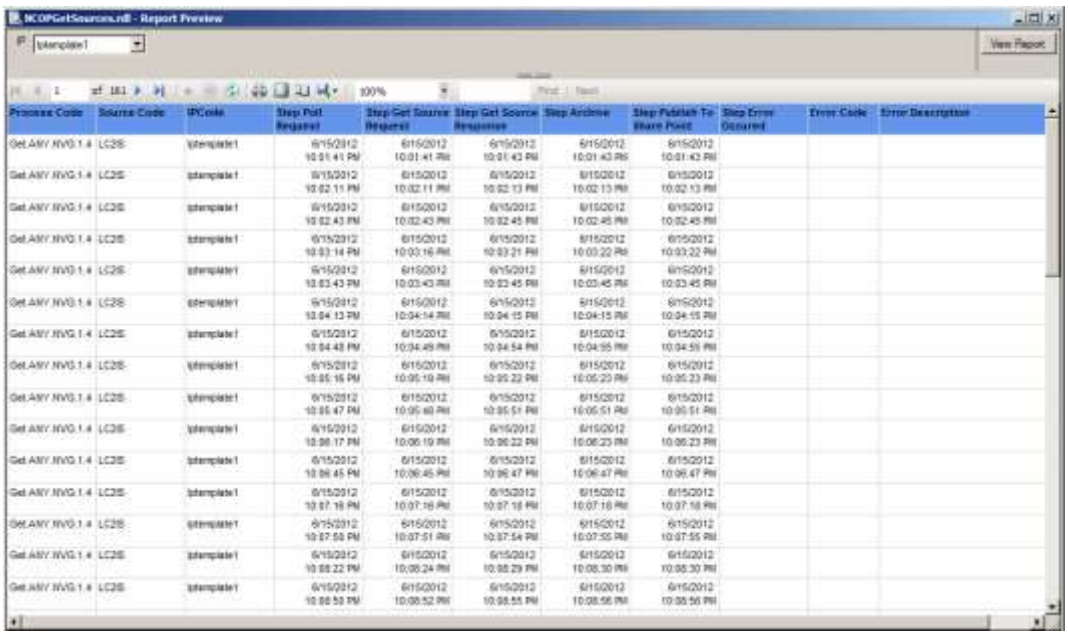


Figure 5-89: BAM activity : "Information Product Instance Get Sources"

This report displays the activity monitoring of the data pulling from the source. In case of failure, the error code and description are available in the report.

5.3.3.1.2.2 NCOP usage BAM

This functionality is composed out of SharePoint and NCOP Services raised events and dedicated database tables. It is implemented using custom C# classes.

The database is called "Nato.NCOP.BAMDb".

For some of the event related to an exchange between SharePoint and the Geographical COP Editor or between BizTalk and SharePoint, an entry is created in the NCOPBam database. Out of these events, several Activity Monitoring entries are gathered:

Activity Name: CopEvents: tracking of events related to COP Management ("NCOP-CMN\Nato.NCOP.BAMDb\CopEvents" table).

Property Name	Type	Description
ID	Attribute:Numeric	Internal ID of the Event
SiteName	Attribute:Text	Name of he site where the COP exists (operational, training, exercise)
SiteId	Attribute:Text	Identifier of the site where the COP exists
CopName	Attribute:Text	Name of the COP
CopId	Attribute:Text	Identifier of the COP
CopState	Attribute:Text	COP State (draft or published)
OwnerEntity	Attribute:Text	Name of the owner entity of the COP
EventType	Attribute:Text	"I" for insertion and "D" for deletion
EventDate	Milestone:Datetime	Date and time start of the event

Activity Name: CopIpAssociationEvents: tracking of events related to associations of Information Products with COPs ("NCOP-CMN\Nato.NCOP.BAMDb\CopIpAssociationEvents" table).

Property Name	Type	Description
ID	Attribute:Numeric	Internal ID of the Event
SiteName	Attribute:Text	Name of he site where the COP exists (operational, training, exercise)
SiteId	Attribute:Text	Identifier of the site where the COP exists
CopName	Attribute:Text	Name of the COP
CopId	Attribute:Text	Identifier of the COP
IpName	Attribute:Text	Name of the Information Product
IpId	Attribute:Text	Identifier of the Information Product
EventType	Attribute:Text	"I" for insertion and "D" for deletion
EventDate	Milestone:Datetime	Date and time start of the event

Activity Name: IpInstanceWriteEvents: tracking of the events related to an IpInstance. Import of an Information Product instance in SharePoint ("NCOP-CMN\Nato.NCOP.BAMDb\IpInstanceWriteEvents" table).

Property Name	Type	Description
ID	Attribute:Numeric	Internal ID of the Event
SiteName	Attribute:Text	Name of he site where the Information Product exists (operational, training, exercise)
SiteId	Attribute:Text	Identifier of the site where the Information Product exists
IpName	Attribute:Text	Name of the Information Product
IpId	Attribute:Text	Identifier of the Information Product
SourceName	Attribute:Text	Name of the Source that provides the Information Product
SourceId	Attribute:Text	Identifier of the Source
BsoCount	Attribute:Numeric	Number of BSOs in the Information Product
FileWeight	Attribute:Numeric	Size of the CDF file representing the data of the Information Product
EventDate	Attribute:DateTime	Date and time of the event

Activity Name: IpInstanceReadEvents: tracking of events of consumers reading IpInstance from SharePoint ("NCOP-CMN\Nato.NCOP.BAMDb\IpInstanceReadEvents" table).

Property Name	Type	Description
ID	Attribute:Numeric	Internal ID of the Event
SiteName	Attribute:Text	Name of he site where the Information Product exists (operational, training, exercise)
SiteId	Attribute:Text	Identifier of the site where the Information Product exists
IpName	Attribute:Text	Name of the Information Product
IpId	Attribute:Text	Identifier of the Information Product

SourceName	Attribute:Text	Name of the Source that provides the Information Product
SourceId	Attribute:Text	Identifier of the Source
EventDate	Attribute:DateTime	Date and time of the event

Activity Name: IpTemplateEvents: tracking of events related to an Information Product Parameter. Creation of an Information Product Parameter in SharePoint ("NCOP-CMN\Nato.NCOP.BAMDb\IpTemplateEvents" table).

Property Name	Type	Description
ID	Attribute:Numeric	Internal ID of the Event
SiteName	Attribute:Text	Name of he site where the Information Product exists (operational, training, exercise)
SiteId	Attribute:Text	Identifier of the site where the Information Product exists
SourceName	Attribute:Text	Name of the Source that provides the Information Product
SourceId	Attribute:Text	Identifier of the Source
IpName	Attribute:Text	Name of the Information Product
IpId	Attribute:Text	Identifier of the Information Product
IpState	Attribute:Text	State of the Information Product (draft or published)
OwnerEntity	Attribute:Text	Name of the entity that owns the Information Product
EventType	Attribute:Text	"I" for insertion and "D" for deletion
EventDate	Milestone:Datetime	Date and time of the event

Activity Name: SharedViewReadEvents: tracking of events of consumers using SharedViews ("NCOP-CMN\Nato.NCOP.BAMDb\SharedViewReadEvents" table).

Property Name	Type	Description
ID	Attribute:Numeric	Internal ID of the Event
SiteName	Attribute:Text	Name of he site where the Shared View exists (operational, training, exercise)
SiteId	Attribute:Text	Identifier of the site where the Shared View exists
CopName	Attribute:Text	Name of the COP
CopId	Attribute:Text	Identifier of the COP
SharedViewName	Attribute:Text	Name of the Shared View
SharedViewId	Attribute:Text	Identifier of the Shared View
EventDate	Attribute:DateTime	Date and time of the event

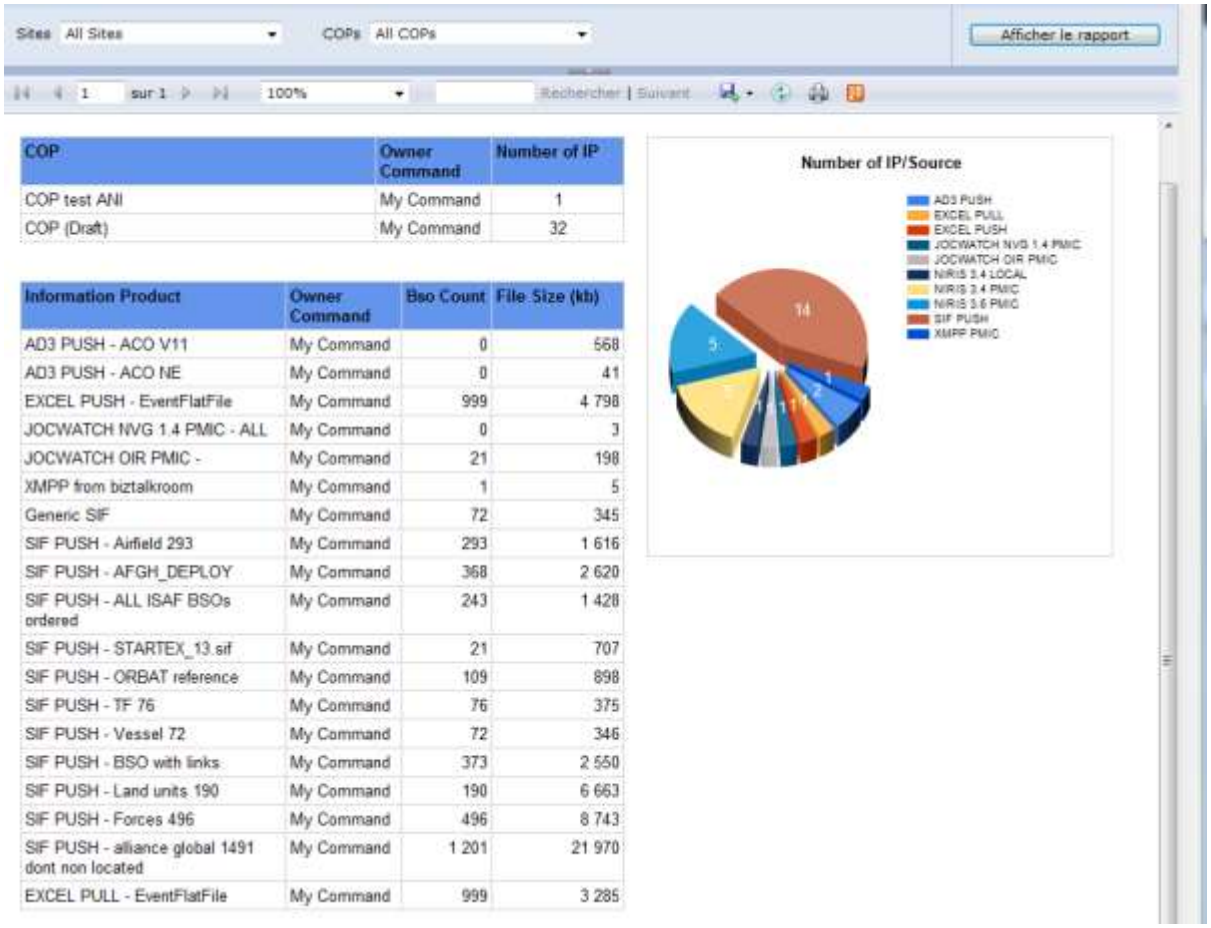
Activity Name: SourceEvents: tracking of events of management of Sources ("NCOP-CMN\Nato.NCOP.BAMDb\SourceEvents" table).

Property Name	Type	Description
ID	Attribute:Numeric	Internal ID of the Event
SiteName	Attribute:Text	Name of he site where the Source exists (operational, training, exercise)
SiteId	Attribute:Text	Identifier of the site where the Source exists
SourceName	Attribute:Text	Name of the Source

SourceId	Attribute:Text	Identifier of the Source
EventType	Attribute:Text	“I” for insertion and “D” for deletion
EventDate	Attribute:DateTime	Date and time of the event

These SharePoint Bam activities are used for 2 reports

“NCOP Statistics”



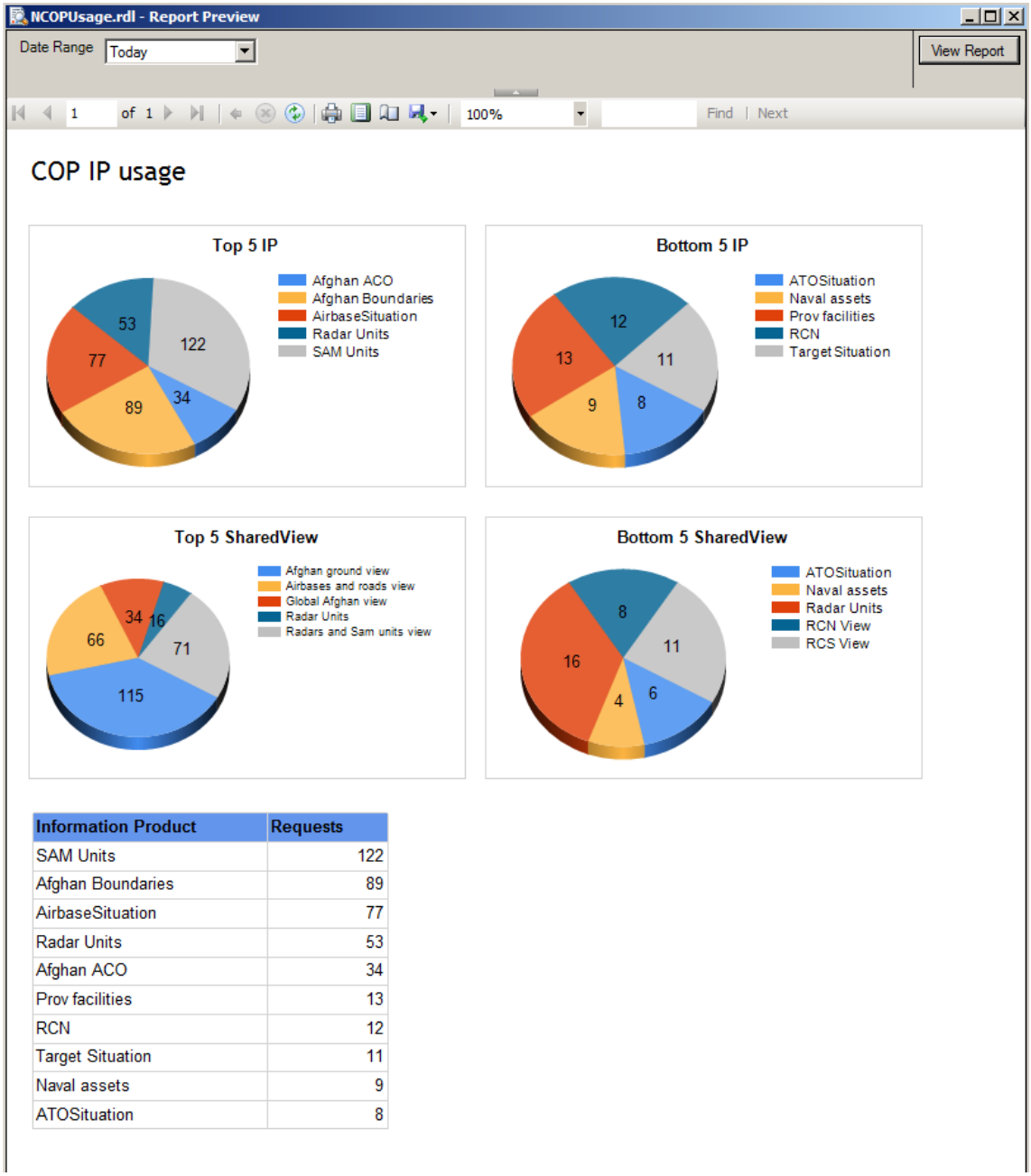
COP	Owner Command	Number of IP
COP test ANI	My Command	1
COP (Draft)	My Command	32

Information Product	Owner Command	Bso Count	File Size (kb)
AD3 PUSH - ACO V11	My Command	0	568
AD3 PUSH - ACO NE	My Command	0	41
EXCEL PUSH - EventFlatFile	My Command	999	4 798
JOCWATCH NVG 1.4 PMIC - ALL	My Command	0	3
JOCWATCH OIR PMIC -	My Command	21	198
XMPP from biztalkroom	My Command	1	5
Generic SIF	My Command	72	345
SIF PUSH - Airfield 293	My Command	293	1 616
SIF PUSH - AFGH_DEPLOY	My Command	368	2 620
SIF PUSH - ALL ISAF BSOs ordered	My Command	243	1 428
SIF PUSH - STARTEX_13.sif	My Command	21	707
SIF PUSH - ORBAT reference	My Command	109	898
SIF PUSH - TF 76	My Command	76	375
SIF PUSH - Vessel 72	My Command	72	346
SIF PUSH - BSO with links	My Command	373	2 550
SIF PUSH - Land units 190	My Command	190	6 663
SIF PUSH - Forces 496	My Command	496	8 743
SIF PUSH - alliance global 1491 dont non located	My Command	1 201	21 970
EXCEL PULL - EventFlatFile	My Command	999	3 285

Figure 5-90: BAM activity : “NCOP Statistics”

This report displays the number of Information Product Parameters per COP with the detail of the number of BSO as well as the file weight for the corresponding Information Product Instances of the COP. The proportion of number of Information Products per source is also displayed. The report allows the consumer to give some input parameters to filter the results of the report: a consumer can filter per NCOP site (operational/training/exercsie) and per COP.

"NCOP Usage"



Information Product	Requests
SAM Units	122
Afghan Boundaries	89
AirbaseSituation	77
Radar Units	53
Afghan ACO	34
Prov facilities	13
RCN	12
Target Situation	11
Naval assets	9
ATOSituation	8

Figure 5-91: BAM activity : "NCOP Usage"

This report displays the Top and Bottom five Information Products queried by the users as well as a complete table for all the Information Products. The same Top and Bottom five statistics is provided for the Shared Views.

5.3.3.1.2.3 Custom reports

NCOP will be installed with preconfigured reports as described above. However it is possible to add new reports and customize existing reports if required. To create or customize reports, the Microsoft Visual Studio tool is required with the Microsoft SQL

Server Reporting Services project templates activated. These project templates allow the creation and modification of reports with integrated wizards and user friendly interface. With these tools, a user will be able to browse the existing NCOP SQL tables, select the required attributes, define some calculation rules and select the rendering method (table, histogram, circular diagram, etc.).

Note that it is not possible to add additional attributes in the existing SQL tables of NCOP. Only existing tables and columns can be used to create or modify reports.

Once a report has been created by a user, Microsoft SQL Server Reporting Services offers an import capability to make the report available to other users.

The procedures required for the creation or updates of reports are described in the NCOP technical manual.

5.3.3.1.3 Audit / Log

Property Name	Description
Identification	Audit / Log
Classification	IS
Behaviour	The Audit/Log component provides the following audit and traceability capabilities (used by all other NCOP Services): Expose a central auditing point for each site as a Service; Provides a time-stamping mechanism to guarantee the time of each audit entry; Report on all data that is developed, accessed, manipulated, published, and disseminated by any NCOP services; Store audit entries in a well-defined and structured format (text or XML based); Enable all audit actions to be audited by any Administrator role. The journal management implementation component is based on the Microsoft Application Event Log database. The NCOP logging manager implementation component record NCOP system events in the native Microsoft Windows Event Log. The Journal Management provides the integration with the Bi-SC AIS Enterprise Management Services (EMS) to automatically report errors, provide suggested corrective measures actions and allow automated monitoring of NCOP devices and services via Simple Network Management Protocol (SNMP). This component is based on the .NET Framework.
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 Installed on the BizTalk Server Installed on the Application Server Installed on the GeoServer

Property Name	Description
	Installed on the SQL Server
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	TypeScript/JavaScript .NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

At the service level, this functionality is provided at three levels:

- Functional log and auditing of the imported Information Product instances
- Technical log and auditing of the BizTalk Flows
- Technical log and auditing of NCOP components

5.3.3.1.3.1 Functional log and auditing

The functional log and auditing consists of logging the Information Product Instances interface activity.

For each interface, a mechanism tracks the success/failure of an interface execution and determines the Information Product status based on the Information Product own criteria. The Information Product status is calculated by BizTalk and is displayed at the user interface level in the Information Product instance and Information Product Parameter screens.

The detail of the log is displayed on a table as shown in the following figure.

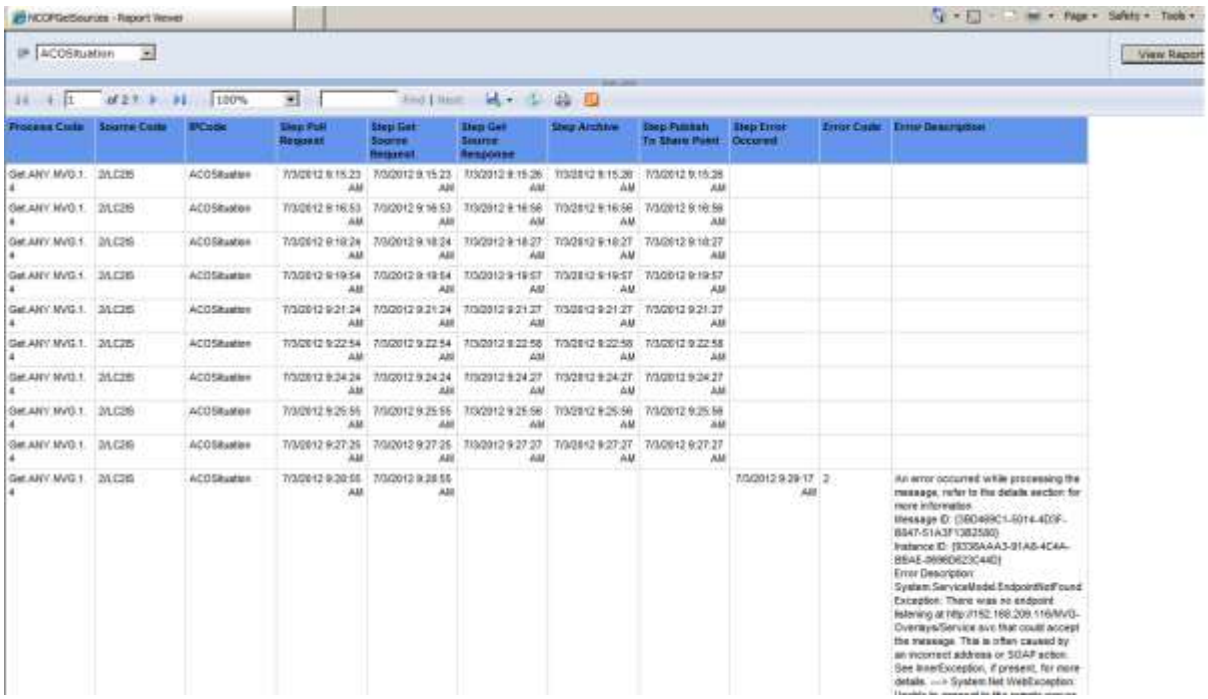


Figure 5-92: Log report on Information Product

See also the User Interface description for more details about the Information Product status definition criteria (see §5.3.2.2.4)

5.3.3.1.3.2 BizTalk log and auditing

This functionality is provided by the BizTalk Tracking mechanism. Referred as “BizTalk Tracking”, it allows the search and visualization of the BizTalk messages activity over a period of time. This tracking data is retained in NCOP for a period of 10 days (configurable parameter set to 10 by default).

The tracking data is made available through the BizTalk Administration Console.

The tool “Group Overview” is available when clicking on the BizTalk Group node in the administration console.

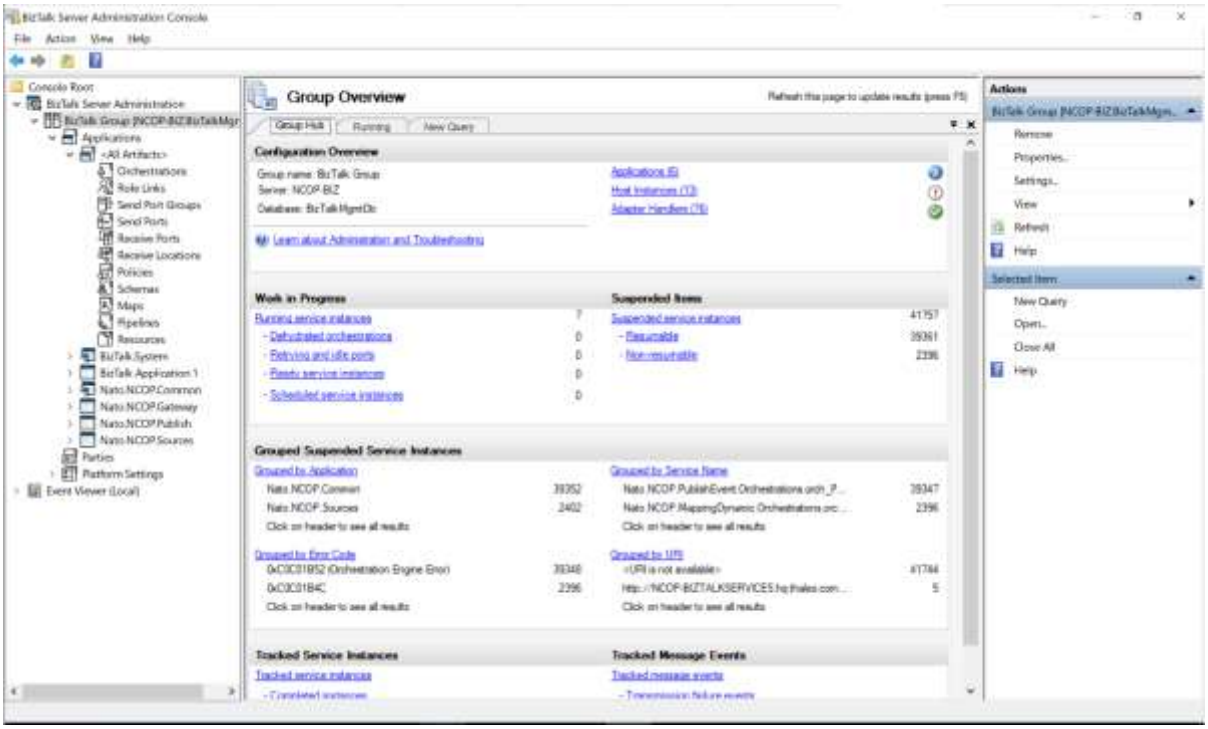


Figure 5-93: BizTalk Administration console

Under Configuration Overview (orange box in the screenshot above Figure 5-93) is an indicator that all BizTalk Applications (interfaces), Host Instances (BizTalk engines) are operational.

In the green box (Figure 5-93) are listed the interfaces that are being currently being processed. This view allows to visualise both “services instances” (that is processes), as well as “messages” (an instance containing data)

- Service instances (processes) can be in the following state:

State	Explanation
In Breakpoint	An active orchestration hits a breakpoint, typically one set by a BizTalk Server solutions developer. This state is valid only for orchestrations. **NCOP context:** should never occur
Ready to run	A service instance that has been activated but has not yet started running, typically due to temporary unavailability of resources, such as a heavy processing load on the server. **NCOP context**:Requires no attention.

Active Dehydrated	Running service instance. Instance state persists in the MessageBox database and no Windows service is running that instance. **NCOP context**:Requires no attention.
Completed with discarded messages	The service instance was completed, but some messages were not consumed by the instance
Suspended (resumable)	Instance suspended, an administrator can resume it. Note that when an administrator suspends a scheduled instance and then resumes it, the instance goes into a dehydrated state. **NCOP context**:Requires attention.
Suspended (not-resumable)	Instance suspended, but cannot be resumed. An administrator can save the Messages referenced by the instance, and then terminate the instance. Note that when an administrator suspends a scheduled instance and then resumes it, the instance goes into a dehydrated state. **NCOP context**:Requires attention.

- Messages can have the following state

State	Explanation
Consumed	The message is being processed by a service instance.
In Process	The message has been delivered to the engine and is being processed. It is in memory.
Queued	Queued encompasses the Queued (awaiting processing), Queued (scheduled for later delivery), and Queued (waiting to retry) instance states.
Queued (awaiting processing)	The message is in an ordered delivery scenario when the preceding message is being retried by the ordered delivery send port.
Queued (scheduled for later delivery)	The message is waiting to be sent by a send port that has a service window set.
Queued (waiting to retry)	The message is associated with a send port that is attempting to resend it because the destination URI is unavailable.
Suspended	Suspended encompasses the Suspended (resumable) and Suspended (not-resumable) instance states.
Suspended (resumable)	The service instance associated with the message is suspended, and can be resumed.

Suspended (not-resumable)	The service instance associated with the message is suspended, and cannot be resumed.

In the purple box (Figure 5-93), two views are available: “Tracked Services Instance” and “Tracked Message Events”. These views give access to the historical data as well as the on-going BizTalk activity.

- For “Tracked Services Instance”, the items can have the status below. Note that for the on-going interfaces, the statuses are all under Started. For completed interfaces instances their status is either Completed or Terminated.

State	Explanation
Started	Any service instance that is presently in the MessageBox, for example, in suspended (resumable) or in-breakpoint state, shows up as Started in the BizTalk Tracking database.
Completed	The service instance processing has completed successfully.
Terminated	The service instance was terminated

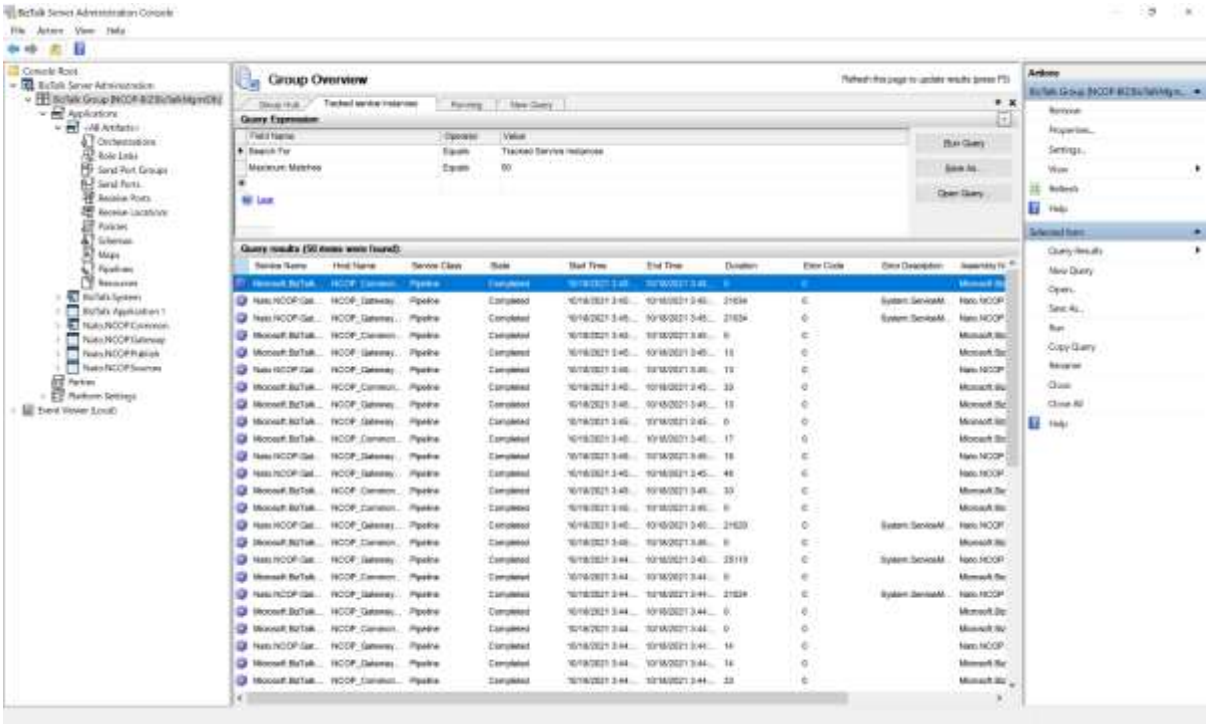


Figure 5-94: BizTalk Track service instances

In the example above, the processes (or services instances) that are visualised are instances of execution of the NVG interface. Service name, start and end date time of the process, as well as the error code and description is provided.

A right-click and “Message Flow” gives access to the detail of the process and the components that were executed. See below:

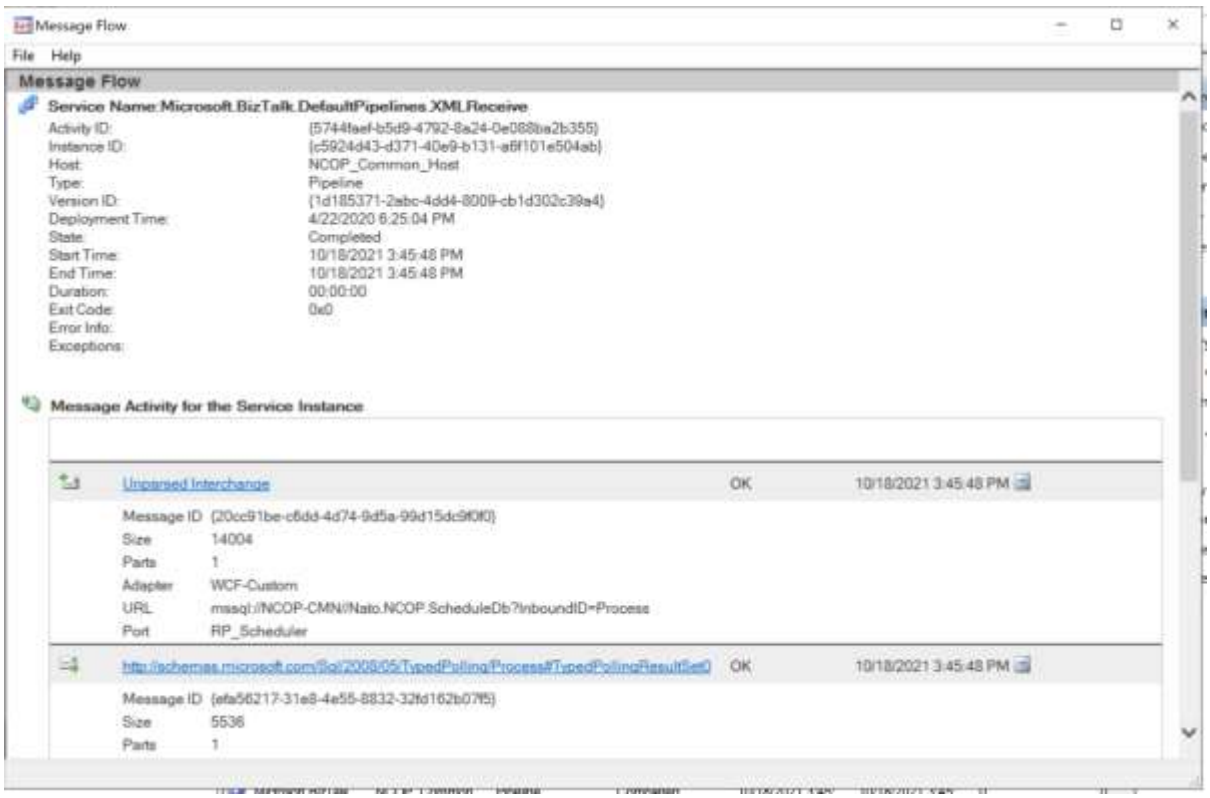


Figure 5-95: BizTalk Message Flow details

A right-click and “Show Tracked Message Events” gives access to the messages corresponding to the selected service instance.

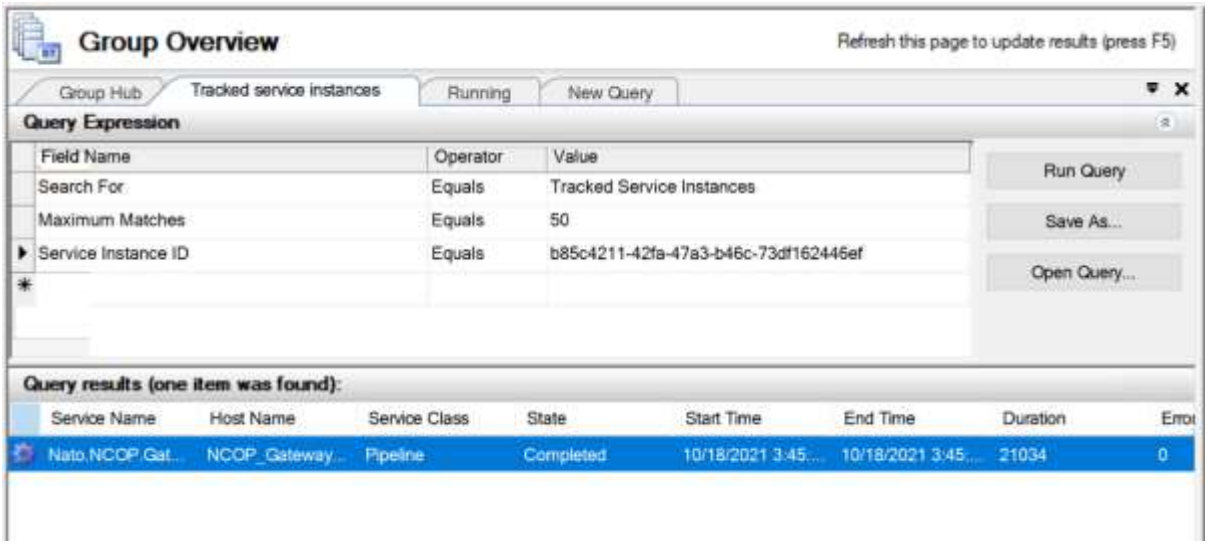


Figure 5-96: BizTalk Tracked Message Events

Each message can be visualise with a right-click on the line and select “Message Details”. The message details screen can be used to visualise the message context properties as well as its content.

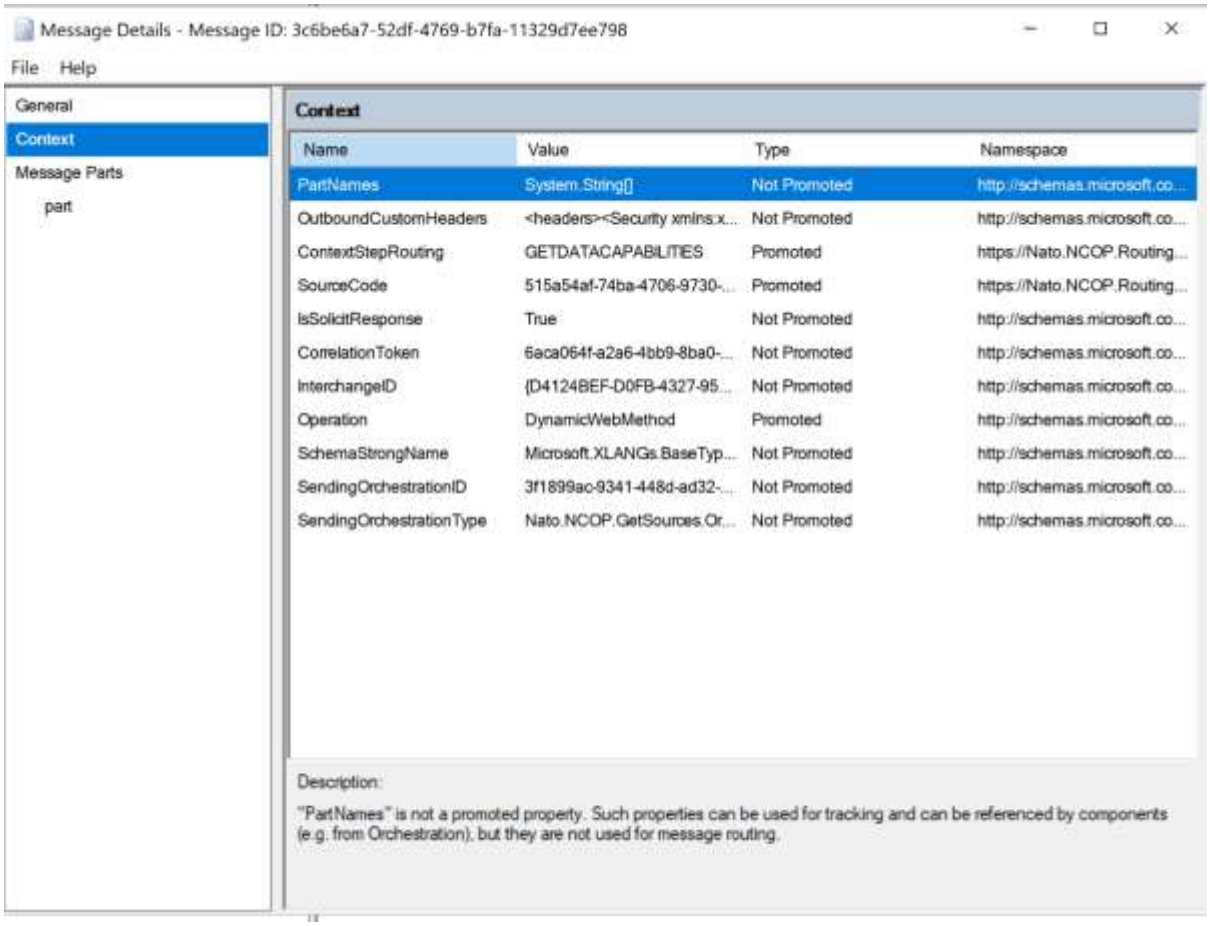


Figure 5-97: BizTalk Tracked Message details

Above, message’s context property. Below, message’s content:

Figure 5-98: BizTalk Tracked Message details

5.3.3.1.3.3 Journal Management

The journal management provide the auditability of the application through permanent log of the Users, the system.

User audit requires:

Login details of all Users to maintain audit traceability;

All necessary information, in order to provide the support staff with interpretable and comprehensive information about the cause and nature of the error/change;

All selected transactions, database activities, technical events (e.g. database replication, directory replication) and accessing of data (ensuring that any information object can always be traced to its original source);

A record of the date, time and User that created an object.

A User is able to view the audit traceability for those objects authorised for that User (including client activity, fault and error logs). A notification of all errors and faults is configurable to a set of Users (e.g. the Organisational Node Administrator) and to a selected output device.

The logs are archived for audit after a period of time, as configured by an authorised User (the log shall be archived after 48 hours by default)

System audit involves:

System start-up and shutdown;

Log-on and log-off of individual Users;

- Changes to permissions and privileges of Users and groups;
- Changes to security relevant system management function;
- Any access to audit log;
- Deletion, creation or alteration of the security audit records;
- All privileged operations;
- All updates of NCOP access rights;
- All attempts to delete, write or append the Audit files.

5.3.3.1.3.4 NCOP Components technical log and auditing

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.

All NCOP components are configured to log their activities in a technical log file. This technical logging capability is provided by the use of the Log4Net and Serilog libraries. These libraries offer flexibility for logging such as:

- Log type (files, Windows Event Logs, smtp, etc.)
- Log files locations and naming
- Log files maximum size
- Log files replacement strategy
- Log files verbosity

For technical logging, NCOP uses the standard file output method. Log files are produced locally on the server where the component logged the event. For easier exploitation, log files are isolated with one folder per logger.

The following table lists the information logged:

TABLE 5-5: INFORMATION LOGGED

Information	Description
Date	Date and time when the event occurred
User name	Name of the user (end user or technical account) that initiated the action
Level	Severity of the event. It can be one of the log levels described below
Message	Detailed message describing the event. It can be a simple message or a full stack trace when an exception occurred.

For a log message, one of the following log levels can be used in descending criticality order:

- FATAL
- ERROR
- WARN
- INFO
- DEBUG

For all its modules, NCOP uses a single configuration file located on each SharePoint server. This file contains the configuration of all loggers for all modules.

In a high availability configuration, each SharePoint server has its own configuration file that will be used by the components hosted on this server. Therefore it is required that the configuration files have the same contents, in order to have consistency in logs generated on each server.

It is possible to adjust log verbosity by selecting the log level threshold. For example, selecting WARN as the log level threshold will generate only logs with the WARN, ERROR and FATAL levels. This verbosity level is configurable per module.

Log configuration changes are taken into account dynamically, without requiring any service or component to be restarted.

For each technical module, a dedicated logger is configured. The following table presents all NCOP loggers with their corresponding purpose:

TABLE 5-6: LOGGERS

Logger name	Description
Technical	Default logger configuration, used if one of the following sub-logger is not configured.
Technical_BSO_BSO Service	Logs created by the BSO indexing service
Technical_Dynamic_DSS	Logs created by the Dynamic Source Server component responsible of sending dynamic Information Product updates to clients.
Technical_Dynamic_MCCIS	Logs created by the MCCIS connector, responsible of the acquisition of MCCIS Information Products
Technical_Dynamic_NFFISIP3	Logs created by the NFFI-SIP3 connector responsible of the acquisition of NFFI-SIP3-based Information Products.
Technical_Dynamic_NIRISConnector	Logs created by the NIRIS connector responsible of the acquisition of NIRIS Information Products.
Technical_Dynamic_NIRISConnector38	Logs created by the NIRIS 3.8 connector responsible of the acquisition of NIRIS Information Products.
Technical_Dynamic_NIRISConfigurator	Logs created by the NIRIS Configurator Web Service
Technical_Dynamic_NVG Streaming	Logs created by the NVG Streaming Protocol connector responsible of the acquisition of NVG Streaming Protocol-based Information Products.
Technical_Events_Alerting	Logs created by the Alerting service, responsible of sending NCOP Alerts to clients.
Technical_Events_Eventing	Logs created by the Event Manager, responsible of routing events to the Alerting, NCOPIPS and Synchronisation components.
Technical_Events_NCOPIPS	Logs created by the NCOPIPS, responsible of sending NCOP data (COP, Information Products, etc.) and notifications to NCOP clients depending on their subscription.
Technical_Services_General	Logs created by the NCOP services, including COP Management services (technical services used for the management of NCOP Information Elements).
Technical_SharePoint_Accessor	Logs created by the SharePoint accessor, technical component used as the NCOP-Portal database access layer.
Technical_SharePoint_Portal	Logs created by the NCOP SharePoint portal, including all NCOP custom activities triggered by scheduled jobs or event receivers.
Technical_Sync_Client	Logs created by the Synchronisation client service, Web service responsible of the acquisition of publication messages sent by other NCOP nodes.
Technical_Sync_Manager	Subscription management web service related logs. For instance : list of available cops to subscribe on, subscription status requests, etc.
Technical_Sync_Server	Logs created by the Synchronisation Windows Service, responsible of sending publication messages to other NCOP nodes.

Regarding log files creation and replacement strategy, the logging framework offers the following options:

- Create a new log file based when a file size threshold is reached
- Create a new log file based on the date (e.g. 1 log file per day)
- Limit the number of log files (e.g. with a limit of 5 log files, when the 6th log file is about to be created, the oldest log file will be removed).

NCOP default configuration is the following:

- Log file size limit: 5 MB

- Maximum number of log files: 100
- Log filename contains the log file creation date

This default configuration applies to each NCOP technical module and can be manually adjusted if required.

5.3.3.1.3.5 User activity logs

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.

NCOP components create Windows Event Logs related to user activity on the NCOP business objects such as:

- Publication of a COP,
- Deletion of an Information Product,
- Approval of a SharedView,
- …

These logs are generated through the use of the Log4Net and Serilog logging libraries that are integrated and used in all NCOP software components.

These user activity logs present the name of the user, and the action he performed.

5.3.3.1.3.6 Log used for NCOP hosting servers monitoring

NCOP proposed that the following Event Logs be used as a basis for monitoring NCOP hosting servers:

- NCOP SQL Server
  - Error & Critical events from the “MSSQL$<instance>” source in the Application Event logs
  - Error & Critical events from the “ENTSSO” source in the Application Event logs
  - Error & Critical events in the System Event Logs

- NCOP BizTalk Server
  - Error & Critical events from the “BizTalk Server” source in the Application Event logs
  - Error & Critical events in the System Event Logs
- NCOP SharePoint Server
  - Error & Critical events from the “SharePoint” source in the Application Event logs
  - Error & Critical events in the System Event Logs
- NCOP Application Server
  - Error & Critical events from the NCOP Applications (Web Services, Geographical COP Editor …) source in the Application Event logs

- Error & Critical events in the System Event Logs

Most of these event logs are created automatically by the COTS (SQL Server, BizTalk, SharePoint and Windows server). Regarding BizTalk event logs, some are generated explicitly by the NCOP orchestrations.

Additionally to these software based alerts, NCOP hosting servers are configured to generate Event Logs based on alerts raised by the performance monitor.

These alerts are based on the following indicators:

- Available disk space,
- Available memory.

When these indicators reach a certain threshold a log is created in the Windows Event log. Default threshold values are set during NCOP installation but can be modified afterwards by an authorized user. Also, other indicators can be added as required.

5.3.3.1.4 Eventing / Alerting / Notification Services

Property Name	Description
Identification	Eventing / Alerting / Notification Services
Classification	IS
Behaviour	This Alert/notification Services propagates incoming alerts, incoming notifications and incoming events from external sources via NCOP services by raising User Notifications. This mechanism is based on subscriptions (Publication-subscription) implemented in the NCOP Web Services component as “NCOP Subscription”. This component provides a User Interface in order to maintain hierarchy of notifications per Entity. The initial hierarchy is: Base Notification; Operational Notification (raising COP User role): o TMD Notification; o COP IP Update Notification; o New COP version notification; COP Management Notification (raising COP Administrator role): o Source change notification; o COP IP change notification (for example: when a non-owned COP IP is removed when part of a owned COP); o Dissemination notification; Technical Notification (raising Enterprise Administrator role): o Synchronisation notification; Internal Service error notification; NCOP allows managing: Notification preferences by each individual user. User shall subscribe/unsubscribe to notifications; Notification preferences by Node administrators.
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 Application Server
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	TypeScript/JavaScript

Property Name	Description
	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

NCOP supports several means of conveying notification to users:

On-screen display via the end-user application;

- Highlight of BSOs involved by a notification;
- In a Information Panel as a rolling list;

Using existing workstation software (such Bi-SC AIS Core Chat clients);

On-screen display via the management interfaces;

Messages sent to and handled by the Bi-SC AIS Core Informal Messaging service for further distribution;

5.3.3.1.4.1 Publish/subscribe event-driven mechanism

The NCOP Alert/Notification system is based on a publish/subscribe mechanism: Users subscribe to specific alerts or alert categories and will be notified when the system generate these alerts.

NCOP Alert/Notification services are made of the following elements:

- A connector to receive events generated by the NCOP Events Manager,
- A database dedicated to the storage of alert/notification settings (lists of alerts users can subscribe to, users' subscriptions and pending alerts),
- A connector to send alerts/notifications to the users according to their subscriptions
- A dedicated BizTalk orchestration and connectors to send notifications using XMPP (instant messaging) and SMTP (mail) transport methods

The alert/notification service is notified by the NCOP Events Manager of all events relevant to user alerts and notifications. Users' subscriptions are taken into account to identify the users that need to be notified when an event is raised. The user preferred methods for receiving alerts is also taken into account to send the notification using the appropriate channel.

The figure below presents on overview of the NCOP alerting/notification system based on the following user selected notification methods:

	Notification reception methods		
User	Geographical COP Editor	XMPP	SMTP

User 1	Yes	No	Yes
User 2	Yes	Yes	No
User 3	No	No	Yes

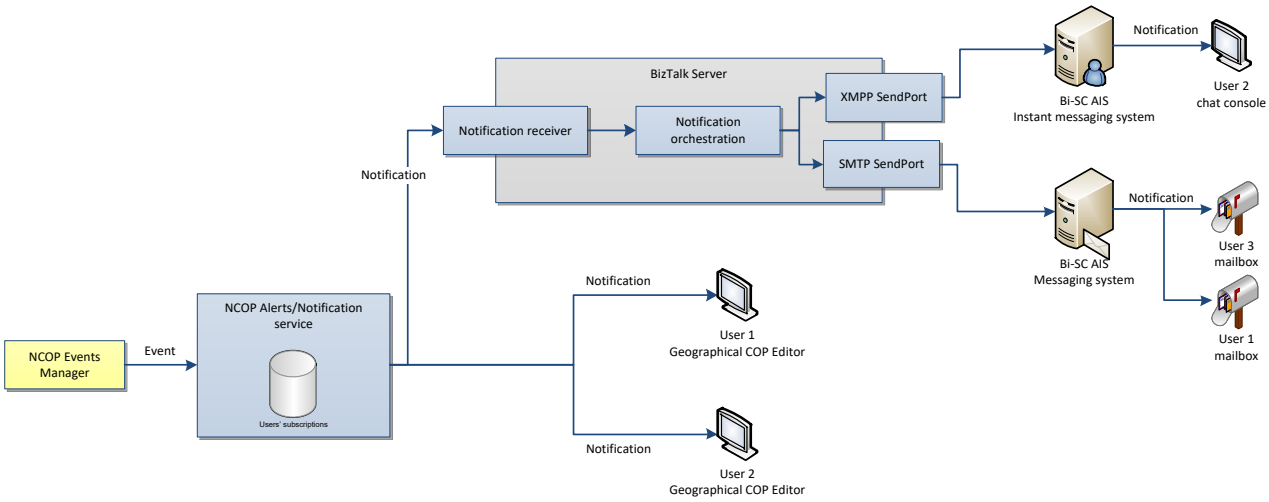


Figure 5-99: Alert/notification service overview

Notifications sent using the XMPP protocol and those sent directly to the Geographical COP Editor are emitted one by one. To avoid message flooding with e-mail notifications, the NCOP alerts and notification service buffers incoming alerts and sends an e-mail containing a batch of notifications according to the frequency defined by the user.

NCOP is not responsible of setting up the Messaging and Instant Messaging environments. NCOP notification service only declares the associated endpoints in its configuration file. The following elements are required:

- Instant messaging system
  - Server name
  - Server XMPP port
  - User account (and password) to be used by BizTalk for sending messages
- Messaging system
  - Server name
  - Server SMTP port
  - User account (and password) to be used by BizTalk for sending messages

It is required that the corresponding ports are accessible from NCOP BizTalk server.

Depending on the availability of the messaging or instant messaging infrastructure on the site were NCOP is deployed, the corresponding notification option will be functional or not.

The user accounts and passwords required for XMPP and SMTP connections are defined in the corresponding “send port” artefact in BizTalk. These credentials are encrypted and stored in the BizTalk database.

5.3.3.1.4.2 Subscriptions parameters

By default, the categories of alerts/notifications a user can subscribe to are the following:

Operational Notification ;

- TMD Notification;
- COP IP Update Notification;
- New COP version notification;

COP Management Notification ;

- Source change notification;
- COP IP change notification (for example: when a non-owned COP IP is removed when part of a owned COP);
- Dissemination notification;

Technical Notification ;

- Synchronisation notification;
- Internal Service error notification

When using the Geographical COP Editor, the alerts management menu allows an authorized user opening an HMI to create, rename, move or delete categories as well as to re-organize the Alerts/Notifications according to these categories. The hierarchical structure of the categories can then be updated.

Users that have previously subscribed to a category that is deleted are losing their subscription to this category. Users that have previously subscribed to an alert type that is moved from one category to another one are not losing their subscription to this alert type. Subscriptions to some categories can be refined by selecting an additional parameter for the subscription. It is the case for the COP and Information Products related events.

For example:

- A user that subscribes to “Information Product updated” receives a notification when any of the Information Product is updated.
- A user that subscribes to “Information Product updated” and specifying a particular Information Product receives a notification when that specific Information Product is updated.

In addition to the types of notifications, the user is able to select his preferred notification method. He can choose one or many options among the following:

- Geographical COP Editor

  Notifications will be received through the Geographical COP Editor notification widget.

- E-mail

  The user defines the mail address to be used for notifications. Notifications will be received in an e-mail sent periodically containing a summary of notifications received.

- Instant messaging

  The user defines the instant messaging address to be used for notifications. Notifications will be received as chat messages in the user's instant messaging client.

The following figure presents the UI used by NCOP users to define their subscription options

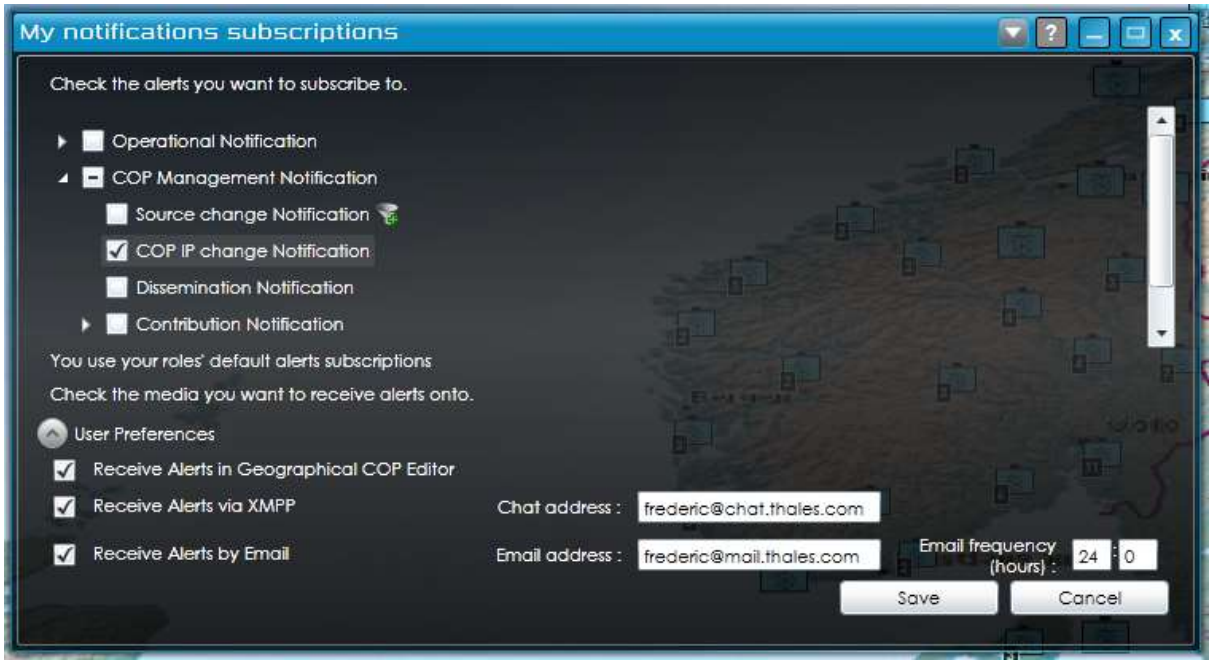


Figure 5-100: Alerts and Notification user preferences

5.3.3.1.4.3 Alert/Notification data model

Alerts and notifications data model is made of the following attributes

- Category
- Type
- Title
- Criticality

- Description
- Date

The *Category* of an alert/notification is based on its location in the alert/notification hierarchy which can be configured by a user with alerts/notification management permission.

The *Type* of an alert/notification is derived from the type of the originating event that is the source of the alert.

The *Title* of an alert/notification is a short label that allows a user to identify quickly the content of an alert.

The *Criticality* of an alert/notification is determined by the type of the originating event. Four criticalities have been identified:

- Info
- Warning
- Error
- Critical

The *Error* criticality applies to alerts/notification generated from an internal technical exception (acquisition or synchronization problem for example), whereas other criticalities apply both technical and operational events.

The *Description* of an alert/notification contains detailed information on the alert. For example, it contains the complete trace for technical errors.

The *Date* of an alert/notification refers to the date at which the originating event occurred.

5.3.3.1.4.4 Alert/Notification visualization in the Geographical COP Editor

Users are notified of alerts in a console embedded in the Geographical COP Editor. Alerts and notifications are sent using the HTTP long polling technique between the Geographical COP Editor client and the NCOP Alerts/Notifications service.

If a user is not connected to the Geographical COP Editor when a notification is emitted by the NCOP Alert/Notification service, the notifications will be stored in a pending state for this user until the user connects to the Geographical COP Editor. Therefore, when a user connects to the Geographical COP Editor, he receives the notifications and alerts that were emitted by the NCOP system since his last connection.

The following figures present how alerts/notifications are displayed in the Geographical COP Editor.

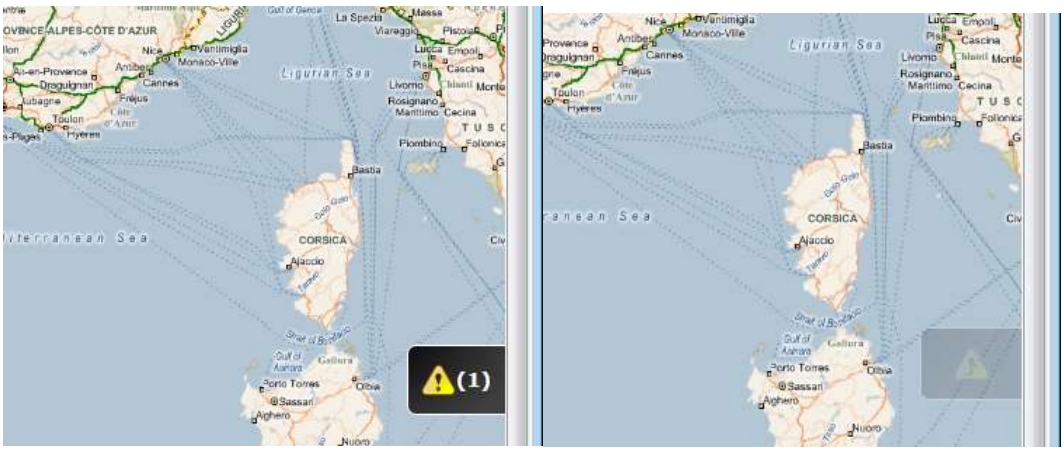


Figure 5-101: Visual notification of alerts in the Geographical COP Editor

The visual notification indicator icon is based on the highest criticality in the current list of notifications for the user. A click on this indicator allows the user to expand a panel displaying the list of incoming alerts/notifications.

In this panel, the alerts/notifications are grouped, based on the alert/notification title to avoid having multiple entries for the same alert/notification.

This panel allows the user to activate the display of incoming alerts/notifications using small pop-up panels that describe shortly the title and content of this alert/notification.

Each Alert/Notification entry in this panel proposes the following actions to the user:

- Discard
- Acknowledge
- View details
- Delete

The “view details” action displays detailed information for the specified alert/notification, allowing the user to visualize previous alerts/notifications.

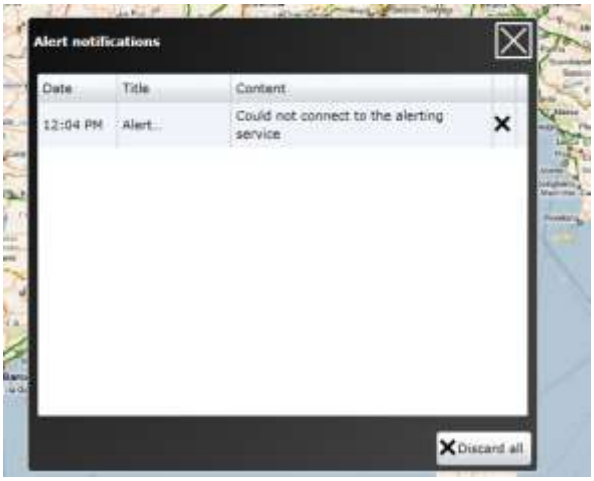


Figure 5-102: Alerts content panel displayed in the Geographical COP Editor

NCOP offers the capability to display notifications like incoming messages in Outlook. This temporary panel displays a short description of the incoming alert and fades out after a few seconds. A click on this notification panel opens the details panel of the corresponding incoming alert:

Figure 5-103: Incoming Alerts quick display panel

NCOP implementation for the publish/subscribe message exchange pattern is based on WS-Eventing and WS-Notification specifications.

Publish/subscribe implementation details are available in sections §5.4.9 (overview for publish/subscribe implementation for Alerts/Notifications, NCOP IPS service and NCOP node synchronization) and 6.2.1.1 (focus on NCOP node synchronization mechanisms) of this document and additional details are provided in the NCOP [ICD].

5.3.3.1.5 Microsoft SQL Server Reporting Services

Property Name	Description
Identification	Microsoft SQL Server Reporting Services
Classification	TI
Behaviour	SQL Server Reporting Services is a server-based reporting platform that provides comprehensive reporting functionality.
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 SQL Server
Interfaces	This IC interacts with SQL Server databases
Collaboration mechanism	-
Local/Configuration data	-

Property Name	Description
Operating context	SQL
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

5.3.3.2 Support

5.3.3.2.1 Event Manager

Property Name	Description
Identification	Event Manager
Classification	IS
Behaviour	This component is responsible for the propagation of NCOP internal events to other NCOP components that will react accordingly. Events are raised by the following: • NCOP Web Services, • NCOP Storage • BizTalk The target components are the following: • Synchronization Manager • Alerting Manager • Publication Manager
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 Application Server
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	TypeScript/JavaScript .NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

5.3.3.2.1.1 Overview

Because NCOP uses an event-driven architecture, an internal component is dedicated to the management of events. This component is the central element that receives events raised by the NCOP infrastructure when something significant occurs (a COP is created, an Information Product is deleted, etc.).

The following NCOP components are able to generate events:

- BizTalk
- NCOP Storage
- NCOP Web services

BizTalk generates events related to data acquisition

The NCOP Storage component generates events related to actions on information elements (COPs, Information Products, etc.)

NCOP synchronization service generates events related to synchronization data exchange.

A single event can be the trigger for different actions, involving different components of the system. Therefore, once an event is raised, the NCOP Events Manager will notify the appropriate NCOP service for further processing.

An overview of the Event managing system is described in the following figure:

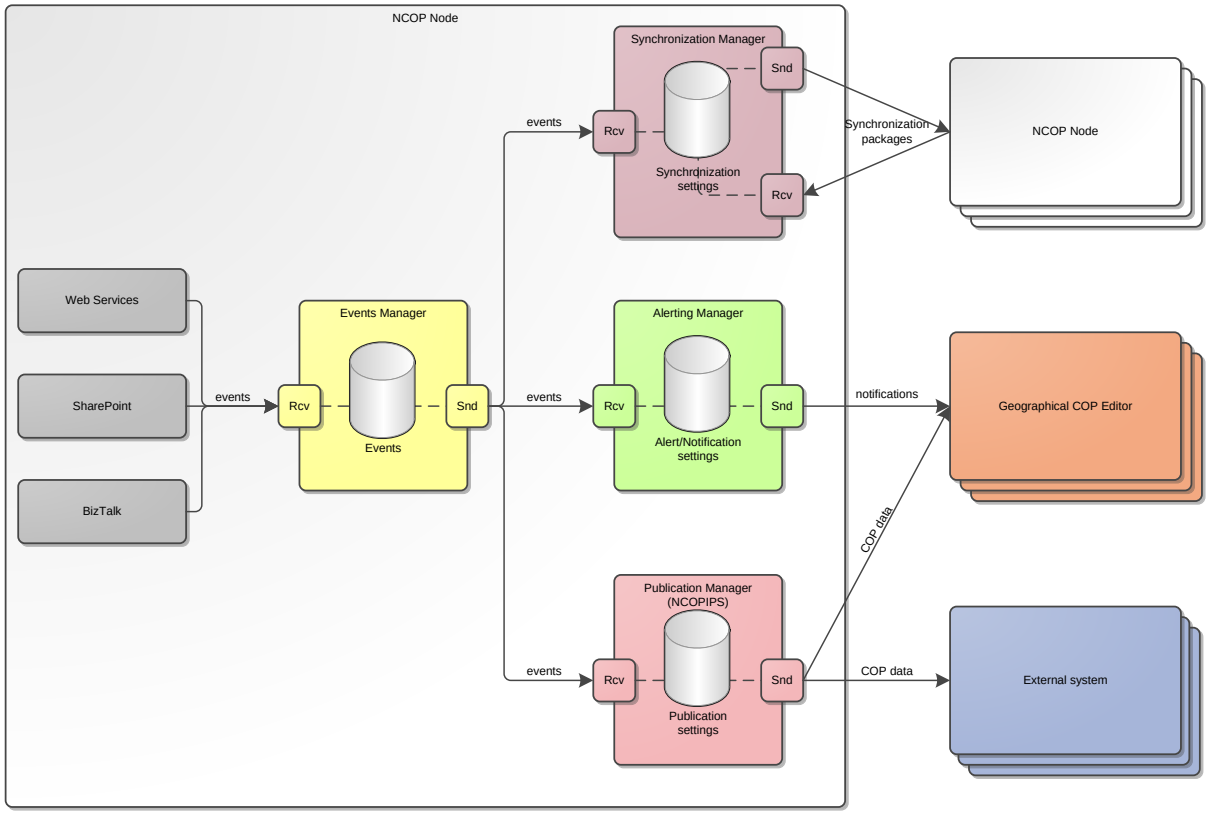


Figure 5-104: Event Managing system overview

5.3.3.2.1.2 Events lists

The following table lists the events generated by the NCOP system. It also describes the components that are notified with the event:

TABLE 5-7: EVENTS GENERATED BY NCOP

Event type	Initiator	Alert/Notif.	Synchronization	Publication
COP created	NCOP Storage	X	X	X
COP modified	NCOP Storage	X	X	X
COP deleted	NCOP Storage	X	X	X
Domain value created	NCOP Storage	X	X	-
Domain value changed	NCOP Storage	X	X	-
Domain value deleted	NCOP Storage	X	X	-
Information Product parameter created	NCOP Storage	X	X	X
Information Product parameter changed	NCOP Storage	X	X	X
Information Product parameter deleted	NCOP Storage	X	X	X
Information Product Status changed	NCOP Storage	X	X	X

Event type	Initiator	Alert/Notif.	Synchronization	Publication
Map created	NCOP Storage	X	X	-
Map changed	NCOP Storage	X	X	-
Map deleted	NCOP Storage	X	X	-
Shared view created	NCOP Storage	X	X	X
Shared view changed	NCOP Storage	X	X	X
Shared view deleted	NCOP Storage	X	X	X
Source created	NCOP Storage	X	X	-
Source changed	NCOP Storage	X	X	X
Source deleted	NCOP Storage	X	X	-
Security classification created	NCOP Storage	X	X	-
Security classification changed	NCOP Storage	X	X	-
Security classification deleted	NCOP Storage	X	X	-
Data Acquisition Error	BizTalk	X	-	-
Source capabilities changed	BizTalk	X	-	-
Information Product content changed	BizTalk	X	-	X
Dissemination parameter changed	NCOP Storage	X	X	
Shared View pending	NCOP Storage	X	-	-
Shared View approved	NCOP Storage	X	-	-
Shared View rejected	NCOP Storage	X	-	-
Annotation pending	NCOP Storage	X	-	-
Annotation approved	NCOP Storage	X	-	-
Annotation rejected	NCOP Storage	X	-	-
Information Product Contribution pending	NCOP Storage	X	-	-
Information Product Contribution approved	NCOP Storage	X	-	-
Information Product Contribution rejected	NCOP Storage	X	-	-

Event type	Initiator	Alert/Notif.	Synchronization	Publication
Information Product parameter pending	NCOP Storage	X	-	-
Information Product parameter approved	NCOP Storage	X	-	-
Information Product parameter rejected	NCOP Storage	X	-	-
COP pending	NCOP Storage	X	-	-
COP approved	NCOP Storage	X	-	-
COP rejected	NCOP Storage	X	-	-
Synchronization notification	Synchronization service	X	X	-
Internal service error	NCOP Web services	X	-	-

5.3.3.2.2 Microsoft SharePoint

Property Name	Description
Identification	Microsoft SharePoint
Classification	TI
Behaviour	This component is standard functionality in the Microsoft Windows Server 2019 platform. Microsoft SharePoint is the cornerstone of the collaborative solution for the NCOP system. The main services provided by SharePoint (latest version identified as SharePoint 2019) are as follows: A storage and collaboration infrastructure: SharePoint supplies Web sites (called SharePoint sites) for team collaboration with document storage and retrieval with check-in and check-out functionality, version history, custom metadata, and customizable views. Team members can find and share data, with the added assurance that data will not be lost. Information-sharing tools: In addition to documents, SharePoint sites can store tasks, event calendars, contacts, Web links, discussions, announcements, and more. SharePoint sites are places that help team members share information and get work done, not just a place to save files. Workflows to attach a business process to items maintained in SharePoint sites and control their life cycle. Workflows can either be initiated by the user or automatically initiated by SharePoint based on some event, such as when an item is created or changed. Workflows can interact directly with the user through workflow forms that allow gathering information at each stage of the workflow. SharePoint workflows rely on the Windows Workflow Foundation (WWF) programming model and engine included in the .NET Framework. They are developed using graphic tools (Visual Studio Designer for WFF) that allow building workflow-enabled applications on Windows. Integration with Microsoft Office System: Thanks to the Web services provided by SharePoint, applications of the Microsoft Office Suite - including Word, Excel, PowerPoint - can use information in SharePoint sites natively. Applications of the Microsoft Office Suite allow users to add members to sites, assign tasks, and communicate with members, all while working on documents stored in SharePoint sites. With Outlook, users can view calendars and contact lists

Property Name	Description
	stored on SharePoint sites and can create and manage sites devoted to editing documents and organizing meetings. A foundation platform for building new Web-based applications and services: By using the Web Parts Infrastructure included in the .NET Framework, and the SharePoint Software Development Kit (SDK), new Web-based applications and Web services can be developed extending those natively provided by SharePoint sites.
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
Interfaces	This IC interacts with SQL Server databases This IC interacts with ADFS for user authentication (SAML) This IC interacts with AD for user authentication (Kerberos)
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

For full-text search capabilities, the NCOP system uses the Search Server add-on for SharePoint.

The Search Server is configured to index the information products stored in the Information Products Instances document library (containing the information products in the CDF format). The indexing process is configured as incremental which means that the index is updated regularly take into account the latest updates in the document library.

The users can access and use the search engine from the SharePoint web site.

As the NCOP system can manage different work environment (e.g. Operational, Training, and Exercise), each data storage corresponding to each SharePoint site collections are indexed by the Search Server add-on. However, when a user uses the search engine, the search will be performed on the information products stored in the work environment in which the user has logged in.

For example, if a user logged in the Training environment performs a search, the search engine will return documents that are stored in the Training environment storage.

The search results will contain only the documents that the user has the permissions to view according to the security settings.

5.3.3.2.3 Authentication and Authorization Services (RBAC)

Property Name	Description
Identification	Authentication and Authorization Services (RBAC)
Classification	IS
Behaviour	This component is composed of a subset of API and a Web Service allowing the implementation of role based access control to NCOP applications and to the data managed through these applications. NCOP applications and some NCOP services rely on this component to offer user functionality and user access to data in accordance with the access rights policy established by the Organizational Node Administrator role for the user's role. This Implementation Component deals only with user roles in the context of NCOP. User authentication to validate user credentials against a local or external identity provider; Authentication service for locally-managed users; Enable usage of the COP Client with no user authentication (non-recognized user). In this mode, a default role using a default level of access according to the Security Classification of the Node within the Security Domain is to be set.
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
Interfaces	This IC interacts with ADFS for user authentication (SAML) This IC interacts with AD for user authentication (Kerberos)
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework TypeScript/JavaScript
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

For NCOP Inc-1, user authentication is implemented through Integrated Windows authentication and Kerberos or NTLM tokens. User authorization is based on the implemented through the RBAC and ABAC mechanisms. The Kerberos delegation is limited only to the needed services in application of the least privilege principle.

For NCOP Increment-2, user authentication and authorization will be based on Kerberos and SAML tokens and the ADFS infrastructure.

Implementation details for the Authentication and Authorization Manager are provided in the design discussion topics at chapters 5.4.14 (Access-rights management across NCOP nodes), 5.4.17 (Anonymous access to NCOP), 5.3.3.2.3 (Authentication and Authorization Services (RBAC)) and 5.4.21.1 (HTTP access) and also in the NCOP SSDS.

NCOP guarantee that end-users have access to system functionality in accordance with access rights associated to their role. The following roles have predefined permissions:

NCOP Functional Administrator role (identified for each mission/domain) is:

- Responsible for local User management, domain value management, services configuration for that particular NCOP organizational node;
- Responsible for adapting and localising workflow sequences;
- Responsible for guiding and controlling processes implementation;
- Able to assign User permissions on Services, COP or COP Information Products and functions (e.g., Read, Create, Modify and Delete) for that particular Organizational Node;
- Able to perform content management functions.
- Responsible for overall management and administration of the system, including both technical and procedural aspects.
- Able to create, provide documentation and enforce the operating policies and procedures associated with functional system such as:
- Configuration;
- Domain management;
- User access and privilege management;
- Data stewardship;
- Workflow management;
- Identification and resolution of functional issues.
- Responsible for overseeing development and maintenance of Standard Operating Procedures (SOPs) and coordination with Organizational Node Administrator role users, etc.
- In charge of:
- Enterprise domain management;
- Collection of performance and accounting data;
- Ensuring security mechanisms are working;
- Responsible for identifying standard production workflow sequences.

NCOP System Administrator role is a technical role:

- Responsible for services deployment, system and network technical issues;
- Responsible for ensuring the proper configuration, network connectivity and recoverability of the system;
- Responsible for network and domain management such as:
- Back-up and recovery of file systems and databases;
- Administration of NCOP applications and servers;
- (Re) installing the system as required.

NCOP Manager role can access to all services and all services permissions. This role can be assumed centrally for one or several missions and therefore for one or several COPs.

NCOP Contributor role can access to services for submitting contribution and COP User role permissions.

NCOP Advanced User role can access to the End-user application (as the Geographical COP Editor) and associated advanced Services to use the COPs.

NCOP User role can access to the End-user application (as the Geographical COP Editor) and associated Services to use the COPs.

Default role for non-recognized user.

5.3.3.2.3.1 NCOP permissions management

In order to implement the different NCOP roles, the NCOP system defines a set of NCOP Permissions. Those permissions are associated with the basic functionalities that are accessible to the users of the NCOP system. The permissions identified are the following:

Permission	Description
Design COPs	Allows a user to : • create, modify, delete COPs • create, modify, delete structure templates • create, modify, delete Information Product sources • create, modify, delete Information Products parameters
View COPs	Allows a user to browse the available COPs and display their content.
Create contributions	Allows a user to : • Create annotations, • Create views, • Create user Information Products (manual augmentation of the COP) • Submit these contributions for inclusion into a COP
Approve contributions	Allows a user to approve or reject user contributions (e.g. Annotations, views and user Information Products).
Manage roles	Allows a user to: • Create, modify, delete NCOP roles.

Permission	Description
	• Associate the roles with NCOP permissions
Manage permissions	Allows a user to associate permissions to users by giving them one or multiple roles
Publish COPs	Allows a user to publish COP to become visible from the consumers.
Access Business Activity Monitoring	Allows a user to visualize the Business Activity Monitoring reports.
Manage domain values	Allows a user to create, modify, delete domain values such as security classifications, information products domains and categorizations.
Backup/restore	Allows a user to achieve backup & restore operations on the NCOP system.
Archive Restore COPs	Allows a user to create COP archives and restore them.
Mission architecture	Deprecated
Dissemination settings	Allows a user to select the data to be visible from other entities.
Synchronization settings	Allows a user to configure the synchronization process by : • selecting the data to be synchronized • selecting the synchronization partners
Secured Pages Access	TBC
Alert Notification Management	TBC

These NCOP permissions are implemented as SharePoint security groups. They are used to restrict access on SharePoint lists and document libraries. They are also used to configure the availability of COP related information panels in the Geographical COP Editor.

5.3.3.2.3.2 NCOP roles management

The NCOP high level roles are managed as groups in the NCOP Directory.

Therefore, the NCOP system allows the creation and customization of roles by associating them with permissions using the native SharePoint security mechanisms.

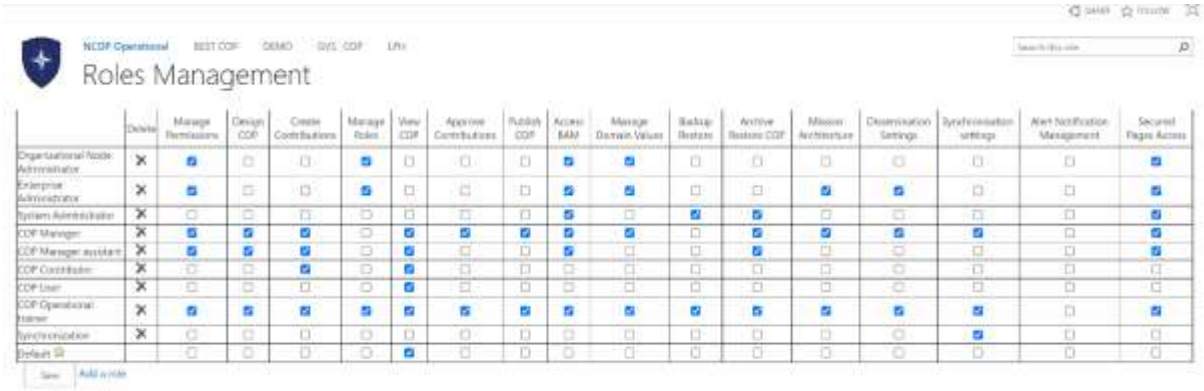


Figure 5-105: Assignment of permissions to roles

The following table describes the factory settings of roles and associated permissions for the NCOP system for Increment-1. *This table will be updated in a future version of this document.*

TABLE 5-8: FACTORY SETTINGS OF ROLES AND ASSOCIATED PERMISSIONS

		NCOP PERMISSIONS													
		Design COPs	Create contributions	Manage roles	Manage permissions	View COP	Approve contributions	Publish COP	Access BAM	Manage domain values	Backup / Restore	Archive COPs	Mission Architecture	Disseminination settings	Synchronisation settings
Organizational Node Administrator		No	No	Yes	Yes	yes	No	No	Yes	Yes	No	No	No	No	Yes
	is responsible for local User management (if applicable), domain value management and services configuration for that particular NCOP organizational node. The Organizational Node Administrator role is also responsible for adapting and localising workflow sequences, guide and control processes implementation. Organizational Node Administrator role is able to assign User permissions on Services, COP or COP Information Products and functions (e.g., Read, Create, Modify and Delete) for that particular Organizational Node. Organizational Node Administrator role will have the capability to perform content management functions.														
Enterprise Administrator		No	No	Yes	Yes	yes	No	No	Yes	Yes	No	No	Yes	Yes	Yes
	is responsible for overall management and administration of the system, including both technical and procedural aspects. In general, the Enterprise Administrator role is identified for each mission/domain. Procedural and administrative responsibilities of the Enterprise Administrators include the creation, documentation and enforcement of operating policies and procedures associated with functional system configuration; domain management; User access and privilege management; data stewardship; workflow management; and identification and resolution of functional issues. Enterprise Administrator role is responsible for overseeing development and maintenance of Standard Operating Procedures (SOPs) and coordination with Organizational Node Administrator role users, etc. The technical responsibilities of Enterprise Administrators include enterprise domain management; collection of performance and accounting data; and ensuring security mechanisms are working. Enterprise Administrators are also responsible for identifying standard production workflow sequences.														
System administrator		No	No	No	No	yes	No	No	Yes	No	Yes	Yes	No	No	No
	Is a technical role, generally an NCSA Sector or other local CIS support personnel fulfilling that role, responsible for services deployment, system and network technical issues in liaison with local CIS personnel, and for ensuring the proper configuration, network connectivity and recoverability of the system. Responsibilities of the System Administrator role include network and domain management; back-up and recovery of file systems and databases; and administration of NCOP applications and servers. System administrators are responsible for (re)installing the system as required.														
COP Manager		Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
	Role that can access all services and all services permissions. This role can be assumed centrally for one or several missions and therefore for one or several COPs. Functional role description is part of AD-8080 [Ref 3].														
COP Manager assistant		Yes	No	No	Yes	Yes	No	No	Yes	No	No	Yes	No	No	No
	Role that can access all services and all services permissions excluding validation permissions. Ideally, this role is focusing on a single COP and the assignment limited to a single Entity. Functional role description is part of AD-8080 [Ref 3]														
COP Contributor		No	Yes	No	No	Yes	No	No	No	No	No	No	No	No	No
	Role that can access services for submitting contribution and COP User role permissions. Functional role description is part of AD-8080 [Ref 3]														
COP User		No	No	No	No	Yes	No	No	No	No	No	No	No	No	No
	Role that can access the End-user application and associated Services to use the COPs. Functional role description is part of AD-8080 [Ref 3]														
COP Operational trainer		Training	Training	Training	Training	Training	Training	Training	Training	Training	Training	Training	Training	Training	Training
	Role that can access all Services for training and support purpose. This role is envisioned to be fulfilled only by NATO personnel such as JWC, NC3A, JFTC personnel. Functional role description is part of AD-8080 [Ref 3]														

Assigning roles to user is made by adding the user as a member of the corresponding role groups in the NCOP directory.

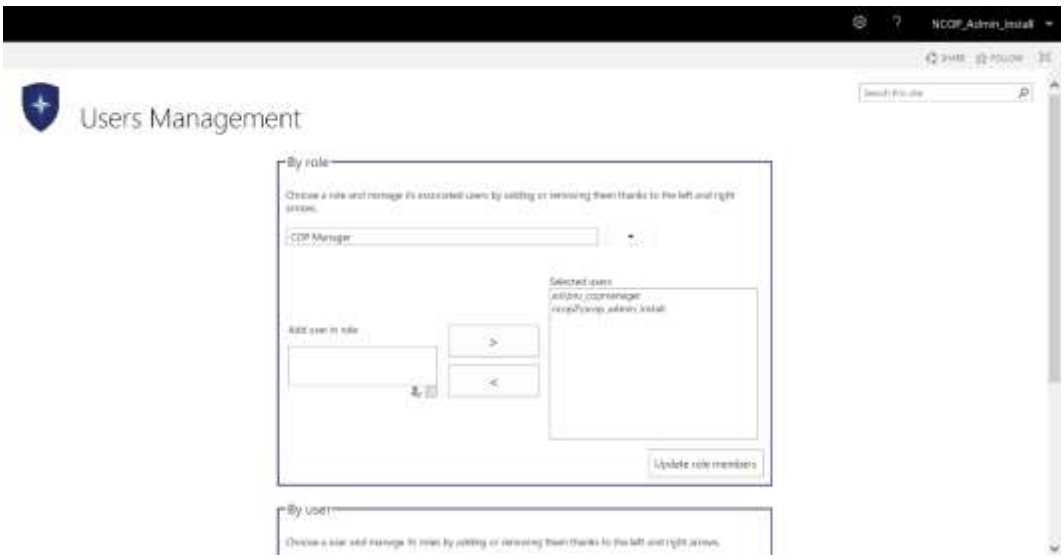


Figure 5-106: Assignment of users to roles

One of the roles in NCOP is identified as the Default Role. The purpose of this role is to give permissions to users that have not been explicitly associated with a role.

5.3.3.2.3.3 Union of roles

NCOP has the capability to create roles that are described by the union of existing roles. In this case the permissions associated to newly created role are the aggregation of the permissions associated with each constituting role.

This union of role is managed by NCOP dynamically, meaning that if a constituting role is modified with new or deleted permissions, any role that was based on this constituting role will have his permissions modified accordingly.

NCOP does not allow the creation of roles based on the union of roles that are already based on the union of roles.

5.3.3.2.3.4 User permissions

Using NCOP administration pages, permissions are not directly associated to users. Permissions are associated to roles and roles are associated to users. However, when a user is associated with a role, he will be granted the underlying permissions.

From a technical point of view, when a user is associated with a role, he is automatically added as a member in the SharePoint security groups that correspond to the role's permissions.

NCOP also allows a group of users to be associated with a role. This capability applies only to security groups defined in Active Directory. In this case, the group itself is added as a member of the SharePoint security groups that correspond to the role's permissions.

When a user connects to NCOP, if he is a member of a role that is a based on the union of roles, the user's permissions are evaluated by aggregating the permissions of the constituting roles and the user is added as a member of all corresponding SharePoint security groups. When a constituting role is modified, all users that were associated to this role directly or indirectly (through a union of role) will be added are removed from the SharePoint security groups accordingly to reflect the resulting permissions.

Regarding a user having multiple roles, it has been decided during an NCOP Joint Technical Review that the user will be granted the aggregation of all permissions associated with its roles.

If a user connects to NCOP and has not been explicitly associated with any role (directly or indirectly through a group), NCOP will use the default role to define its permissions.

5.3.3.2.3.5 Users, Groups , roles, and permissions relationships

The following figure presents the relationships than can exist between:

- Users,
- Groups,
- Roles,
- Permissions,
- Content

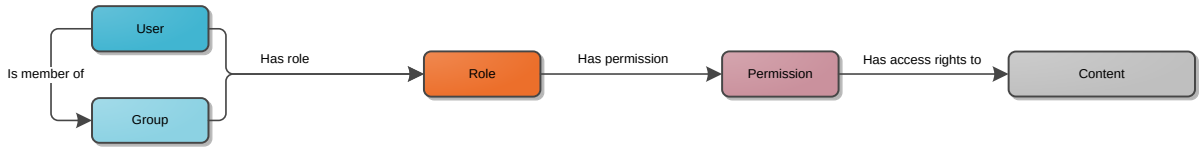


Figure 5-107: Users, Groups, Roles, Permissions relationships

The following presents a typical scenario involving all these concepts:

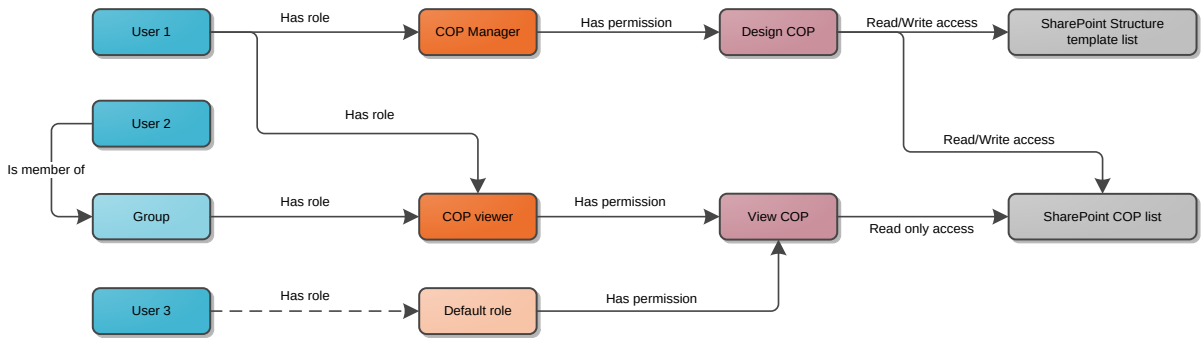


Figure 5-108: Users, groups, roles and permission sample scenario

In this scenario the users are given the following access rights:

User 1 has 2 roles (COP Manager, COP Viewer). Therefore, he is granted the View COP and Design COP permissions. These permissions gives him read/write access to the SharePoint COP Structure templates list, and also read/write access to the SharePoint COP list (when a user has multiple permissions, low-level access rights (read, write, delete) are cumulated)

User 2 is a member of Group. Since this group has the COP Viewer role and this role has the View COP permission, when User 2 connects to NCOP he will be granted a read/only access to the SharePoint COP list and will have the View COP permission because he is a member of Group.

User 3 has no role (directly or indirectly through a group membership). Therefore when he connects to NCOP he is associated with the NCOP roles and will have the View COP permission associated with this default role. It allows him to be granted a read only access to the SharePoint COP list.

5.3.3.2.3.6 RBAC management in multiple environments

When multiple environments are available simultaneously on a NCOP node, the NCOP system handles the roles management in a way that will allow a user to have different roles depending on the data he accesses. For example, a user can access operational data with a “COP contributor” role and he can access the training data with a “COP Manager” role.

In order to allow this, the NCOP roles are defined for each work environment.

Also each SharePoint site collection stores and manages its own NCOP permissions that will apply to their specific data.

The following picture presents the different items involved in the RBAC mechanism and depicts how the roles and permissions are handled in a multiple mode configuration (e.g. operational, training and exercise modes).

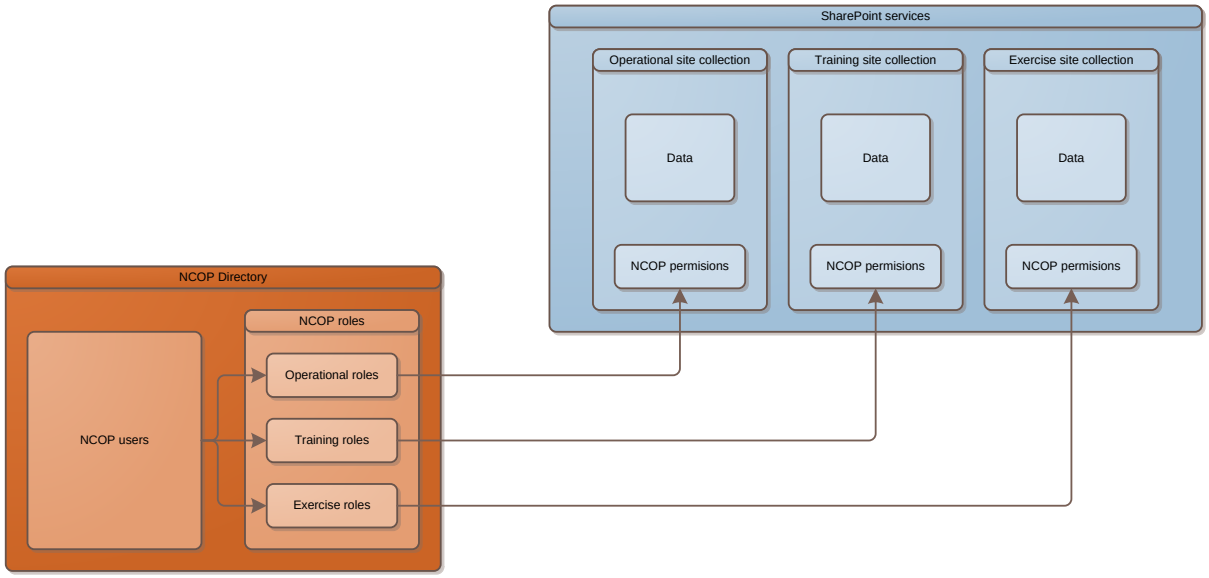


Figure 5-109: Multiple modes configuration

5.3.3.2.4 Security Classification Manager and Cross Domain Manager

Property Name	Description
Identification	Security Classification & Cross Domain Manager
Classification	IS
Behaviour	Security Classification Manager is used by all NCOP services in order to create the security labels. NCOP Web Services includes a Security Classification to determine the sensitivity of the data that is sent. This label is used by XML guards and NATO Information Exchange Gateway (IEG) in cross domain data exchange. Cross Domain Manager supports: Cross-security domain information exchange; Cross-security domain for all spatially-distributed services and external services; Cross-domain management is necessary when NCOP is used in a distributed environment for creating and feeding the Information Products from various sources spread across different Security Domains.
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
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework TypeScript/JavaScript
References	-

Property Name	Description
Quality of Service requirements (QoS)	
Complexity	Medium

The Security Classification Manager is responsible for including the Security labels:

- In the SOAP header of web services messages exchanged between two nodes in different security domains.
- In the CDF itself, before the data is stored in the NCOP Storage component

Regarding the SOAP header of web services messages exchanged, the Security Classification labels are included in the following scenarios (STANAG 4774 [Confidentiality labelling]):

- When NCOP retrieves Information Products from a source
- When NCOP exposes the COP and Information Products to consumers
- When an NCOP node synchronizes its data with a remote NCOP node

Depending on the nature of the requests and responses, different Security Classification labels are set in the SOAP headers. NCOP strategy for defining Security Classification labels is based on the following principles:

- Security Classification label is set to “UNMARKED” if the message is technical or does not contain any data
- Security Classification label is based on the Security Classification of the content if the message contains data

This strategy applies to both requests and responses produced by an NCOP node.

Example of Security Classification label set to UNMARKED:

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
   <s:Header>
      <wsse:Security      xsi:schemaLocation="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd"
actor="http://schemas.xmlsoap.org/soap/actor/XMLGUARD"                    mustUnderstand="1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"        xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
         <MetadataBindingContainer
xsi:schemaLocation="urn:int:nato:ia:metadatabinding:draft..\schemas\MetadataBindingContaine
r-v1d3.xsd"    Id="MetadataBindingContainer"    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="urn:int:nato:ia:metadatabinding:draft">
            <MetadataBinding>
               <Metadata metadataType="OriginatorConfidentialityLabel">
                  <ConfidentialityLabel
xsi:schemaLocation="urn:int:nato:ia:xmlsecuritylabel:draft..\schemas\ConfidentialityLabel-
v1d7.xsd" xmlns="urn:int:nato:ia:xmlsecuritylabel:draft">
                     <ConfidentialityData>
                        <PolicyIdentifier>NATO</PolicyIdentifier>
                        <Classification>UNMARKED</Classification>
                        <Category Type="PERMISSIVE"/>
                     </ConfidentialityData>
                  </ConfidentialityLabel>
               </Metadata>
               <DataReference URI=""/>
            </MetadataBinding>
         </MetadataBindingContainer>
```

```
      </wsse:Security>
   </s:Header>
```

Example of Security Classification label based on the Security Classification of the content (NATO UNCLASSIFIED):

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
   <s:Header>
      <wsse:Security      xsi:schemaLocation="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-utility-1.0.xsd"
actor="http://schemas.xmlsoap.org/soap/actor/XMLGUARD"                    mustUnderstand="1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"        xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
         <MetadataBindingContainer
xsi:schemaLocation="urn:int:nato:ia:metadatabinding:draft..\schemas\MetadataBindingContaine
r-v1d3.xsd"    Id="MetadataBindingContainer"    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="urn:int:nato:ia:metadatabinding:draft">
            <MetadataBinding>
               <Metadata metadataType="OriginatorConfidentialityLabel">
                  <ConfidentialityLabel
xsi:schemaLocation="urn:int:nato:ia:xmlsecuritylabel:draft..\schemas\ConfidentialityLabel-
v1d7.xsd" xmlns="urn:int:nato:ia:xmlsecuritylabel:draft">
                     <ConfidentialityData>
                        <PolicyIdentifier>NATO</PolicyIdentifier>
                        <Classification>UNCLASSIFIED</Classification>
                        <Category Type="PERMISSIVE"/>
                     </ConfidentialityData>
                  </ConfidentialityLabel>
               </Metadata>
               <DataReference URI="">
                  <Transforms xmlns="http://www.w3.org/2000/09/xmldsig#">
                     <Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
                        <XPath>//*[local-name()='SimpleData'         and          ./*[local-
name()='SimpleData' and text()='3faec399-313d-4660-bb29-e78770e8a804']]</XPath>
                     </Transform>
                  </Transforms>
               </DataReference>
            </MetadataBinding>
            <MetadataBinding>
               <Metadata metadataType="OriginatorConfidentialityLabel">
                  <ConfidentialityLabel
xsi:schemaLocation="urn:int:nato:ia:xmlsecuritylabel:draft..\schemas\ConfidentialityLabel-
v1d7.xsd" xmlns="urn:int:nato:ia:xmlsecuritylabel:draft">
                     <ConfidentialityData>
                        <PolicyIdentifier>NATO</PolicyIdentifier>
                        <Classification>UNMARKED</Classification>
                        <Category Type="PERMISSIVE"/>
                     </ConfidentialityData>
                  </ConfidentialityLabel>
               </Metadata>
               <DataReference URI=""/>
            </MetadataBinding>
         </MetadataBindingContainer>
      </wsse:Security>
   </s:Header>
```

5.3.3.2.5 NCOP Directory

Property Name	Description
Identification	NCOP Directory
Classification	IS
Behaviour	This component provides application directory services for storing and maintaining the configuration data of the NCOP system. NCOP users, roles and associated access rights to NCOP data and applications are the main configuration data centrally managed by this component. This component is based on SQL Database.
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 SQL Server
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	SQL
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

5.3.3.3 Transformation

5.3.3.3.1 Microsoft BizTalk

Property Name	Description
Identification	Microsoft BizTalk
Classification	TI
Behaviour	This component is standard functionality in the Microsoft Windows Server 2019 platform. The main services provided by BizTalk 2020 are as follows: **Messaging**. The BizTalk Messaging Engine: o Receives inbound messages; o Parses inbound messages to identify their specific formats; o Evaluates message content to identify how the message is to be routed and processed; o Delivers messages to their respective destinations; o Tracks the status and state of documents. **Orchestration**. BizTalk orchestration is a flexible and powerful capability that provides various services and tools to enable to: o Design business processes by using the BizTalk Orchestration Designer tool; o Automate business processes by using the BizTalk Orchestration Engine; o Manage business processes. **Business Rules Framework** is a stand-alone .NET-compliant class library that includes a number of modules, support components, and tools. The primary modules include: o The Business Rule Composer for constructing policies; o The Rule Engine Deployment Wizard for deploying policies created in the Business Rule Composer; o The Run-Time Business Rule Engine that executes policies on behalf of a host application. **Business Activity Monitoring (BAM)**. Business Activity Monitoring (BAM) in BizTalk Server allows monitoring and analyzing data from business process information sources in real time. By using BAM, users can get information about business state, trends, and critical conditions; BAM activities and BAM views allow the customization of activity report: o BAM activities: to indicate the needed data to collect for reports, administrator must define a BAM activity; o BAM views: administrator must define how to present the information to users. Using BAM, the Enterprise Administrator role can monitor business metrics as well as IT metrics (for example, SLA and execution times).
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 BizTalk Server
Interfaces	This IC interacts with SQL Server databases
Collaboration mechanism	-
Local/Configuration data	-

Property Name	Description
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

The following figure shows the BizTalk Server Administration Console.

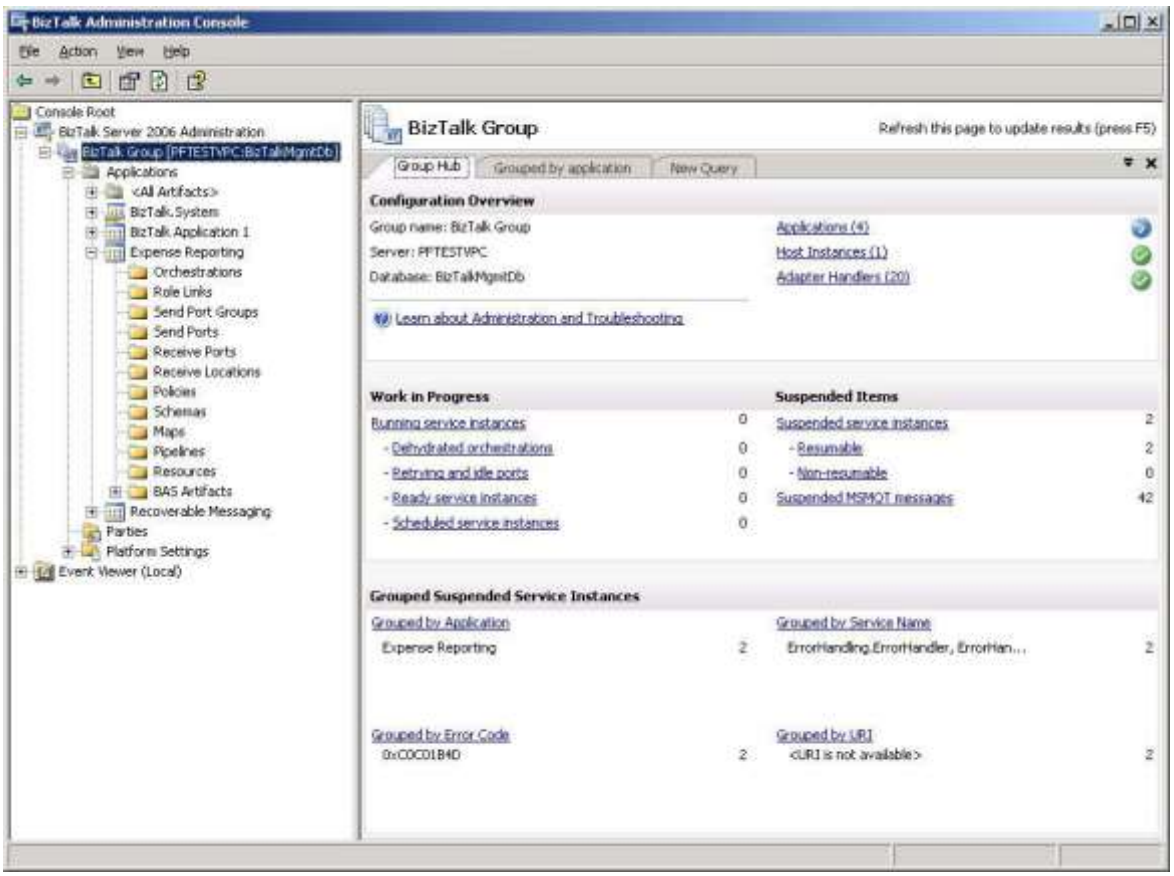


Figure 5-110: BizTalk Administration console

The BizTalk Administration console allows managing the following artefacts:

BizTalk Group. The BizTalk Group node in the console tree contains additional nodes that represent the artefacts (BizTalk applications, parties, and platform settings) for that BizTalk group. BizTalk groups are units of organization that usually represent enterprises, departments, hubs, or other business units that require a contained BizTalk Server implementation. A BizTalk group has a one-to-one relationship with a BizTalk Management database. In the case of NCOP, there will be only one BizTalk Group.

Orchestration. An orchestration is designed by using Orchestration Designer and is deployed to the BizTalk group under which it appears in the Administration console.

In the case of NCOP, orchestrations are used for the sequencing of technical steps in the BizTalk flow of the CDF data in the “pull” and “push” mode.

Role Links. A role link defines the relationship between roles by defined by the message and port types used in the interactions in both directions. These artefacts are not used in the case of NCOP.

Send port groups. A send port group is a named collection of send ports that can be used to send the same message to multiple destinations in a single configuration. These artefacts are not used in the case of NCOP.

Send ports. A send port is a BizTalk object that sends messages. In NCOP, these artefacts are used for sending Request/Response to sources in order to get the CDF data in the “pull” mode.

Receive ports. A receive port is a logical grouping of similar receive locations. In NCOP, these artefacts are used for the Scheduler as well as the one-way logical receive endpoints in order to get the CDF data in “push” mode. A Receive port contains one or many receive location detailed below.

Receive locations. A receive location is defined as a specific address at which inbound documents arrive combined with a BizTalk Server pipeline that processes the messages received at that address. In NCOP, the receive locations implements the technical endpoints used in the “push” mode.

Policies. A policy is a versioned collection of business rules. These are not used in the case of NCOP.

Schemas. A schema is the structure for a message. A schema can contain multiple sub schemas. These are used for the XML definition of the messages that are handled in BizTalk. Used in the case of NCOP.

Maps. A map is an XML file that defines the correspondence between the records and fields in one specification and the records and fields in another specification. A map contains an Extensible Stylesheet Language (XSL) stylesheet that is used by BizTalk Server to perform the transformation described in the map. In NCOP, maps are used for transferring the incoming messages’ format to the SharePoint interpretable NVG format.

Pipelines. A pipeline is a software infrastructure that defines and links one or more processing stages, running them in prescribed order to complete a specific task. Pipelines divide processing into stages, abstractions that describe a category of work. They also determine the sequence in which each category of work is performed. In NCOP, these are used for technical data processing and conversion of the messages to XML.

Resources. A resource is a script, deployed assembly, or other file associated with an application. In NCOP, all resources present will be of type “Nato.NCOP…”

5.3.3.3.1.1 BizTalk Applications

NCOP uses the following 4 BizTalk applications:

- Nato.NCOP.Gateway,
- Nato.NCOP.Source,
- Nato.NCOP.Publish,
- Nato.NCOP.Common,

These applications are provided with the NCOP system as deployable packages (.msi). No particular customization of BizTalk is required for these applications to be installed or run.

5.3.3.3.1.1.1 Nato.NCOP.Gateway

This application is dedicated to host the send ports involved in the data acquisition process. These send ports are created dynamically when a source of Information Products is declared by the COP Manager.

5.3.3.3.1.1.2 Nato.NCOP.Source

This application contains all the orchestrations needed by NCOP to acquire and transform the data of incoming Information Products into CDF.

5.3.3.3.1.1.3 Nato.NCOP.Publish

This application contains the orchestrations used to publish the Information Products into the NCOP Storage in both native and CDF format. This application also contains the orchestration dedicated to errors and logs management.

5.3.3.3.1.1.4 Nato.NCOP.Common

This application contains all the common components used by the various NCOP orchestrations. It contains the core element Nato.NCOP.Scheduler used to schedule data acquisition according to the parameters specified by the COP Manager when he defines the Sources and the Information Products. It also contains the web services used for communication of information between SharePoint and BizTalk.

Description of the Nato.NCOP.Scheduler orchestration

This orchestration hosts the heartbeat process that triggers the start of the “pull” mode interfaces.

It uses a receive location of type SQL Server that polls every second, a database table (dbo.process) that contains the list of “pull” mode interfaces and the interval delay for which it must be queried. The receive location then generates a command message that will start the corresponding Information Product interface.

From a maintenance point of view, it is important to note that he receive location “RL_Scheduler” must always be active”. In case of failure of this receive location, all the Information Product Interfaces in “pull” mode will be out of service.

Artifacts Type	Artifacts Name	Description
Receive Port	RP_Scheduler	Logical port for the scheduler receive location
Receive Location	RL_Scheduler	Technical endpoint connecting and polling the SQL database table: Uri: mssql://[sqlservername]/[database name]?InboundID=Process

5.3.3.3.1.2 Error handling

When errors occur, all error messages are routed to a dedicated error handling flow. The error handling flow logs the error message as a failure and terminates the instance. As part of its tracking mechanism, BizTalk keeps a copy of the error message but the generated message is no longer displayed in the message box. This behaviour is recommended to avoid piling-up error messages and also because a new attempt will automatically be launched shortly.

5.3.3.3.1.3 Incoming and outgoing data validation

NCOP Orchestrations can be configured to validate incoming data before processing them. The validation step is optional and can be activated or not per source. The configuration can be done at runtime.

If the validation step is activated, BizTalk analyzes the incoming message and tries to validate it against the appropriate schema. If the data is considered valid, it can be processed through all required orchestration to be converted and published in the NCOP storage. If the data is considered invalid, the data is processed anyway. In addition a warning alert is raised in order for an authorized user to get notified of the problem.

If the validation step is not activated, BizTalk will process the data without knowing if it’s valid or not: NCOP orchestrations are flexible enough to allow the processing and conversion of incoming data. It means that a specific data structure may be required by the original data schema but it can be non-critical in the acquisition process for NCOP. For example, some NCOP orchestrations are tolerant to field in wrong order or to absence of certain attributes or data elements. However, if a critical element is missing in the incoming data, it is possible that a specific processing step fails. In this case, an alert is raised in order for an authorized user to get notified of the problem that occurred in the processing step that has failed.

Regarding outgoing data validation (CDF produced by BizTalk), as for incoming data validation, it can be performed on demand by enabling the feature for the corresponding Source. If the feature is enabled on a source, all CDF data produced from the acquisition of data provided by this specific source will be validated against the XML CDF schema (based on NVG 2.0.2).

As illustrated in the figure below, BizTalk provides a graphical tool called the “BizTalk Orchestration Designer” to create and modify orchestrations. In this sample, the orchestration is consuming the NVG 1.4 Web Service, provided by a source entity.

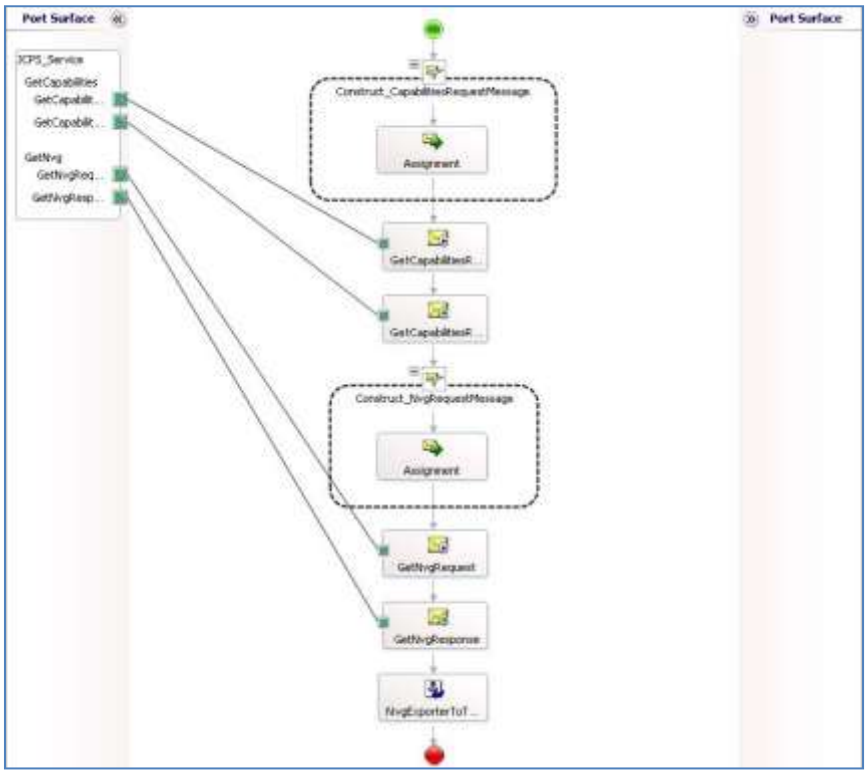


Figure 5-111: BizTalk Orchestration Designer sample: NVG 1.4 interface consumed by an orchestration

5.3.3.3.1.4 BizTalk flow: Interfaces implementation

On NCOP, BizTalk is used as a messaging service bus that collects Information Products from different sources. All data BizTalk flows are implemented using the same pattern with BizTalk capabilities where appropriate:

BizTalk Messaging: features that allow connecting to remote source or exposing service endpoints that consumer can send data to. It also manages the parsing the messages from their original format to CDF.

Orchestration: feature that is used in the solution for sequencing technical steps in the flow process steps.

BizTalk will mainly be used for getting data “in” NCOP i.e. the inbound of Information Product. This is implemented via two different patterns.

- Pull: BizTalk sends a request to the sources and get an Information Product document in response. The solution includes a scheduling mechanism as a trigger for the pull sessions.
- Push: Sources solicit BizTalk endpoints and send Information Product

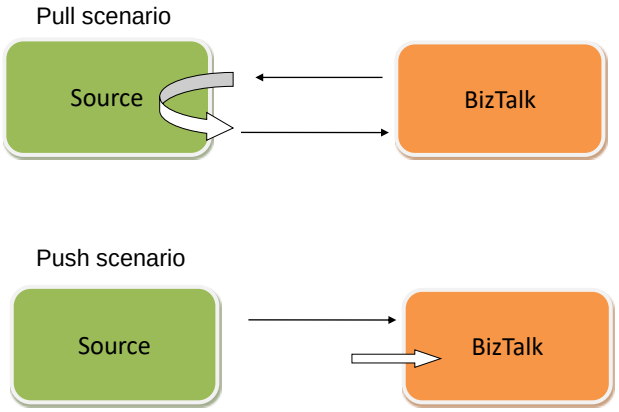


Figure 5-112 MISSING CAPTION

5.3.3.3.1.4.1 Information Product creation

The process of creating an IP (Information Product) is described below. It starts in the NCOP Web portal and involves the creation of a BizTalk entry registering the source for the data pulling phase.

In case of NATO Vector Graphics, an intermediate step of GetCapabilities is executed by BizTalk in order to obtain the available NVG filters from the source.

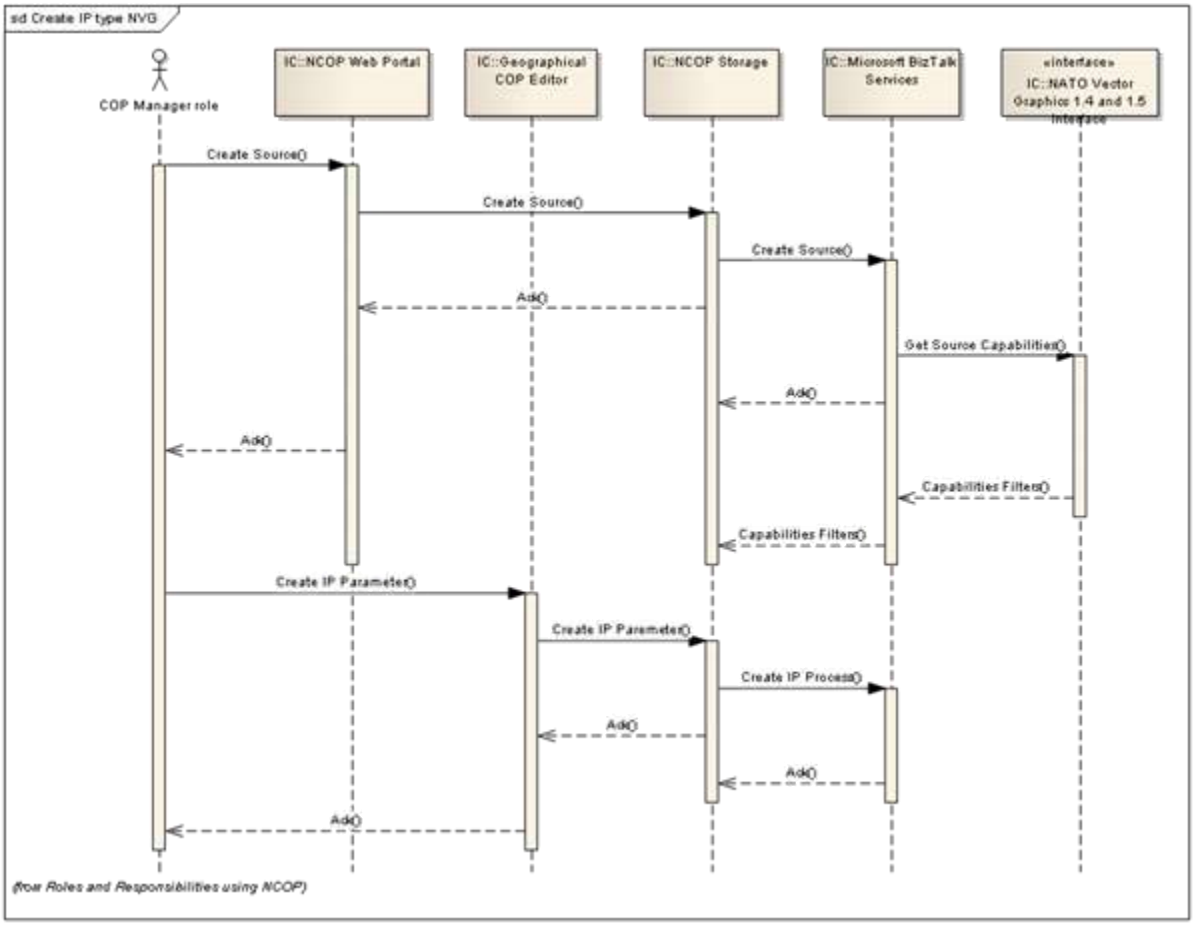


Figure 5-113: Information Product parameter creation for NVG source

For other sources such as SQL, the process is simplified

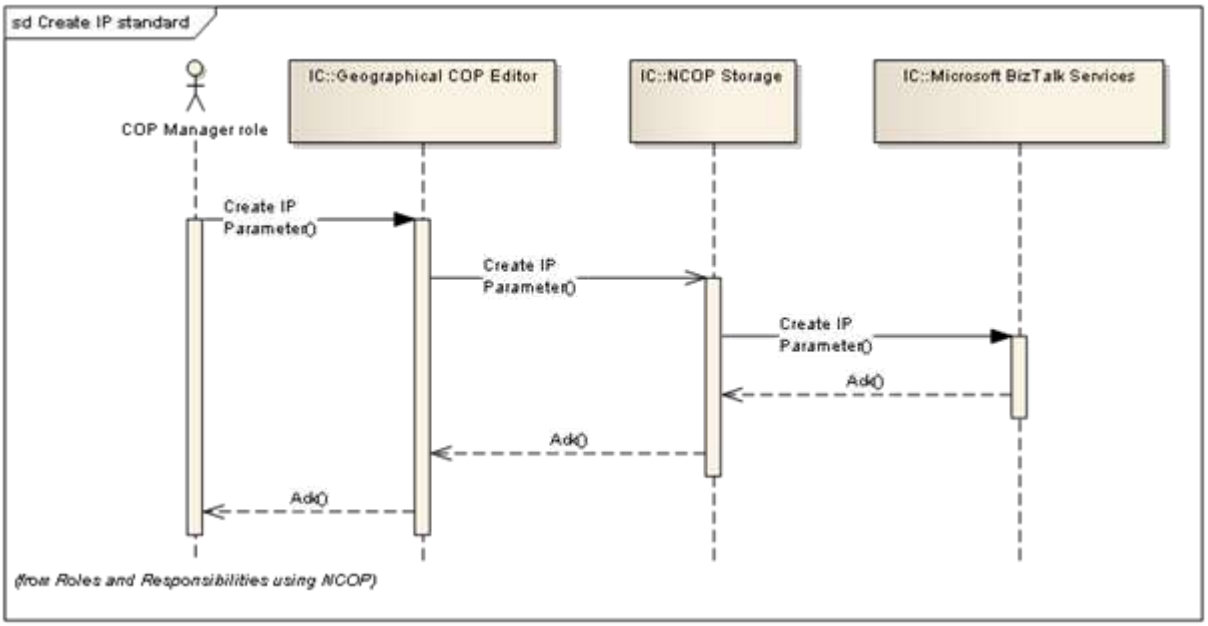


Figure 5-114: Information Product parameter creation for other sources

5.3.3.3.1.4.2 Pull Information Product instances

The pull process is triggered with the BizTalk scheduler mechanism. (see 5.3.3.3.1.1.4 Nato.NCOP.Scheduler for more details). The process is described below for the NVG format. The call to the source may vary depending on the protocol and data and service contract of the source.

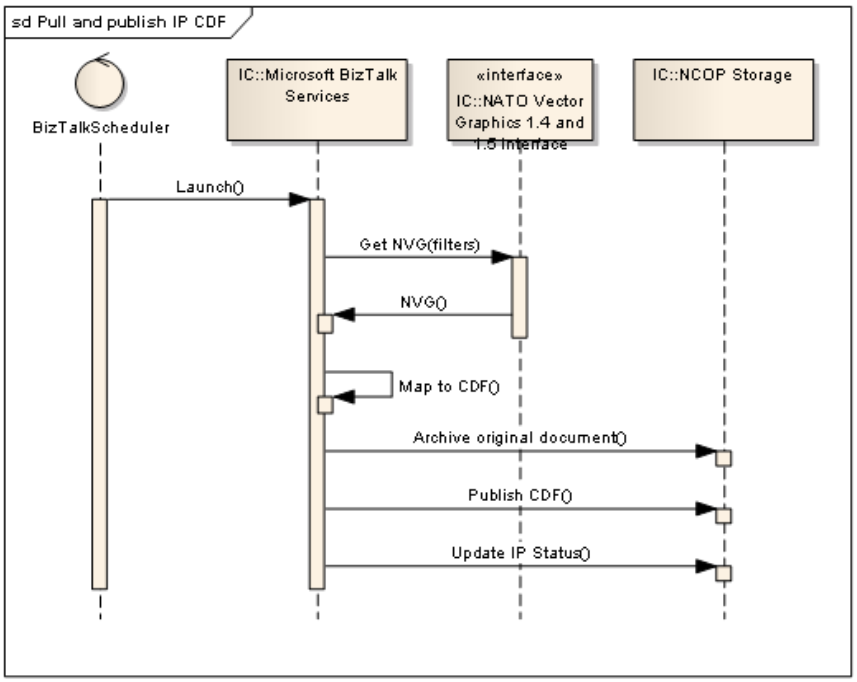


Figure 5-115: BizTalk pull and publication

5.3.3.3.1.5 BizTalk customization for NCOP

For NCOP, all data processing that involves BizTalk is based on the usage of standard BizTalk artefacts (applications, orchestrations, send ports, receive locations, etc.). For NCOP needs, some specific code has been developed and integrated in some orchestrations using the standard BizTalk API.

Regarding external connectivity, NCOP uses the standard adapters provided by default on BizTalk servers (File, POP3, Web service, etc.). However, some additional adapters (/n Software adapters) have to be installed on the NCOP BizTalk server to allow XMPP, REST API and email (SMTP) connectivity which is required for NCOP. Also to allow connectivity to SQL databases it is required that the appropriate drivers be installed on the BizTalk Server. By default, NCOP installation comes with Microsoft SQL Server drivers and Access engine drivers that allow connectivity to Excel files via OLEDB.

5.3.3.3.2 Composition / Orchestration

Property Name	Description
Identification	Composition/Orchestration
Classification	IS
Behaviour	This component is a set of “Composed Business Services” provided by the Contractor based on Microsoft BizTalk Orchestration capabilities. The set runs the following elements: ADatP-3 and OTH-T Gold Message Processing; Geographic format Processing; Entity sources end-points; Generic XML Message Processing; Generic Text Message Processing; NVG Streaming Protocol; SQL Database, SharePoint List and Microsoft Excel Processing These “Composed Business Services” are deployed into the BizTalk Server as BizTalk applications. The Microsoft Visual Studio application, allows the Node Administrator role to create, build and deploy the BizTalk applications.
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 BizTalk Server

Property Name	Description
Interfaces	This IC interacts with external sources through a set of adapters (FILE, SOAP, FTP, POP3, WCF-BasicHttp …)
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework XSLT
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

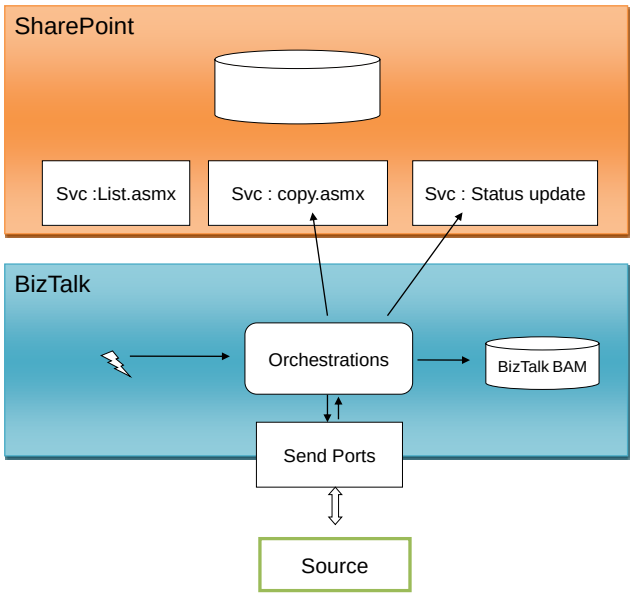
The steps for developing an orchestration are as follows:

- Define the schemas to describe the format of the messages to be processed by the orchestration;
- Add and configure the shapes to represent the various actions that are required to define the business process;
- Define new message instances to be processed within the orchestration;
- Define the orchestration ports to receive and send messages;
- Define and assign orchestration variables to declare and manage the data used in the orchestration;
- Bind the send and receive shapes to ports, and specify the physical ports that they will use;
- Build, deploy, and test the orchestration;

5.3.3.3.2.1 Service composition in NCOP

Most interface services will be implemented using dedicated services in order to implement the specificities of a source, but also relying on services that implement canonical formats and generic interfaces toward SharePoint CDF import, logs and archive mechanism. BizTalk orchestrations are at the forefront of this implementation.

The diagram below illustrates the central role that take a BizTalk orchestration in the technical process of getting CDF documents from a source in the pull mode and publishing to SharePoint



5.3.3.3.2.2 Publish NVG

BizTalk implements a technical process in order to import NATO CDF to SharePoint. This process has been designed as a generic interface so that all existing and future

interfaces can easily be added and plugged into the BizTalk CDF publication mechanism.

This principle is illustrated below with some typical interfaces example:

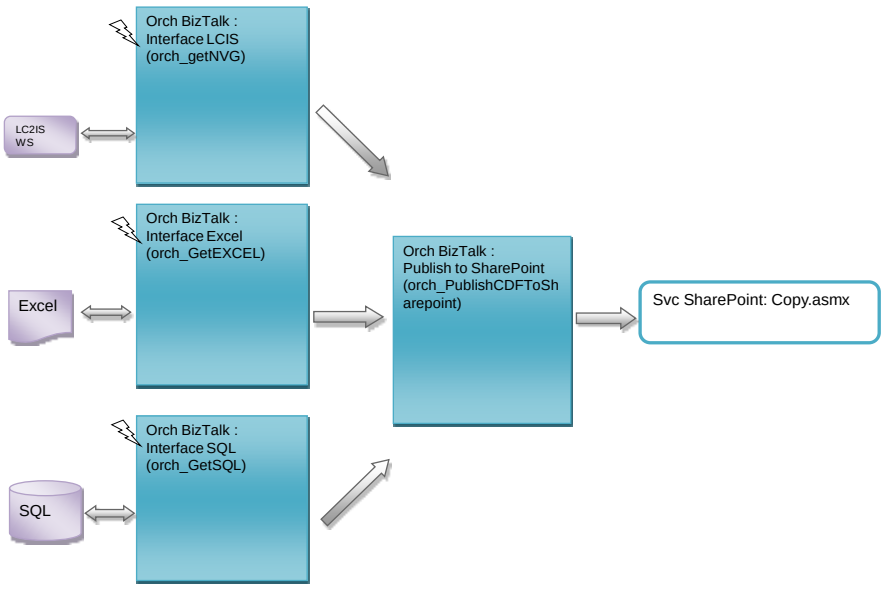


Figure 5-116: Orchestrations consuming external interfaces

The orchestration “orch_getSQL” is illustrated below:

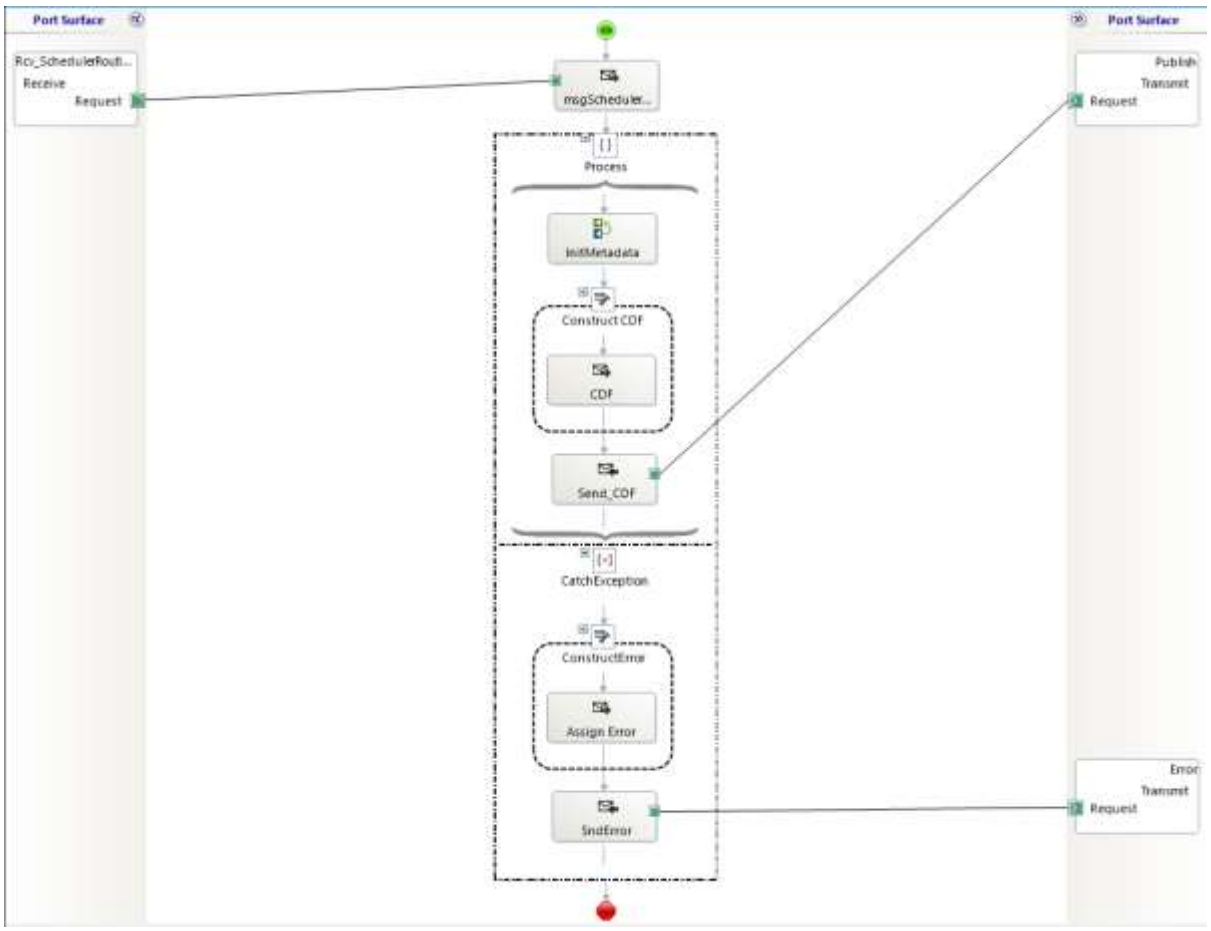


Figure 5-117: BizTalk orchestration allowing GetSQL

The first step is to receive a command message from the scheduler mechanism. The next step is to acquire the Information Product from the source (via a send port) and then transform it to CDF format. Next it is archived to disk. The last step it to publish it to the pub/sub repository of BizTalk in CDF format. It will be automatically collected by the generic “Publish CDF” orchestration. In case of error, an error is logged and the process is aborted.

The generic orchestration “orch_PublishCDFToSharepoint” is illustrated below:

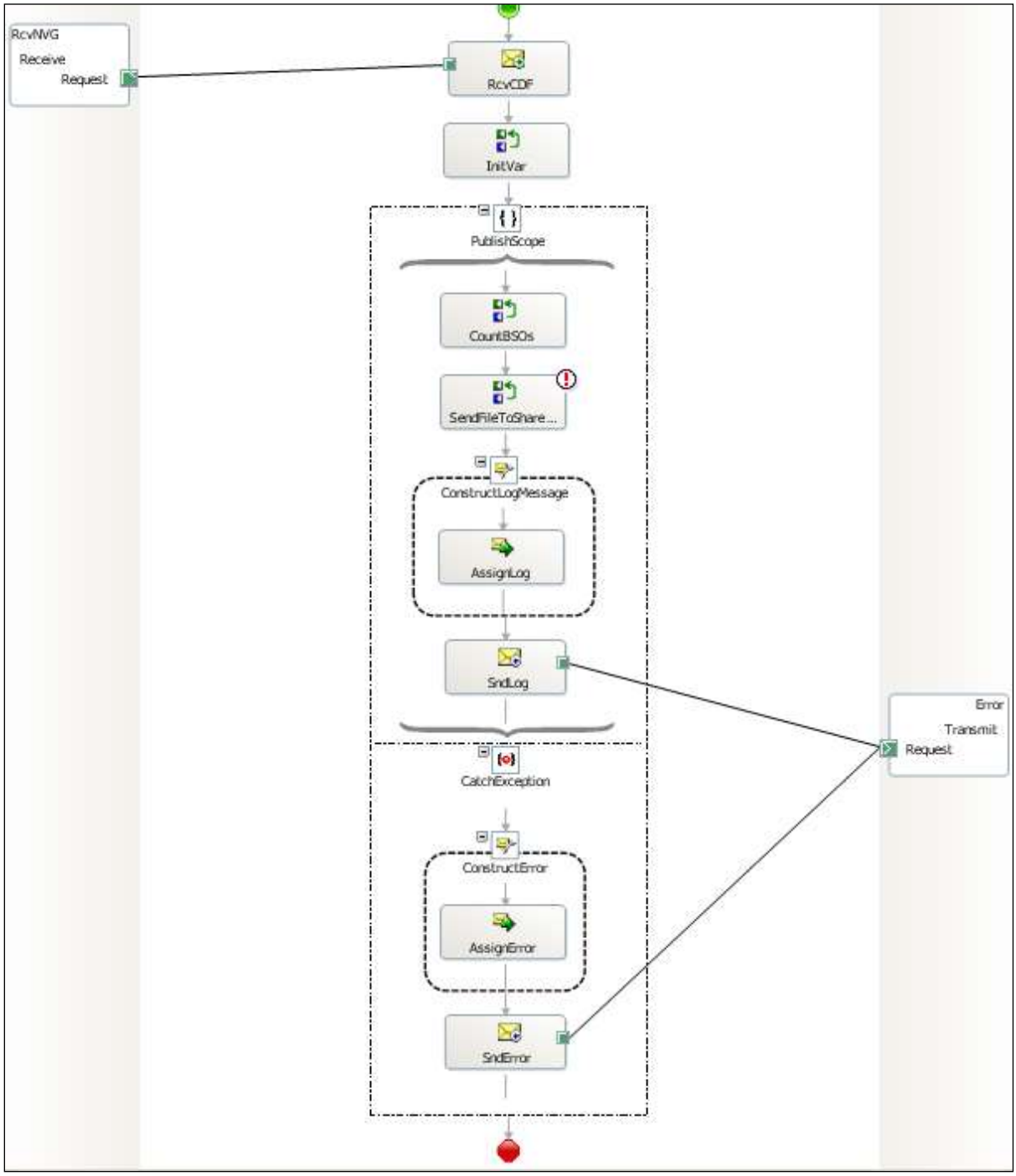


Figure 5-118: BizTalk orchestration allowing publication to portal

Above: This orchestration collects all the messages of format NVG1.4. These are then published to SharePoint via a C# class that consumes SharePoint web services (copy.asmx).

5.3.3.3.3 SQL Database, SharePoint List and Microsoft Excel Processing

Property Name	Description
Identification	SQL Database, SharePoint List and Microsoft Excel Processing
Classification	IS
Behaviour	This component implements automatic transformation of any given SQL Database or Excel data format into NCOP CDF. These transformations are available since a bi-directional mapping is performed between the CDF XML Schema and the given SQL data or Excel data structure. This mapping is implemented using technologies such as XSLT, C# allowing calls to functions (scripts or .NET assemblies) to perform more complex processing: geo coordinates conversion ...
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 BizTalk Server
Interfaces	This IC interacts with SQL Database, SharePoint List and Microsoft Excel external sources through connection strings or DSN
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework SQL XSLT
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

5.3.3.3.3.1 Microsoft Excel Processing

This functionality is implemented with BizTalk components with the same process pattern that is used for the other interfaces. The process is described below:

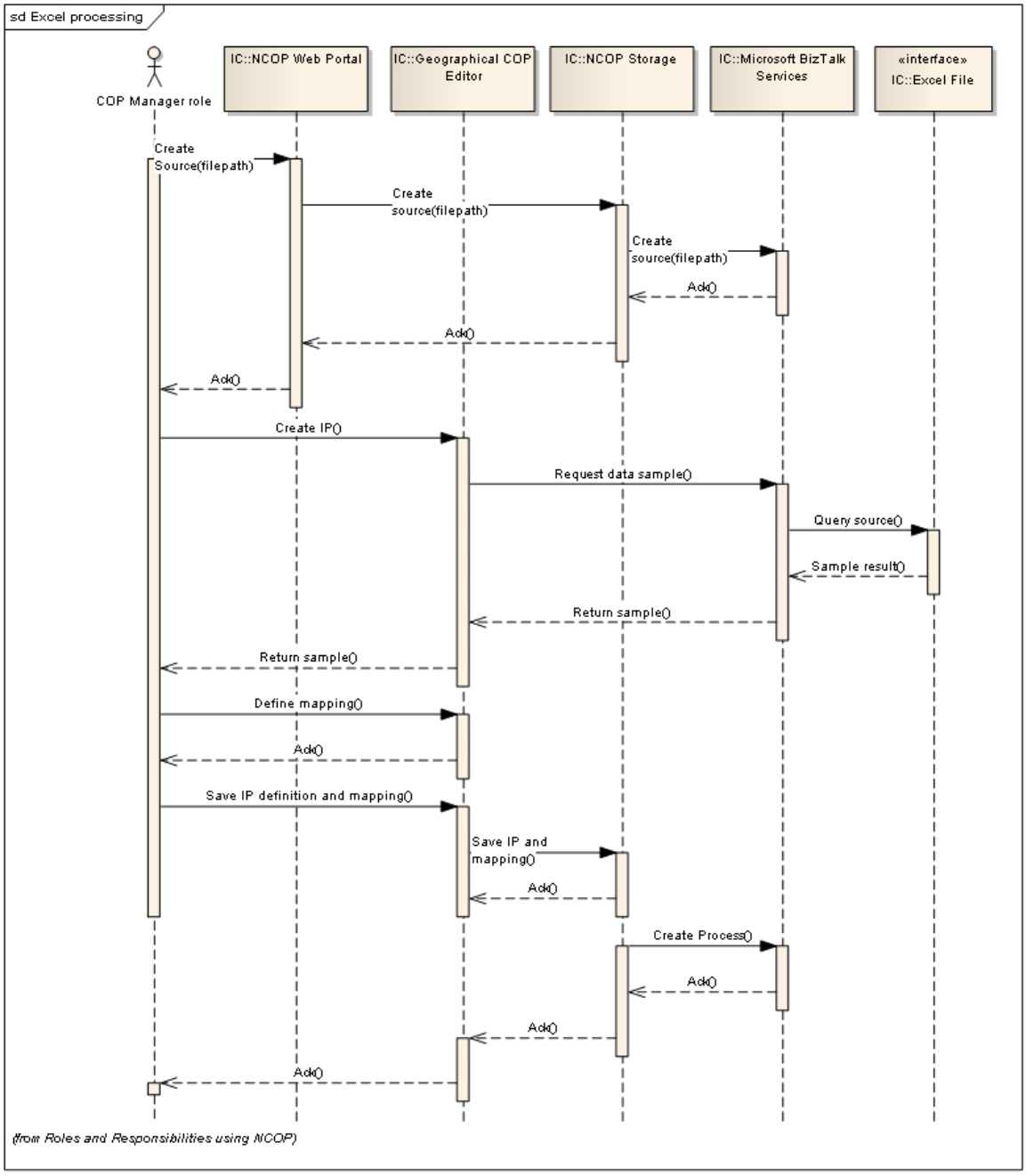


Figure 5-119: BizTalk orchestration allowing Excel processing

In case of Excel file, the operator will always start the same way as for other interfaces. First create the source. This will create the corresponding element on the BizTalk side. The source will be used a first time in order to acquire a data sample to help the user create the Information Product Parameter.

Once the Information Product Parameter has been created, the process in BizTalk will proceed the same way that for other pull interfaces i.e. the Excel file will be read at regular intervals. The Excel file name used will be the name of the file as specified in the source definition.

5.3.3.3.3.2 Database source Processing

This functionality is implemented with BizTalk components with the same process pattern that is used for the other interfaces. The process is described below:

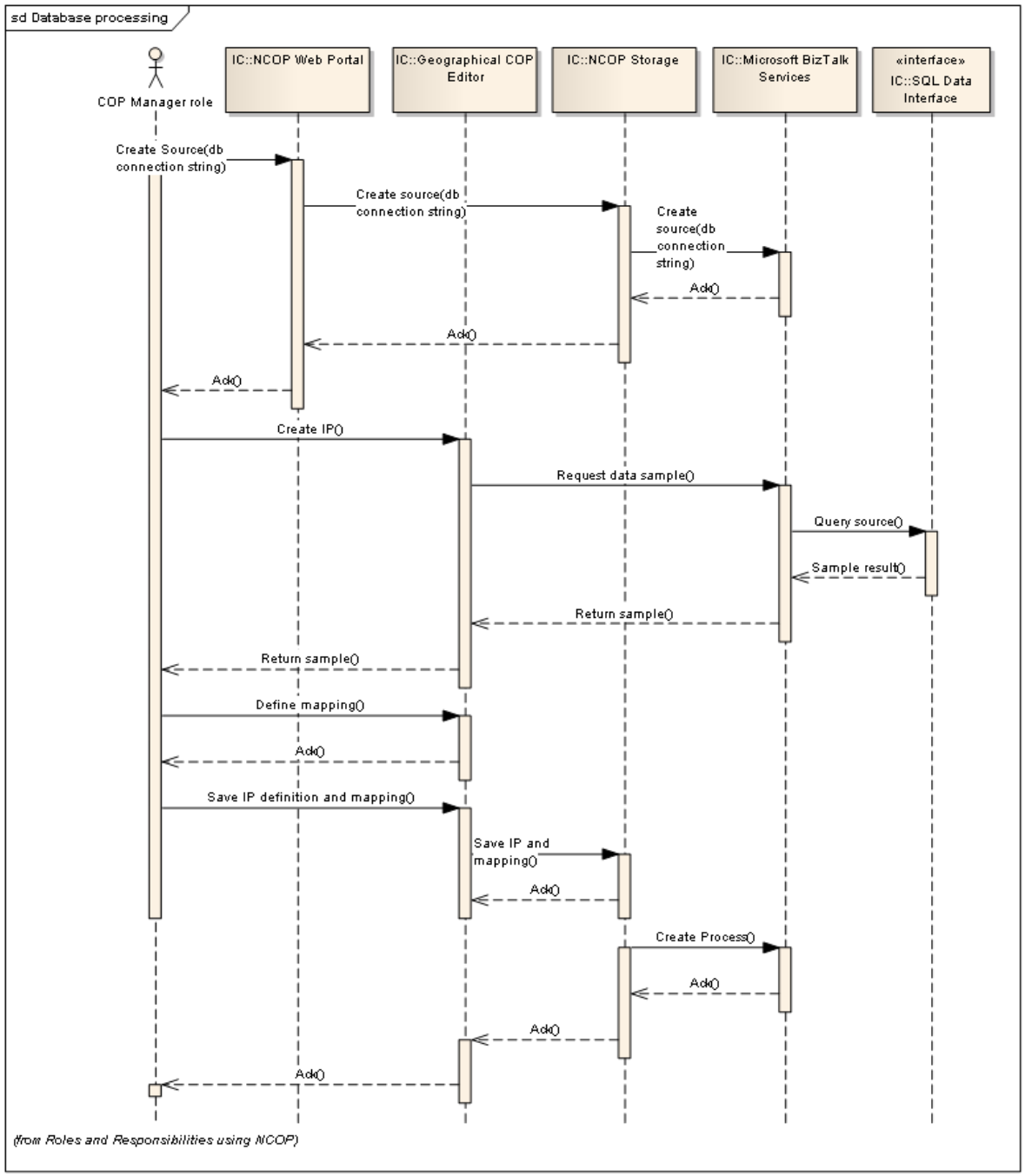


Figure 5-120: BizTalk orchestration allowing SQL processing

In case of a SQL database source, the operator will always start the same way as for other interfaces. First create the source. This will create the corresponding element on the BizTalk side. The source will be used a first time in order to acquire a data sample to help the user create the Information Product Parameter.

Once the Information Product Parameter has been created, the process in BizTalk will proceed the same way that for other pull interfaces i.e. the database will be queried at regular intervals.

The source corresponds to a Server name + database name.

The Information Product parameter defines the objects queried with an SQL statement.

5.3.3.3.4 Generic XML Message Processing

Property Name	Description
Identification	Generic XML Message Processing
Classification	IS
Behaviour	This component implements automatic transformation of any given XML data format into NCOP CDF. These transformations are available since a bi-directional mapping is performed between the CDF XML Schema and the given XML data Schema. This mapping is implemented using technologies such as XSLT, C# allowing calls to functions (scripts or .NET assemblies) to perform more complex processing: geo coordinates conversion ...
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 BizTalk Server
Interfaces	This IC interacts with external sources through a set of adapters (FILE, SOAP, FTP, POP3, WCF-BasicHttp …)
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework XSLT
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

Generic XML message processing is implemented with the standard XSLT data transformation mechanism. This component is used to convert all XML-based incoming data into NCOP CDF. It is integrated in BizTalk orchestrations used in the data acquisition process for NCOP.

Implementation details of mapping used for Generic XML message processing are available in the NCOP [ICD].

5.3.3.3.5 ADatP-3 and OTH-T Gold Message Processing

Property Name	Description
Identification	ADatP-3 and OTH-T Gold Message Processing
Classification	IS
Behaviour	This component implements automatic transformation of MTF formatted messages according to the ADatP-3 V11, V12 & V13 standards into NCOP CDF (including BSOs). Correctness verification against ADatP-3 message grammar and syntax is also provided by this IC that exploits corresponding message definition. This component implements automatic transformation of MTF formatted according to the OTH-T Gold standard into NCOP CDF (including BSOs). Correctness verification against OTH-T Gold message grammar and syntax is also provided by this IC that exploits corresponding message definition.
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 BizTalk Server
Interfaces	This IC interacts with external sources through a set of adapters (FILE, SOAP, FTP, POP3, WCF-BasicHttp …)
Collaboration mechanism	-
Local/Configuration data	-
Operating context	JRE XSLT
References	-
Quality of Service requirements (QoS)	-
Complexity	Difficult

This component is based on a text parser that is integrated in BizTalk orchestrations used in the data acquisition process for NCOP.

Implementation details of mapping used for ADatP-3 and OTH-T Gold message processing are available in the NCOP [ICD].

In addition to built-in ADatP-3 mappings, NCOP proposes a tool that allows a user to analyse an ADatP-3 file. This tool can be used when an incoming file is not processed correctly: it provides information about incorrect syntaxic and semantic errors detected in an ADatP-3 file. This tool is deployed only on the BizTalk servers and can be used by an authorized user to understand why an incoming ADatP-3 file could not be processed by BizTalk (if configure accordingly, BizTalk is able to copy original files in a dedicated folder when it detects an anomaly during the CDF conversion. The following figure presents the UI of this tool:

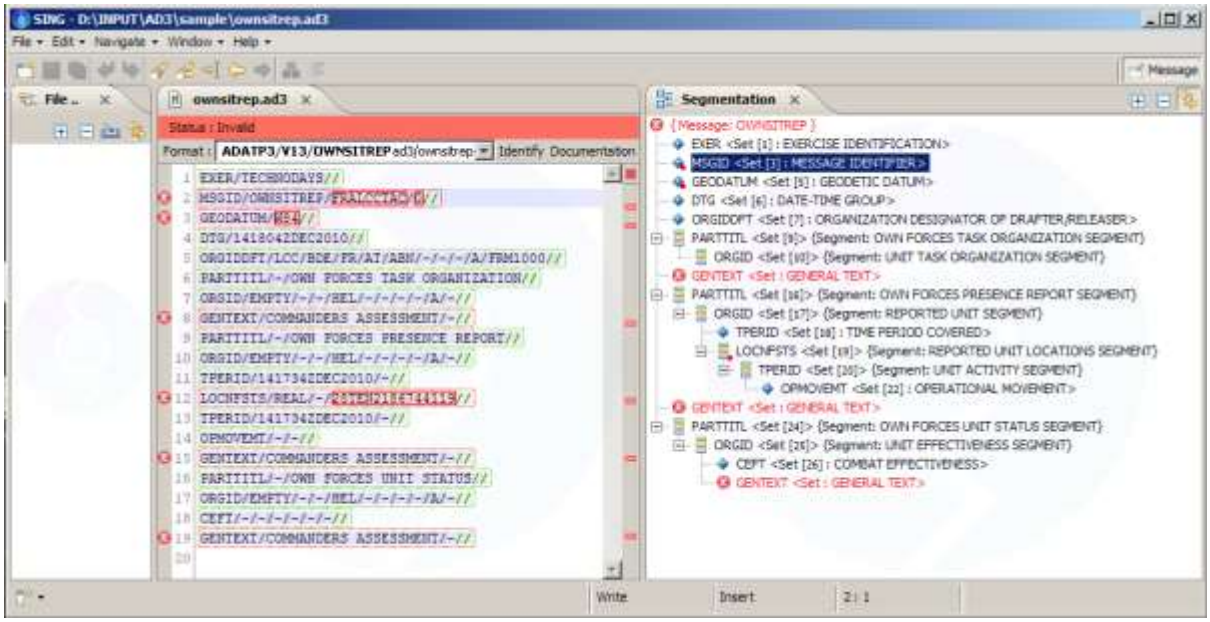


Figure 5-121: ADatP-3 analysis UI

Implementation details of mapping used for OTH-T Gold message processing are available in the NCOP [ICD].

5.3.3.3.6 Generic Text Message Processing

Property Name	Description
Identification	Generic Text Message Processing
Classification	IS
Behaviour	This component implements automatic transformation of any given text-based data format into NCOP CDF. These transformations are available since a bi-directional mapping is performed between the CDF XML Schema and the given Text data structure. This mapping is implemented using technologies such as XSLT, C# allowing calls to functions (scripts or .NET assemblies) to perform more complex processing: geo coordinates conversion ...
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 BizTalk Server
Interfaces	This IC interacts with external sources through a set of adapters (FILE, SOAP, FTP, POP3, WCF-BasicHttp …)
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework XSLT

Property Name	Description
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

NCOP comes with built-in orchestrations that are dedicated to the acquisition of specific formats and protocols. However, to offer more flexibility, NCOP offers the possibility to acquire additional formatted text messages for which the format is not known in advance. This capability relies on the use of an external tool that allows an administrator to define the mapping between formatted text files and CDF. The tool to be used is Altova Map Force with its FlexText plug-in.

- FlexText is used to allow the conversion of a formatted text file into an XML message.
- MapForce is used to define the mapping between the resulting XML file and CDF.

The integration of these conversion tools in NCOP is done as follows.

- Create a MapForce project dedicated to the management of a specific formatted text file format
- Use the FlexText plug-in to analyse the message format and design an intermediary output XML file.
- Use MapForce to design the mapping of this temporary XML file into a CDF file.
- Export the MapForce project as C# classes
- Compile the resulting C# files to create a DLL assembly
- Put this DLL assembly in a dedicated BizTalk folder

Additional information and samples of MapForce project files are provided in the NCOP [ICD].

The conversion assemblies will be used by an internal web service designed to convert an incoming formatted text message into CDF using the required conversion assembly. This Web service is used as an NCOP Source and its capabilities are the list of available conversion assemblies: the same web service is used to convert files with different formats; the conversion assembly to be used is an input parameter of the conversion method.

New conversions can be added at runtime without requiring the redeployment of built-in BizTalk orchestration. The only actions required are:

- Creating the MapForce project with all instructions to convert an input file into CDF
- Building the corresponding C# classes and placing the resulting DLL assembly in the appropriate folder (documentation is provided in the Administration manual).

The following figure presents an overview of the components involved to manage the acquisition of formatted text file:

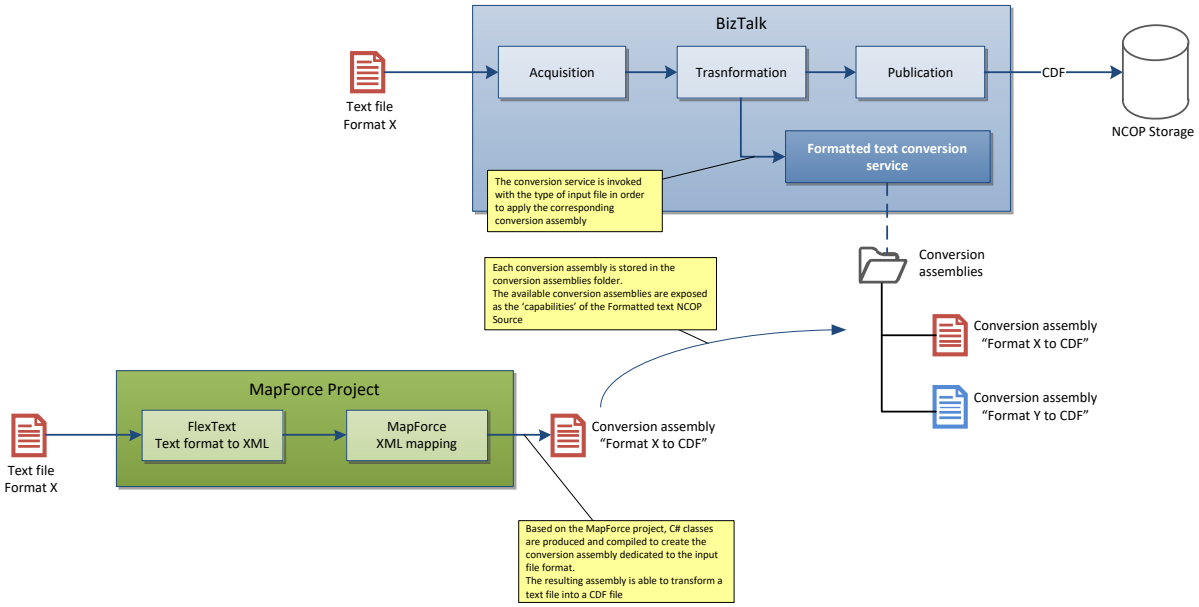


Figure 5-122: Generic formatted text acquisition process overview

5.3.3.3.7 LC2IS Overlays Processing

Property Name	Description
Identification	LC2IS Overlays Processing
Classification	IS
Behaviour	This component implements the LC2IS data model to NVG mapping.
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 BizTalk Server
Interfaces	This IC interacts with external sources through a set of adapters (FILE, SOAP, FTP, POP3, WCF-BasicHttp …)
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework XSLT
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

5.3.3.3.8 Geographic format Processing

Property Name	Description
Identification	Geographic format Processing
Classification	IS
Behaviour	It allows receiving into NCOP several information and geographical formats such as OGC Web Map Service, OGC Web Feature Service, OGC GML, OGC Keyhole Markup Language, and OGC Web Map.
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 Application Server
Interfaces	This IC interacts with http/https OGC end-points
Collaboration mechanism	https
Local/Configuration data	-
Operating context	TypeScript/JavaScript
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

5.3.3.3.8.1 Inclusion of geographic formats in a COP

It is possible in NCOP to add Geographical Information Products in a COP. The following data formats are allowed:

- WFS layers
- KML files
- WMS layers
- WMC files

These services and file formats can be consumed by the Geographical COP Editor (whether they are referenced in a COP context or not).

WFS services and layers are consumed by the Angular Geographical COP Editor.

KML files must be hosted on a Web site and are referenced using the appropriate URL.

WMS layers are referenced by the following elements:

- Map Service URL
- Layer identifier as exposed by the Map Service WMS capabilities

WMC files must be hosted on a Web site and are referenced using the appropriate URL. WMC files reference a set of Map Layers. The content of the WMC file is

evaluated dynamically in the Geographical COP Editor. It means that if the contents of a WMC file changes over time, the COP manager doesn't need to update the COP structure to reflect the changes.

5.3.3.3.9 NVG Streaming Protocol Processing

Property Name	Description
Identification	NVG Streaming Protocol Processing
Classification	IS
Behaviour	NCOP provides the NVG Streaming Protocol processing as consumer and as producer based on a SOAP Web Service description. The NCOP NVG Streaming Protocol Producer subcomponent has the following capabilities: Implement generic Tide Publish-Subscribe Streaming Protocol for Producer; Accept subscription request from consumers (including filters); Send with a "subscriptionId" as a response to the subscription request; Publish updates to the original NVG document using TIDE XML Diff attributes; Stop publishing updates corresponding to a subscription upon the reception of a Cancel message. The NCOP NVG Streaming Protocol Consumer subcomponent has the following capabilities: Discover NVG Streaming Service Producer and the related Request-Response NVG Service; Implement generic Tide Publish-Subscribe Streaming Protocols requirements for Consumer; Handle updates received using a NVG document augmented with TIDE XML Diff attributes; Is able to correlate received updates to subscriptions based on the "subscriptionId" attribute; Send a Cancel message with a "subscriptionId" attribute to stop receiving updates.
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 Application Server
Interfaces	This IC interacts with http/https NVG Streaming Protocol end-points
Collaboration mechanism	http, https
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

5.3.3.3.10 Aggregation Association Correlation Processing

Property Name	Description
Identification	Aggregation Association Correlation Processing
Classification	IS
Behaviour	This component implements the automatic extraction of aggregations, associations and correlations between BSOs. This extraction relies on a list of rules that define the criteria to generate an aggregation, an association or a correlation. These rules are edited with the Aggregation Association Correlation Manager IC. BSOs in the system are matched against these rules. When a rule matches, the resulting objects and relationships are created in the system.
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 Application Server
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Difficult

5.3.3.3.11 Dynamic Source Server

Property Name	Description
Identification	Dynamic Source Server
Classification	IS
Behaviour	The Dynamic Source Server is a web services that broadcast the BSO coming from dynamic sources (NIRIS tracks, MCCIs tracks, …) to Geographical COP Editor clients:
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 Application Server
Interfaces	This IC interacts with Angular Geographical COP Editor through SignalR This IC interacts with dynamic connectors (NIRIS, MCCIS Tracks, NVG Streaming, NFFI SIP-3) through REST API
Collaboration mechanism	https
Local/Configuration data	Configuration file to customize the DSS
Operating context	.NET Framework

Property Name	Description
References	-
Quality of Service requirements (QoS)	-
Complexity	Difficult

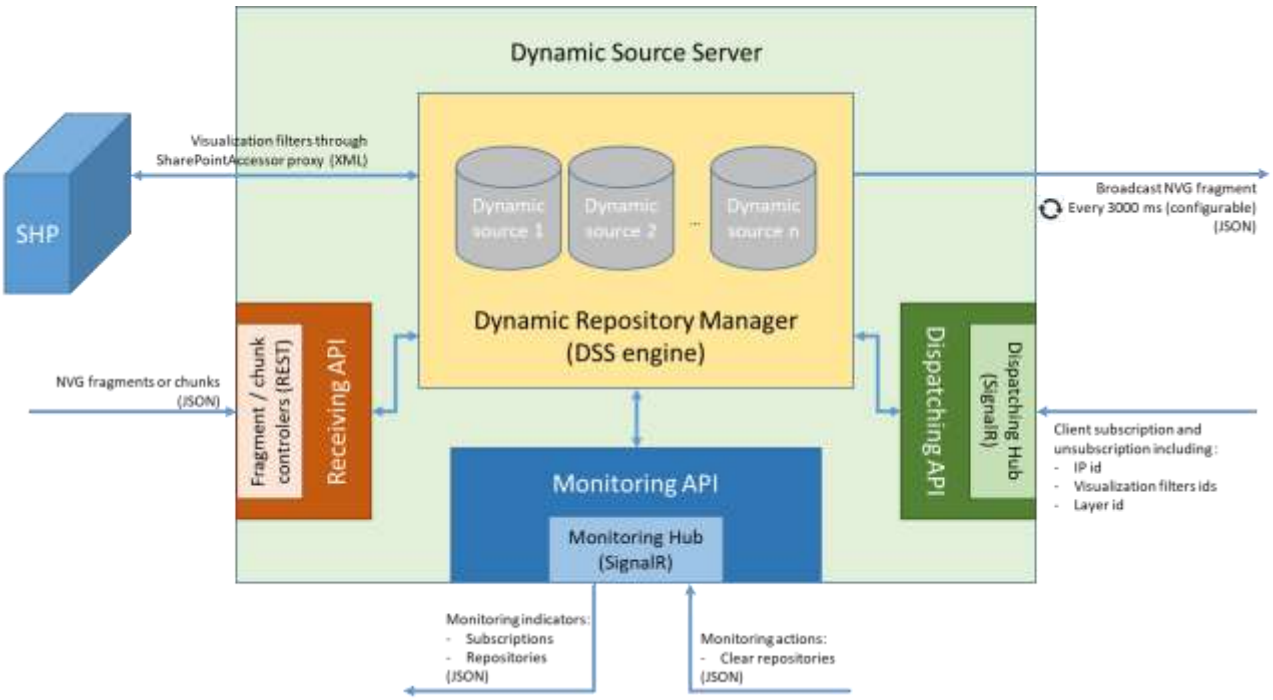


Figure 5-123: Dynamic Source Server architecture

The Dynamic Source Server exposes 3 different interfaces:

- **Receiving API**, for the dynamic fragment providers. This RESTful service accepts partial items merged with those in the repository
- **Dispatching API**, for the clients (JavaScript or .NET Core). This service uses SignalR, and sends partial items when possible to optimize network load
- **Monitoring API**, to get information about the DSS and carry out management actions. This services uses SignalR.

If required, the DSS engine applies Visualization filters before sending the fragments to the clients.

Details are provided in §5.4.19.

5.3.3.4 Interoperability

This section describes the implementation components that are being used by NCOP for external communication with consumers (publication/subscription), data providers (NCOP MRR) and other NCOP nodes (synchronization).

5.3.3.4.1 Node Synchronisation

Property Name	Description
Identification	Node Synchronisation
Classification	IS
Behaviour	The Node Synchronization component allows Enterprise Administrator role or Organizational Node Administrator role on a NCOP Node, to control its synchronization settings (incoming or outgoing), including: Toggle on / off all activity; Selection of COPs selection of COP IPs; Management Information; Synchronization frequency. COPs and COP IPs are synchronized by using the NCOP Synchronization Web Service.
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 Application Server
Interfaces	This IC interacts with other NCOP nodes through WCFweb services end-points
Collaboration mechanism	https
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Difficult

This chapter describes the main concepts related to COP and Information Products synchronization. The event-driven synchronization mechanisms, software components and interactions are described in more details in the Detailed design section at chapter 6.2.1 Synchronization.

5.3.3.4.1.1 Synchronization principles

NCOP synchronization is a mechanism whose purpose is to replicate NCOP elements from one NCOP node to another. This synchronization will allow an NCOP Node to have a local copy of COP elements that were created on other nodes.

Synchronization is involved in the following scenarios:

- If an Entity uses multiple NCOP nodes deployed in different locations, all the Nodes of that Entity shall be able to view the same COP elements, even in case of loss of connectivity between those nodes.

- When Entities are hosted on different nodes, COP elements can be synchronized between different Nodes of different Entities, if the dissemination settings allow it.

The COP and Information Products synchronization process is strongly related to the following concepts:

- Entities (Commands)
- Nodes
- Dissemination settings
- Security classifications

These items, part of the Management Information, are widely used de define the synchronization settings and process the data accordingly.

5.3.3.4.1.2 Synchronization technical details

5.3.3.4.1.2.1 Publish/Subscribe Web service based data exchange

The elements are replicated from one Node to another by the use of Web services between two Nodes. The Publish/Subscribe data exchange pattern is used for synchronization.

A client Node must subscribe to a server Node, indicating which elements it wants to obtain from that server Node. When the server Node identifies that an element needs to be replicated, it will publish the information associated with the element to all the client nodes that have subscribed to this particular element.

The NCOP implementation for this publish/subscribe data exchange mechanism is based on the WS-Eventing specification.

The following Web services are implemented on each Node:

- Subscription service

This service is exposed in order to allow client Nodes to subscribe to COP elements.

- Publication service

This service is exposed to receive notifications and data elements from server Nodes.

The subscription service exposes the following method in compliance with the WS-Eventing specification:

- Subscribe()
- Unsubscribe()
- Renew()
- GetStatus()

The subscription exposes an additional method used to ask a node about the information elements it is able to provide.

- ListAvailableContent()

The publication service exposes a set of methods dedicated to:

- Receive an acknowledgement of the subscription orders,
- Receive data from the publisher.

A NCOP node can subscribe to the following elements:

- COPs
- Information Products

When subscribing to a specific COP, a node will be notified of any element updated within this COP, including Information Products, Shared Views and Annotations. It has to be noted that a node cannot subscribe to a specific shared view or annotation since these elements have a meaning in the context of a COP.

Subscription to a single Information Product will only replicate the data related to this Information Product.

The synchronization mechanism is designed in a way that allows a node to act as a server and as a client at the same time.

The NCOP synchronization mechanism also allows a Node to re-publish some COP elements provided by another node.

The following figure presents a scenario that brings to light those two concepts.

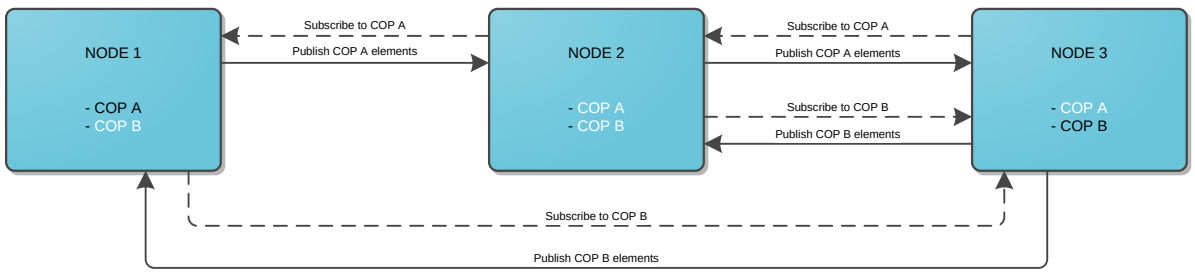


Figure 5-124: Synchronisation scenario

5.3.3.4.1.2.2 Event-driven synchronization

This synchronization mechanism is event-driven. It means that when a particular event is raised for a particular element on an NCOP Node, this element will be sent to all client Nodes that have subscribed to the element. The synchronization process is not scheduled; elements are synchronized as soon as a change has been detected.

For each element that can be synchronized, the events that will trigger a synchronization process are the following:

- Element created,
- Element updated,
- Element deleted.

Since the synchronization is an event-driven process, the NCOP synchronization service proposes a function to force the resynchronization of two nodes if the client node was not reachable when the event was raised.

When a node subscribes to a COP or an Information Product on another node, the synchronization mechanism requires an initialization phase. The goal of this phase is to publish the current version of all COP or Information Product related elements. Once done, the event-driven process is set up and the client node will only receive subscribed COP or Information Product elements updates.

5.3.3.4.1.2.3 Multi-master synchronization

NCOP synchronization is designed to allow the modification of a data on every node of the system where it has been synchronized.

However, some elements (COP sources and Information Products) can only be modified on the node where they have been created. This limitation is due to the fact that those elements are strongly linked with the acquisition infrastructure (BizTalk) of the Node where they have been created.

Because an element can be modified simultaneously on different nodes, it is possible that some synchronization conflicts occur. The NCOP synchronization service is able to detect such conflicts. A manual operation is required to solve those synchronization conflicts.

5.3.3.4.1.3 Synchronized elements

The following table lists the NCOP elements that are synchronized:

TABLE 5-9: NCOP ELEMENTS THAT ARE SYNCHRONIZED

Element type	Modifiable on a replicated node
COP	Yes
Information Product	No
Source	No
Shared view	Yes

Annotation	Yes
Contributed Information Product	Yes
Alert related to data acquisition	N/A

5.3.3.4.1.4 Synchronization security

The NCOP synchronization service is aware that it has to replicate data to a node only if it has been configured through the synchronization settings and authorized by the dissemination settings and the cross-domain security policy.

Before sending any information element to a node, the dissemination settings are taken into account to verify if the information element is authorized to be disseminated to the target entity.

Once the dissemination settings have been verified, the synchronization service will verify that the cross-domain security policy allows to transmit the data to the target node.

5.3.3.4.1.5 Synchronisation technical components

The following technical components are being involved in the NCOP synchronization mechanism:

- The Event Manager component (described in chapter §5.3.3.2.1)

  It is the source of all events related to COP items (creation / modification / deletion)

- The synchronization database

  All synchronization-related events are being stored here for later processing

- NCOP Synchronization windows service

  It hosts to sub-components used in the synchronization mechanism

  - Synchronization broker service

    Analyzes the incoming synchronization events and generates broker messages for each potential target node (according to subscription settings)

  - Synchronization send service

    Processes all broker messages and send the data to target nodes

- Credential secure store

Stores the credentials to be used when Web Services are being invoked across nodes during the synchronization processes

Interaction between these components are being described in more details in the Detailed design section at chapter §6.2.1.

5.3.3.4.2 NCOP Tools

Property Name	Description
Identification	Event Manager
Classification	IS

Behaviour	This component is gathering:
	• A set of independent tools provided in the NCOP Repository.
	  ○ NCOP Feedback Extractor Tool: Extracts data produced with the "Provide feedback" function so that it can be exported.
	  ○ NCOP Import Geonames Tool: Import Gazetteer data from iGeoSIT, Geonames files or Excel files.
	  ○ NCOP WebService Consumer Tool: Consumes JIPS and/or NCOPIPS Web services in order to provide COP data to disconnected external systems.
	• Tools allowing build, test and deployment of NCOP Software:
	  ○ Software Build Tools
	  ○ Software Build Instruction
	  ○ Test Automation Tool
	  ○ NCOP Installer
	  ○ Data Migration Tool
	  ○ Training Data for Training database

Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved
Location (Types)	Not deployed on a particular server
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework SQL
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

5.3.4 Data

5.3.4.1 COP and IP History storage

Property Name	Description
Identification	COP and IP History Storage
Classification	I
Behaviour	COP and IP History storage process BSO history from Information Product Overlay history.
Actors involved	See details in Appendix K IC vs Actors Involved
Objects involved	See details in Appendix L IC vs Objects Involved

Property Name	Description
Location (Types)	Installed on the SQL Server
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework SQL
References	-
Quality of Service requirements (QoS)	-
Complexity	Difficult

In order to manage BSO History information, this component relies on a relational database storage solution.

This relational database is filled and updated during the acquisition process of the information products that contain BSOs. This database stores the following information:

- Originating Information Product identifier,
- BSO identifier,
- BSO last update date & time,
- BSO base properties (label, symbol, etc.),
- BSO metadata & extended data,
- BSO coordinates,
- BSO NVG representation.

BSO history management, storage and consumption are described in more details the chapter 5.4.7.2.

5.3.4.2 COP and IP storage

Property Name	Description
Identification	COP and IP storage
Classification	I
Behaviour	This is the central database used to store all the COPs and IPs consumed and/or produced by Organisational Entities during operations, exercises or training. On each NCOP Node, the NCOP storage relies on the deployment of SharePoint sites. Each COP is stored in CDF into a SharePoint site and IPs are stored in a SharePoint Document Library. In SharePoint sites, Documents Library is used for storing and managing documents (IPs). Documents properties are stored using predefined metadata. It is possible to add columns to Documents Library to associate custom metadata with each document that is added to the library. Then the expected NCOP IP properties can be stored as metadata in the Document Library. The NCOP Data Format (CDF) Interface is based on XML format and relies on NATO Vector Graphics for part of its geographical content (such as BSOs) and defines XML structures for the Information Products, Shared Views, Annotations, COP maps and COP structures definitions that reuse NVG types where appropriate NCOP also relies on an additional SQL storage solution to handle BSO history.
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
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework SQL
References	-
Quality of Service requirements (QoS)	-
Complexity	Difficult

5.3.4.2.1 COP related data storage

NCOP uses SharePoint as its main storage solution. The COP elements managed by NCOP are stored in SharePoint document libraries and SharePoint lists. Document libraries are used to store the Information Products in CDF format and in original format. Lists are used to store the technical elements such as COPs definition, Sources definition, Domain values, etc.

The Information product concept has been split in two elements:

- The Information Product parameter which describes the information product and defines its acquisition contract (source, filter, update frequency, etc.)
- The Information Product instance which is the result of the acquisition as declared with the associated Information Product parameter.

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

Information Product instances are stored in a SharePoint document library. In order to keep a history of all incoming data in NCOP, when a data-driven Information Product is acquired, the CDF version of this Information Product is stored in this document library and the previous version of this same Information Product is kept using the native SharePoint versioning mechanisms. The same mechanism is used for the original data (Information Product in its native format).

In order to prevent the SharePoint database to grow indefinitely, NCOP comes with a default setting that limits the number of successive versions for an Information Product to 100 (one hundred). This limit applies to both Information Products in CDF format and native format. This limit can be configured by an authorized user using the standard SharePoint configuration user interface for the associated Document libraries.

5.3.4.2.2 BSO related data storage

NCOP stores BSO related data for BSO history management. Therefore, NCOP uses an additional storage solution based on a SQL Server relational database which is more appropriate than the SharePoint storage. This storage benefits from the use of the geographical capabilities of SQL Server to handle geographical search on BSOs.

The data model is described in more details in chapters 5.4.7.2 and 5.4.7.3.

The BSO indexing process for BSO search and BSO history usage is described in chapter 6.2.9.

5.3.4.2.3 Operational, training and exercise data management

In order to separate each type of data, NCOP uses one SharePoint site collection to manage one type of data. It means that on an NCOP node that has to manage Operational data, Training data and exercise data, NCOP will use one site collection to store the Operational data, one site collection to store the Training data and one site collection to store the Exercise data. Using different site collections allows the data to be stored into separated underlying databases. One BSO related storage is also instantiated for each type of data (e.g. Operational, Training and Exercise).

5.3.4.2.4 Detailed COP and IP storage

All logical objects that were stored in XML format in NCOP Increment-1 will remain in XML in NCOP Increment-2. The web services allowing get/set actions on these logical objects will be provided in 2 formats in NCOP Increment-2:

- SOAP XML as in Increment-1(NCOP IPS, JIPS …) for backward compatibility
- REST API JSON for HTML 5 JavaScript web clients.

TABLE 5-10: COMPARISON BETWEEN INCREMENT-1 AND INCREMENT-2 PHYSICAL IMPLEMENTATION

Logical object	Physical implementation in NCOP Increment-1	Physical implementation in NCOP Increment-2	Involved by History (time-aware)
COP	SharePoint list with versioning. It contains several attributes with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	Yes
Sources	SharePoint list without versioning	Same as in Increment-1	No
Structure Templates	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Security Classifications	SharePoint list without versioning	Same as in Increment-1 The Security Classifications will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Information Product templates	SharePoint list without versioning. It contains several attributes with embedded XML.	SharePoint list with versioning. It will contain several attributes with embedded XML.	No
Information Product instances (CDF)	XML files in NVG 2.0.1 format in a SharePoint list with versioning set to 100 last versions The CDF is exposed to the Geographical COP Editor in NVG 1.4 XML format.	XML files in NVG 2.0.2 format in a SharePoint list with versioning set to 100 last versions. The CDF will be exposed to the Geographical COP Editor in NVG 2.0.3 JSON format.	Yes
Information Product instances (Original Data)	Files of any format stored in a SharePoint list with versioning set to 100 last versions	Same as in Increment-1	Yes
Contributed Information Products	XML files in NVG 2.0.1 format in a SharePoint list with versioning set to 100 last versions The CDF is exposed to the Geographical COP Editor in NVG 1.4 XML format.	XML files in NVG 2.0.2 format in a SharePoint list with versioning set to 100 last versions. The CDF will be exposed to the Geographical COP Editor in NVG 2.0.3 JSON format.	Yes
Geographic Information Products (KML)	SharePoint list without versioning	Same as in Increment-1	No

		The Geographic IP definition will be transformed and exposed to the Geographical COP Editor in JSON format.	
Geographic Information Products (WMS Map)	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Geographic Information Products (WMS Map Service)	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Aggregated Information Products definition	SharePoint list without versioning. It contains several attributes with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Annotations	SharePoint list without versioning. It contains an attribute with embedded XML NVG 1.5.	SharePoint list without versioning. It will contain an attribute with embedded XML NVG 2.0.2. The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Shared Views	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Named Views	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Shared Briefings	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Private Briefings	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
User Layers	SharePoint list without versioning and SQL tables	Same as in Increment-1	No

		The user layers will be transformed and exposed to the Geographical COP Editor in JSON format.	
COP Worksheets	SharePoint list without versioning. It contains an attribute with embedded Excel.	Same as in Increment-1	No
Mission architecture diagrams	XML file stored in the file system	Deprecated	No
Feedbacks	SharePoint list without versioning	Same as in Increment-1	No
BSO Charts Definition Templates	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Commands	SharePoint list without versioning. It contains an attribute with embedded LDAP queries.	Same as in Increment-1	No
Nodes	SharePoint list without versioning	Same as in Increment-1	No
Domains Values	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Level of Detail templates	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Icon Mapping Table (used for SQL and Excel mappings)	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Information Product Relation Rule set Templates	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Information Product Status	SharePoint list without versioning	SharePoint list with versioning The IP status will be transformed and exposed to the Geographical COP Editor in JSON format.	Yes
User Icons (NCOP Symbology)	SQL tables in BSORefDB	Same as in Increment-1	No

Information Product Status Rules Table	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Synchronisation subscriptions	SharePoint list without versioning	Same as in Increment-1	No
User display Context	SharePoint list without versioning. It contains an attribute with embedded XML.	Stored in JSON format	No
User Favorite Tactical Overlays	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
User settings	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
User Spatial Bookmarks	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1 The XML will be transformed and exposed to the Geographical COP Editor in JSON format.	No
Visibility Groups	SharePoint list without versioning. It contains an attribute with embedded LDAP queries.	Same as in Increment-1	No
Visibility Rights	SharePoint list without versioning. It contains an attribute with embedded XML.	Same as in Increment-1	No
Visualization filters templates	SharePoint list without versioning. It contains an attribute with embedded Script.	Same as in Increment-1	No
BSO for History capability	SQL tables in BSORefDB	These tables are deprecated and will be replaced by tables used for BSO search (see below)	Yes
BSO for Search capability	SQL tables in BSORefDB	Tables will be extended as temporal tables to allow history	Yes
Geo Processing definition (Core GIS interface)	NA	SharePoint list without versioning. It will contain an attribute with embedded JSON.	No
Analysis and Analytics templates	NA	SQL tables and files	Yes
Information Products Versions			
Information Products Substitution Rules			

Service Authorisation Request			
User Favorite User Layers			

Figure 5-125 displays several COP IPs stored into a SharePoint Document Library filtered by domain:

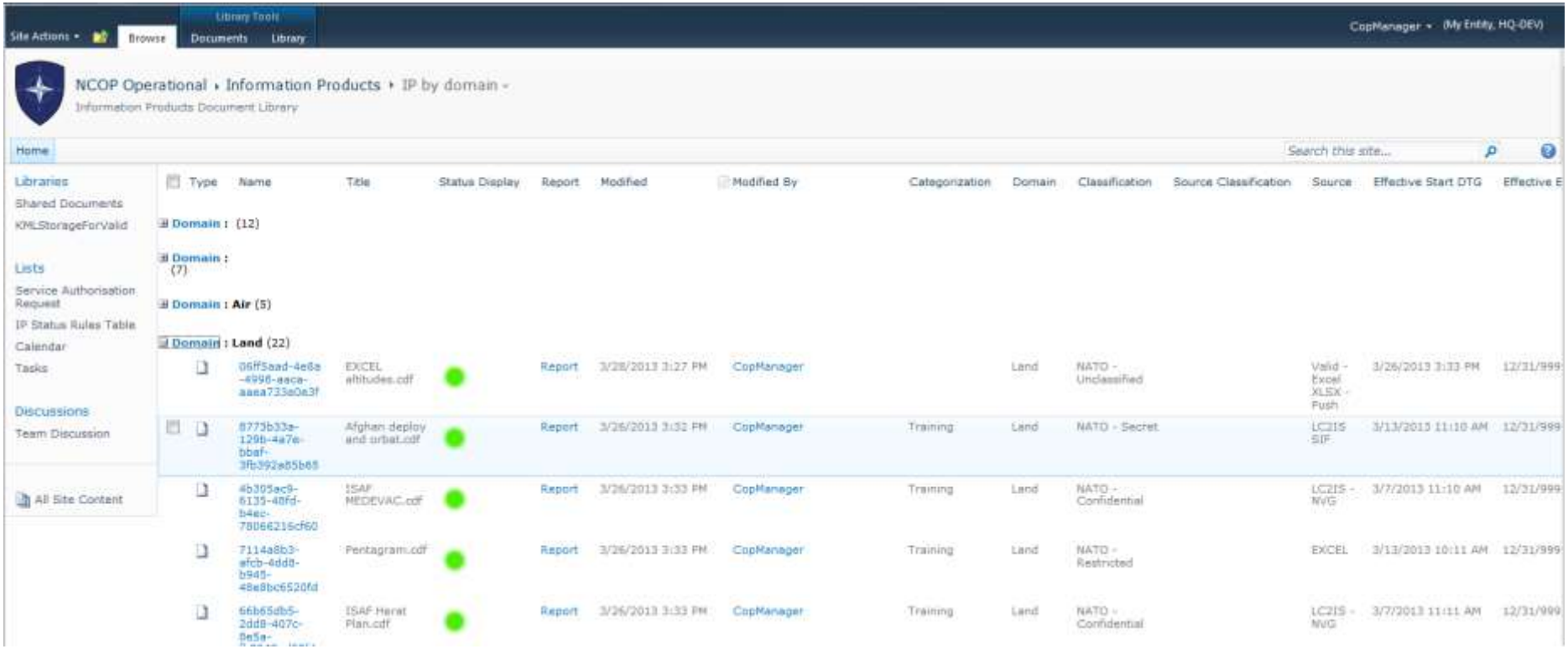


Figure 5-125: List of COP IPs displayed into SharePoint and filtered by domain

5.3.4.3 Management Information Storage

Property Name	Description
Identification	Management Information Storage
Classification	I
Behaviour	Management Information Storage is the repository used for storing the following Management Information: Policies & Security settings; Synchronization settings; Dissemination settings; Entities Information; Visibility groups Information and rules; Nodes Information; User settings; Domain values Security classifications
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
Interfaces	This IC interacts with the SQLback-end natively (SharePoint mechanism)
Collaboration mechanism	https
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Difficult

5.3.4.3.1 Policies & security settings

Policies & security settings are based on the native SharePoint security management settings.

They are linked to the NCOP RBAC management. As described in the NCOP RBAC management chapter, NCOP roles are based on fine grained permissions that are related to NCOP modules access and NCOP data visibility. These permissions are implemented using SharePoint security groups and are associated with low-level

native SharePoint security permissions (read, contribute, approve, etc.) for each SharePoint list.

5.3.4.3.2 Synchronization settings

Synchronization settings are stored in a dedicated SharePoint list.

The following attributes are used to describe the synchronization parameters between two nodes:

Attribute name	Attribute description
Title	Name of the synchronization item
Type of subscription	Indicates if the synchronization is dedicated to subscribe to COPs (include all linked IPs) or independent IPs)
Node	Name of the source node
Subscribed objects	List of objects (COPs or IPs) that have been subscribed to
Expiration date	Limit date and time after which a client node will not receive updates from the source node.
Is read/write	Boolean value indicating if the synchronization is declared as bi-directional or not

Synchronization settings items must be created when an NCOP node wants to subscribe to another NCOP node to retrieve COPs or Information Products.

The use of the synchronization settings attributes is described in more details in the Synchronization manager chapter cf. §5.3.3.4.1.

5.3.4.3.3 Dissemination settings

Dissemination settings can be defined for both COPs and Information Products. These settings are stored as an attribute of each Information Element item in the NCOP storage allowing dissemination settings to be automatically synchronized from node to node when a COP or an Information Product is updated.

The dissemination settings are described in an XML document. An example is given below:

```
<DisseminationRights xmlns="Nato.NCOP.Dissemination">
  <CopEntitiesPermissions>
    <EveryEntityPermission Grant="true" Deny="false" EntityName="Every entity" />
    <EntityPermission Grant="true" Deny="false" EntityName="ISAF" />
  </CopEntitiesPermissions>
</DisseminationRights>
```

Regarding COPs, dissemination settings can be defined:

- For a whole COP
- For a part of the COP (structure, folder or layer).

Dissemination settings can be defined at the Information Product level, regardless of their association with any COP. In case of conflict, a 'deny' rule defined at the Information Product level prevails on an 'allow' rule defined at the COP level.

A virtual entity named "Every Entity" can be used to allow the COP Manager to quickly define dissemination rules for all entities. This virtual entity is also used to evaluate visibility rights when NCOP is accessed anonymously.

By default, COPs and Information Products are not disseminated and are therefore only visible to users that belong to the owner entity associated with the Information elements.

5.3.4.3.4 Entities information

NATO entities are logical organizational units. A user can belong to one, many entities, or no entity at all.

These entities and associated users organization are reflected in the NATO Active Directory. However, depending on the deployment configuration and more particularly depending on the Active Directory structure of each site, the way to identify the entities a user belongs to can vary. It can be based on:

- the location of user in the directory (for example, users in the "JHQ" organization unit belong to the "JHQ" entity);
- a set of attributes for each user (for example, user entries that have the attribute "entity" value set to "JHQ" belong to the "JHQ" entity;
- the user's membership to a particular group (for example, user that are members of the "JHQ" LDAP group belong to the "JHQ" entity;
- any combination of the statements above.

The NCOP mechanism used to identify the entity of authenticated users is based on an LDAP search criteria in order to allow flexibility to comply with various possible scenarios.

Entities are stored in a dedicated SharePoint list.

The following attributes are used to define an Entity:

Attribute name	Attribute description
Title	Name of the entity
Base DN	LDAP base DN to be used to search the users that belong to the entity
Filter	LDAP filter to be used to search the users that belong to the entity
Scope	LDAP scope to be used to search the users that belong to the entity (valid values are : BASE, ONE and SUBTREE)
Properties to load	List of LDAP user properties to retrieve when a user is found in this entity

When a user connects to a node, NCOP will iterate on each entity defined in this node and will search the user in Active Directory using the LDAP v3 API and search parameters that have been defined for this entity.

At runtime, entities (commands) can be created on an NCOP node and the LDAP search criteria can also be adjusted by an authorized user if required.

Since LDAP attributes can be used to identify the entity (or command) of a user and the user's entity can be used to allow access to a COP in a dissemination scenario, NCOP implementation of Entities contributes to the implementation of ABAC requirements.

5.3.4.3.5 Visibility groups information and rules

5.3.4.3.5.1 Visibility groups

Visibility groups are used to define visibility rules for COPs and Information Products. The purpose of these groups is to allow or deny access to a COP or specific parts of a COP to a particular category of users. A visibility group can be common to multiple entities.

Visibility groups are defined using the same principles as for the definition of NATO entities (or commands): depending on the deployment configuration and more particularly depending on the Active Directory structure of each site, the way to identify the visibility groups a user belongs to can vary. It can be based on:

- the location of user in the directory (for example, users in the "Intel" organization unit belong to the "Intelligence" visibility group);
- a set of attributes for each user (for example, user entries that have the attribute "mainDomain" value set to "Intelligence" belong to the "Intelligence" visibility group;
- the user's membership to a particular group (for example, user that are members of the "Intelligence" LDAP group belong to the "Intelligence" visibility group;
- any combination of the statements above.

The NCOP mechanism used to identify the visibility group membership of authenticated users is based on an LDAP search criteria in order to allow flexibility to comply with various possible scenarios.

Visibility groups are stored in a dedicated SharePoint list.

The following attributes are used to define a visibility group:

Attribute name	Attribute description
Title	Name of the visibility group
Base DN	LDAP base DN to be used to search the users that belong to the visibility group
Filter	LDAP filter to be used to search the users that belong to the visibility group
Scope	LDAP scope to be used to search the users that belong to the visibility group(valid values are : BASE, ONE and SUBTREE)
Properties to load	List of LDAP user properties to retrieve when a user is found in this visibility group

Since LDAP attributes can be used to identify the visibility groups of a user and the user's visibility groups can be used to allow access to a COP (in a dissemination scenario or not), NCOP implementation of visibility groups contributes to the implementation of ABAC requirements.

5.3.4.3.5.2 Visibility rules

Visibility rules are set by the COP Manager and are based on visibility groups. The COP Manager can allow or deny access to visibility groups for:

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

By default, COPs and Information Products are visible to all users. However, the dissemination settings are verified first.

5.3.4.3.6 Nodes information

Nodes items must be declared on an NCOP node in order to allow synchronization. A Node item contains the necessary information to locate the associated synchronization service. It also contains attributes that allow NCOP to control the inbound and outbound synchronization data flow.

Nodes information is stored in a dedicated SharePoint list.

The following attributes are used to describe a Node:

Attribute name	Attribute description
Title	Name of the NCOP Node
Local	Boolean value indicating if the Node is local or remote
Entities	List of Entities hosted on that Node
Security classification	Security classification of the NCOP node
URL	URL of the portal homepage for that Node
Synchronization URL	URL of the synchronization service for that Node
Inbound Sync Active	Boolean value indicating if the Node accepts incoming data from remote Nodes

Outbound Sync Active	Boolean value indicating if the Node sends data to remote Nodes.

For synchronization purposes, each external Node is associated with credentials to be used by the local node Synchronization service in order to authenticate when using HTTP synchronization Web services.

5.3.4.3.7 User settings

User settings are stored in dedicated SharePoint lists.

Three (3) SharePoint lists are used to store the following settings for each user:

- Display context
- Overlay settings
- Spatial bookmarks

The display context list stores the following information

- Map background
- Zoom scale
- Windows placement and settings
- Personal preferences (Default date format, default coordinates system, default measurement units)

The overlay settings list stores the following information

- Tooltips configuration (Placement and content)
- Labels configuration (Placement, content, style, visibility)
- BSO filter
- BSO size preferences

The spatial bookmarks list stores the list of spatial bookmarks for each user (Centring point, bounding box)

All three user settings types are described using an XML document stored in the appropriate SharePoint list. For each setting, one XML document is stored per user.

5.3.4.3.8 Domain values

Domain values are lists of values that can be selected from to set properties of Information Elements in the CDF.

All NCOP nodes are preconfigured with a set of Domain Values for:

- Information Products domains
- Information Products categorization
- BSO types and sub-types (from ADEM semantics)
- BSO affiliations (from ADEM semantics)

- BSO hostilities (from ADEM semantics)
- BSO operational statuses (from ADEM semantics)
- BSO operation statuses qualifiers (from ADEM semantics)
- Association types (from ADEM semantics)

Domain values are stored in a dedicated SharePoint list. Each list item is defined by the following attributes:

Attribute name	Attribute description
Title	Name of the domain value
Description	Description of the domain value
Content	XML document that describes all possible values for the domain value
Accepts null values	Boolean value that indicates if it is required to select a value when this domain value is used
Protected	Boolean value that indicates if the domain value content can be modified from the HMI

The use of an XML document to describe the domain values allows the management of hierarchical values (for example object types and object sub-types). Each value is defined by the following attributes:

- Label,
- Short name,
- Description,
- Sub-value

The following presents a sample of the XML document describing a domain value:

```
<?xml version="1.0" encoding="utf-8"?>
<DomainValuesStructure         xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
  <DomainValue Label="Unit">
    <Description>A military ORGANISATION whose structure is prescribed by
competent authority.</Description>
    <SubValues />
  </DomainValue>
  <DomainValue Label="Facility">
    <Description>An OBJECT-ITEM that is built, installed or established to
serve some particular purpose and is identified by the service it provides
rather than by its content.</Description>
    <SubValues>
      <DomainValue Label="AirborneEarlyWarningGroundFacility">
        <Description>A facility on the ground that has an electromagnetic
link to an airborne early warning system.</Description>
        <SubValues />
      </DomainValue>
      <DomainValue Label="AlternateDecontaminationFacility">
        <Description>A decontamination facility designated as the alternate
to the primary decontamination facility that can be used in place of the
where personnel and/or materiel (incl. vehicles) can be cleaned after
(potential) contamination of radioactive, biological, or chemical
material.</Description>
        <SubValues />
```

```
      </DomainValue>
.......
....
```

In the Association types, the <SubValues> are used to store optional information:

- The color of the association when it is displayed as a line in the Geographical COP Editor
- The pattern of the association when it is displayed as a line in the Geographical COP Editor
- A boolean to define if the association is automatically displayed on the map background or not

```
      <DomainValue ShortName="C2 Relationship" Label="C2 Relationship">
          <SubValues>
            <DomainValue                      ShortName="AutoDisplayHide"
     Label="AutoDisplayHide">
              <SubValues />
              <Description>true</Description>
            </DomainValue>
            <DomainValue ShortName="Colors"  Label="Colors">
              <SubValues />
              <Description>Cyan</Description>
            </DomainValue>
            <DomainValue ShortName="Patterns"  Label="Patterns">
              <SubValues />

     <Description>LinePatterns.Strokes.ShortDashLine</Description>
            </DomainValue>
          </SubValues>
          <Description></Description>
        </DomainValue>
```

As shown below, the colors and styles of the following associations are determined by the Domain Values:

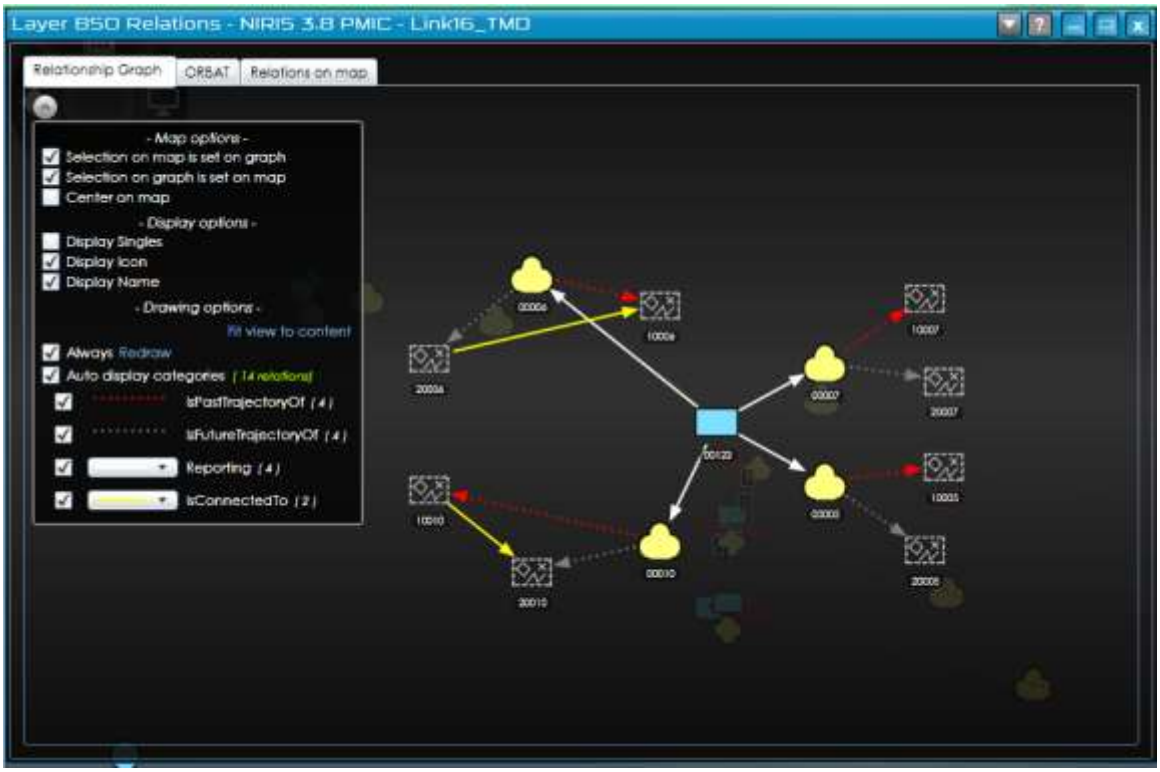


Figure 5-126: Domain values applied on the display of associations

NCOP proposes a web UI dedicated to the management of domain values. This UI is accessible to authorized users (“Manage domain values permission”) from the Geographical COP Editor. The following figure presents the Domain values administration UI:

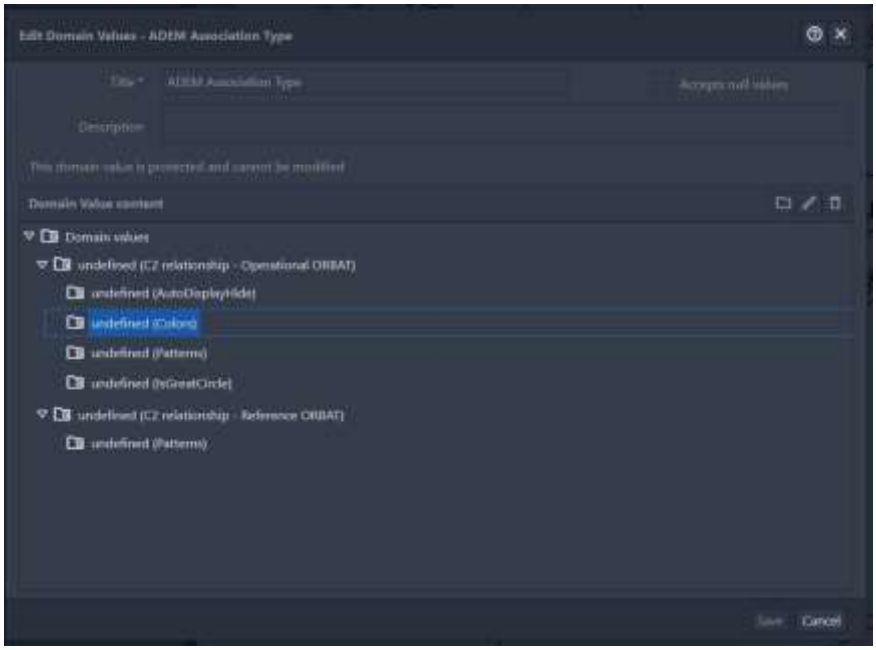


Figure 5-127: Domain values management UI

5.3.4.3.9 Security classifications

Security classifications are managed in NCOP using four different SharePoint lists:

- Security classification policy identifiers (NATO, Public, etc.)
- Security classification markings (Unclassified, Confidential, etc.)
- Security classification categories (Releasable to ISAF, etc.)
- Security classifications

Policy identifiers, Markings and categories are defined with the following attributes:

- Short description,
- Description.

Security classification list items are defined with the following attributes:

Attribute name	Attribute description
Short description	Automatically calculated by the concatenation of policy identifier, marking and classification.
Description	Free text used to describe the security classification
Policy identifier	Lookup to the policy identifiers list
Marking	Lookup to the Markings list
Category	Lookup to the Categories list
Aliases	Free text used to define alternate names and syntaxes for the security classification
Order	Numeric value used to describe the level of the security classification
Color	Hexadecimal colour code associated with the security classification (Ex:#FF0000 for red)

The “aliases” attribute is a free text field that allows an authorized user to declare alternative names for a Security classification. This attribute is used during the normalization phase of the Information Product acquisition process described in chapter 6.2.2 (Security classification handling of incoming Information Product)

The “Order” attribute is used by the following components:

- In the Geographical COP editor to display the highest security classification level according to all loaded Information Products or maps.
- In the Synchronization Manager to filter outgoing data according to the classification level of the remote NCOP node.
- In the Security Manager to generate appropriate security labels for all outgoing data

The “Colour” attribute is used by the Geographical COP editor to display the security classification banner with the appropriate colour.

5.3.5 NCOP Infrastructure

5.3.5.1 Microsoft Windows Server

Property Name	Description
Identification	Microsoft Windows Server
Classification	TI
Behaviour	Microsoft Windows Server 2019 is the operating system installed on the NCOP hosting servers.
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

5.3.5.2 Microsoft SQL Server

Property Name	Description
Identification	Microsoft SQL Server
Classification	TI
Behaviour	SQL Server 2019 is the underlying relational database used to store information maintained in the NCOP storage. It provides database administration, monitor and management tools and utilities.
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 SQL Server
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

SQL Server is used in NCOP as the base persistence infrastructure used by NCOP COTS (SharePoint and BizTalk) and NCOP storage.

For performance reasons and following Microsoft recommendations, NCOP recommends the use of multiple SQL Server instances instead of storing all NCOP data in one unique SQL Server instance.

Using multiple instances allows:

- the configuration and allocation of resources (RAM and CPU) for each instance
- the isolation of processes
    - reducing the impact of data processing on other instances
    - minimizing impact during maintenance

NCOP distribution of SQL Server instances is as follows:

Instance name	Instance content
BizTalk	Databases required by BizTalk Server
SharePoint	Databases required by SharePoint Server
Common	Databases used to store NCOP common data and configuration: • Acquisition scheduling configuration • RBAC management data • Alerts/Notifications data and settings • Synchronization settings • BAM data • BSO Search data
History	Databases used to store NCOP history data: • BSO History data

Sometimes (Data Centre deployment) the SQL Server installation is not expected by the NCOP installation process. The SQL Server shall be considered as a PAAS (Platform As A Service). It will be prepared by NATO according to NCOP requirements, as a pre-requisite before NCOP Increment-2 installation.

The detailed description of the NCOP databases content is provided in Appendix M Databases Diagrams.

The HA and XL nodes configurations shall provide a high availability mechanism (cluster as in Increment-1 or SQL Server AlwaysOn (prefered).

SQL Server AlwaysOn.

SQL Server AlwaysOn is a marketing term which refers to the high availability and disaster recovery solution introduced when SQL Server 2012 was launched.

To be more specific, SQL Server AlwaysOn consists of two technologies:

- AlwaysOn Failover Clustering Instances (AlwaysOn FCI)
- AlwaysOn Availability Groups (AlwaysOn AG)

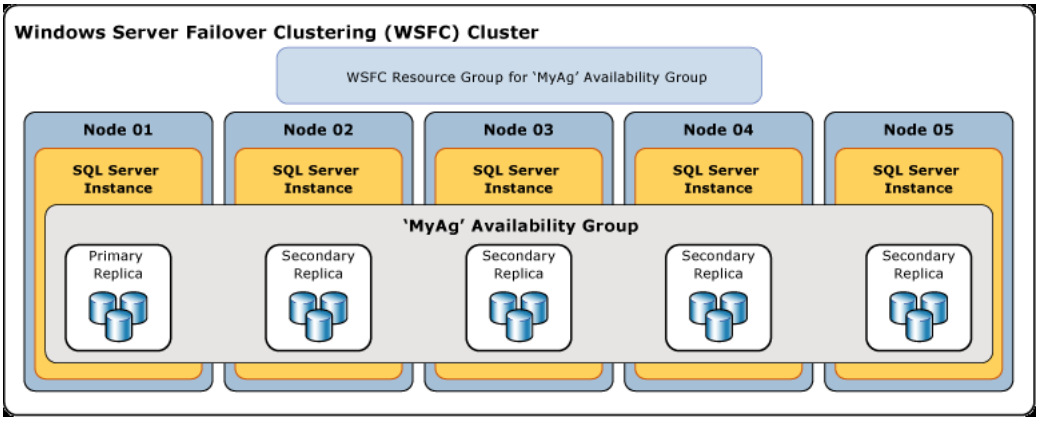
SQL Server AlwaysOn Availability Groups is currently analysed in the NCOP context:

An availability group consists of the following components:

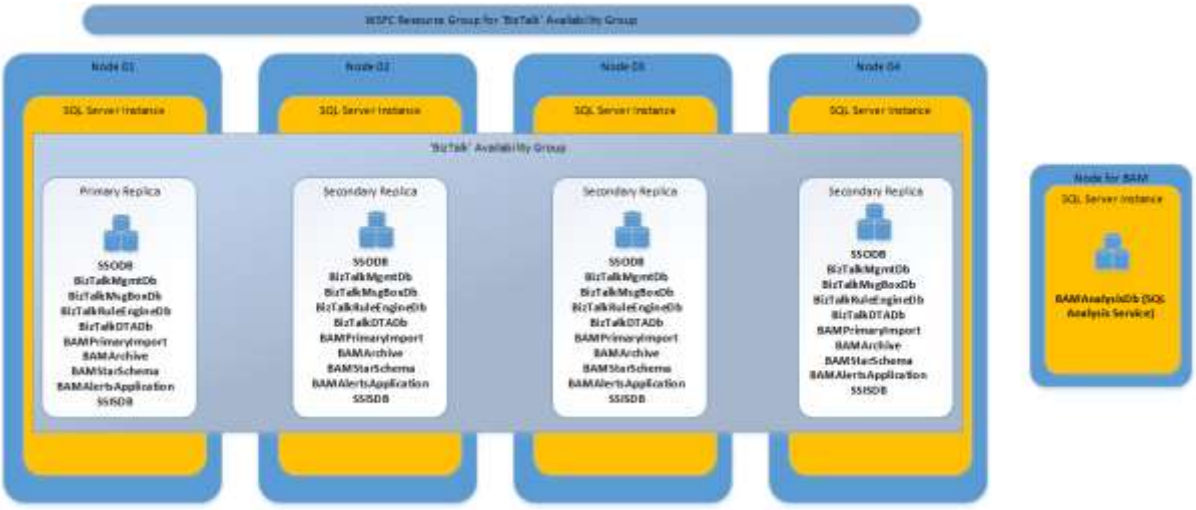
- Replicas, which are a discrete set of user databases called availability databases that fail over together as a single unit.
- A specific instance of SQL Server to host each replica and to maintain a local copy of each database that belongs to the availability group.

Deploying AlwaysOn Availability Groups requires a Windows Server Failover Clustering (WSFC) cluster. Each availability replica of a given availability group must reside on a different node of the same WSFC cluster. A WSFC resource group is created for every availability group that you create. The WSFC cluster monitors this resource group to evaluate the health of the primary replica.

The following illustration shows an availability group that contains one primary replica and four secondary replicas.



Starting with BizTalk Server 2020 and newer, high availablity for BAM DTS packages is supported using SSIS Catalog. Add the SSISDB database to the same availability group as the BizTalk Server databases. This configuration is shown in the following image, and recommended for BizTalk databases in Availability Groups

- 

5.3.5.3 Microsoft .NET Framework

Property Name	Description
Identification	Microsoft .NET Framework
Classification	TI
Behaviour	This implementation component is a COTS product (with latest patches) providing standard functionality in the Microsoft Windows Server platform. This implementation component is the execution environment of NCOP implementation components. The .NET Framework Common Language Runtime (CLR) also enables interaction between reused software components, mostly developed in C++, with newly developed software components, mostly developed in C#. The implementation component is using .NET Framework 4.7.2, 4.8 and .NET Core versions.
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

Three versions of the .NET framework are used in NCOP:

- .NET Framework 3.5 is a pre-requisite for SharePoint
- .NET Framework 4.7.2 is used for the majority of C# developments
- .NET Framework 4.8 is used for of C# developments related to NCOP databases
- .NET Core is used for SignalR (used by the DSS and the Eventing REST API consumed by the Angular Geographical COP Editor).

5.3.5.4 Microsoft Internet Information Server

Property Name	Description
Identification	Microsoft Internet Information Server
Classification	TI
Behaviour	This component is a COTS product (with latest patches) providing standard functionality in the Microsoft Windows Server platform. This implementation component is a Web server providing the infrastructure for the execution of all the NCOP Web-based applications and Web Services (either developed or provided by

Property Name	Description
	COTS software components) built using Microsoft ASP.NET and the Microsoft .NET Framework. A configuration of several IIS servers is required to handle 3000 concurrent active Users on a XL Node, and 500 on a SC Node. The server is configured with the latest patches and withholds readable information until acceptance from the User management implementation component. This configuration prevents the “forced browsing” and “path transversal” attack.
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 and the SQL Server
Interfaces	http, https
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

5.3.5.5 Java Runtime Environment

Property Name	Description
Identification	Java Runtime Environment
Classification	TI
Behaviour	The Java Runtime Environment (JRE) provides the libraries, the Java Virtual Machine and other components to run applets and applications written in the Java programming language. The Java JRE is OpenJDK 17 (with latest patches).
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 GeoServer Installed on the BizTalk Server
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	JRE
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

5.3.5.6 GeoServer

Property Name	Description
Identification	GeoServer
Classification	TI
Behaviour	The GeoServer component provides processing tools to manage map backgrounds.
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 GeoServer
Interfaces	This IC exposes maps through WMS end-points
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Medium

The GeoServer provided by NCOP is used for the following purposes:

- Expose background maps and geographic layers when Core GIS is not available.

GeoServer can leverage the ImageI/O-Ext GDAL libraries to read selected coverage formats. GDAL is able to read many formats, but for the moment GeoServer supports only a few general interest formats and those that can be legally redistributed and operated in an open source server.

JPEG2000 (Still Image Coding) is one of the image formats can be read by GeoServer using GDAL.

5.3.5.7 Installation

Property Name	Description
Identification	Installation
Classification	IS
Behaviour	This component is a set of installation packages to be installed on each NCOP node. It allows the System Administrator role to install NCOP software.
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

Property Name	Description
Interfaces	This IC interacts with the Windows Server Operating system with PowerShell
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework PowerShell WinRM (CredSSP)
References	-
Quality of Service requirements (QoS)	-
Complexity	Difficult

The following UML Use Case Diagram shows the main responsibilities of the System Administrator role.

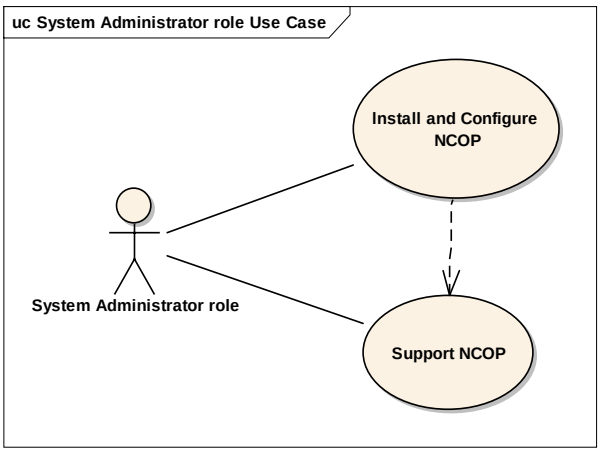


Figure 5-128: UML Use Case Diagram for System Administrator role

NCOP Installation packages are created using the InstallShield tool.

In order to offer flexibility and allow multiple deployment configurations, the NCOP installation component is made of individual packages. The following table presents the different packages and the required COTS prerequisite:

TABLE 5-11: INSTALLATION PACKAGES

Package identifier	Package description	Required COTS(*)
NCOP-SQL-Deploy	Installation of all NCOP Databases	MS SQL Server 2019
NCOP-SHP-Deploy	Installation of solutions and features for SharePoint Servers	MS SharePoint 2019
NCOP-APP-Deploy	Installation of the Geographical COP Editor (including JavaScript libraries) and all NCOP web services	IIS
NCOP-BIZ-Deploy	Installation of Host Instances and applications for BizTalk Servers	MS BizTalk Server 2020

NCOP-Maps-Deploy	Installation of NCOP default maps	GeoServer
NCOP-OLH-Deploy	Installation of NCOP Online Help	*To be installed on the same servers where NCOP-APP-Deploy is deployed*
NCOP-CBT-Deploy	Installation of NCOP Computer Based Training	*To be installed on the same servers where NCOP-APP-Deploy is deployed*
NCOP-SCC-OP-Deploy	Standalone installation of the Operational Geographical COP Editor on an external server or workstation	IIS
NCOP-SCC-Deploy	Standalone installation of the Operational, Training and Exercise Geographical COP Editors on an external server or workstation	IIS
NCOP-DYN-Deploy	Installation of the NIRIS connector 3.8 and 3.10, MCCIS, NVGStreaming, NFFI-SIP 3 connectors on a dedicated server in order to improve performances (optional).	Windows server 2019. It can be installed on the same servers where NCOP-APP-Deploy is deployed.

(*) It means that an installation package must be installed on a server where the corresponding COTS has already be installed.

Having multiple packages allows the System Administrator to be able to deploy NCOP on various hardware or virtualized configurations with different numbers of servers. It means that if multiple servers are available, NCOP components can be distributed on these servers.

For example in a standard SN configuration, each server can be used to host a specific NCOP service and the corresponding installation packages must be deployed accordingly:

- One server hosting SQL Server
  - NCOP-SQL-Deploy
- One server hosting NCOP Web services, online help and CBT
  - NCOP-APP-Deploy
  - NCOP-OLH-Deploy
  - NCOP-CBT-Deploy
- One server hosting SharePoint
  - NCOP-SHP-Deploy
- One server hosting BizTalk
  - NCOP-BIZ-Deploy
- One server hosting GeoServer cartographic server
  - NCOP-Maps-Deploy (optional)
- Optionally, another server can be dedicated to the installation and the configuration of the NIRIS connector in order to allocate all CPU resources to tracking data acquisition.
  - NCOP-DYN-Deploy

Also, NCOP installation packages are designed to be used for both basic and fail-over deployment configuration. In particular, NCOP-BIZ-Deploy and NCOP-SHP-Deploy installation packages contain specific wizard panels so the System Administrator specifies the installation type.

Prior to the deployment, an Excel template is filled with the NCOP configuration to deploy. This file is used to generate the deployment scripts. The NCOP installation packages are then deployed on top of prepared servers. There are two deployment modes available:

- **Full automated**, with a silent/verbose option. This mode is preferred for remote deployments
  - using WinRM and CredSSP (eg. DCIS deployment);
- **Semi-automated**. This mode is dedicated for environments where no deployment tool exist;

The On-Line Help and CBT applications are provided into dedicated installation packages in order to allow updates of these features independently of the other packages. The ISO image containing the On-Line Help and CBT can also be used as a standalone resource to visualize and use NCOP On-Line Help and CBT on a workstation without any installation.

5.3.6 NATO Infrastructure

5.3.6.1 Microsoft Edge

Property Name	Description
Identification	Microsoft Edge
Classification	TI
Behaviour	Edge Chromium component is standard functionality in the Windows platform since 2020. It is the Web browser giving Users' access to the NCOP Web Portal and the NCOP Web-based applications. Some specific features provided by the browser are also used to: Display the JPEG, GIF images; Print using the resolutions supported by the local and network printers or output device (using the print preview); Download some document provided as an URL to the User desktop. The web UI includes the WebParts allowing the display of IPs in many views (Geographical COP Editor, Table View …).
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 any Windows 10 workstation

Property Name	Description
Interfaces	http, https
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

NCOP allows using alternative Web Browser such as Firefox if the HTML5 is supported by the browser.

5.3.6.2 Microsoft Office

Property Name	Description
Identification	Microsoft Office
Classification	TI
Behaviour	This component is a suite of COTS software products of the Microsoft Office System, namely; Microsoft Office Word; Microsoft Office Excel; Microsoft Office PowerPoint; Microsoft Office Outlook; Microsoft Office Project.
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 any Windows 10 workstation
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

Source Information Products defined as Microsoft Office documents will be stored in their native format in the NCOP Storage and displayed with Microsoft Office software installed on each workstation.

Microsoft Excel Information Product versions supported by NCOP consumption mechanism are defined in the [ICD] (I_NCOP_EXCEL interface).

5.3.6.3 Microsoft Windows

Property Name	Description
Identification	Microsoft Windows
Classification	TI
Behaviour	Microsoft Windows 10 is the operating system installed on the workstations allowing access to NCOP services.
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 any Windows 10 workstation
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

5.3.6.4 PDF Reader

Property Name	Description
Identification	PDF Reader
Classification	TI
Behaviour	This component allows COP Users roles to use as primary output format, the Portable Document Format (PDF) for all printing purposes. PDF viewing and printing capability is a regular feature for Bi-SC AIS workstations.
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 any Windows 10 workstation
Interfaces	-
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-
Quality of Service requirements (QoS)	-
Complexity	Easy

5.3.6.5 Antivirus

Property Name	Description
Identification	Antivirus
Classification	TI
Behaviour	This component is the anti-virus COTS product (with latest patches) software installed on each NCOP hosting server and on each NCOP-delivered training workstation. The software has the ability to scan any file or directory to detect any malicious software.
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 any Windows 10 workstation 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

In order to improve performances, some folders shall be excluded from the scanning process such as temporary folder for SharePoint, BizTalk and SQL Server.

The list of folders to be excluded for each server is provided in the NCOP Installation and Configuration Guide [ICG-03] in the section 4.1 Antivirus exclusion list.

5.3.6.6 Active Directory

Property Name	Description
Identification	Active Directory
Classification	TI
Behaviour	This component is the core Bi-SC AIS directory service, Microsoft 2016 Active directory. This component provides comprehensive directory services within a Microsoft Windows-based 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	NCOP interacts with this IC through LDAP protocol
Collaboration mechanism	-
Local/Configuration data	-
Operating context	.NET Framework
References	-