FORM

IST-1999-10357

Engineering a Co-operative Inter-Enterprise Management Framework Supporting Dynamic Federated Organisations Management

Document Number:	IST-1999-10357/LMD/WP4/0522_AnnexC
Title of Deliverable:	Deliverable 11 Final Inter-Enterprise Management System Model **Annex C: Assurance System Model**
Deliverable Type: (P/R/L/I)*	P
Nature of the Deliverable: (P/R/S/T/O)**	R
Contractual Date of Delivery to the CEC:	28 February 2002
Actual Date of Delivery to the CEC:	28 February 2002

Workpackage responsible for the Deliverable:	WP4
Editor:	Brian Cullen (TCD), Jens Dyhre Mouritzen (TDC)
Contributor(s):	Niamh Quinn (BRI)
Reviewer(s):	Vincent Wade (TCD), Stefan Penter (DLT)

ABSTRACT

This Annex to FORM Deliverable 11presents the final inter-enterprise management system model for Assurance.

KEYWORDS

Assurance, GQIPS, Business Model, System Model, Analysis Model, Building Block, Contract specification

* Type: P:Public, R-Restricted, L-Limited, I-Internal

** Nature: P-Prototype, R-Report, S-Specification, T-Tool, O-Other

IST-1999-10357

FORM

Deliverable D11

Final Inter-Enterprise Management System Model

Annex C, Assurance System Model

Editor : Brian Cullen (TCD),
Jens Dyhre Mouritzen (TDC)

Status – Version : Final
Date : **28 February 2002**
Distribution : Public
Code : IST-1999-10357/LMD/WP4/0522_AnnexC

The FORM Consortium consists of:

Atos Origin Intégration (France) – *Project Coordinator*
Broadcom Eireann Research Ltd. (Ireland)
DELTA Danish, Electronics, Light & Acoustics (Denmark)
Fraunhofer FOKUS (Germany)
LM Ericsson A/S (Denmark)
TDC Tele Danmark A/S (Denmark)
Trinity College Dublin (Ireland)
UH Communications A/S (Denmark)
University College London (UK)
Waterford Institute of Technology (Ireland)
KPN Research (The Netherlands)

Table of Contents

1 Introduction

This document presents the final system model done in FORM within the Assurance Business Process Area. It demonstrates how the FORM methodology is applied to the problem of providing service assurance. However, it should be noted that only key functionality is handled. The system models can be regarded as the result of the first system development iteration.

The FORM methodology "Building Block Development Guideline" [FORM D12] is applied to the Assurance Domain in the following way:

FORM D12 Building Block Development Guideline – Workflows:	FORM D11 – FORM methodology applied in Sections:
1.Perform Business Modelling Workflow	Section 2 Business Model 2.1 Business Use Case Model 2.2 Business Object Model
2. Define Reference Architecture Workflow	2.3 Reference Architecture
3. Define Requirements Analysis Workflow	Section 3 System Model 3.1 Use case Model
4. Develop Analysis Models Workflow	3.2 Analysis Model
5. Re-organise Analysis Models Workflow	3.3 Re-organise Analysis Model and Group to Building Blocks 3.4 Building Block Specification

Table 1-1 Mapping between FORM Methodology and Assurance System Models

The Assurance Business Model in Section 2 sets the context for the system models by presenting the business use cases and business object model. The reference architecture is also presented.

The "System Models" are presented in Sections 3,4,5, and 6. Section 3 presents the Assurance Customer System Model, Section 4 presents the Assurance IESP System Model, Section 5 presents the Assurance GQIPSP System Model, and Section 6 presents the Assurance ASP System Model. System modeling involves the identification of the functionality necessary to support the system and the design of the software components necessary to provide that functionality.

First use cases and actors are identified and explained in Section 3.1. Then analysis objects that implement the use cases are identified and the interactions documented in Section 3.2. Having identified the analysis object the next step is to group these object into Building Blocks and specify their contracts, this is shown in Section 3.3 and 3.4. The complete set of contract specifications can be found in the on-line contract catalogue at the FORM website [FORM Contracts]. The same workflow is applied for Section 4,5, and 6.

2 Assurance Business Model

This section sets the context for the Assurance management business by presenting the business use cases and business object model. The assurance reference architecture is also presented.

2.1 Business Use case Model

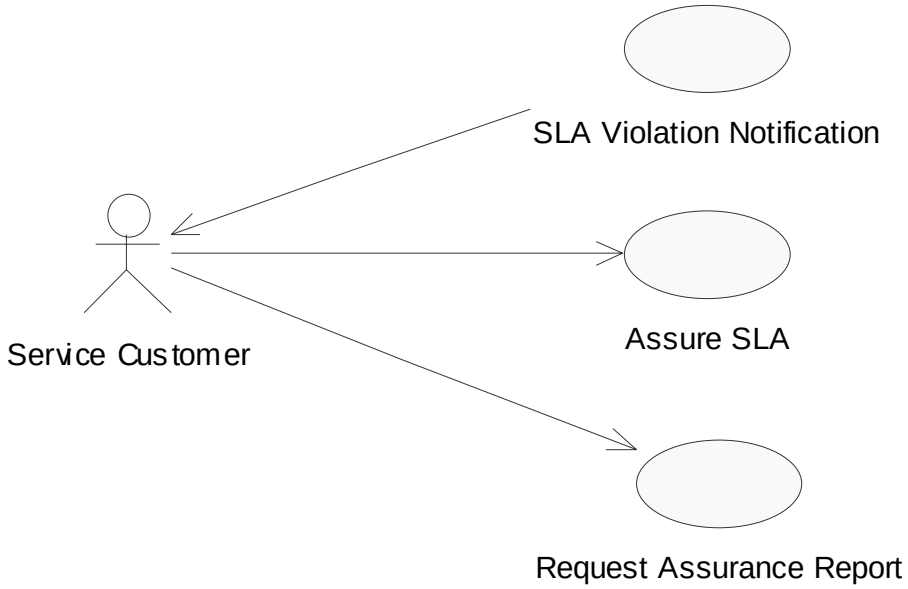

Figure 2-1 Business Use case diagram for Assurance

The business use case diagram for the Assurance System identifies three different use cases that are to be supported by the system. The first of these, *"Assure SLA"*, allows the customers SLA to be submitted to the system for assurance support. After the successful completion of this use case the customer can be assured that the metrics set forth in their SLA are being monitored. The next use case, *"Request Assurance Report"*, allows the customer to request customised reports containing processed service assurance statistics relating to both the SLA and the service as a whole. The final use case, *"Send SLA Violation Notification"*, models the situation when a metric specified in the SLA breaks its threshold. In this case the system will produce a violation report and send it to the customer immediately so that the customer is aware of the problems with their service.

2.2 Business Object Model

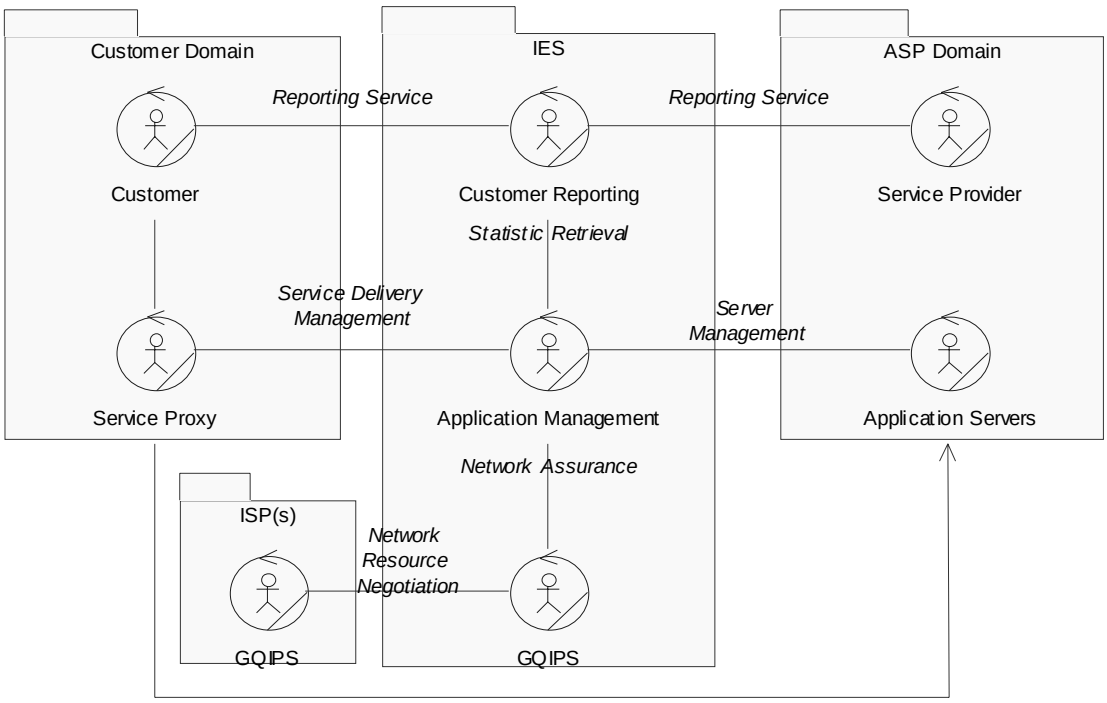

Figure 2-2 - Business Object Model for Assurance

Business Worker/Entity	Description
Customer	Subscriber of Inter-Enterprise Services. The customer negotiates and signs a SLA with the IES Provider. It receives and pays bills for serviced used. It also validates, checks against the records, and controls the usage of service.
Customer Reporting	System responsible for producing customised reports that contain data on how the service received by the customer is performing.
Service Provider	A third-party SP that provides information or multimedia services (video or VoIP teleconference).
Service Proxy	System responsible for the accepting delivery of the service for the Customer Domain. All customer access to the service is through this system.
Application Management	System responsible for managing the application in a manner to ensure that the specified SLA for the service is adhered to.
Application Servers	The systems responsible for providing the service used by the Customer.
GQIPS	System responsible for ensuring guaranteed connectivity between the ASP Domain and the Customer Domain.

Table 2-1 Assurance Business Workers

2.3 Reference Architecture

The part of the FORM reference architecture relating to the assurance system is shown in the diagram below.

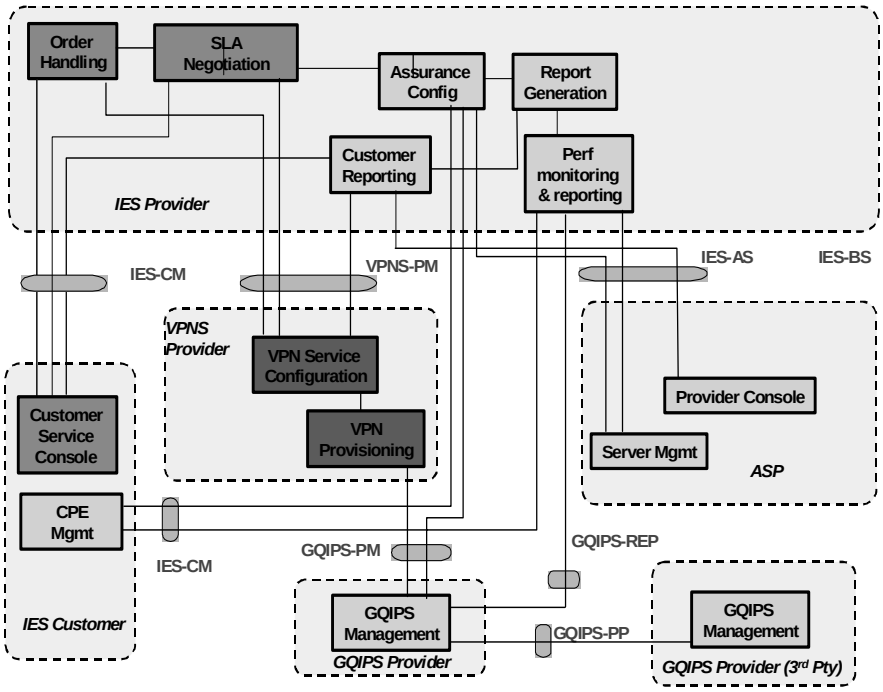

Figure 2-3 – Reference Architecture for Assurance

The figure above contains the assurance reference architecture, the system boundary definitions and a decomposition of the system into logical subsystems containing building blocks.

The relationships between these processes and the other business roles via reference points are also outlined in the reference architecture above. Each of the assurance reference points are described separately below.

IES-CM

This is the main domain boundary between the IES Customer and the IES Provider responsible for managing the customer's communication. This reference point have been divided into two separate reference point segments, one for Customer Service Console processes and one for Customer Premises Equipment (CPE) Management processes. As shown above the Service Console interacts with the Customer Reporting Process to receive reports regarding service assurance.

The Assurance Configuration process interacts with the CPE management process to manage equipment necessary to provide end-to-end assurance services. The CPE management process also interacts with the Performance Monitoring and Reporting processes to enable information about the quality of the service delivered to the IES Customer to be reported to the Assurance System.

IES-AS

This is one of two domain boundaries between the IES and Application Service Providers (ASP). The Performance Monitoring and Reporting processes interact with the ASP Server Management process in order to monitor servers in the ASP domain. The Assurance Configuration process interacts with the ASP Server Management process in order to manage configuration of servers in the ASP domain.

The ASP Provider Console interacts with the Customer Reporting in order to receive reports on how the services that they are offering are performing.

VPNS-PM

This is the main domain boundary between the IES Provider and the VPNS Provider. The Customer Reporting process interacts with the VPN Service Configuration process in order to get access to status and statistics regarding the underlying VPN Service connections.

GQIPS-PM

This is the main boundary between the Guaranteed Quality IP Service Provider and other domains that have processes that use or rely on the GQIPS Service. In this case the IES Provider and the VPNS Provider rely on the GQIPS. GQIPS-PM provides support for resource allocation requests. The Assurance Configuration process interacts with the GQIPS Management process to manage assurance of the underlying IP Services.

GQIPS-REP

This reference point enables the Performance Monitoring & Reporting process to receive statistics relating to the how the requested network connectivity being provided to the Customer is performing.

GQIPS-PP

This is the boundary between different ISPs that need to interact in order to provide guaranteed IP connectivity across multiple domains. It logically represents the management interactions between two GQIPS providers. Support is provided for resource allocation requests between ISPs.

3 Assurance Customer System Model

In this section the Customer System Model for the assurance system will be presented. This will involve the identification of the functionality necessary to support the assurance system in the customer domain and the design of the software components necessary to provide that functionality.

3.1 Use case Model for Assurance Customer System Model

In this section the use cases that must be supported in the Customer Domain and the actors that use these use cases are identified and explained.

Actor Name	Role Taken
IESP	Represents the IESP systems when they are shown interacting with system in other domains.

Table 3-1 Assurance Actor

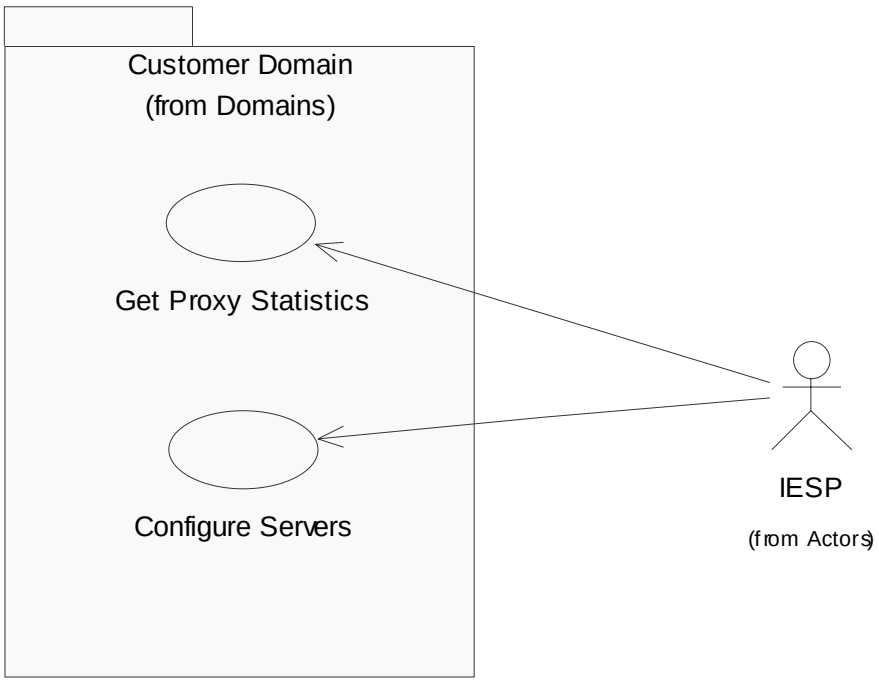

Figure 3-1 Use case diagrams for the Assurance System

Use case Name	Get Proxy Statistics
Summary	Statistics generated at the service proxy are necessary to monitor how an SLA is being conformed to. This use case allows server statistics to be polled as necessary.
Actors	IESP
Pre-Conditions	There is a valid SLA
Begins When	The proxy statistics are requested.
Steps	1. The system requests statistics from the proxy. 2. The proxy collates the necessary statistics. 3. The report is returned to the system.
Ends when	The proxy statistics are reported.
Post-Conditions	None
Exceptions	None
Traceability	Requirements: [IA-II.10] [IA-II.07]

Table 3-2 Use case description of "Get Proxy Statistics"

Use case Name	Configure Servers
Summary	When SLAs are introduced/removed from the system then the underlying servers need to be reconfigured to monitor them.
Actors	IESP
Pre-Conditions	A new server configuration has been produced.
Begins When	The new configuration is being deployed.
Steps	1. A new configuration for the servers has been formulated and is ready for deployment. 2. The configuration is deployed to the servers.
Ends when	The new configuration is deployed.
Post-Conditions	None
Exceptions	None
Traceability	Requirements: [EC-II.28]

Table 3-3 Use case description of "Configure Servers"

3.2 Analysis Model for Assurance Customer System Model

In this section analysis objects deemed necessary to implement the previously identified use cases are identified and the interactions documented.

3.2.1 Boundary Objects

Boundary Objects	Responsibility
Instrumentation Interface	The interface through which statistics related to the servers/proxy being monitored may be accessed.

Table 3-4 Boundary Objects for Assurance Customer System

3.2.2 Control Objects

Control Objects	Responsibility
Server Components	Represents the components of the assurance system locally managing the servers/proxy involved in providing the service.

Table 3-5 Control Objects for Assurance Customer System

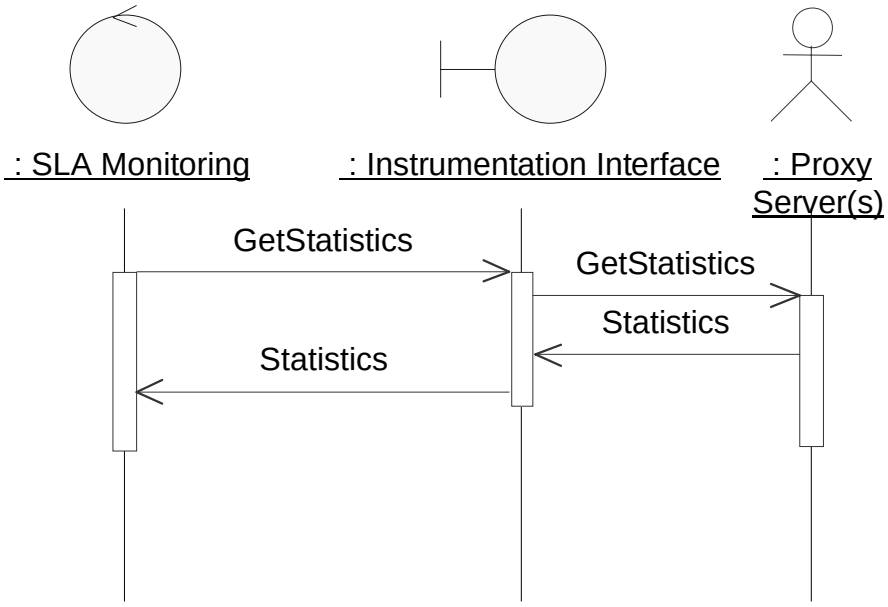

Figure 3-2 Object diagram with analysis objects implementing use case "Get Proxy Statistics"

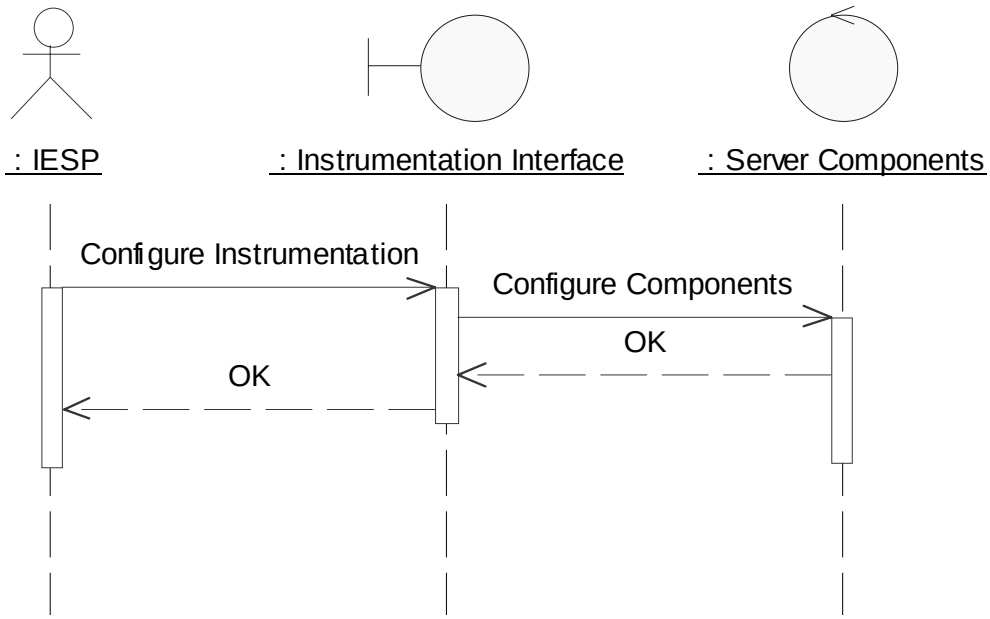

Figure 3-3 Object diagram showing analysis objects implementing use case "Configure Servers"

3.3 Re-organise Analysis Model and Group to Building Blocks for Assurance Customer System Model

Having identified the analysis object necessary to implement the necessary use cases the next step is to group these object into Building Blocks. In this domain it was felt that one Building Block was sufficient, as shown below.

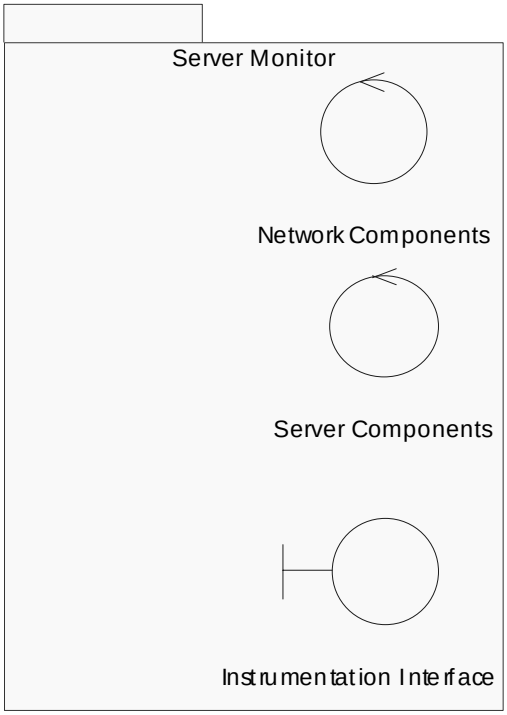

Figure 3-4 Collaboration diagram showing Building Blocks and Building Block Contracts

The following interaction diagram shows more details about the relations between the building blocks and the actors and how they interact to fulfil the identified use cases.

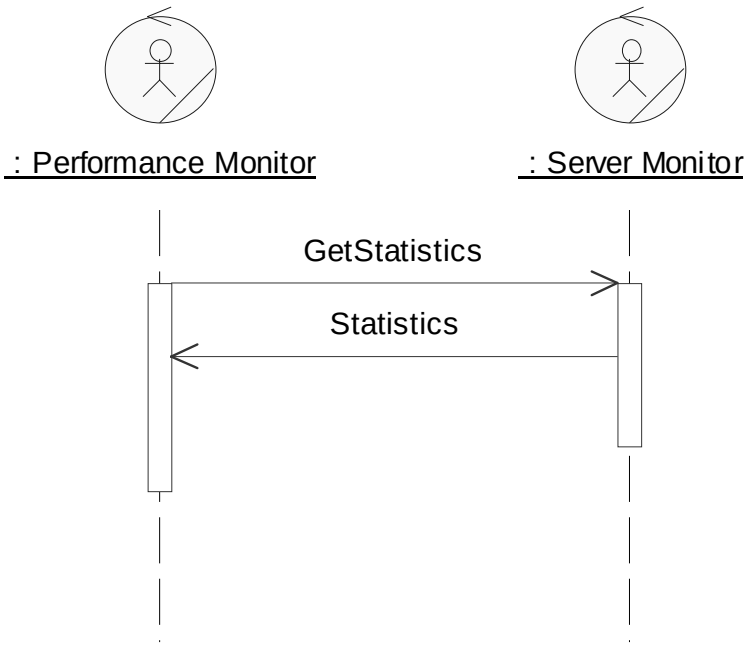

Figure 3-5 Interaction diagram for the use case "Get Proxy Statistics" showing the use of BB

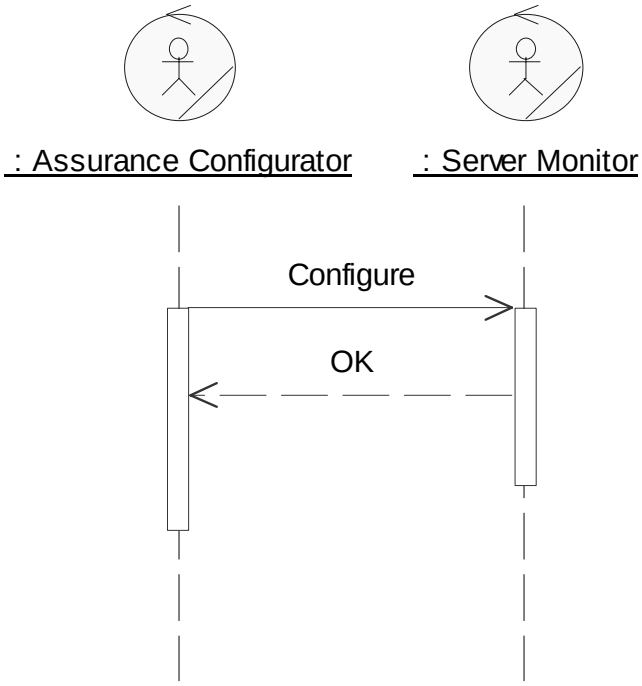

Figure 3-6 Interaction diagram for the use case "Configure Servers" showing the use of BB

3.4 BB Contract specification for Assurance Customer System Model

One contract has been specified for the Assurance system within the Customer System Model (this contract is shared with the ASP System Model). This contract is based on the XML Schema described in Annex E. A summary of this contract is provided below. This and other contract specifications can be found in the on-line contract catalogue at the FORM website [FORM Contracts].

Contract Name	Description
ServerMonitor	This contract allows access to the CIM information base stored in the Server Monitor building block. This building block monitors server statistics, calculating secondary combinatory statistics when necessary. Both primary and secondary statistics are stored within the information base for retrieval. Objects facilitating the management of the Server Monitor itself are also present in the information base. These objects perform a number of different tasks such as initialising and managing downloadable extensions to the module.

Table 3-6 Assurance Customer System contract description

4 Assurance IESP System Model

In this section the IESP System Model for the assurance system will be presented. This will involve the identification of the functionality necessary to support the assurance system in the IESP domain and the design of the software components necessary to provide that functionality.

4.1 Use case Model for Assurance IESP System Model

Actor Name	Role Taken
Customer Care	The part of the IES involved with dealing with customers.
Customer Domain Manager	The person or persons in charge of the customer domain. It is this person who would originally order the service that is being assured.
Order Handling	The part of the IES concerned with introducing new orders.
Application Servers	The different nodes and servers that when used together provide the service being offered by the Application Service Provider.
Application Service Manager	The person or persons with the responsibility of managing the part or all of the service that the customer wants to use.
Underlying Network	Represents the underlying software and hardware that provide the IP connectivity between the various parties.
Assurance Event Listener	Individuals or organisations interested in receiving notifications from the system when errors occur or certain thresholds are met.
IES Manager	The individual or organisation responsible for managing the IESP system and specifying the policies to be implemented by it.
Service Proxy	Represents the point of delivery of the service within the customer domain. Assurance is to this point only.

Table 4-1 Assurance IESP Actors

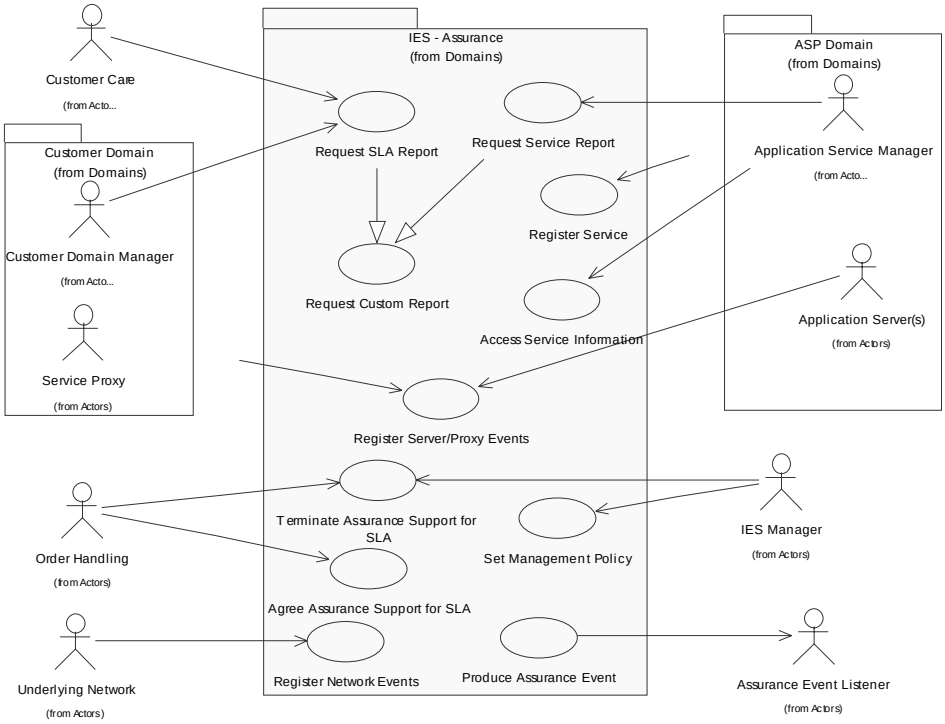

Figure 4-1 Use case diagram for the Assurance IESP System

Use case Name	Request SLA Report
Summary	Allows a report on the conformance of a service to a particular SLA to be obtained.
Actors	Customer Care, Customer Domain Manager
Pre-Conditions	An valid SLA must be specified
Begins When	A report is requested
Steps	1. A report is requested for a particular SLA. 2. The specified SLA is checked to ensure that it is valid. 3. Statistics related to the SLA are collated and a report is produced.
Ends when	A report is issued
Post-Conditions	None
Exceptions	An invalid SLA is specified
Traceability	Business Case: "*Request Assurance Report*" Requirements: [EC-II.28] [EC-II.29][IA-II.10]

Table 4-2 Use case description of "Request SLA Report"

Use case Name	Produce Assurance Event
Summary	When an SLA term is violated an asynchronous notification or event is produced to inform interested parties of that fact.
Actors	Assurance Event Listener
Pre-Conditions	At least one SLA must be registered in the system
Begins When	A threshold in a SLA registered with the system has been violated.
Steps	1. The performance of a service monitored by the system degrades below the level specified in an SLA. 2. An even is produced detailing the degradation and sent to interested parties.
Ends when	The event has been delivered.
Post-Conditions	None
Exceptions	None
Traceability	Business Case: "*SLA Violation Notification*" Requirements: [EC-II.27][IA-II.07][IA-II.09][IA-V.16]

Table 4-3 Use case description of "Produce Assurance Event"

Use case Name	Request Service Report
Summary	Allows a report on the performance of a service that is monitored by the Assurance system.
Actors	Application Service Manager
Pre-Conditions	The service specified must be one for which the system is monitoring for SLA conformance.
Begins When	A service performance report is requested
Steps	1. A report is requested for a particular service. 2. The specified service is checked to ensure that it is valid. 3. Statistics related to the SLA are collated and a report is produced.
Ends when	The report has been produced
Post-Conditions	None
Exceptions	An invalid service was specified
Traceability	Business Case: "*Request Assurance Report*" Requirements: [EC-II.28][IA-II.10]

Table 4-4 Use case description of "Request Service Report"

Use case Name	Register Server/Proxy Event
Summary	When errors on a server occur it is not always sufficient for these errors to be reported at the next poll. It is possible therefore for asynchronous notification of problems to be produced.
Actors	Application Server(s), Service Proxy
Pre-Conditions	The server is part of a service being monitored.
Begins When	The performance of the service degrades
Steps	1. The performance of a service at a particular server/proxy degrades. 2. Information about the degradation is retrieved and sent in a notification/event.
Ends when	The degradation has been reported.
Post-Conditions	None
Exceptions	None
Traceability	Requirements: [EC-II.27] [IA-II.08]

Table 4-5 Use case description of "Register Server/Proxy Event"

Use case Name	Register Network Events
Summary	When errors in the network occurs it is not always sufficient for these errors to be reported at the next poll. It is possible therefore for asynchronous notification of problems to be produced.
Actors	Underlying Network
Pre-Conditions	The network is part of a service being monitored.
Begins When	The performance of the network degrades
Steps	1. The performance of the network degrades. 2. Information about the degradation is retrieved and sent in a notification/event.
Ends when	The degradation has been reported.
Post-Conditions	None
Exceptions	None
Traceability	Requirements: [EC-II.27][IA-II.08]

Table 4-6 Use case description of "Register Network Events"

Use case Name	Set Management Policy
Summary	This use case allows the IES Manager to use policy to control the behaviour of the overall system.
Actors	IES Manager
Pre-Conditions	None
Begins When	A new policy is formulated.
Steps	1. The IES Manager submits the new policy to the system. 2. The policy is checked to ensure it is valid. 3. The policy is adopted by the system.
Ends when	The policy is adopted by the system.
Post-Conditions	The new policy is enforced in the system
Exceptions	The policy is not valid.
Traceability	Requirements: [IA-V.15]

Table 4-7 Use case description of "Set Management Policy"

Use case Name	Terminate Assurance Support for SLA
Summary	When a customer no longer wishes to use a particular service then he can request that the SLA be terminated.
Actors	Order Handling, IES Manager
Pre-Conditions	The SLA must be registered with the system
Begins When	A request to terminate the SLA is made.
Steps	1. A request is made to terminate assurance support for a particular SLA. 2. The SLA is removed from the system.
Ends when	The SLA is terminated.
Post-Conditions	The system is no longer monitoring the SLA.
Exceptions	The specified SLA is not valid
Traceability	Requirements: [EC-II.26][IA-I.05][IA-II.06][IA-I.02][IA-I.03][IA-V.17]

Table 4-8 Use case description of "Terminate Assurance Support for SLA"

Use case Name	Agree Assurance Support for SLA
Summary	When a customer wishes to use a service with the assurance of particular service guarantees then this usecase can be used to introduce the SLA to the system.
Actors	Order Handling
Pre-Conditions	An SLA has been agreed between the customer and the service provider.
Begins When	The agreed SLA is sent to the assurance system
Steps	1. The agreed SLA is introduced to the system. 2. The SLA is checked to ensure it is valid. 3. The system is configured to support the SLA.
Ends when	The SLA has been excepted by the system
Post-Conditions	The system is now monitoring the SLA
Exceptions	The SLA is invalid
Traceability	Business Case: "*Assure SLA*" Requirements: [EC-II.26][IA-I.05][IA-II.06][IA-I.02][IA-I.03] [IA-V.17]

Table 4-9 Use case description of "Agree Assurance Support for SLA"

Use case Name	Register Service
Summary	To support an SLA for a particular service then it is necessary to know the structure of the service. This use case allows this structure to be registered with the assurance system.
Actors	Application Service Manager
Pre-Conditions	A new service for which assurance support is desired has been produced.
Begins When	The ASM tries to register the service.
Steps	1. The ASM passes the service information to the assurance system. 2. The system checks to ensure that the information is valid. 3. The service is then registered with the system.
Ends when	The service is registered
Post-Conditions	None
Exceptions	The service information is not valid.
Traceability	Requirements: [IA-I.04]

Table 4-10 Use case description of "Register Service"

Use case Name	Request Custom Report
Summary	Supports display of service details on customers fixed or mobile terminals, on demand from the customer.
Actors	Customer Care, Customer Domain Manager.
Pre-Conditions	An valid SLA must be specified. Details of a customers service and communication must be available to the Customer Reporting Sub-system.
Begins When	A report is requested
Steps	1. Customer selects report context from his terminal. 2. The data to be reported are collected and filtered to fit the customer needs. This includes data requested via the Request Service Report or Request SLA report use cases. 3. The resulting report is displayed on the customer's terminal.
Ends when	A report is issued
Post-Conditions	None
Exceptions	An invalid SLA is specified
Traceability	Business Case: "*Request Assurance Report*" Requirements: [EC-II.28][EC-II.29][IA-II.10]

Table 4-11 Use case description of "Request Custom Report"

Use case Name	Access Service Information
Summary	When SLAs are introduced/removed from the system then the underlying network needs to be reconfigured to monitor them.
Actors	Application Service Manager
Pre-Conditions	At least one service is registered with the system
Begins When	Access to the service information is requested.
Steps	1. Access to all or part of the information relating to services registered with the system is requested. 2. The requested information is retrieved.
Ends when	The requested information is returned.
Post-Conditions	None
Exceptions	The requested information does not exist.
Traceability	Requirements: [IA-I.04]

Table 4-12 Use case description of "Access Service Information"

4.2 Analysis Model for Assurance IESP System Model

In this section the analysis object necessary to fulfill the use cases identified in the previous section are identified and explained. Also provided are interaction diagrams showing how these use cases must interact with each other to fulfill the use case requirements.

4.2.1 Boundary Objects

Boundary Objects	Responsibility
Terminate SLA	Used to accept requests to terminate support for a particular SLA.
Start Assurance	Used to accept requests to start assurance support for an SLA.
Register Service	Used to accept requests to register a service with the system.
Get Service Information	Used to accept requests for information on registered services
Request Service Report	Used to accept requests for assurance reports for an entire service.
Request SLA Report	Used to accept requests for assurance reports for an SLA.
Set Management Policy	Used to accept requests to change the Assurance System policy.
Accept Events	Used to accept requests to accept asynchronous notifications.
Event Channel	Used to send assurance notifications to interested listeners.

Table 4-13 Boundary Objects for Assurance IESP System Model

4.2.2 Entity Objects

Entity Objects	Responsibility
SLA Details	Holds information on the SLAs to be supported by the system.
SLA Statistics	Holds information on how a particular SLA has been conformed to.
Service Information	Holds information about how the supported service can be monitored.
Management Policy	Holds information on how the Assurance System should behave.

Table 4-14 Entity Objects for Assurance IESP System Model

4.2.3 Control Objects

Control Objects	Responsibility
Configure Assurance	Configures the assurance system to support a specified set of SLAs.
Manage Service Info	Manages changes and access to service information.
Generate Custom Report	Customises an assurance report for viewing by a particular user.
Generate Report	Gathers statistics and information to produce service assurance report.
Validate Management Policy	Manages changes to management policy governing Assurance System.
SLA Monitoring	Monitors the components of the different services to ensure that the supported SLAs are conformed to.

Table 4-15 Control Objects for Assurance IESP System Model

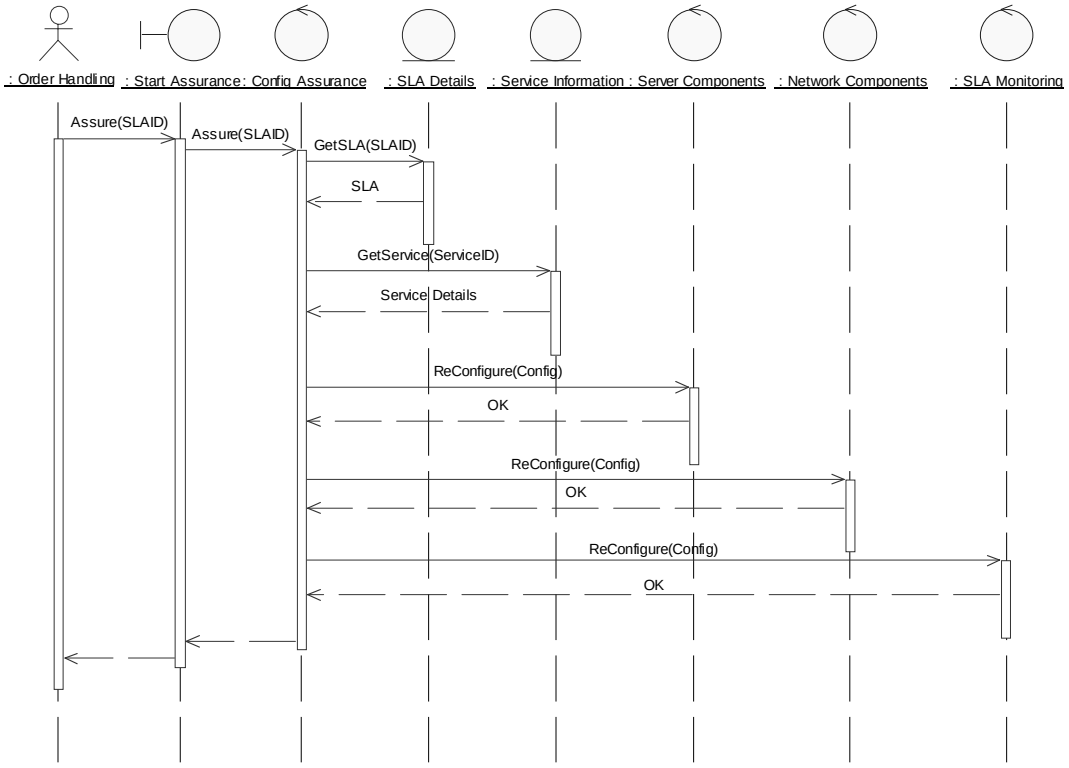

Figure 4-2 Analysis objects implementing use case "Agree Assurance Support for SLA"

The control objects for server- and network components are part of the ASP system model explained in section 6.

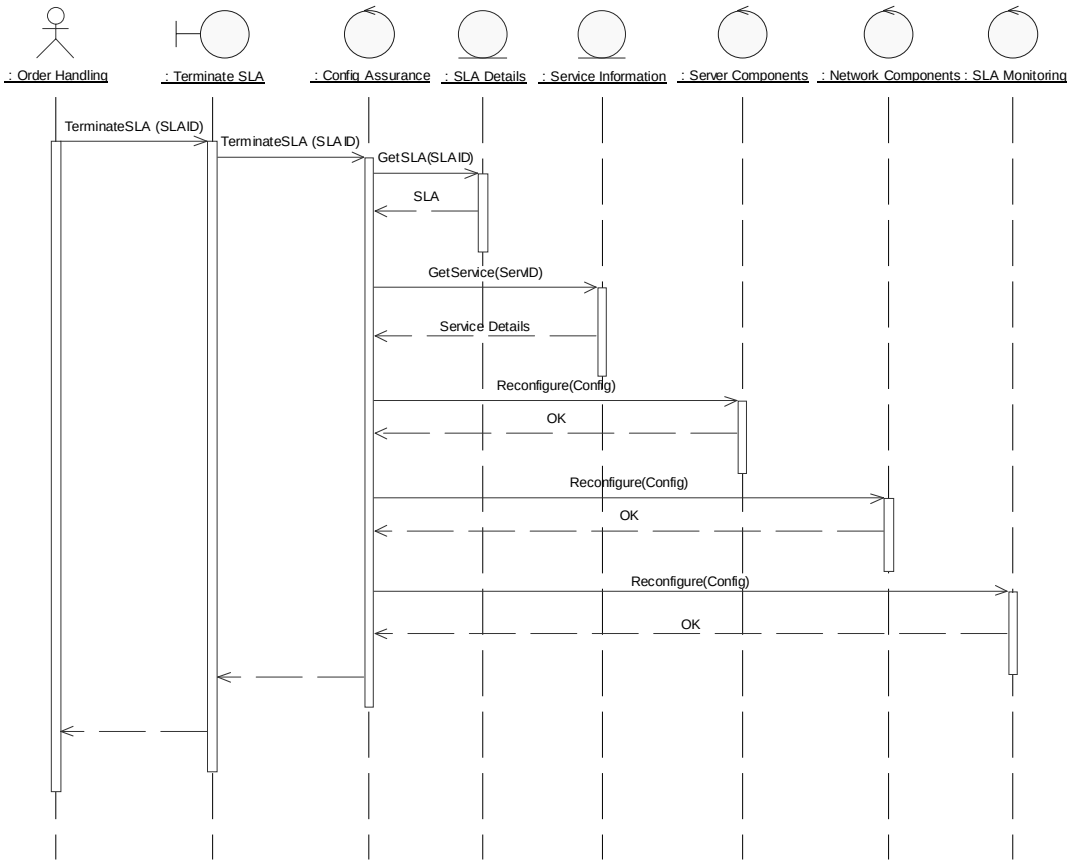

Figure 4-3 Analysis objects implementing use case "Terminate Assurance Support for SLA"

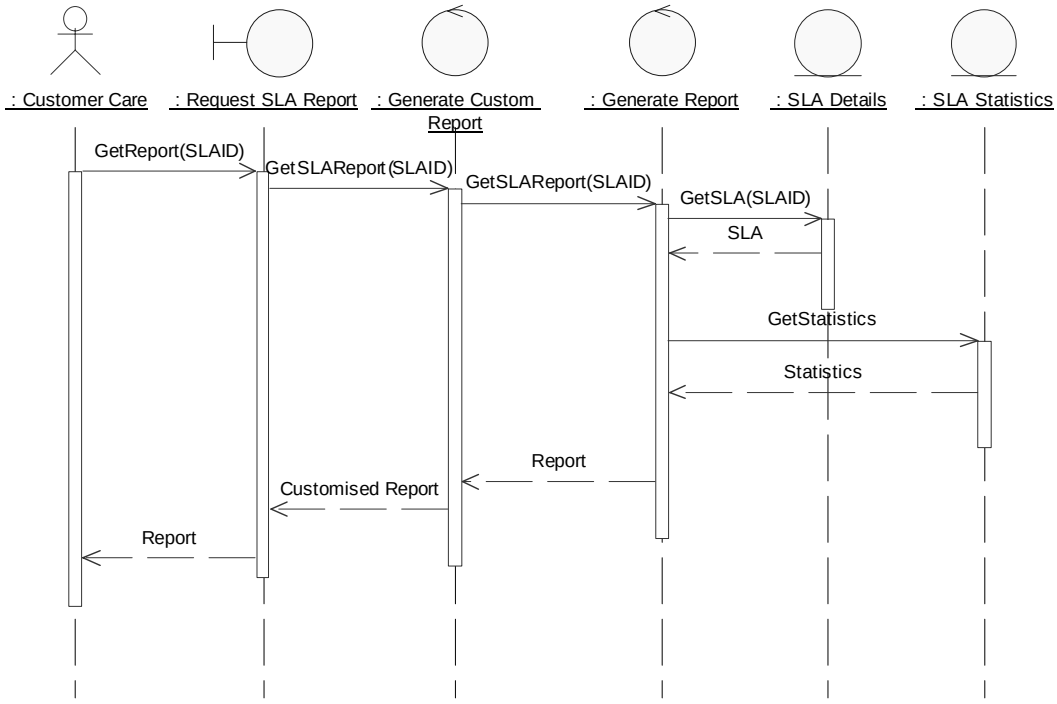

Figure 4-4 Object diagram of the analysis objects implementing use case "Request SLA Report"

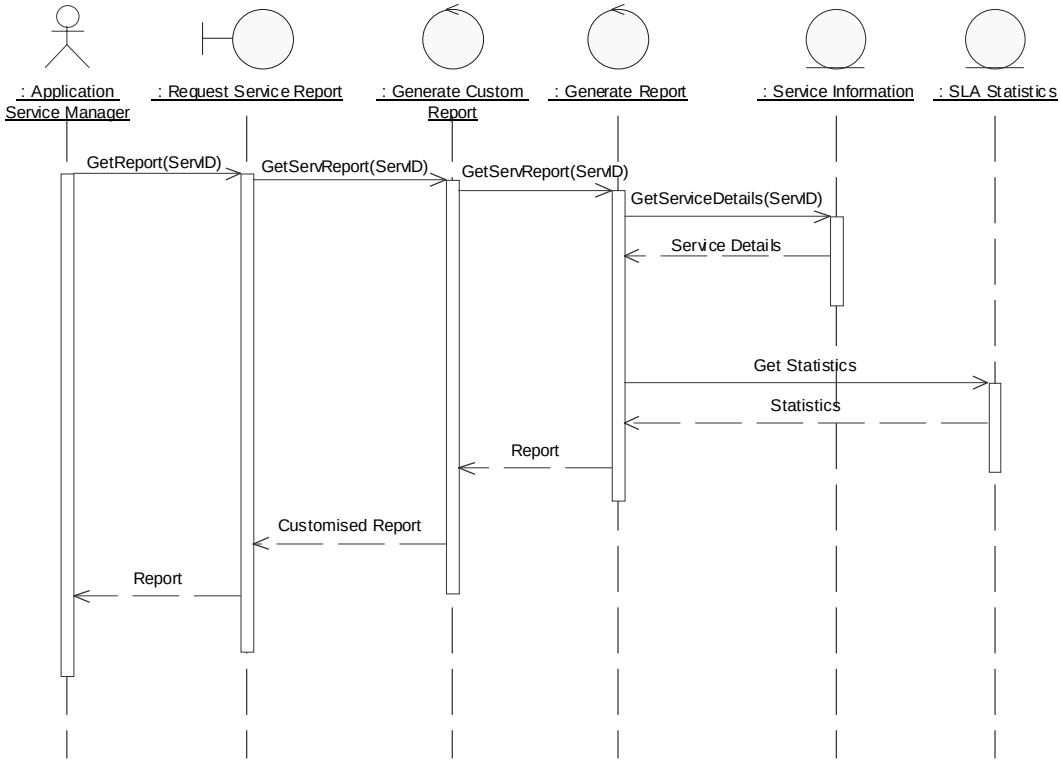

Figure 4-5 Object diagram of analysis objects implementing use case "Request Service Report"

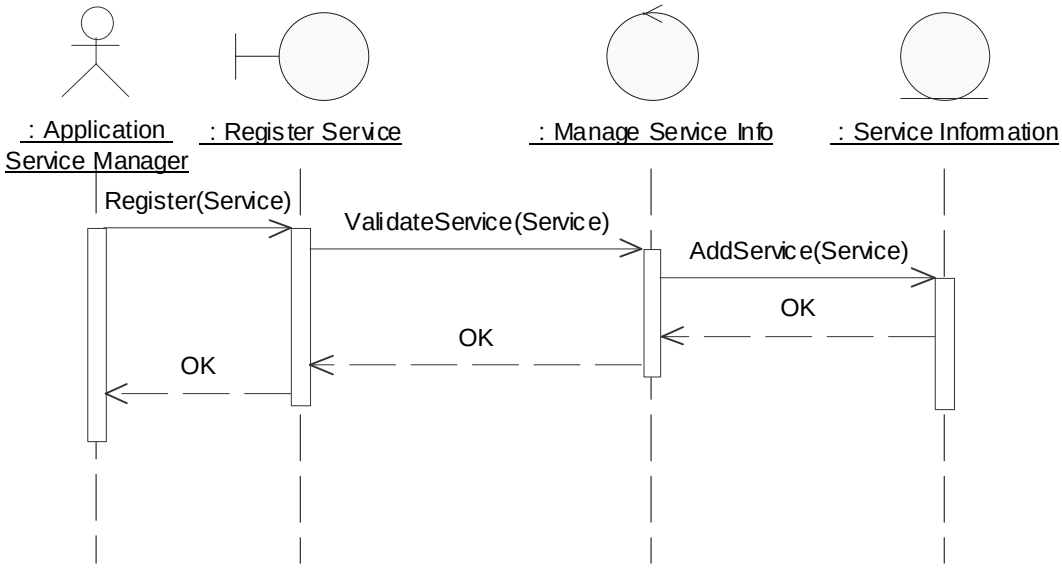

Figure 4-6 Object diagram of the analysis objects implementing use case "Register Service"

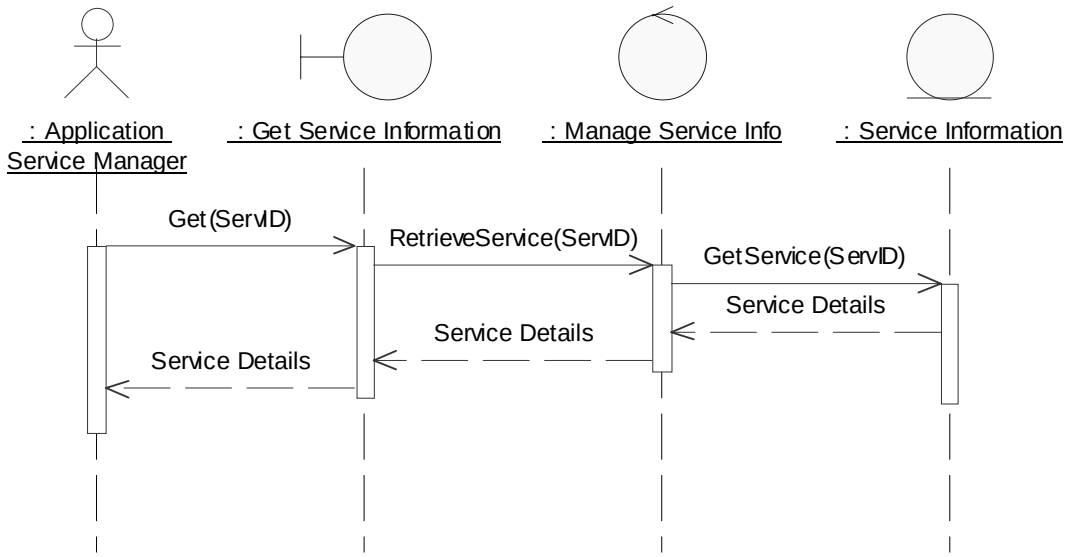

Figure 4-7 Object diagram of analysis objects implementing "Access Service Information"

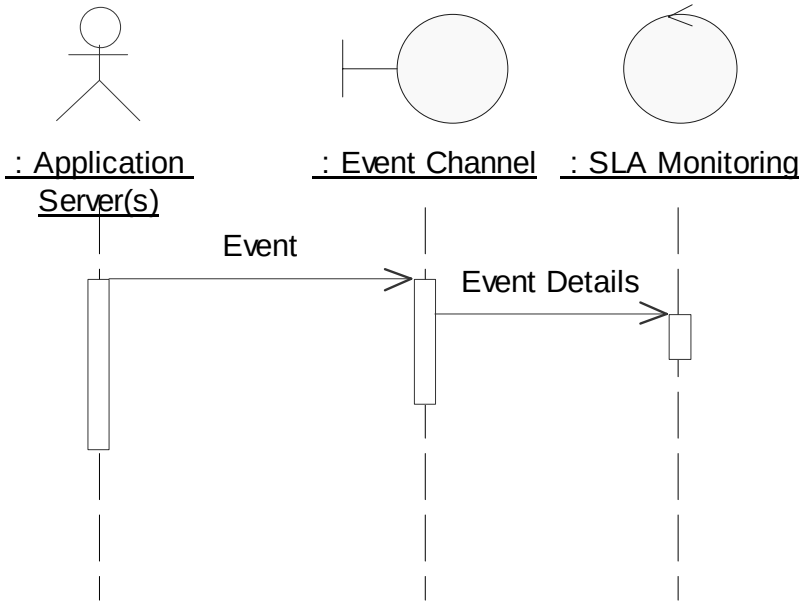

Figure 4-8 Analysis objects implementing use case "Register Server/Proxy Events"

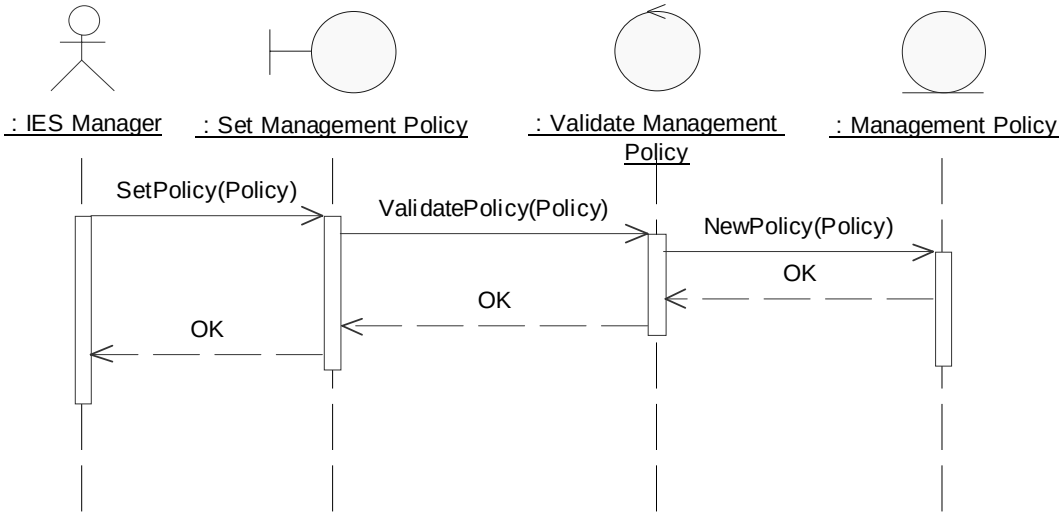

Figure 4-9 Object diagram showing analysis objects implementing "Set Management Policy"

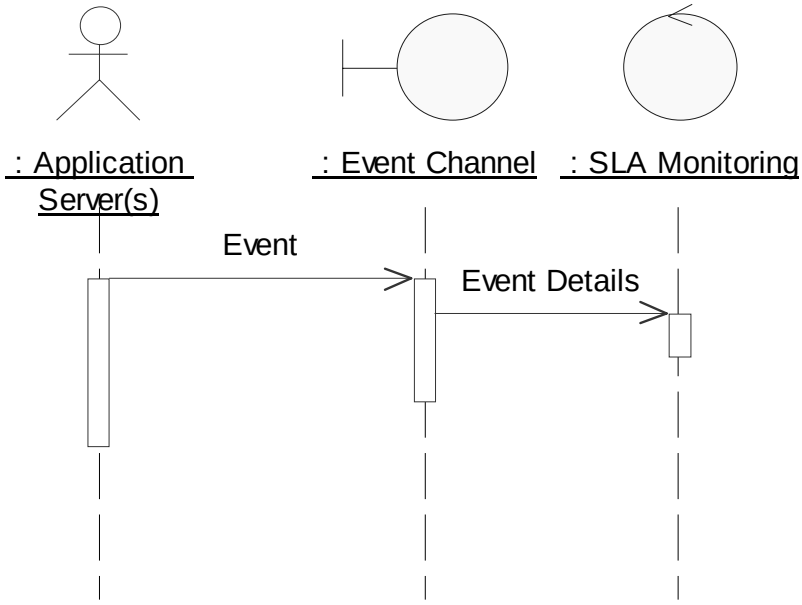

Figure 4-10 Analysis objects implementing use case "Register Network Events"

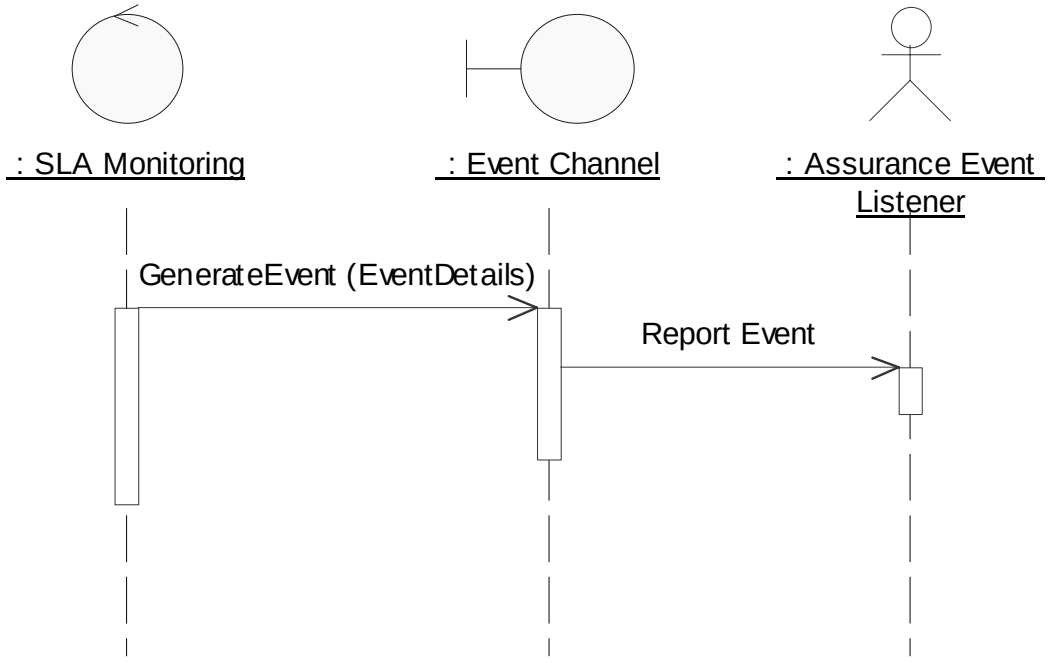

Figure 4-11 Analysis objects implementing use case "Produce Assurance Event"

4.3 Re-organise Analysis Model and Group to Building Blocks for Assurance IESP System Model

Having identified the analysis objects necessary to fulfill the use cases the next step is to group them into units or Building Blocks. For the IESP it was decided that there should be four different BBs as shown in the diagram below. For each grouping the associated analysis object and the points of interaction between them are shown.

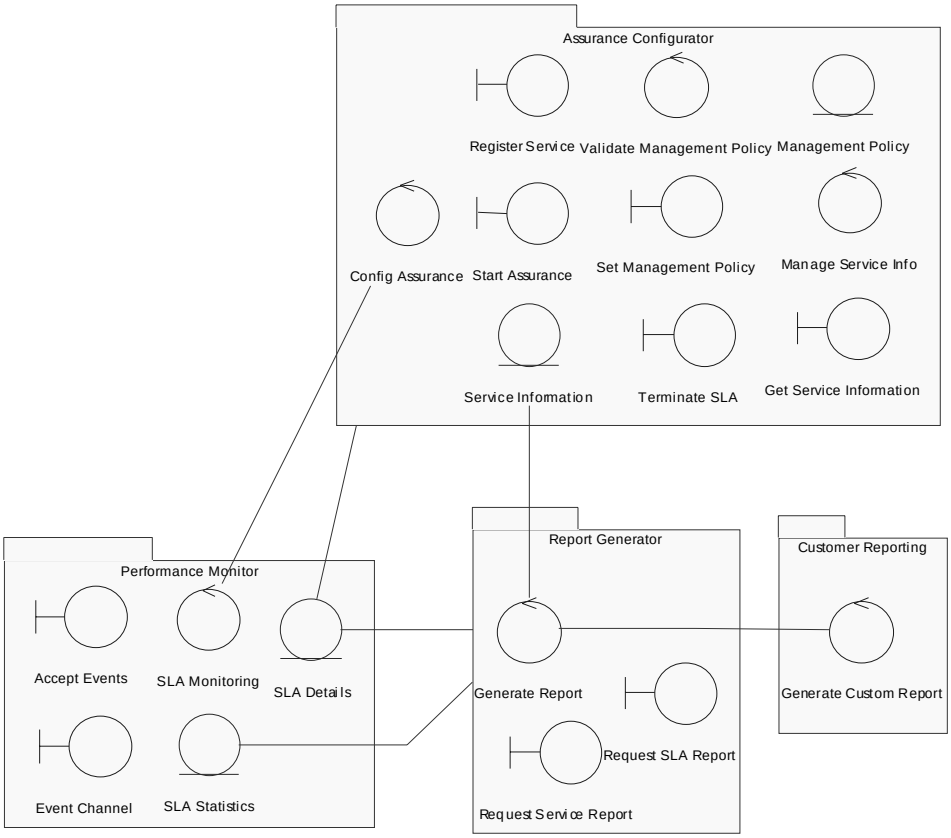

Figure 4-12 Collaboration diagram showing Building Blocks and Building Block Contracts

The following interaction diagram shows more details about the relations between the building blocks and the actors necessary to fulfil the use cases.

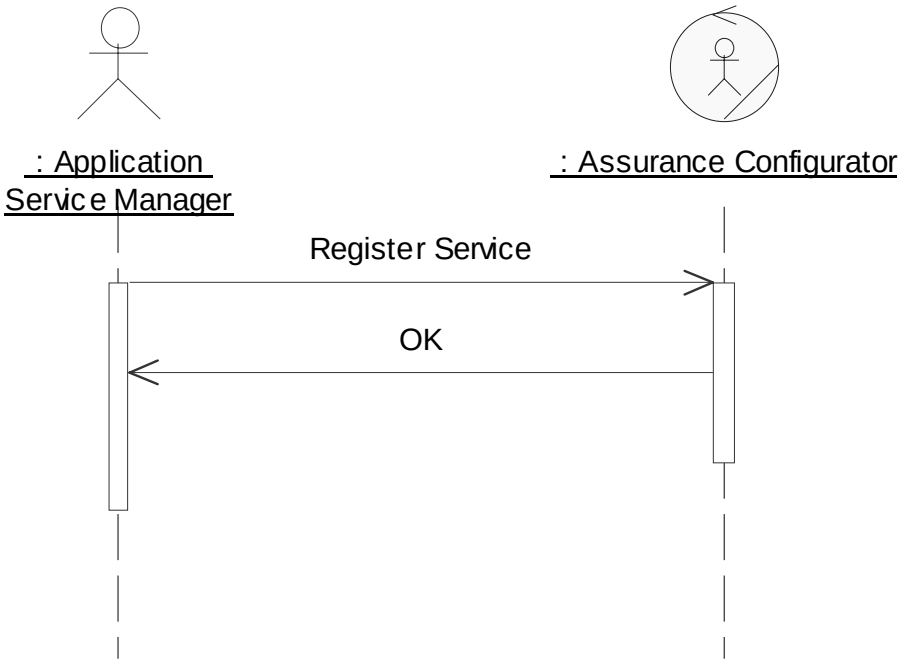

Figure 4-13 Interaction diagram for the use case "Register Service" showing the use of BB

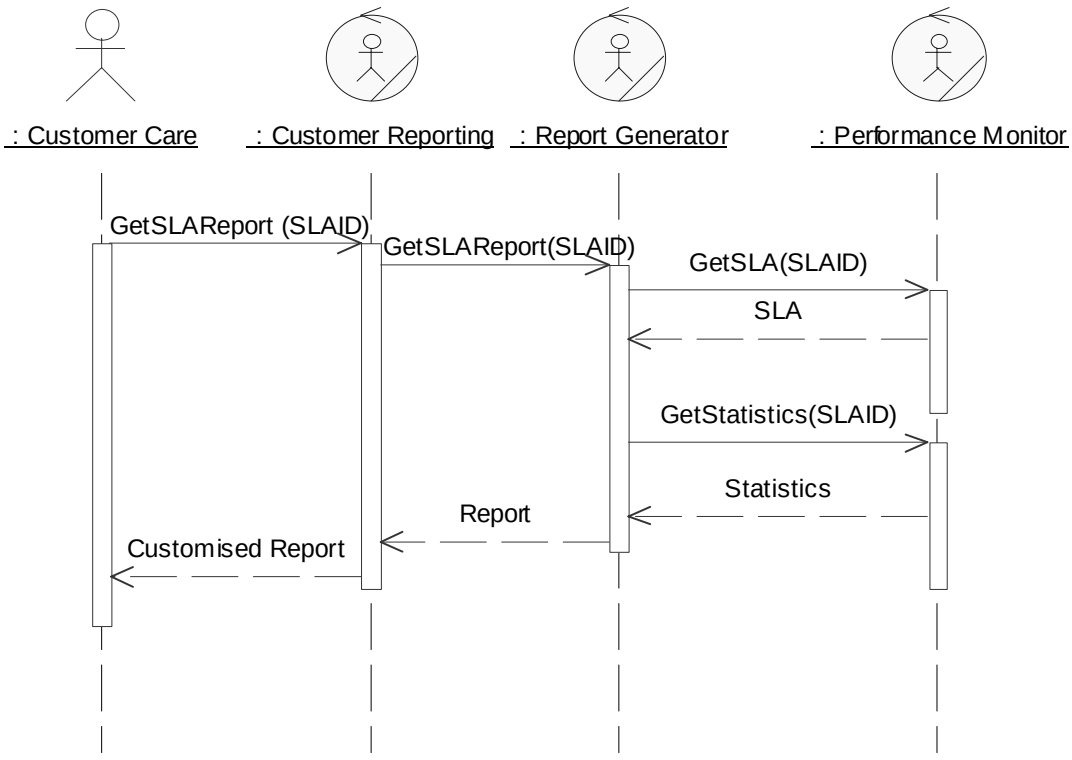

Figure 4-14 Interaction diagram for use case "Request SLA Report" showing the use of BB

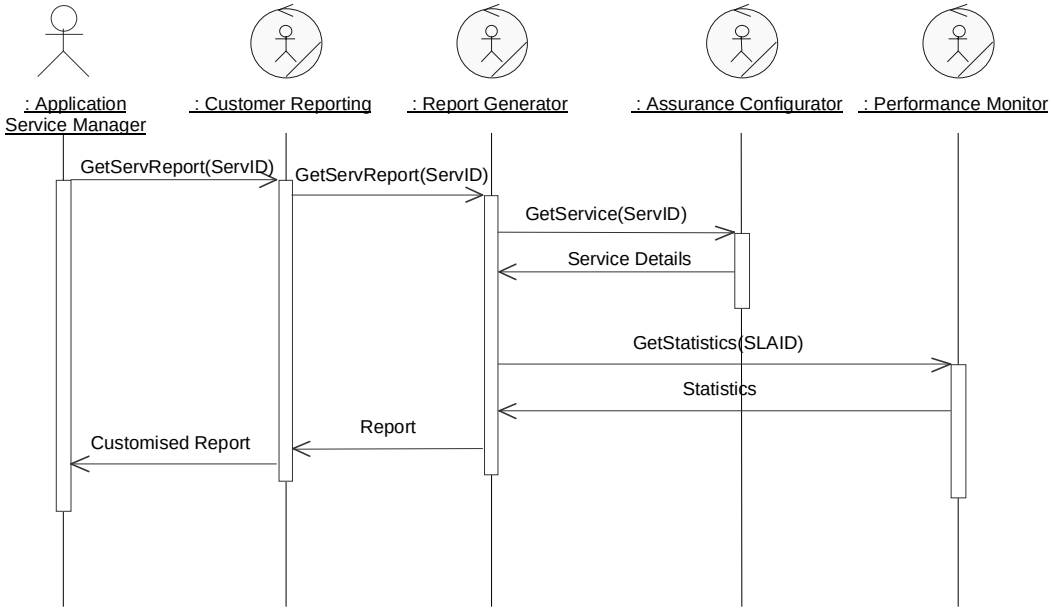

Figure 4-15 Interaction diagram for use case "Request Service Report" showing the use of BB

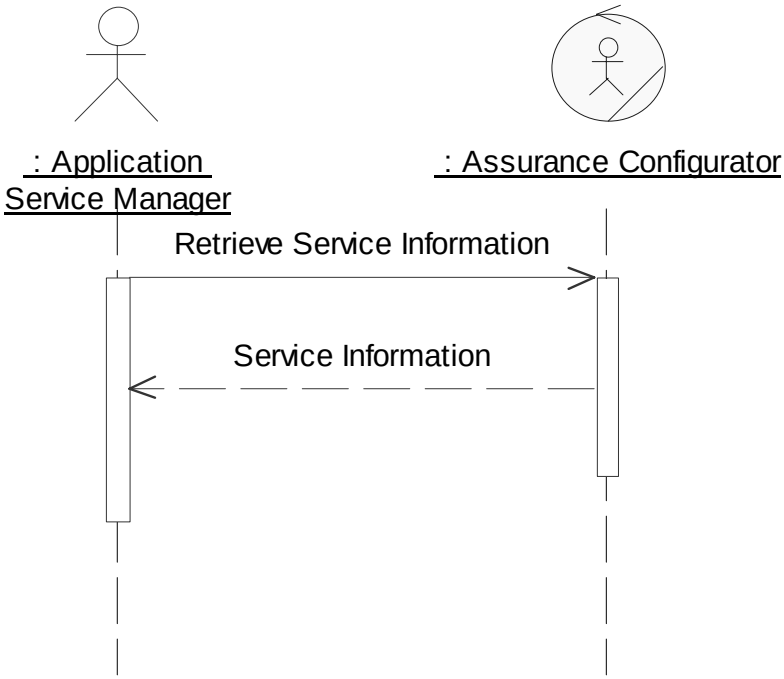

Figure 4-16 Interaction diagram for use case "Access Service Information" showing use of BBs

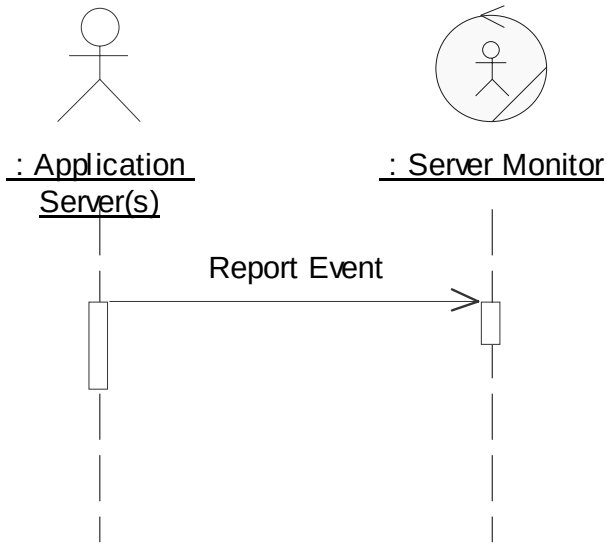

Figure 4-17 Interaction diagram for use case "Register Server/Proxy Events" showing use of BB

The Server Monitor BB is part of the ASP System Model explained in section 6.

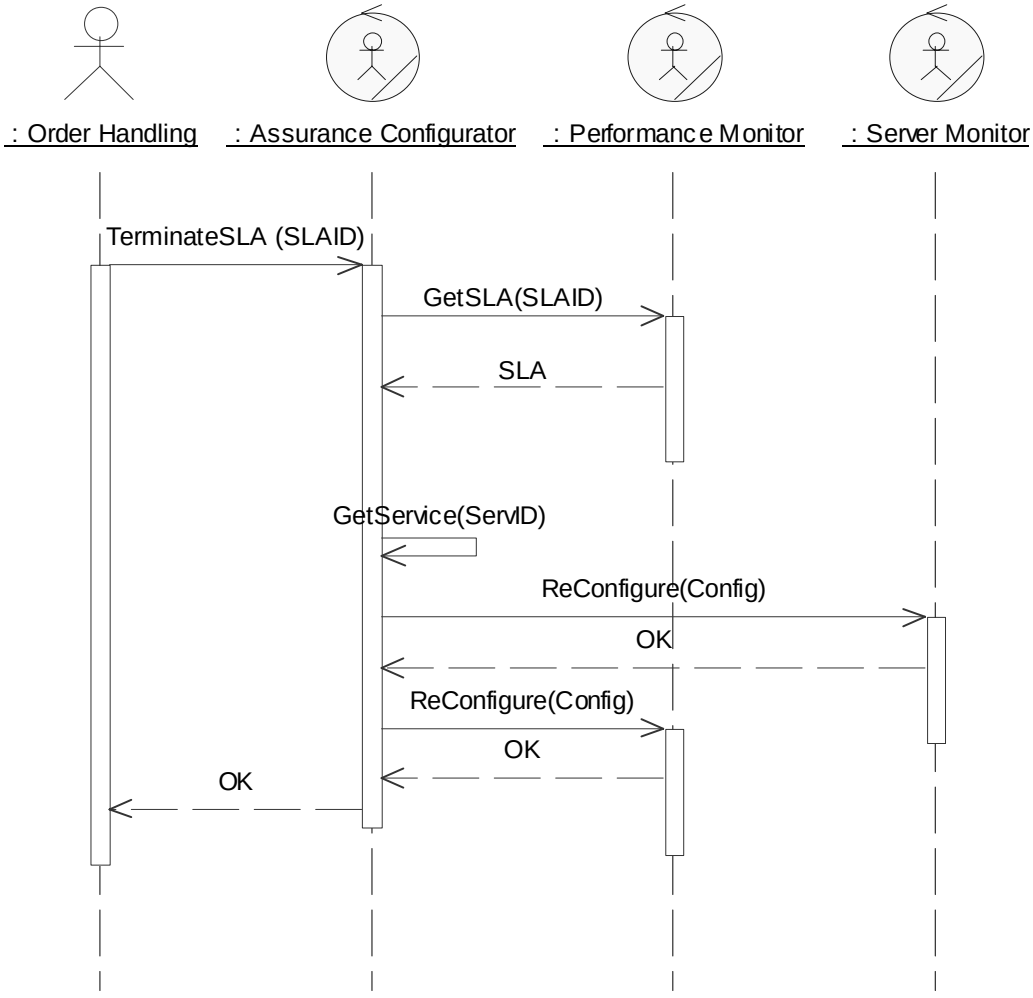

Figure 4-18 Interaction diagram for "Terminate Assurance Support for SLA"

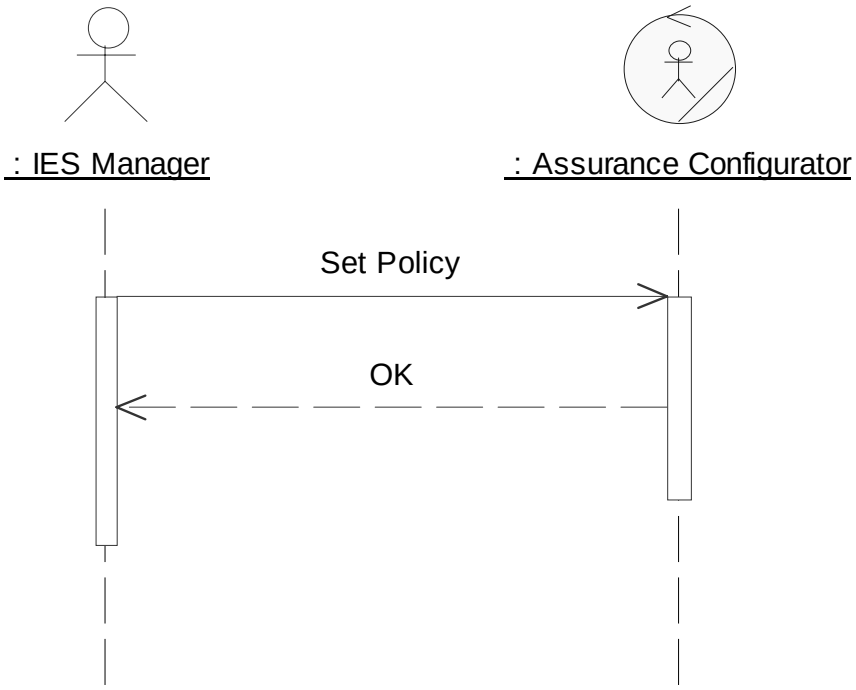

Figure 4-19 Interaction diagram for use case "Set Management Policy" showing the use of BB

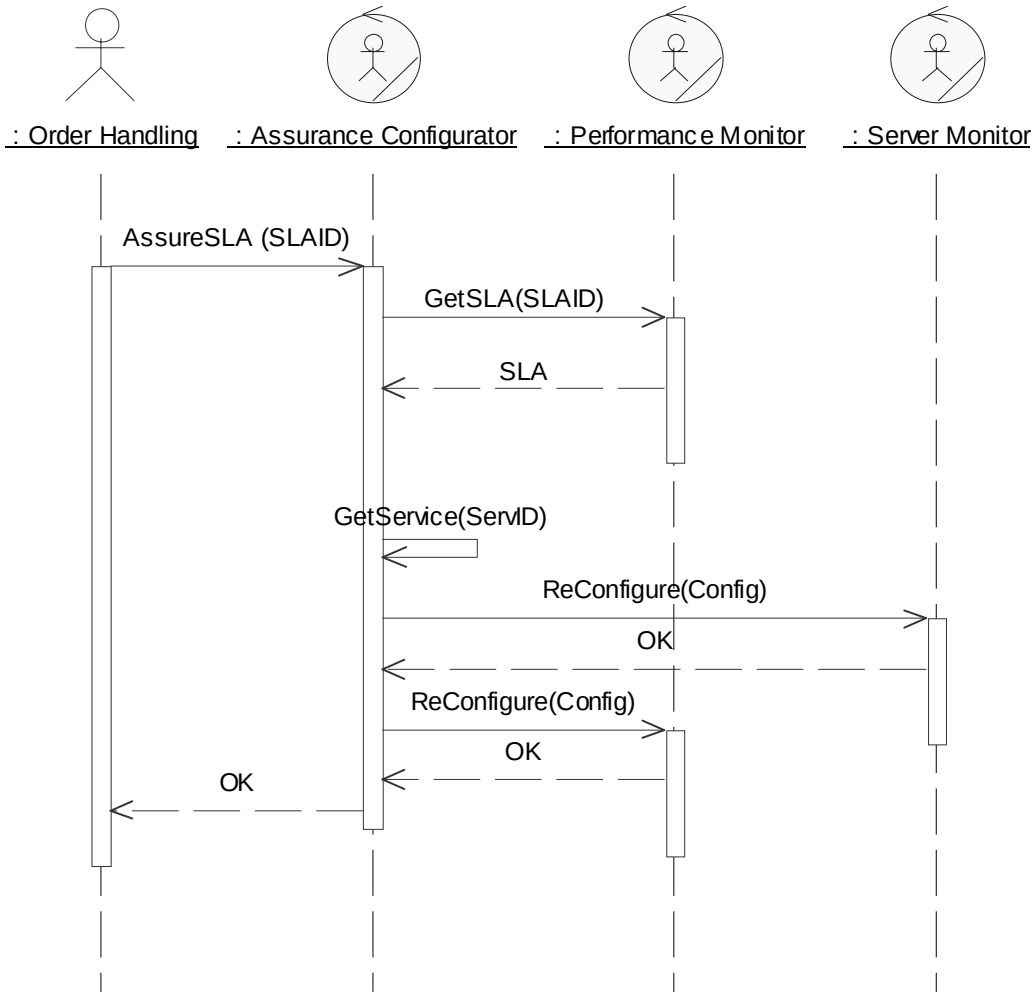

Figure 4-20 Interaction diagram for use case "Agree Assurance Support for SLA"

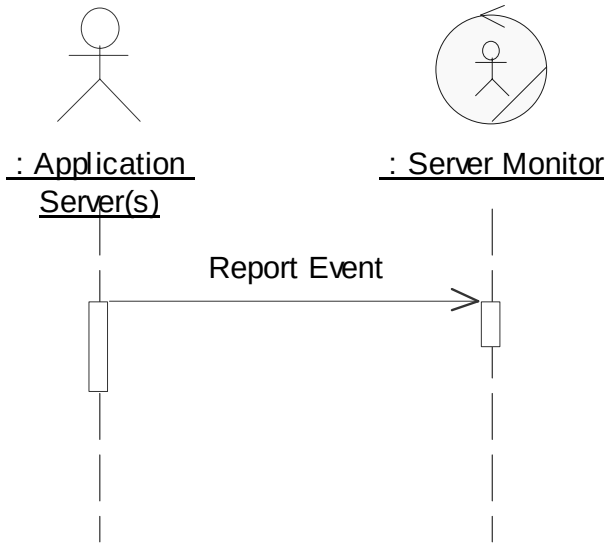

Figure 4-21 Interaction diagram for use case "Register Network Events" showing the use of BB

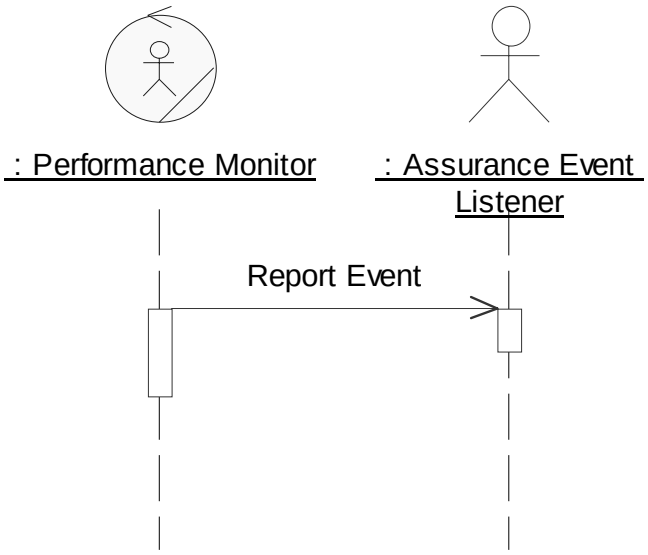

Figure 4-22 Interaction diagram for use case "Produce Assurance Event" showing the use of BB

4.4 BB Contract specification for Assurance IESP System Model

Five contracts have been specified for the Assurance system within the IESP System Model. These contracts are based on the XML Schema described in Annex E. A summary of these contracts is provided below. These and other contract specifications can be found in the on-line contract catalogue at the FORM website [FORM Contracts].

Contract Name	Description
AssuranceConfiguration	The purpose of this contract is to allow access to CIM policies that are used to configure the distributed managment components.
AssuranceService	This contract provides the operational interface to a Assurance service. This contract serves two main functions. The first is to allow services that the system is to support to be registered and the second is to allow SLAs to be introduced or removed.
PerformanceMonitor	This contract has a dual purpose. The first is to allow the statistics collected by the Performance Monitor to be accessed. The second is to allow policies to be downloaded through the contract to specify which statistics to collect and calculate.
ReportGenerator	The purpose of this contract is to allow access to XML reports of the statistics collected on the Service Provider.
CustomerReportingService	This contract offers a Web-based service which enable a customer to login as service user and use the web service to request selected data to be displayed on his browser or saved in a file.

Table 4-16 Contracts for Assurance IESP System

5 Assurance GQIPSP System Model

In this section the GQIPS Provider System Model for the assurance system will be presented.

5.1 Use case Model for Assurance GQIPSP System Model

Actor Name	Role Taken
Resource User	This actor represents either the VPN Provisioning BB or the Assurance Configuration BB, which rely on the GQIPS.

Table 5-1 GQIPSP System Actors

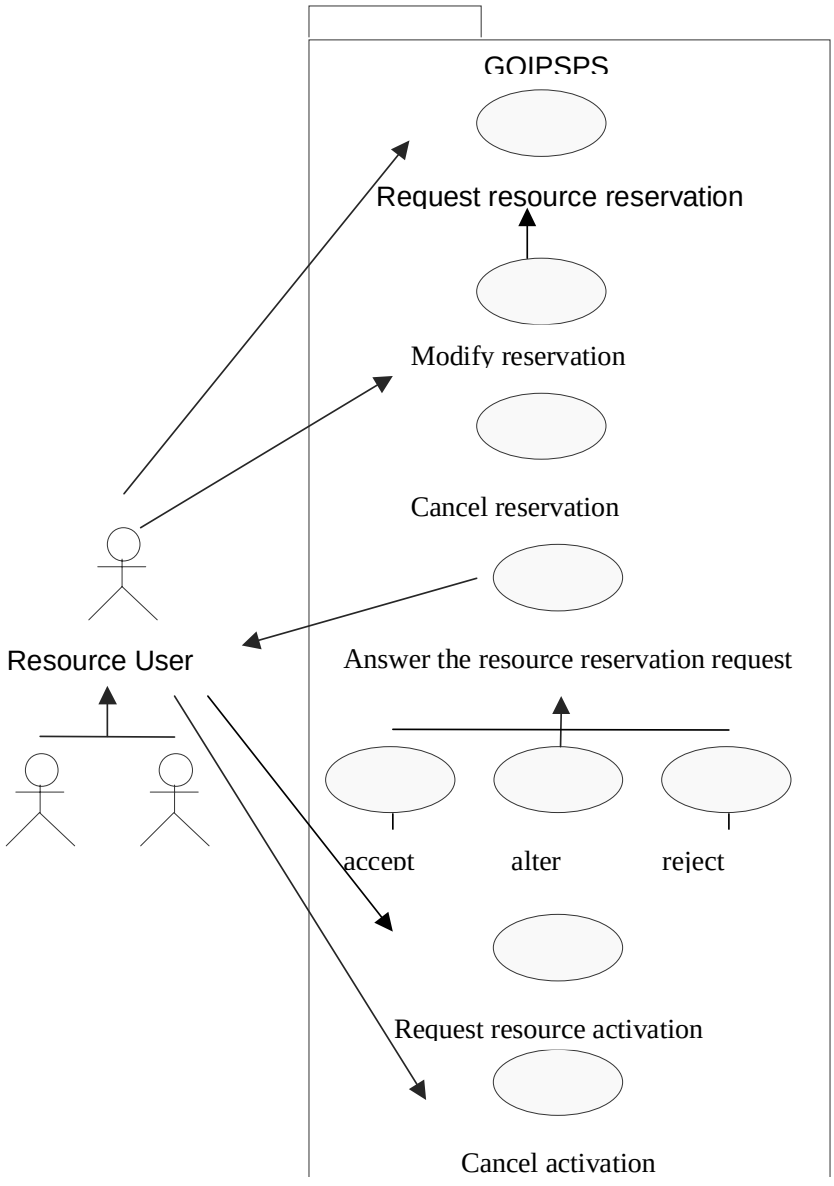

Figure 5-1 Use case diagram for the GQIPS System

Use case Name	Request Resource Reservation
Summary	Either the VPN Service or Assurance Configuration requires network resources from the GQIPS Management System.
Actors	Resource User
Pre-Conditions	An SLA has been defined and exists for the requested QoS allocation.
Begins When	A resource reservation is requested to the GQIPS
Steps	1. Resource User requests a QoS allocation 2. The SLA database is checked to ensure that there is effectively a service concluded for this end-customer, for the specified QoS parameters and the specified period. 3. The request is recorded and ready to be handled.
Ends when	A response is sent: “accept”, “alter” or “reject”
Post-Conditions	None
Exceptions	An invalid SLA is specified
Traceability	Business Case: “*Request Assurance Report*” QA-I.01, QA-I.02, QA-I.03, QA-I.04, QA-I.05, QA-I.06, QA-I.07, QA-II.09, QA-II.10, QA-II.19

Table 5-2 Use case description of “Request Resource Reservation”

Use case Name	Answer the resource allocation request
Summary	An RAR has been requested of the GQIPS that spans more than the network domain that the GQIPS manages.
Actors	Resource User
Pre-Conditions	A QoS allocation has been requested. The requester has fulfilled the authentication test.
Begins When	GQIPS receives information from other domains regarding resource allocation
Steps	1. The path to reach the destination end-user, in terms of intra-domain resources, is computed. 2. These domain resources are checked to see whether or not the QoS request could be fulfil on each hop of the path, according the current available resource.
Ends when	A response is sent: “accept”, “alter” or “reject”
Post-Conditions	None
Exceptions	An invalid SLA is specified
Traceability	Business Case: “*Request Assurance Report*” Requirements: QA-II.09, QA-II.11, QA-II.18, QA-II.19, QA-V.26

Table 5-3 Use case description of “Answer the resource allocation request”

Use case Name	Cancel Reservation
Summary	The Resource User cancels a previously made reservation.
Actors	Resource User
Pre-Conditions	The Resource User has made a resource reservation. The reservation is no longer required.
Begins When	Resource User no longer requires a previously made reservation.
Steps	1. The Resource User sends a cancellation request to the GQIPS.
Ends when	A response is sent: "cancellation success" or "cancellation failuare"
Post-Conditions	None
Exceptions	An invalid reservation is made.
Traceability	Business Case: "*Request Assurance Report*" Requirements: QA-II.08, QA-II.09, QA-II.19

Table 5-4 Use case description of "Cancel Reservation"

Use case Name	Request Activation Reservation
Summary	Either the VPN Service or Assurance Configuration require activation of network resources from the GQIPS Management System.
Actors	Resource User
Pre-Conditions	An SLA has been defined and exists for the requested QoS allocation.
Begins When	A resource reservation is requested to the GQIPS
Steps	a. Resource User requests a QoS activation, for which it has previously negotiated a SLA, and indicates the source and destination users, the QoS parameters values, the start and end times. b. The SLA database is checked to ensure that there is effectively a service concluded for this end-customer, for the specified QoS parameters and the specified period.
Ends when	Activation response from GQIPS – accept, reject, alter
Post-Conditions	None
Exceptions	An invalid SLA is specified
Traceability	Business Case: "*Request Assurance Report*" QA-I.01, QA-I.02, QA-I.03, QA-I.04, QA-I.05, QA-I.06, QA-I.07, QA-II.09, QA-II.10, QA-II.19

Table 5-5 Use case description of "Request Activation Reservation"

5.2 Analysis Model for Assurance GQIPSP System Model

5.2.1 Boundary Objects

Boundary Objects	Responsibility
Bandwidth Broker Interface	Used to receive resource allocation reservations and activations

Table 5-6 Boundary Objects for Assurance GQIPSP System Model

5.2.2 Entity Objects

Entity Objects	Responsibility
SLAs/Contol Parameters MIB	Holds information regarding the resource requests
Network Topology	Holds information about the network topology

Table 5-7 Entity Objects for Assurance GQIPSP System Model

5.2.3 Control Objects

Control Objects	Responsibility
Bamdwidth Broker	Responsible for processing resource requests.
Policy Server	Maintains policies
Policy Decision Point	Re-acts to requests based on policy information
Policy Mediation Device	Mediates requests between policy server and the underlying network.

Table 5-8 Control Objects for Assurance GQIPSP System Model

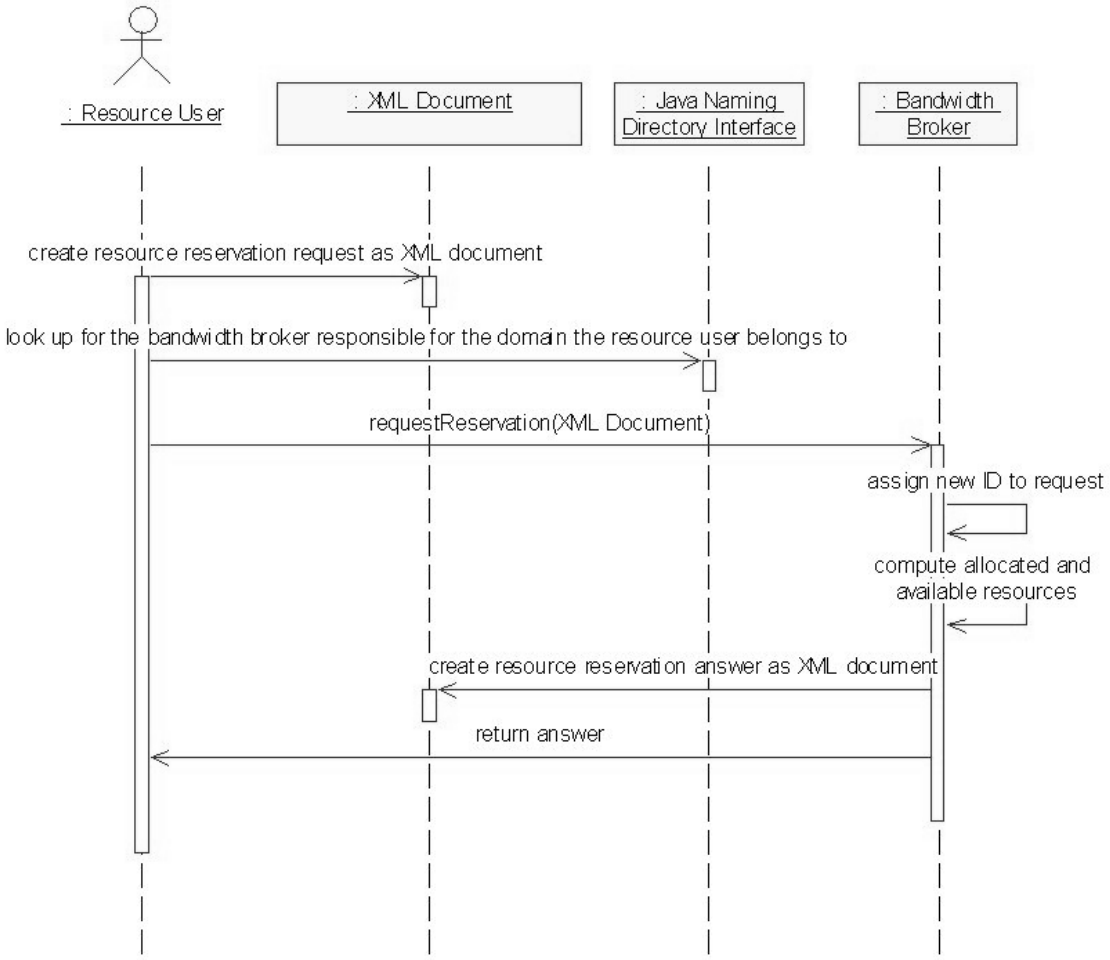

Figure 5-2 Object interaction diagram for resource allocation reservation request and answer

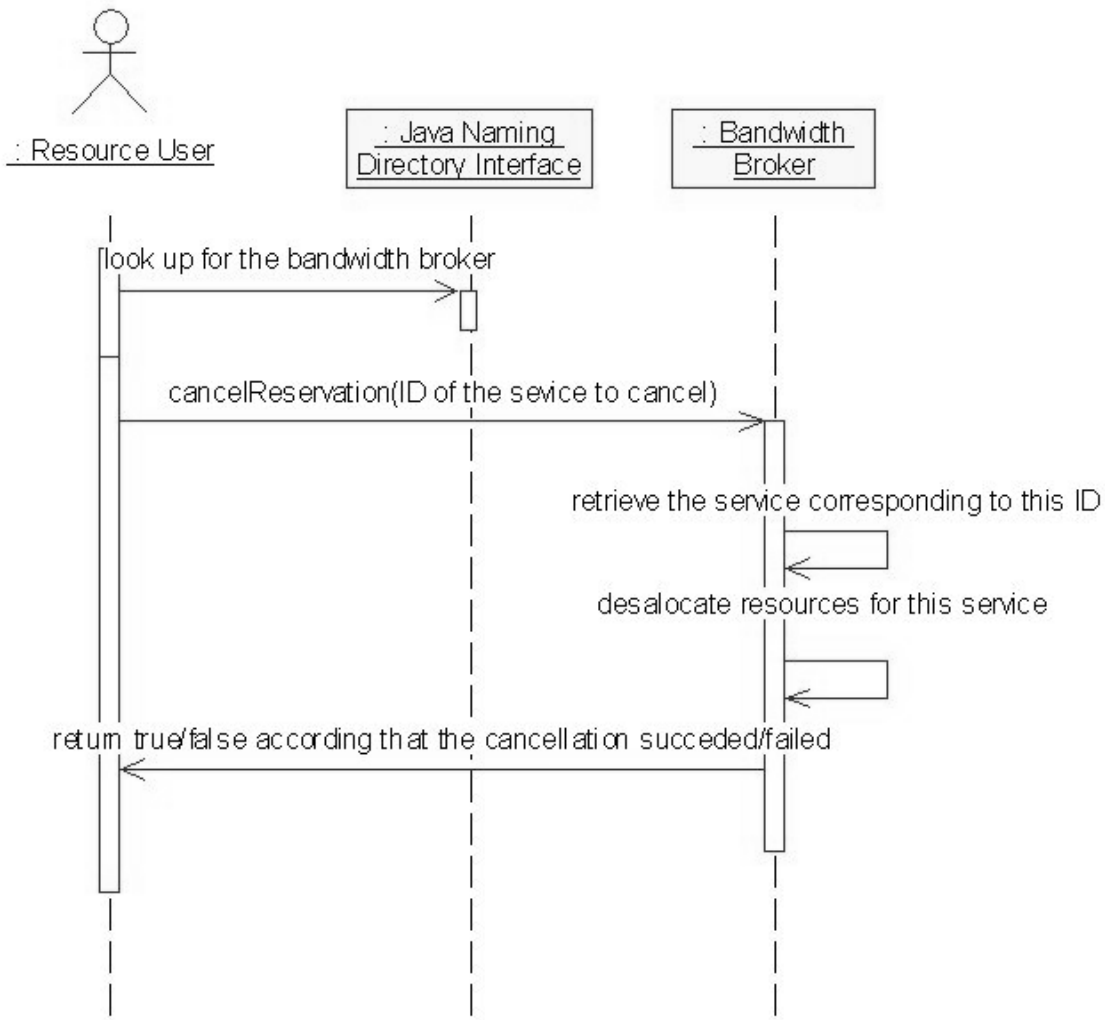

Figure 5-3 Object interaction diagram showing the cancellation of a resource reservation

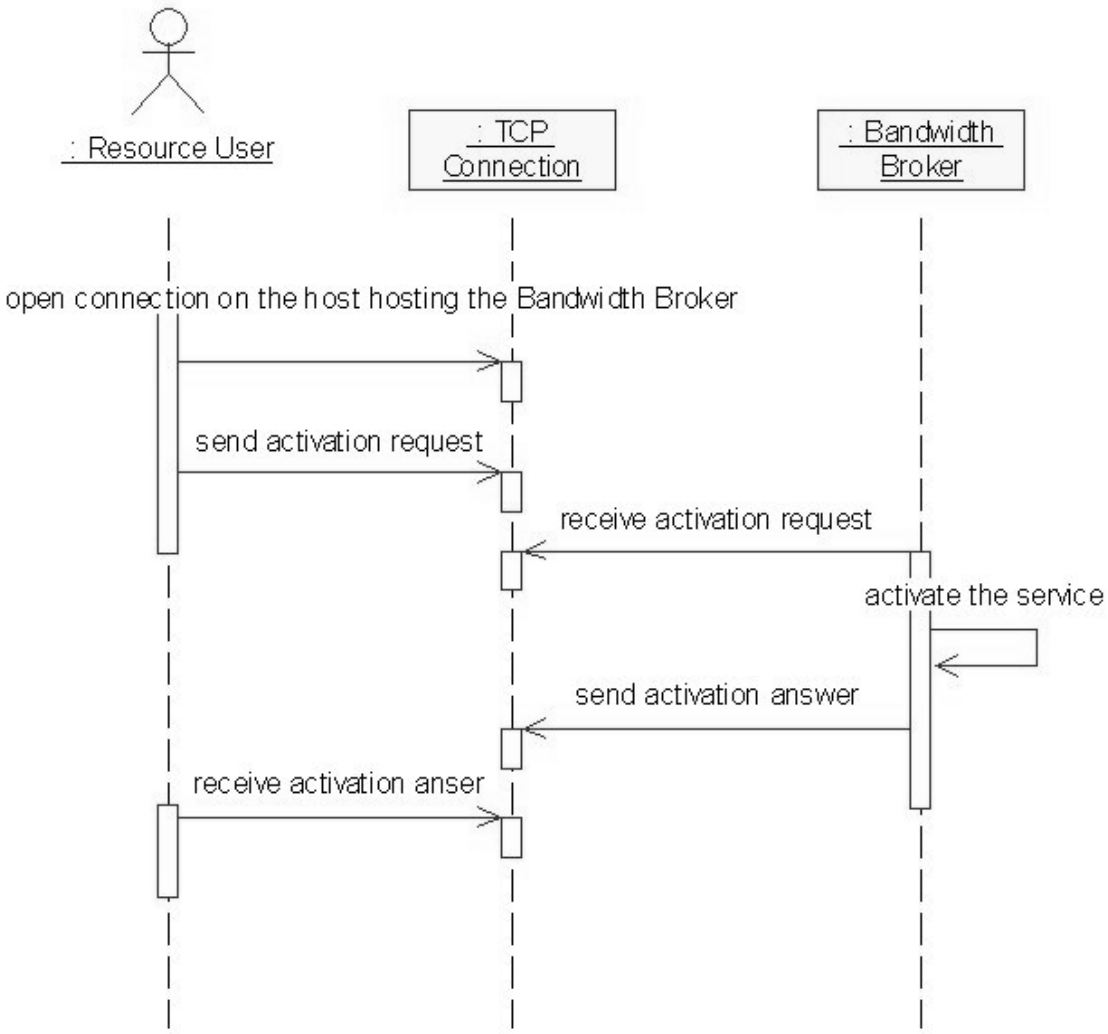

Figure 5-4 Object interaction diagram for resource allocation activation request and answer

5.3 Re-organise Analysis Model and Group to Building Blocks

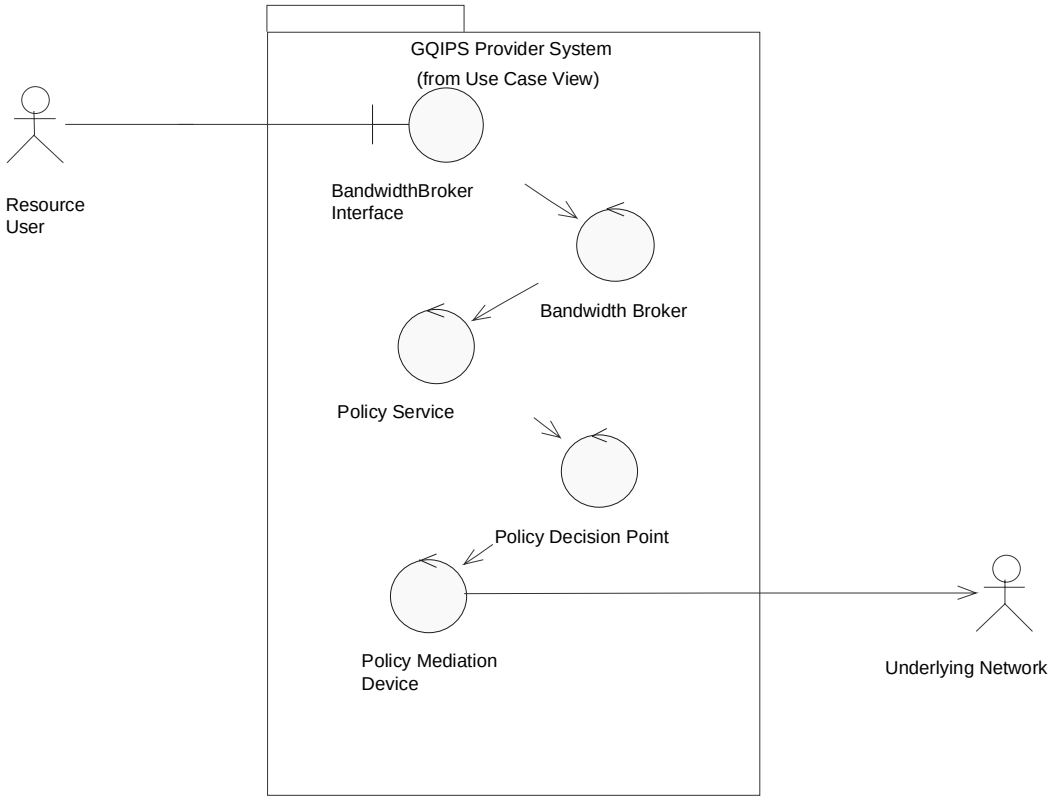

Figure 5-5 Broadcom Bandwidth Broker BB connects to Broadcom's existing Policy Framework

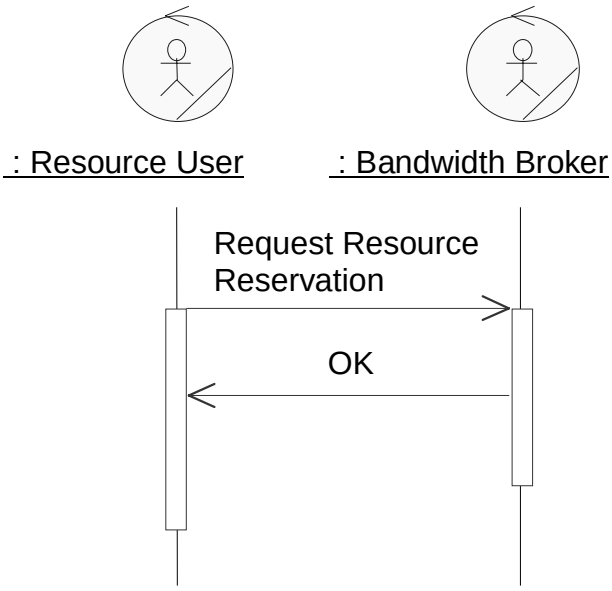

Figure 5-6 Interaction diagram for use case "Request Resource Reservation"

5.4 BB Contract specification for Assurance GQIPSP System Model

One contract have been specified for the GQIPS Fulfilment system based on the XML Schema described in Annex E. It can be found in the on-line contract catalogue at the FORM website [FORM Contracts].

6 Assurance ASP System Model

In this section the ASP System Model for the assurance system will be presented. This will involve the identification of the functionality necessary to support the assurance system in the ASP domain and the design of the software components necessary to provide that functionality.

6.1 Use case Model for Assurance ASP System Model

In this section the use cases that must be supported in the ASP Domain and the actors that use these use cases are identified and explained.

Actor Name	Role Taken
IESP	Represents the IESP systems when they are shown interacting with system in other domains.

Table 6-1 ASP System Actors

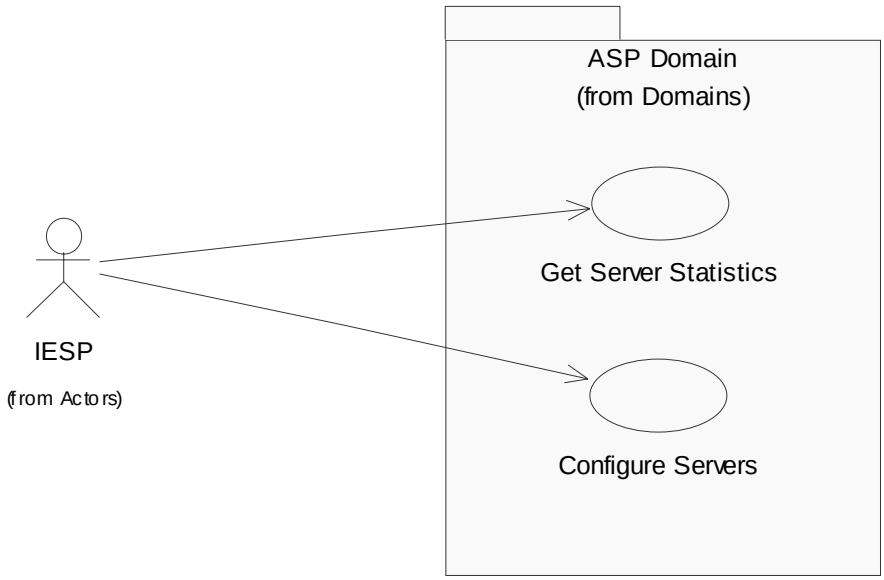

Figure 6-1 Use Case Diagram for the ASP System Model

Use case Name	Configure Servers
Summary	When SLAs are introduced/removed from the system then the underlying servers need to be reconfigured to monitor them.
Actors	Application Server(s), Service Proxy
Pre-Conditions	A new server configuration has been produced.
Begins When	The new configuration is being deployed.
Steps	1. A new configuration for the servers has been formulated and is ready for deployment. 2. The configuration is deployed to the servers.
Ends when	The new configuration is deployed.
Post-Conditions	None
Exceptions	None
Traceability	Requirements: [IA-II.10][IA-II.07]

Table 6-2 Use case description of "Configure Servers"

Use case Name	Get Server Statistics
Summary	Statistics generated by servers are necessary to monitor how an SLA is being conformed to. This use case allows server statistics to be polled as necessary.
Actors	Application Server(s)
Pre-Conditions	The server is part of a service being monitored.
Begins When	The server statistics are requested.
Steps	1. The system requests statistics from the server. 2. The server collates the necessary statistics. 3. The report is returned to the system.
Ends when	The server statistics are reported.
Post-Conditions	None
Exceptions	None
Traceability	Requirements: [EC-II.28]

Table 6-3 Use case description of "Get Server Statistics"

6.2 Analysis Model for Assurance ASP System Model

Having identified the use case and actors the next step is to identify the analysis object necessary to implement these use cases. The identified analysis object are described below and followed by interaction diagrams that document how these objects interact to fulfill the system model.

6.2.1 Boundary Objects

Boundary Objects	Responsibility
Instrumentation Interface	The interface through which statistics related to the servers/proxy being monitored may be accessed.

Table 6-4 Boundary Objects for Assurance ASP System Model

6.2.2 Control Objects

Control Objects	Responsibility
Network Components	Represents the components of the assurance system managing the network resources involved in providing the service.
Server Components	Represents the components of the assurance system locally managing the servers/proxy involved in providing the service.

Table 6-5 Control Objects for Assurance ASP System Model

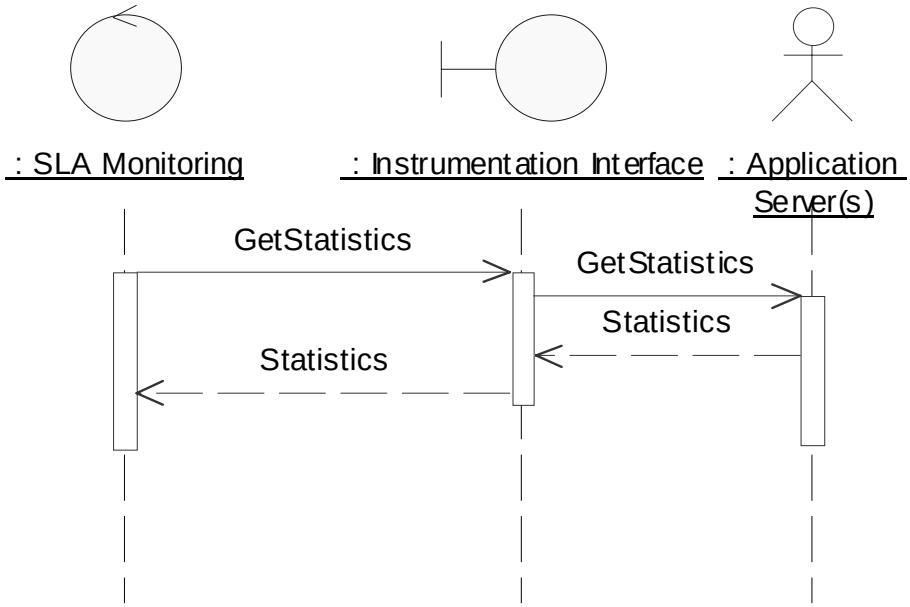

Figure 6-2 Object diagram of analysis objects implementing the use case "Get Server Statistics"

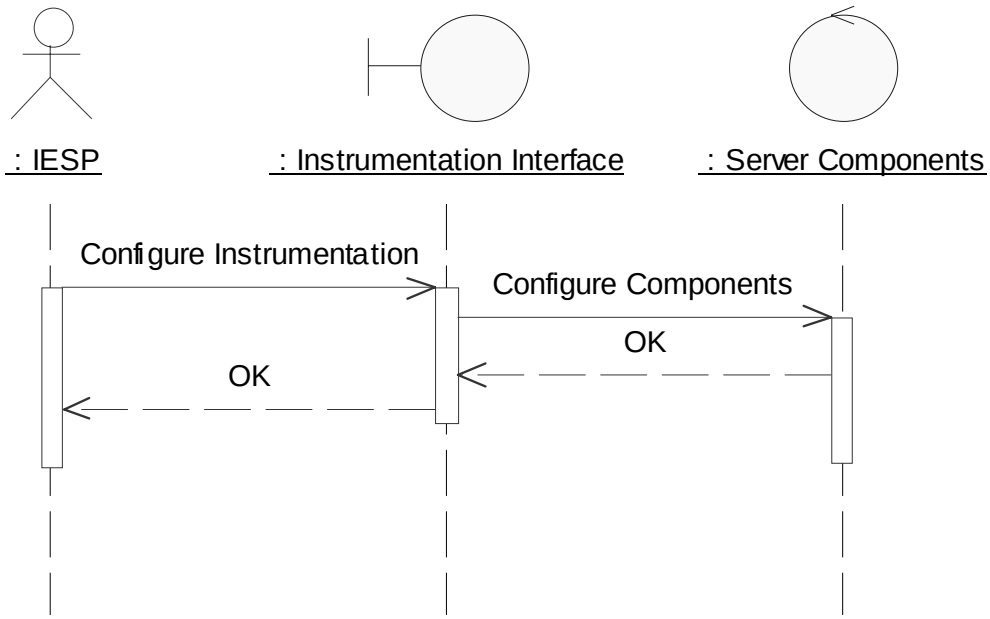

Figure 6-3 Object diagram of analysis objects implementing use case "Configure Servers"

6.3 Re-organise Analysis Model and Group to Building Blocks for Assurance ASP System Model

After identifying the analysis objects the next step is to group these object into Building Blocks. As with the Customer Domain model it was felt that one BB was sufficient for this domain, as shown in the diagram below.

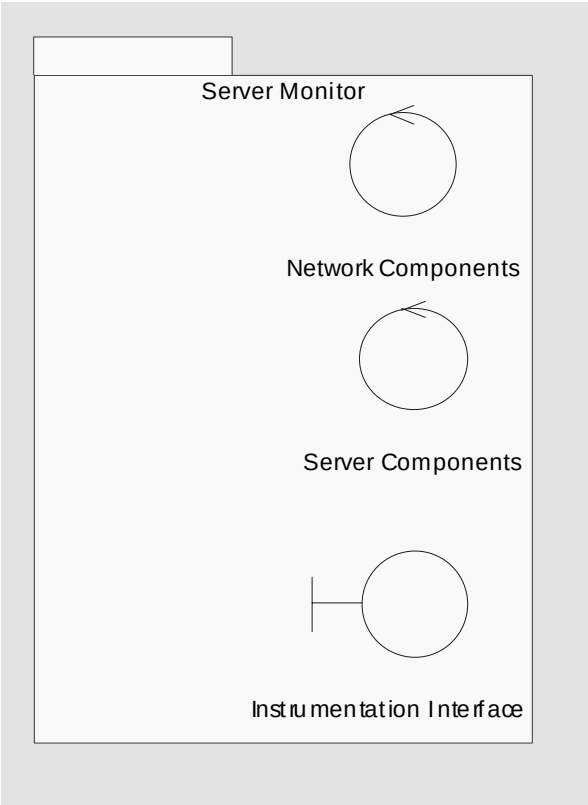

Figure 6-4 Collaboration diagram showing Building Blocks and Building Block Contracts

The following interaction diagram shows more details about the relations between the building blocks and the actors and how they must interact to fulfil the use cases for this system.

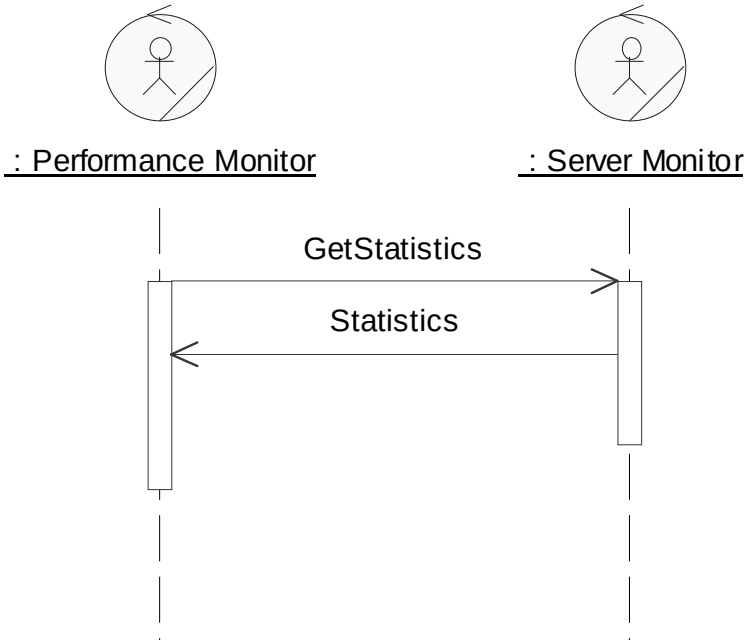

Figure 6-5 Interaction diagram for the use case Get Server Statistics showing the use of BB

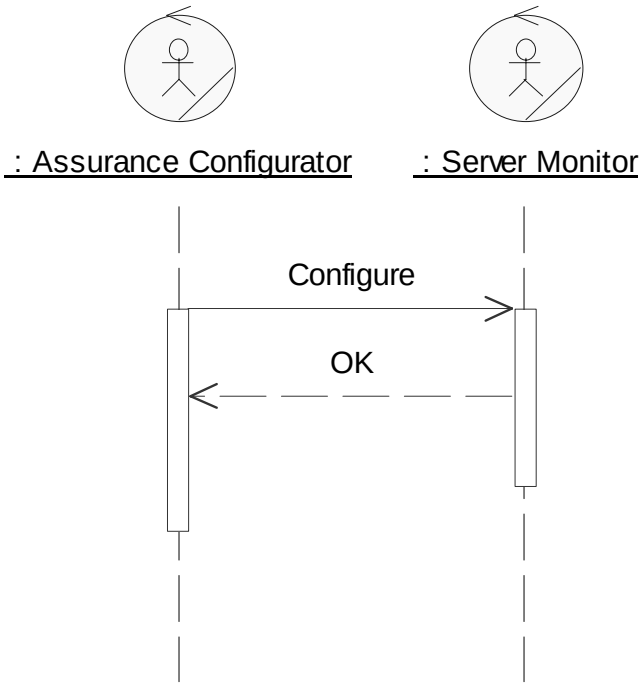

Figure 6-6 Interaction diagram for the use case Configure Servers showing the use of BB

6.4 BB Contract specification for Assurance ASP System Model

One contract has been specified for the Assurance system within the ASP System Model (this contract is shared with the Customer System Model). This contract is based on the XML Schema described in Annex E. A summary of this contract is provided below. This and other contract specifications can be found in the on-line contract catalogue at the FORM website [FORM Contracts].

Contract Name	Description
ServerMonitor	This contract allows access to the CIM information base stored in the Server Monitor building block. This building block monitors server statistics, calculating secondary combinatory statistics when necessary. Both primary and secondary statistics are stored within the information base for retrieval. Objects facilitating the management of the Server Monitor itself are also present in the information base. These objects perform a number of different tasks such as initialising and managing downloadable extensions to the module.

Table 6-6 Contracts for Assurance ASP System Model

7 Conclusion

Contained within this document is the final system models produced by the FORM Assurance Group. It demonstrates how the FORM methodology was applied to the problem of providing service assurance. The Business Model / Use Case driven approach suggested in the guidelines helped to model the necessary management business processes which span several organisational domains and involves several actors and roles in the world of business to business communication. It should be noted however that only key areas of the problem domain were addressed and further work would be necessary to completely address the issues involved in providing service assurance.

8 References

[FORM Contracts] Index to the Contract catalogue:

http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/

[FORM D12] Wade, Vincent, "D12: Guidelines for Co-operative Inter-Enterprise Management", IST-1999-1057/TCD/WP3/012, February 2002.

