7302 INTELLIGENT SERVICES ACCESS MANAGER
7330 INTELLIGENT SERVICES ACCESS MANAGER FTTN
7356 INTELLIGENT SERVICES ACCESS MANAGER FTTB
7360 INTELLIGENT SERVICES ACCESS MANAGER FX
7362 INTELLIGENT SERVICES ACCESS MANAGER DF/SF
7363 INTELLIGENT SERVICES ACCESS MANAGER MX
7367 INTELLIGENT SERVICES ACCESS MANAGER SX/DX
RELEASE 5.x

Software Installation Guide

3HH-07196-AAAA-RJZZA

Issue:22

December 2017

Table of contents

List of figures

List of tables

1 Preface

.

1.1 Scope

This document provides information about all software installation aspects for this set of ISAM products:

- the 7302 Intelligent Services Access Manager (7302 ISAM)
- the 7330 Intelligent Services Access Manager Fiber to the Node (7330 ISAM FTTN).
- the 7356 Intelligent Services Access Manager Fiber to the Building (7356 ISAM FTTB).
- the 7360 Intelligent Services Access Manager FX (7360 ISAM FX)
- the 7362 Intelligent Services Access Manager DF (7362 ISAM DF)
- the 7362 Intelligent Services Access Manager SF (7362 ISAM SF)
- the 7363 Intelligent Services Access Manager MX (7363 ISAM MX)
- the 7367 Intelligent Services Access Manager SX (7367 ISAM SX)
- the 7367 Intelligent Services Access Manager DX (7367 ISAM DX)

1.2 Audience

This documentation set is intended for planners, administrators, operators, and maintenance personnel involved in installing, upgrading, or maintaining the 7302 ISAM, the 7330 ISAM FTTN, the 7356 ISAM FTTB, the 7360 ISAM FX, the 7362 ISAM DF/SF, the 7363 ISAM MX or the 7367 ISAM SX/DX.

1.3 Required knowledge

The reader must be familiar with general telecommunications principles.

1.4 Acronyms

See the dedicated *ISAM Glossary* document included in the documentation set of this release for the expansion of acronyms and mnemonics and the explanation of abbreviations used in this documentation set.

1.5 Safety information

For safety information, see the *Safety Manual* for your product.

1.6 Documents

Refer to the *Product Information* document for your product to see a list of all the relevant customer documents and their part numbers for the current release.

1.7 Product Naming

When the term “ISAM” is used alone, then the 7302 ISAM, the 7330 ISAM FTTN, the 7356 ISAM FTTB, the 7360 ISAM FX, the 7362 ISAM DF/SF, the 7363 ISAM MX and the 7367 ISAM SX/DX are meant. If a feature is valid for only one of the products, the applicability will be explicitly stated.

When the term “xHub-based systems” is used, then the 7302 ISAM, the 7330 ISAM FTTN, the 7356 ISAM FTTB and the 7360 ISAM FX are meant.

If a feature is valid for all but one or only one of the products, the applicability will be explicitly stated.

1.8 Special information

The following are examples of how special information is presented in this document.

Danger — Danger indicates that the described activity or situation may result in serious personal injury or death; for example, high voltage or electric shock hazards.

Warning — Warning indicates that the described activity or situation may, or will, cause equipment damage or serious performance problems.

Caution — Caution indicates that the described activity or situation may, or will, cause service interruption.

Note — A note provides information that is, or may be, of special interest.

1.8.1 Procedures with options or substeps

When there are options in a procedure, they are identified by letters. When there are required substeps in a procedure, they are identified by roman numerals.

Procedure 1 Example of options in a procedure

At step 1, you can choose option a or b. At step 2, you must do what the step indicates.

1 This step offers two options. You must choose one of the following:

- **a** This is one option.
- **b** This is another option.

2 You must perform this step.

Procedure 2 Example of required substeps in a procedure

At step 1, you must perform a series of substeps within a step. At step 2, you must do what the step indicates.

1 This step has a series of substeps that you must perform to complete the step. You must perform the following substeps:

- **i** This is the first substep.
- **ii** This is the second substep.
- **iii** This is the third substep.

2 You must perform this step.

1.9 Release notes

Be sure to refer to the release notes (such as the Customer Release Notes or Priority Package Release Note) issued for software loads of your product before you install or use the product. The release notes provide important information about the software load.

2 Introduction

2.1 Introduction

This document contains all software-installation-related procedures for the system.

The SHub subsystem, which is integrated in the NT boards NANT-A and NRNT-A, has a specific software file and database. These are integrated in the system software and database from R2.3 (for NANT-A) and from R4.2 (for NRNT-A) onwards.

The IHub subsystem, which is integrated in the NANT-D, NANT-E and FX NT boards, has a specific software file and database. These are integrated in the system software and database from R3.7.10 (for NANT-D), R4.3 (for NANT-D MPLS), R4.2 (for NANT-E), R4.2.30 (for FANT-F) and R5.5 (for FANT-G) onwards.

Note — When xHub is used in this manual, this means both SHub and IHub.

The 7367 ISAM SX has a specific software file and database. These are integrated in the system software and database from R5.0 onwards.

The 7367 ISAM DX has a specific software file and database. These are integrated in the system software and database from R5.7 onwards.

The 7363 ISAM MX has a specific software file and database. These are integrated in the system software and database from R5.0.00a onwards.

The 7362 ISAM DF and 7362 ISAM SF have a specific software file and database. These are integrated in the system software and database from R5.5 onwards for 7362 ISAM DF and R5.7.01 for 7362 ISAM SF.

Note — This document focuses on the actions during the Software Installation phase. For all Software Upgrade and Migration actions after the Software Installation phase it is important to check the “Software Upgrade and Migration Application Procedures” document (SUMAP: 3HH-10318-AAAA-TCZZA). When doing Software Upgrade/Migration actions it is important not to mix manual Software Upgrade actions with script-driven Software Upgrade actions (as described in the SUMAP document).

2.2 Applicable Releases

This software installation guide is applicable for the ISAM from release 5.7.01 onwards.

2.3 Network Management

This section describes the network management for:

- xHub-based Systems
- 7363 ISAM MX/7367 ISAM SX/DX
- 7362 ISAM DF/SF

2.3.1 xHub-based Systems

Figure 1 shows how the ISAM can be managed in a network.

Figure 1 **ISAM Management in a Network**

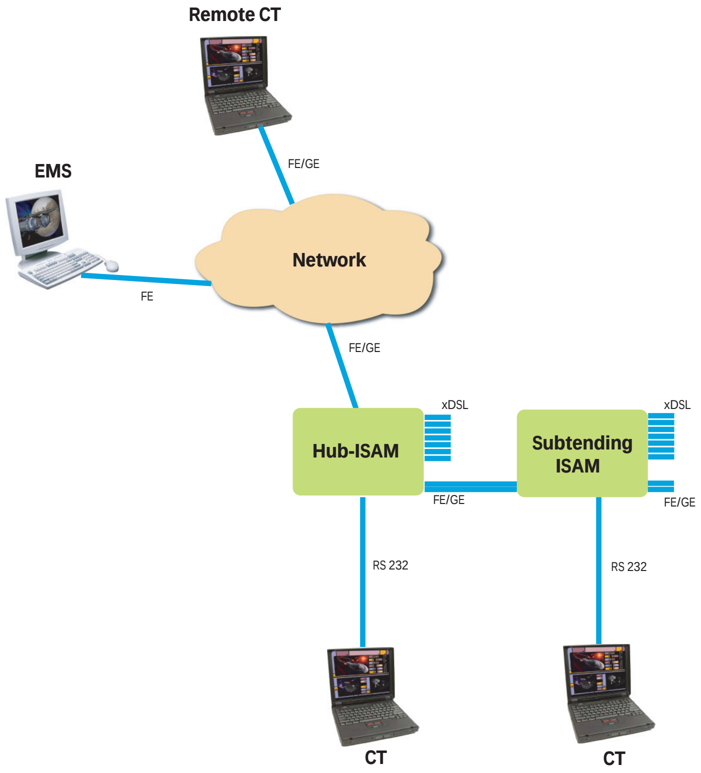


Figure 2 shows the management topology of SHub-based ISAMs.

Figure 2 **SHub-based ISAM Management Topology**

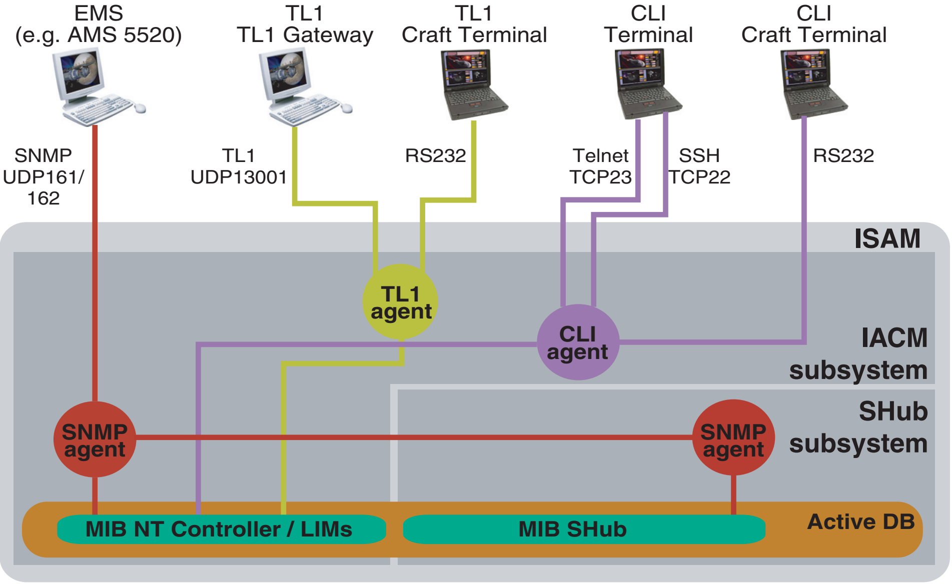
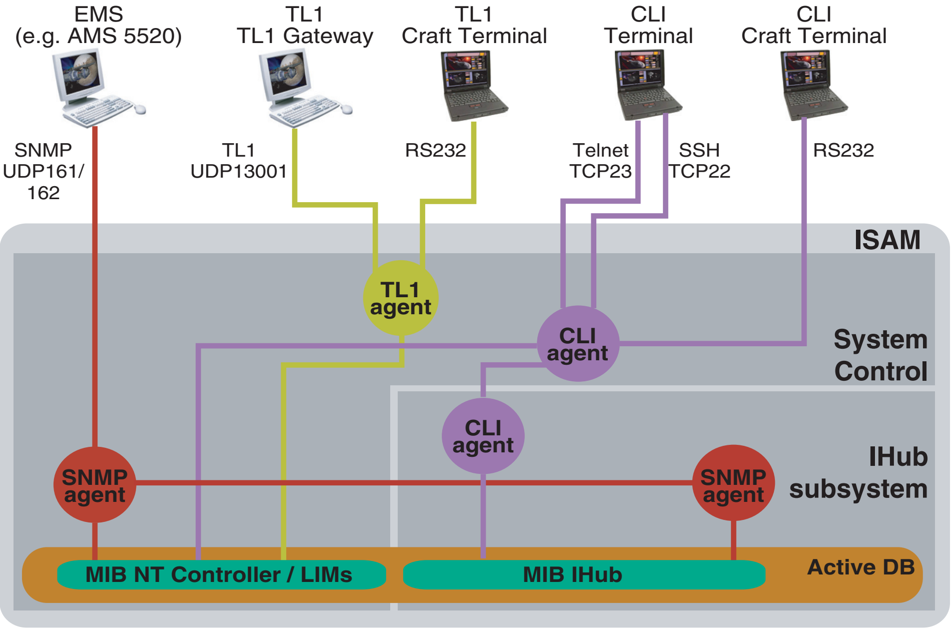


Figure 3 shows the management topology of IHub-based ISAMs.

Figure 3 **IHub-based ISAM Management Topology**



The Intelligent Access termination, Control and Management (IACM) subsystem and xHub subsystem contain each a separate Simple Network Management Protocol (SNMP) agent. The IACM can be managed via an Element Management System (EMS).

Note — A third SNMP agent is present on the Application Intelligence (AI) platform. For more details, see the *System Description for FD 100/320 Gbps NT and FX NT* document.

The xHub subsystem is managed via the SNMP agent of the IACM.

A CLI agent, located on the NT board, implements CLI commands for both the IACM subsystem and the xHub subsystem. This means that there is a single entry-point into the system that allows to manage the complete ISAM via a single TELNET/SSH session or via the serial interface integrated on the IACM subsystem. However there is no semantic integration. The CLI command tree is divided in two logical sub-trees.

It is also possible to use the TL1 agent on the NT board to manage the IACM and the xHub. TL1 commands can be sent to the TL1 agent via the TL1 Gateway, a TL1 terminal or a TL1 craft terminal.

Table 1 shows an overview of the managers which are involved:

Table 1 **Manager Overview**

Type	Description
EMS (for example, 5520 AMS)	Element Management System based on SNMP. The Nokia WorkStation (5520 AMS) is commonly used.
TL1 Gateway	TL1 gateway application using TL1 protocol and commands.
Terminal	VT100 terminal TELNET/SSH session using TL1/CLI commands.
Craft Terminal	Craft Terminal using TL1/CLI commands.

The interface to the manager is either a TL1/CLI interface (in case of Terminal/Craft Terminal) or an SNMP interface (in case of 5520 AMS). The craftsman is an operator who manipulates the system in a physical way (installation of boards and so on) and performs the basic configuration via the serial interface using TL1/CLI. In case no EMS or remote CT is used, the craftsman takes over the responsibility of the manager as well.

Note — Important note:

When a firewall is in place between the network management stations and the ISAM network, for troubleshooting and migration reasons it is required following UDP ports are opened on the firewall:

- UDP port 23 as destination port
- UDP ports 928 – 939 (928 and 939 included) as source and destination ports

Not opening these ports on the firewall may lead to a reduced or failed troubleshooting access and/or a failure to perform an ISAM migration.

2.3.2 7363 ISAM MX/7367 ISAM SX/DX

Figure 4 shows how the 7363 ISAM MX and 7367 ISAM SX/DX can be managed in a network.

Figure 4 7363 ISAM MX and 7367 ISAM SX/DX Management in a Network

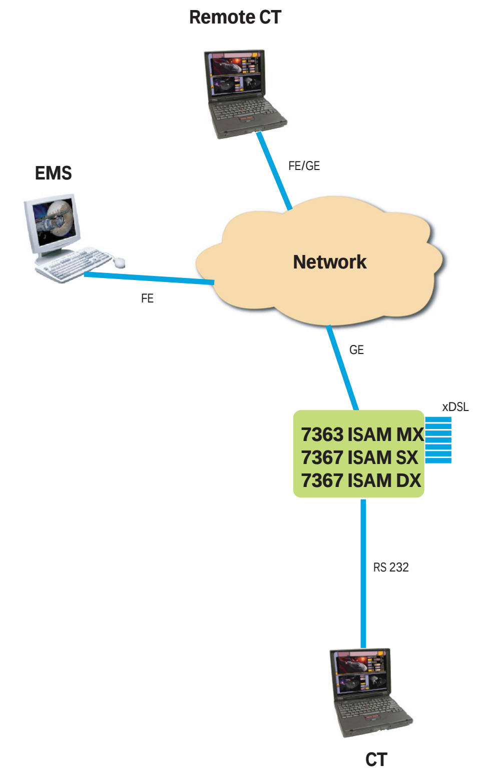
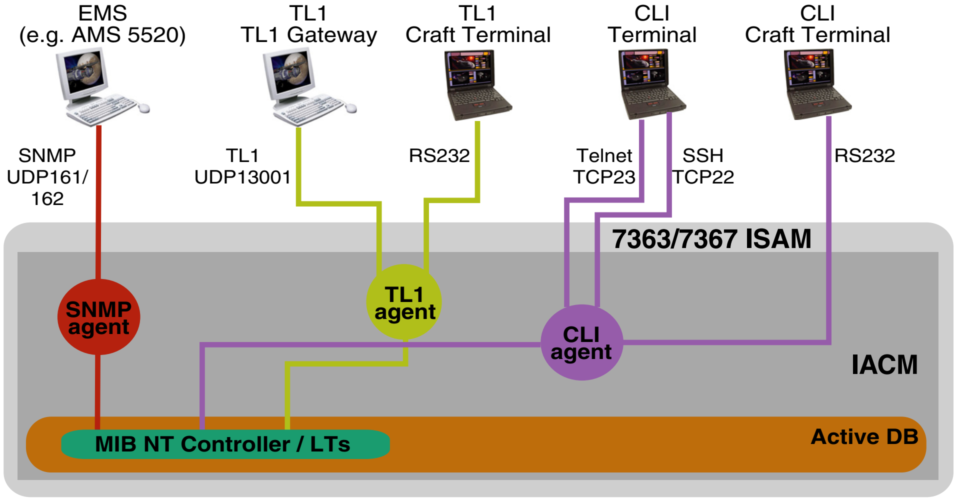


Figure 5 shows the management topology of the 7363 ISAM MX and 7367 ISAM SX/DX.

Figure 5 7363 ISAM MX and 7367 ISAM SX/DX Management Topology



A CLI agent, located on the NT board, implements CLI commands. It is accessible via the serial interface (outband management) or via the uplink (inband management). A TL1 agent on the NT board, implements TL1 commands. It is accessible via the serial interface (outband management) or via the uplink (inband management).

Note: Outband management is done on a link where no user data is configured, that is, an uplink reserved for management traffic.

Table 2 shows an overview of the managers which are involved:

Table 2 **Manager Overview**

Type	Description
EMS (for example, 5520 AMS)	Element Management System based on SNMP. The Nokia WorkStation (5520 AMS) is commonly used.
TL1 Gateway	TL1 gateway application using TL1 protocol and commands.
Terminal	VT100 terminal TELNET/SSH session using TL1/CLI commands.
Craft Terminal	Craft Terminal using TL1/CLI commands.

The interface to the manager is either a TL1/CLI interface (in case of Terminal/Craft Terminal) or an SNMP interface (in case of 5520 AMS). The craftsman is an operator who manipulates the system in a physical way (installation of boards and so on) and performs the basic configuration via the serial interface using TL1/CLI. In case no EMS or remote CT is used, the craftsman takes over the responsibility of the manager as well.

Note — Important note:

When a firewall is in place between the network management stations and the ISAM network, for troubleshooting and migration reasons it is required following UDP ports are opened on the firewall:

- UDP port 23 as destination port
- UDP ports 928 – 939 (928 and 939 included) as source and destination ports

Not opening these ports on the firewall may lead to a reduced or failed troubleshooting access and/or a failure to perform an ISAM migration.

2.3.3 7362 ISAM DF/SF

Figure 6 shows how the 7362 ISAM DF/SF can be managed in a network.

Figure 6 **7362 ISAM DF/SF Management in a Network**

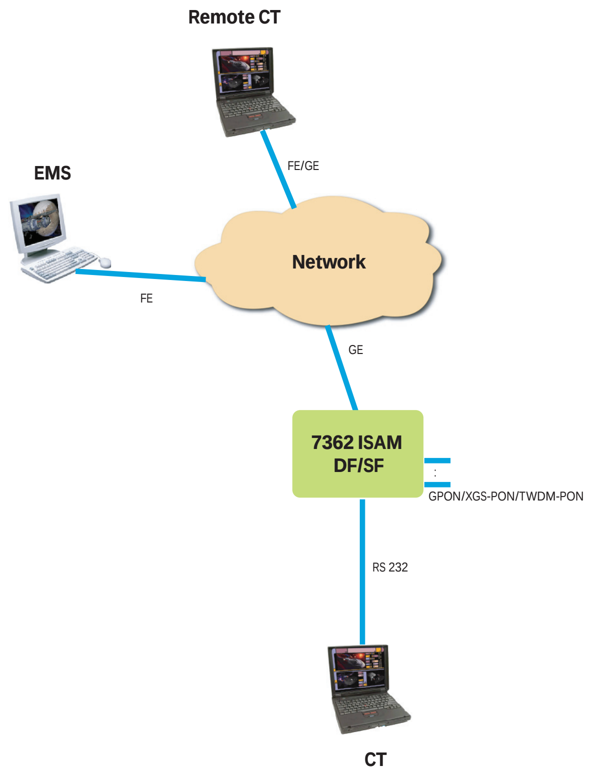
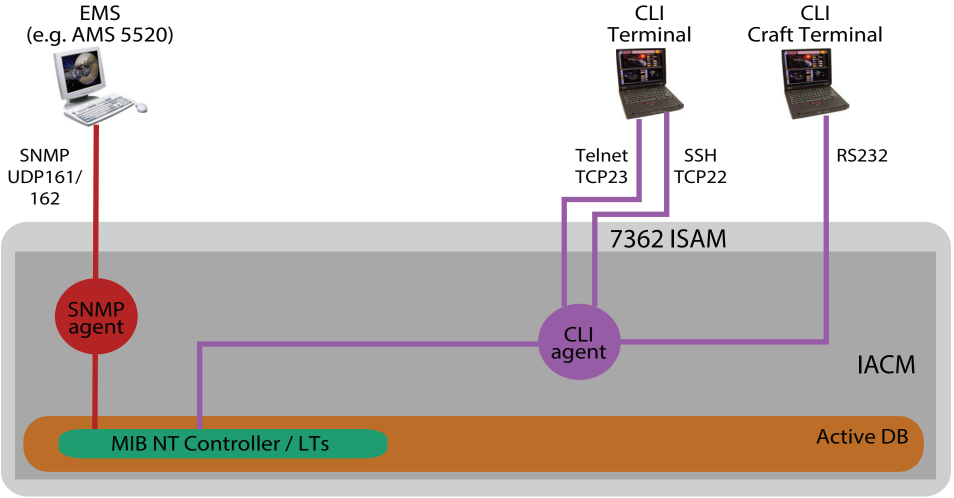


Figure 7 shows the management topology of the 7362 ISAM DF/SF.

Figure 7 **7362 ISAM DF/SF Management Topology**



A CLI agent, located on the NT board, implements CLI commands. It is accessible via the serial interface (outband management) or via the uplink (inband management).

Note: Outband management is done on a link where no user data is configured, that is, an uplink reserved for management traffic.

Table 3 shows an overview of the managers which are involved:

Table 3 **Manager Overview**

Type	Description
EMS (for example, 5520 AMS)	Element Management System based on SNMP. The Nokia WorkStation (5520 AMS) is commonly used.
Terminal	VT100 terminal TELNET/SSH session using CLI commands.
Craft Terminal	Craft Terminal using CLI commands.

The interface to the manager is a CLI interface (in case of Terminal/Craft Terminal) or an SNMP interface (in case of 5520 AMS). The craftsman is an operator who manipulates the system in a physical way (installation of boards and so on) and performs the basic configuration via the serial interface using CLI. In case no EMS or remote CT is used, the craftsman takes over the responsibility of the manager as well.

Note 1 — Important note:

When a firewall is in place between the network management stations and the ISAM network, for troubleshooting and migration reasons it is required following UDP ports are opened on the firewall:

- UDP port 23 as destination port
- UDP ports 928 – 939 (928 and 939 included) as source and destination ports

Not opening these ports on the firewall may lead to a reduced or failed troubleshooting access and/or a failure to perform an ISAM migration.

Note 2 — The 7362 ISAM DF/SF does not support TL1.

2.4 Software Management

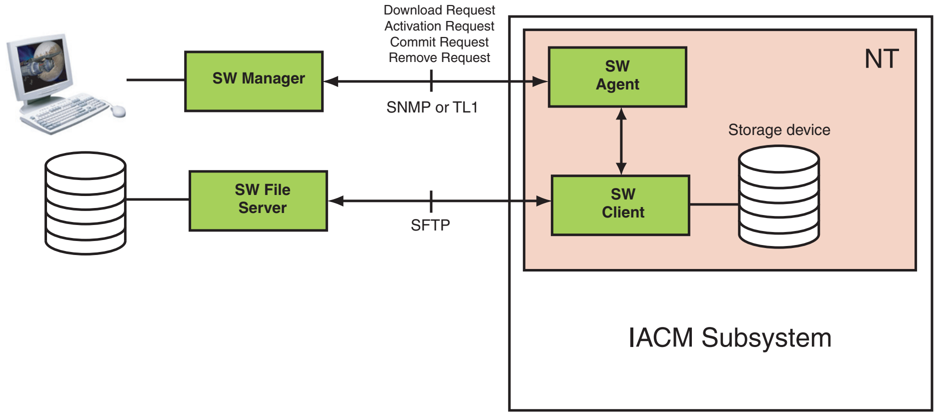
2.4.1 Software

The ISAM software management is package based: all the software files of the different boards (LT boards, NT board,...) of the ISAM are grouped in an Overall Software Package (OSWP).

Software management is related to the management of these OSWPs (download of a new OSWP, activation of an OSWP,...). At most two different OSWPs can be stored inside the IACM part of the ISAM.

The general architecture of the software management follows the manager-agent/client-server philosophy. This is shown in Figure 8.

Figure 8 **General Software Management Architecture**



The following table shows the different types of NT boards with their corresponding factory software:

Table 4 **NT Board Types and their Factory Software**

Product(s)	NT Board Type	Factory Software Installed
7302 ISAM 7330 ISAM FTTN	NANT-A Ax	From R3.1: simplex only From R3.3 onwards: duplex
	NANT-A Dx	From R4.3.02 onwards: duplex
	NANT-D	From R3.7.10: simplex only From R4.0.10 onwards: duplex
	NANT-D MPLS	From R4.3: simplex From R4.3.02 onwards: duplex
	NANT-E	From R4.2 onwards: duplex
7356 ISAM FTTB	NRNT-A	From R4.2 onwards: simplex only
7360 ISAM FX	FANT-F	From R4.2.30 onwards: duplex
	FANT-G	From R5.5 onwards: duplex
7362 ISAM DF		From R5.5 onwards: simplex
7362 ISAM SF		From R5.7.01 onwards: simplex
7363 ISAM MX	RANT-A	From R5.0.00a onwards: simplex
	RANT-B	From R5.5 onwards: simplex
7367 ISAM SX		From R5.0 onwards: simplex
7367 ISAM DX		From R5.7 onwards: simplex

Note — For more information about OSWPs, refer to Chapter “Overall Software Package Concept”.

In case of an NT of the NANT-A and NRNT-A family, the Shub and the IACM subsystems are positioned on the same board and are controlled by the same OBC.

In case of an NT of the NANT-D, NANT-E and FX NT family, the IHub and IACM subsystems are positioned on the same board but on different cores of the dual core processor (for NANT-D), or the quad core processor (for NANT-E and FX NT). There is no difference in the installation and migration procedures compared with the NANT-A family. Only the factory software is different.

There is also no difference in the installation and migration procedures for the 7363 ISAM MX, 7367 ISAM SX/DX and 7362 ISAM DF/SF compared with the other ISAM products. Only the factory software is different.

2.4.2 Software Installation Procedure

The operational procedure (performed by the manager) for the software installation of the ISAM is as follows:

1 Install the software of each SWP in a specific directory on your server. Make sure that the SW file and descriptor file of a specific SWP are stored in the same directory. To do so repeat the following steps for each SWP:

- Log on to the server.
- Create the directory where you want to store the software. If the directory already exists, go to the directory.
- Load the SW CD-ROM.
- Copy the software from the CD-ROM to the directory on the server.

2 Create an Overall Descriptor file (see Appendix A *"Syntax of Descriptor Files"* for the layout of this file). The Overall Descriptor file must contain following information about the different SWPs:

- The name (i.e. the path name) of the SWPs.
- The IP address of the Secure File Transfer Protocol (SFTP)(*) server where the SWP can be found.

3 Download the OSWP (see section 5.3 for more details).

4 Activate the OSWP (see section 5.6 for more details).

Note — For security reasons, usage of TFTP during installation/backup/restore must be avoided. SFTP should be used instead of TFTP.

The ISAM has to be restarted after the software is installed and activated. The system will start up with the new software.

2.5 CDE Profile Management

Note — CDE profile management is only applicable in case the H.248/SIP-signaling-based integrated voice service must become operational.

Besides the regular management interface to configure the network and end-user side associated database parameters for the integrated voice service, the access node makes use of additional configuration data input under the format of a downloadable file. As to allow the integrated voice service to become fully operational, it requires the presence of CDE profiles at the Voice server and the Voice LT.

The contents of CDE profiles are customer dependent. CDE profiles are produced off-line at the factory. The contents are collected by means of a questionnaire that needs to be filled in by the customer. The contents are considered to be of static nature. It concerns mainly the physical line characteristics of the Narrow Band (NB) user interface together with the Voice LT hardware related configuration data and configuration data for the protocols that run at the end-user side.

There is a dedicated CDE profile for the POTS Voice LT, the ISDN BRI Voice LT and the Voice Server.

The CDE profiles for the POTS/ISDN BRI Voice LT and Voice Server are included in 1 CDE.tar file. This .tar file must be downloaded and activated in the individual ISAM Voice access nodes, i.e the hub node, the subtending nodes and the remote nodes.

The CDE.tar file, and all other associated files that are required to install an ISAM Voice in the access network, is delivered to the customer as part of the SW package.

The system itself takes care that a CDE profile is downloaded to the Voice Server and /or Voice LT.

The system supports at run-time CDE profile upgrade. They are as well an integral part of the off-line database migration during SW upgrade.

2.5.1 CDE Profile Installation Procedure

The operational procedure (performed by the manager) for the installation of the CDE profiles is as follows:

1. Download the CDE profile
2. Monitor the CDE profile download status
3. Activate the CDE profile

Note — See the *Operations and Maintenance Using CLI for 24Gbps NT* or the *Operations and Maintenance Using CLI for FD 100/320Gbps NT and FX NT* documents for more information on the commands.

2.6 Database Management

2.6.1 IACM Subsystem

The ISAM is able to manage a maximum of three databases at the same time. Each stored database will have a specific operational status with respect to each available OSWP (i.e. Active OSWP and/or NotActive OSWP). The different values of the operational status are listed in Table 5. Only one of the available databases will be operational and each available OSWP will be linked to at most two available databases at the same time.

Table 5 **Operational Status of a Database with respect to the Available OSWPs**

Available OSWP	Value	Definition
Active: currently operational	Actual	The database is currently used by the Active OSWP.
	Preferable	The database has not been used yet, but will be used after a successful activation of the Active OSWP.
	Previous	The database has already been used by the Active OSWP. It corresponds to the previous ‘Actual’ database of the Active OSWP.
	Failed	The database is compatible with the Active OSWP, but for some reason (e.g. corrupted database) the Active OSWP is not able to interpret it.
	Not Useful	The database can not or may not be used by the Active OSWP (e.g. since the database is not compatible).
NotActive: not operational	Actual	The database has not yet been used by the NotActive OSWP and it is the first database for the NotActive OSWP. It will be used after a successful activation of the NotActive OSWP.
		The database has already been used by the NotActive OSWP. It will be used again after the successful activation of the NotActive OSWP on condition that no preferable database is available for the NotActive OSWP.
	Preferable	The database has not been used yet by the NotActive OSWP and there is also a ‘Actual’ database available for this OSWP. The ‘Preferable’ database will be used after the successful activation of the NotActive OSWP.
	Previous	The database has already been used by the NotActive OSWP. It corresponds to the ‘Previous’ database at the time the current NotActive OSWP was still active.
	Failed	The database is compatible with the NotActive OSWP, but for some reason (e.g. corrupted database) the NotActive OSWP was not able to interpret it.
	Not Useful	The database can not or may not be used by the NotActive OSWP (e.g. since the database is not compatible).

2.6.2 Database Processes

The ISAM supports following database management processes:

1 The backup/restore process. This process is always related to the database currently used by the Active OSWP.

2 At any time the manager can request the ISAM to upload one of the available databases from the system to a specified file server. Refer to section "Upload a Database (SNMP based)" for more information.

3 At any time the manager can request the ISAM to download a new database from a specified file server to the system. Refer to section "Upload a Database (SNMP based)" for more information.

4 Online database cloning: this process is activated when a DB or OSWP is downloaded that cannot be linked due to database version incompatibility. There will be an on-line cloning from a release-compatible database (that is, copy and paste with adaptation of the database version) if the OSWP is activated *with linked database*.

Processes 2 and 3 can be used by the manager to perform an *off-line database conversion* used in case of a software upgrade whereby the new OSWP is not able to interpret the database currently used by the active OSWP:

These last two processes can be used by the manager to perform an *off-line database conversion* used in case of a software upgrade whereby the new OSWP is not able to interpret the database currently used by the active OSWP:

1 First the manager requests the ISAM to transfer the currently used database to a specified file server.

2 The manager converts the database off-line.

3 Finally the manager requests the ISAM to download this new converted database from the specified file server.

3 Overall Software Package Concept

3.1 Composition of an OSWP

In case of a software upgrade of the ISAM, the operator must define the applicable ASAM-CORE SoftWare Package (SWP).

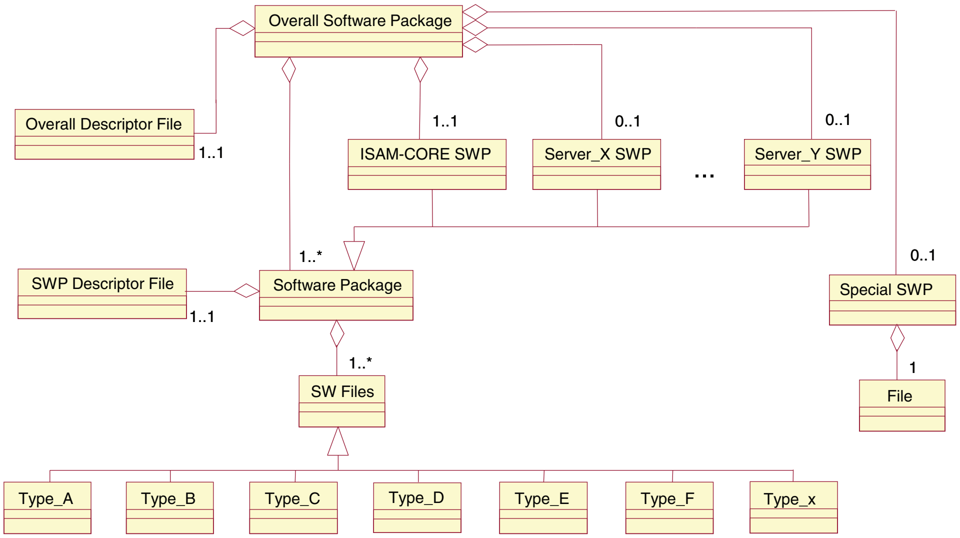
Note — For xHub-based systems only: The SWP contains the required software files for both the IACM subsystem and the xHub subsystem. The software for the different subsystems is always upgraded together.

Therefore an OSWP will be created. An OSWP consists of:

- one Overall descriptor (1..1)
- one ASAM-CORE SWP (1..1).

The composition of an OSWP is shown in Figure 9.

Figure 9 **Composition of an OSWP**



The following sets of files exist for an OSWP:

- the overall descriptor file and the descriptor files of the supported SWPs.
- the files applicable for LT types that are detected and/or planned (but without board type mismatch and without being blocked).
- the files applicable for board types that are detected and/or planned at the NT-B position for 7363 ISAM MX.

3.1.1 Overall Descriptor File

The Overall descriptor file contains information about the ASAM-CORE SWP that belongs to the OSWP. The following information is available:

- The name (i.e. the path name) of the SWP
- The IP address of the SFTP-server(s) where the SWP can be found (primary file server and secondary file server).

The operator creates the Overall descriptor file in function of its systems configuration. The Overall descriptor file is typically stored on a SFTP-server managed by the operator himself.

The syntax and an example of a Overall descriptor file are described in Appendix 7.

3.1.2 ASAM-CORE SWP

Note — The concept of multiple SWP descriptors has been introduced from release 5.4.01 on.

The ASAM-CORE SWP consists of the following:

- One or more SWP descriptor files (1..n)
  The name of a SWP descriptor file is equal to the name of the corresponding SWP but the functional variant is an indication of the product family and NT type used.
  The mapping between the NT type and the SWP Descriptor functional variant is listed in the NT_SWP_Mapping.txt file (also part of the ASAM CORE SWP). This file lists the NT type and the matching SWP Descriptor file.
  The correct SWP Descriptor must be used in the OSWP Descriptor.

- At least one SoftWare (SW) file (1..*)
  A SW file corresponds to an executable for a specific IACM board type or server board type.

Note — The SWP descriptor file and the SW files of a specific SWP must be located in the same directory on the same SFTP server. However the ASAM-CORE SWP can be located on different SFTP servers.

3.1.3 SWP Descriptor File

The SWP descriptor file contains the following information:

- The version number of the compatible database: this version number is also related to the database structure and the allowed database contents.
  - Compatible database definition:
    The database version in the SWP Descriptor File and the version of the linked database are identical.
  - Release-compatible database definition:
    The database version in the SWP Descriptor file (aX.Xbc) and the version of the linked database (dX.Xef) are equal for XX.
  - Online database cloning will copy the dX.Xef database, paste it into a free database container and change the version from dX.Xef to aX.Xbc.
- For each supported board type the SWP descriptor file indicates whether:
  - The board expects the applicable SW files in a decompressed format or not.
  - The related SW files belong to the minimum set of files of the considered OSWP or not.
- For each applicable SW file of a specific board type, the SWP descriptor file contains the file name, the file format and the file size.

The syntax and an example of a SWP descriptor file are described in Appendix 7.

Note — On the use of the minimum set:

The minimum set indication per board type can be used by the operator to indicate that files of this board type should be downloaded (during an OSWP Download action) although no board of the type is detected or planned in the NE. This is a helpful tool for long-term planning because an operator can avoid an OSWP re-download when he wants to introduce a new board type later on in the same OSWP context or plans to replace an existing board type with a new board type (for example, replace a VDSL board with a Vectoring-VDSL board). 7362 ISAM DF/SF and 7367 ISAM SX/DX have no optional boards and have a limited space. As a consequence, usage of a minimum set is to be prevented.

3.1.4 ASAM-CORE SWP example

From release ISR5.4.01 on, you will see multiple SWP descriptor files like the ones below for release 5.4 buildcode 451:

```
L6GQAA54.451

L6GQAB54.451

L6GQAC54.451

L6GQAE54.451
```

Depending on the type of NT board used, a different SWP descriptor file is required. The file NT_SWP_Mapping.txt contains the mapping between SWP descriptor file and NT board. See the example below:

```
AGNT-A L6GQAA54.451

NANT-A L6GQAA54.451

NANT-D L6GQAA54.451

NANT-E L6GQAA54.451

NRNT-A L6GQAA54.451

CFNT-A L6GQAB54.451

FANT-F L6GQAB54.451

FANT-G L6GQAB54.451

RANT-A L6GQAC54.451

NRNT-I L6GQAE54.451

SRNT-A L6GQAE54.451

...
```

So, for example, when using FANT-F as NT, then you will no longer be able to use the standard L6GQAA54.451, but instead have to use the L6GQAB54.451 version.

3.2 OSWP-Database Relationship

Maximum two different OSWPs and three different ASAM-CORE databases can be stored persistently in the system at any time. Each ASAM-CORE database structure is identified by its version number which is related to the database structure and to the allowed database contents.

Each ASAM-CORE SWP descriptor file specifies the version number of the database that can be interpreted by the considered ASAM-CORE SWP. An OSWP will be linked to a specific ASAM-CORE SWP database when the version number reference inside the corresponding ASAM-CORE SWP descriptor file is identical to the version number mentioned in the database itself.

When the operator requests an “activate OSWP with linked database” and no linked database is available, the system shall (contrary to the original behavior where the action is refused) look whether the database of the actual active is a one-way compatible one (one-way compatible = the first two digits are the same and the alphanumeric digit is lower that the one expected). In this case software management will free a database container, copy the compatible actual active database and change the database version in the new container to the database version defined in the SWP descriptor. After these actions, the activation with linked database can be executed.

3.2.1 Database Version Algorithm

The database version follows the syntax [A-Za-z0-9{2}”.”[0-9]{3}. The database version has to be assigned according to a specific algorithm because the offline migration tool requires knowledge of the correlation between the database version and the ISAM release.

The algorithm to assign the database version is composed as follows:

- The last four digits of the database version are taken from the ISAM release version (e.g. ISR2.4.01). The ISAM release version is defined by four digits in which the first two digits specify the major release and the last two digits the sub release.
- The first digit (alphanumeric) of the database version is reserved for future development.
- In case the first three digits of the database version differ an offline database migration has to be performed. Otherwise no database conversion has to be performed.

Table 6 clarifies the algorithm.

Table 6 **Example of Algorithm**

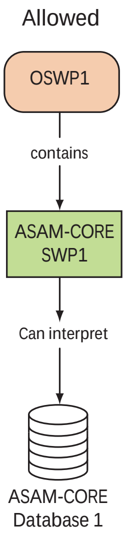
ISAM Release Version	Database Version
ISR2.3	A2.300
ISR2.4	A2.400
ISR2.4.01	A2.401
ISR2.4.02	B2.402
ISR3.0	A3.000

Note — The used ISAM releases and database versions may only be interpreted as examples.

3.2.2 “One-to-One” Relationship

The relation between OSWPs and the ASAM-CORE database version number is a “one-to-one” relationship (see Figure 10). Each ASAM-CORE database (version number) can be interpreted by one OSWP and a specific OSWP can only interpret one ASAM-CORE database (version number).

Figure 10 **One to One Relationship between OSWPs and ASAM-CORE Database**



4 Software Installation

4.1 Introduction

The interface to the manager is either a TL1/CLI interface (in case of remote CT) or an SNMP interface (in case of 5520 AMS). The craftsman is an operator who manipulates the system in a physical way (installation of boards and so on) and performs the basic configuration via the serial interface using TL1/CLI. In case the IACM subsystem is managed by an AMS or remote CT, the configuration actions during installation to be done by the local craftsman are limited to the following parameters:

- For SHub-based ISAM:
  - The configuration of the IP address of the IACM subsystem (not needed in case the IP address is retrieved via BOOTP).
  - The IP address of the default router (only needed in case the IP address of the IACM subsystem is directly configured) and the subnet mask if required.
  - External VLAN configuration.
- For IHub-based ISAM:
  - The configuration of the IP address of the IACM subsystem (not needed in case the IP address is retrieved via BOOTP).
  - The IP address of the default router (only needed in case the IP address of the IACM subsystem is directly configured) and the subnet mask if required.
  - Configuration of an external management v-VPLS.
- For 7363 ISAM MX and 7367 ISAM SX/DX:
  - The configuration of the IP address and subnet mask.
  - The IP address of the default router (only needed in case the IP address of the IACM subsystem is directly configured) and the subnet mask if required.
  - External VLAN configuration.
  - Configuration of the uplink ethernet port and SFP MAU type

- For 7362 ISAM DF/SF:
  - The configuration of the IP address and subnet mask.
  - The IP address of the default router (only needed in case the IP address of the IACM subsystem is directly configured) and the subnet mask if required.
  - External VLAN configuration.
  - Configuration of the uplink port.

In case no AMS or remote CT is used, the craftsman takes over the responsibility of the manager as well.

4.1.1 For xHub-based Systems

The initial steps of the installation of an ISAM has to be performed via TL1/CLI by the craftsman. The serial interface of the IACM subsystem is used to perform the initial configuration of both the IACM subsystem and the SHub/IHub subsystem. From the moment the OAM connectivity is setup, the configuration can be done either via TL1, CLI or SNMP by the manager.

Note 1 — There is no need to make a selection between inband and outband management in the IACM subsystem because in both cases the management channel will always go via the control link between the NT board.

Note 2 — For more information about the specific configuration procedures and the used commands, refer to the *Operations and Maintenance Using CLI for FD 24Gbps NT* or the *Operations and Maintenance Using CLI for FD 100/320Gbps NT or FX NT* documents.

4.1.2 For 7363 ISAM MX and 7367 ISAM SX/DX

The initial steps of the installation of a 7363 ISAM MX and 7367 ISAM SX/DX has to be performed via TL1/CLI by the craftsman. The serial interface of the IACM subsystem is used to perform the initial configuration. From the moment the OAM connectivity is setup, the configuration can be done either via TL1, CLI or SNMP by the manager.

Note — For more information about the specific configuration procedures and the used commands, refer to the *Operations and Maintenance Using CLI for 7363 ISAM MX and 7367 ISAM SX/DX* document.

4.1.3 For 7362 ISAM DF/SF

The initial steps of the installation of a 7362 ISAM DF/SF have to be performed via CLI by the craftsman. The serial interface of the IACM subsystem is used to perform the initial configuration. From the moment the OAM connectivity is setup, the configuration can be done either via CLI or SNMP by the manager.

Note — For more information about the specific configuration procedures and the used commands, refer to the *Operations and Maintenance Using CLI for 7362 ISAM DF/SF* document.

4.2 Preparation

Following prerequisites for the different systems are listed in this chapter.

4.2.1 For xHub-based Systems

- The rack, shelf and boards (except the NT board) of the system are installed or inserted. The system is not powered-up yet. The system has no configuration data yet; no database is available.
- For SHub-based ISAM:

  The SMAS board has to be inserted as the system retrieves the items listed below. If the system does not have SMAS functionality, the MAC addresses have to be configured by the manager.
  - The “AsamId” and the MAC addresses of the SHub interface.
  - The 10baseT interface (outband management) and the SHub system MAC address from the remote inventory of the SMAS board.
- For IHub-based ISAM: the MAC address is always retrieved from the SMAS board.
- The remote file servers (xFTP) are operational. Remote file servers are needed with respect to the SW and database backup.
- BOOTP server is operational and configured correctly (only needed in case the IP address of the xHub/IACM subsystem has to be retrieved dynamically).
- The craftsman is able to manage the IACM subsystem with TL1 and CLI and the xHub subsystem with CLI via the serial interface of the IACM subsystem.
- The manager is installed and able to manage the system.

- The way of installing depends on the type of NT board:
  - NANT-A: Installation from factory software R3.1.
  - NRNT-A: Installation from factory software R4.2.
  - NANT-D: Installation from factory software R3.7.10.
  - NANT-D MPLS: Installation from factory software R4.3
  - NANT-E: Installation from factory software R4.2.
  - FANT-F: Installation from factory software R4.2.30
  - FANT-G: Installation from factory software R5.5
- The system should be ready to startup the NT board upon insertion.

4.2.2 For 7363 ISAM MX and 7367 ISAM SX/DX

- The needed LT and/or NT-B boards of the 7363 ISAM MX system are inserted. The system is not powered-up yet. The system has no configuration data yet; no database is available.
- The remote file servers (xFTP) are operational. Remote file servers are needed with respect to the SW and database backup.
- The craftsman is able to manage the system with TL1 and CLI via the serial interface of the system.
- The manager is installed and able to manage the system.
- The system has pre-installed SW
  - 7367 ISAM SX: Installation from factory software R5.0 (SX)
  - 7367 ISAM DX: Installation from factory software R5.7 (DX)
  - 7363 ISAM MX RANT-A: Installation from factory software R5.0.00a (MX)
  - 7363 ISAM MX RANT-B: Installation from factory software R5.5 (MX)
- The ISAM MX system should be ready to startup the NT board upon insertion.

4.2.3 For 7362 ISAM DF/SF

- The system is not powered-up yet. The system has no configuration data yet; no database is available.
- The remote file servers (xFTP) are operational. Remote file servers are needed with respect to the SW and database backup.
- The craftsman is able to manage the system with CLI via the serial interface of the system.
- The manager is installed and able to manage the system.
- The system has pre-installed SW
  - 7362 ISAM DF: Installation from factory software R5.5 (DF)
  - 7362 ISAM SF: Installation from factory software R5.7.01 (SF)

4.3 Installation of a Simplex System

Note — This section is only applicable for xHub-based systems.

The installation of a system with one NT board consists of the three following parts:

- Initialization
- Setting up OAM connectivity
- Configuration.

4.3.1 Initialization

The *craftsman* has to perform the following procedure to initialize the system.

1 Power up the system.

2 Insert the prepared NT board:

- NANT-A, NANT-D or NANT-E in slot A of the ISAM FD (for NANT-A and NANT-D: at this moment only an NT board in slot A is supported).
- FX NT in slot A of the 7360 ISAM FX
- NRNT-A in 7356 ISAM FTTB
- AGNT-A in ERAM-A

3 When the system is powered up, the xHub subsystem starts up with the factory SW, stored on the NT board. After startup the xHub subsystem has the initial configuration:

- All the ports on the switch are by default administratively auto-up. This state corresponds to the administrative state up but no alarms are reported to avoid unnecessary alarms in case certain ports are not used.
- By default one control port and 16 IACM ports are configured. All IACM subsystem ports and controller port are by default associated with IC_VLAN (4094) and are designated as tagged ports.
- By default 7 network ports are configured. All network ports are set to “unused”.
- Because of security reasons, the network ports has to be configured by default to discard all frames with VLAN equal to the IC_VLAN.
- The IP interface towards the NT through the controller port is created by default. The private IP addresses assigned for that interface are 127.0.0.2 at the NT and 127.0.0.3 at the xHub subsystem. This IP interface is operationally up and is pingable once the xHub subsystem initialization is complete.

4 Once inserted the NT board powers up, initializes and becomes operational with the factory SW. No linked database is found and the system creates a default database.

At this point of the IACM subsystem installation, the xHub subsystem has to be available to set up the internal communication and the external management. From the moment the xHub subsystem is initialized, the internal communication between the NT board and the LTs is established and the NT board shall be able to download the factory OSW to the LTs (via multicast), which will restart with the new software. Because the database on the NT board is empty, the LTs are not further configured. The NT board can however read out the remote inventory of the entire (detected) system.

5 At this moment, the LEDs on the IACM subsystem equipment (NT board and LTs) give information about the state of the system.

4.3.2 Setting up OAM Connectivity

The *craftsman* has to perform the following procedure to set up the Operation, Administration and Maintenance (OAM) connectivity:

1 When the prepared NT board becomes active, configure the basic parameters on the NT board to set up OAM connectivity with the *manager*.

- *The IP address of the prepared NT board:* Configure directly the IP address or retrieve it via BOOTP using the physical address present in the remote inventory.
- *The IP address of the default router:* Only needed in case the IP address is directly configured and the management system is located in another subnet with respect to the IACM subsystem.
- *The subnet mask* (if required)
- *The VLAN of the external management*

2 Connect to the xHub subsystem using the serial port on the IACM subsystem and log into the system.

3 Ensure that the xHub subsystem holds a valid universally unique MAC address. These MAC addresses come from the remote inventory of the SMAS board. At startup the NT reads out the xHub subsystem MAC address and configures it.

Note: In case of IHub, if there is no valid MAC address present, configure a valid MAC address.

4 Configure the external NT OAM VLAN (4093). The xHub subsystem adds the NT-xHub controller port and the network ports to this management VLAN.

The configuration of the external OAM VLAN and the network ports has to be performed according the selected management: inband or outband.

5 Configure a filter on the xHub subsystem that drops received frames on the network/subtending/user ports with Destination Address (DA) equal to the LT meta MAC address.

6. Store this configuration so that the changes take effect.
    - For SHub systems, use the command **admin software-mngt shub database save**.

      SHub has a single command to save both the regular and the protected configuration and this should be used for all configuration save actions.
    - For IHub systems, use the command **admin software-mngt ihub database save-protected**.

      IHUB has two commands, one to save the protected part (**admin software-mngt ihub database save-protected**) and one to save the regular part (**admin save**).

      The command **admin software-mngt ihub database save-protected** should only be used to save the OAM configuration during the installation phase, not during the further configuration of the system.

Note — From this step onwards it is recommended to backup the configuration in the local flash on a regular basis and to configure the flash restore operation to restore from flash on subsequent restarts.

4.3.3 Configuration

The *Manager* can now configure the system. The configuration the IACM subsystem and the SHub/IHub subsystem can now be done in parallel.

4.3.3.1 Configuration of the IACM Subsystem

The *manager* has to perform the following procedure to install the IACM subsystem:

1. Detect when the IACM subsystem is available again. This happens once the IACM subsystem has its basic parameters configured and thus the isolated state for the IACM subsystem is cleared.
2. For SHub-based ISAM only:

   Configure the system name consistent with the name configured in the SHub subsystem.
3. In case the factory SW differs from the target release, configure the IP address of the SFTP server which allows the IACM to retrieve the missing target SW OSWP files.

   Specify the path name of the overall descriptor file and the set of the OSWP files. The system downloads now the target SW OSWP.

   Activate the target SW. If the DB version differs between factory and target release, an offline migration (i.e. database upload, database conversion and database download) is mandatory.

   After the SW activation, the NT board will perform a WARM RESET and start up with the converted database. The NT board will now download the target OSW to the LTs (via multicast), which will restart with the new software.

4 Launch a command that plans automatically all detected equipment that is not yet planned according to the database.

Applique cards will be automatically planned by this operation. In case of a splitterless IACM subsystem only the NT I/O will be detected and planned. The applique boards in the separate splitter shelf will not be detected and they will not be planned.

5 Start configuring the ISAM (refer to the *“Operations and Maintenance Using CLI”* or *“Operations and Maintenance Using TL1”* of your system for more information).

4.3.3.2 Configuration of the SHub Subsystem

Note — The configuration of the common parameters (system name, external NT OAM VLAN) have to be performed in a consistent way with the configuration on the IACM subsystem.

Setup of system infrastructure

The *craftsman* has to perform the following procedure to configure the SHub subsystem:

1 Configure the system name in the SHub subsystem.

2 Reconfigure the default network port mapping to the desired network/subtending/user precompiling if required.

Provisioning of the SHub Subsystem

From this moment onwards the *manager* can manage the SHub subsystem:

1 Register for traps and alarms by configuring the IP address and port.

2 Perform the trap configuration for each type.

3 Configure the severity and reporting mode of the alarms.

4 In case of access protection to the system, configure the SHub access list to filter unauthorized management traffic.

5 Change the administrative state of all used ports to *“UP”*. By this the reporting of the alarms on these ports is enabled.

There are two options for the *manager* to provision a configuration:

- **Configuration via backup**
  If the configuration was backed up in a remote server, the configuration can be restored using a CLI command from a remote server to the NT disk. The SHub subsystem reports using a trap, the result of the restore operation.

- **Configuration via command**
  In case of first installation, configure the SHub subsystem via separate commands.

Note — Refer to the *Operations and Maintenance Using CLI for FD 24Gbps NT* for more information about the configuration of the SHub subsystem.

Backup of configuration

The *manager* has to perform the following procedure to make a backup of the configuration:

1 Perform a backup of the configuration in the local flash of the NT disk.

2 *OPTIONAL:* Perform a backup of the database to a remote server for backup purposes.

4.3.3.3 Configuration of the IHub Subsystem

The *craftsman* has to perform the following procedure to configure the IHub subsystem:

1 Configure an external management V-VPLS on the IHub

2 Configure a management IP address on the IHub

Provisioning of the IHub Subsystem

From this moment onwards the *manager* can manage the IHub subsystem:

Note 1 — Trap management and alarm management for the IHub is integrated in the IACM.

Note 2 — All ports are set to “admin up” by default; each port will, relevant to its type and configuration, become “operational up” or stay “operational down”.

1 Configure the severity and reporting mode of the alarms.

2 Configure the security access policy to the NT OBC on the IHub (configuration of CPU filters).

There are two options for the *manager* to provision a configuration:

- **Configuration via backup**
  If the configuration was backed up in a remote server, the configuration can be restored using a CLI command from a remote server to the NT disk. The IHub subsystem reports using a trap, the result of the restore operation.
- **Configuration via command**
  In case of first installation, configure the IHub subsystem via separate commands.

Note — Refer to the *Operations and Maintenance Using CLI for FD 100/320Gbps NT and FX NT* for more information about the configuration of the IHub subsystem.

4.4 Installation of a Duplex System

Note — This section is not applicable for 7362 ISAM DF/SF, 7363 ISAM MX and 7367 ISAM SX/DX.

It is also possible to install a Duplex System (with two redundant NT boards).

Note — To see which NT boards support redundancy, please check the *ISAM Product Information.*

The same procedure as for a simplex system (refer to section 4.3) can be done for a duplex system.

Installation procedure notes:

- When the Craftsman powers up the system, both NT boards will initialize independently. The NT board in slot A will be selected as the active NT board.
- When inserting the prepared NT boards, one has to be inserted in slot A and one in slot B.
- When setting up OAM connectivity, this is done on the active NT board in slot A.

After the installation, both NT boards are fully synchronized and the 1+1NT redundancy can be activated.

4.5 Installation of a 7363 ISAM MX and 7367 ISAM SX/DX

The installation of a 7363 ISAM MX and 7367 ISAM SX/DX consists of the three following parts:

- Initialization
- Setting up OAM connectivity
- Configuration.

4.5.1 Initialization

The *craftsman* has to perform the following procedure to initialize the system.

1 Power up the system.

2 For 7363 ISAM MX: insert the prepared NT board in the NT-A slot of the system.

3 When the system is powered up, it starts up with the factory SW. For 7363 ISAM MX system it is stored on the EPROM/NAND of the NT-board. For 7367 ISAM SX/DX it is stored on the EPROM/NAND of the unit.

After startup the system has the following uplink port configuration:

For 7363 ISAM MX

- the uplink port nt-a:xfp:1 is by default administratively up
- the uplink port is configured for 1G (1000basebx10d) SFP, the SFP status is power up.

For 7367 ISAM SX/DX

- the uplink port nt:xfp:1 is by default administratively up
- the uplink port nt:xfp:2 is by default administratively down

4 No linked database is found and the system creates a default database.

On 7363 ISAM MX system, the LT SW is not started up until boards are planned. The NT board can read out the remote inventory of the inserted boards

5 At this moment, the LEDs on the IACM subsystem equipment give information about the state of the system. Table 7 for 7367 ISAM SX/DX and table 8 or 7363 ISAM MX.

Table 7 **LED behavior 7367 ISAM SX/DX**

LED		**Operational state**
Green	**Red**	
Off	Off	Off

(1 of 2)

LED		Operational state
Green	**Red**	
On	Off	Self test / initialization
Blinking	Off	Operational
Blinking	Blinking	LOS indication of the uplink
Blinking	On	Major or Critical alarm (the alarm LED will blink 50/50)

(2 of 2)

Table 8 LED behavior 7363 ISAM MX NT

LED	Color	Description
DC	Green	DC status of the 7363 ISAM MX NT board: • On - Correct DC voltage on cable, i.e. the input voltage is high enough for normal operation • Off - No or incorrect voltage on cable, i.e. the input voltage is out of range for normal operation
1	Green	Network Link channel 2 status (only relevant when a 2x 1 GE cSFP is injected in the SFP cage on the front panel): • On - Channel up but idle • Blinking - Channel is receiving/transmitting data • Off - No link detected
X1	Green	Network Link channel 1 status: • Green - Channel up but idle • Blinking - Channel is receiving/transmitting data • Off - No link channel detected
VECT	Green	Vectoring status of the 7363 ISAM MX NT board: • Green - Vectoring is enabled. VCE is operational and a VCE profile is assigned to this card and at least one line has a vectoring profile assigned. • Off - Vectoring is not enabled (no VCE profile nor vectoring profile assigned). The SLV LT units have not been synchronized with the 7363 ISAM MX NT board.
SYS	Green	7363 ISAM MX NT Board System status: • Green - Active, board inserted • Off - Locked, board alive, SW loading to start • Blinking - Operational, SW loaded
PWR	Green	Power status: • Green - Power present and switched on • Off - Power not switched on
ALM	Red	Alarm status of the 7363 ISAM MX NT board: • Red - Alarm condition exists, board failure. • Off - No alarm condition exists, normal board operation.

4.5.2 Setting up OAM Connectivity

The *craftsman* has to perform the following procedure to set up the Operation, Administration and Maintenance (OAM) connectivity:

1 When the 7363 ISAM MX or 7367 ISAM SX/DX becomes accessible, configure the basic parameters on the board to set up OAM connectivity with the *manager*.

- *The IP address*
- *The IP address of the default router:* Only needed in case the management system is located in another subnet with respect to the 7363 ISAM MX or 7367 ISAM SX/DX.
- *The subnet mask* (if required)
- *The VLAN of the external management*
- *On 7363 ISAM MX configure mau type and/or/ autonegotiate option of nt-a:xfp:1*

2 Configure SNMP authentication/authorization parameters when further configuration is only done via SNMP

3 The system stores this configuration in the database so that the changes take effect.

Note — From this step onwards it is recommended to backup the configuration in the local flash on a regular basis and to configure the flash restore operation to restore from flash on subsequent restarts.

4.5.3 Configuration

The *manager* has to perform the following procedure:

1 In case the factory SW differs from the target release, configure the IP address of the SFTP server which allows the system to retrieve the missing target SW OSWP files.

Specify the path name of the overall descriptor file and the OSWP file. The system downloads now the target SW OSWP.

Activate the target SW. If the DB version differs between factory and target release, an offline migration (i.e. database upload, database conversion and database download) is mandatory.

After the SW activation, the 7367 ISAM SX/DX will perform a WARM RESET and start up with the converted database.

2 Start configuring the ISAM (refer to the *“OAM Using CLI for 7363 ISAM MX and 7367 ISAM SX/DX”* or *“OAM Using TL1 for 7363 ISAM MX and 7367 ISAM SX/DX”* for more information).

There are two options for the *manager* to provision a configuration:

- **Configuration via backup**
  If the configuration was backed up in a remote server, the configuration can be restored using a CLI command from a remote server to the NAND flash.
- **Configuration via command**
  In case of a first time installation, configure the 7363 ISAM MX or 7367 ISAM SX/DX via separate commands.

Note — Refer to the *Operations and Maintenance Using CLI for 7363 ISAM MX and 7367 ISAM SX/DX* for more information.

Backup of configuration

The *manager* has to perform the following procedure to make a backup of the configuration:

1 Perform a backup of the configuration in the local NAND flash of the system.

2 *OPTIONAL:* Perform a backup of the database to a remote server for backup purposes.

4.6 Installation of a 7362 ISAM DF/SF

The installation of a 7362 ISAM DF/SF consists of the three following parts:

- Initialization
- Setting up OAM connectivity
- Configuration.

4.6.1 Initialization

The *craftsman* has to perform the following procedure to initialize the system.

1 Power up the system.

2 When the system is powered up, it starts up with the factory SW stored on the EPROM/NAND of the unit.

After startup the system has the following uplink port configuration:

- all uplink ports are by default administratively down and
- all uplink ports are configured for 10G (10GBase-LR) XFP, the XFP status is power down.

3 No linked database is found and the system creates a default database.

4 At this moment, the LEDs on the IACM subsystem equipment give information about the state of the system.

For 7362 ISAM DF, see Table 9 for LED behavior.

For 7362 ISAM SF, see Table 10 for LED behavior.

Table 9 **LED behavior 7362 ISAM DF**

LED	Description
Fan Status	Fan status LED: • Green: all fans in the fan unit are operating normally • Red: one or more fans in the fan unit have failed or tripped a fuse • Off: power supply not present
PWR	Power LED: • Green (always on): the system is shutting down • Flashing green (3,5 s on, 1 s off): the system running and operating normally • Flashing green (0.5 s on, 0.5 s off): the system is starting up • Off: the system is not receiving power
ALM	Alarm LED: • Red (always on): an alarm has been detected • Off: the system is operating normally or receives no power
FSM Optical ports	LED status: • Green: link up at this port • Flashing green: transmitting or receiving packet in link up state • Off: no link detected at this port
GPON/CP Optical ports	LED status: • Off: PON is not provisioned or PON is admin down. It is safe to remove the XFP or the fiber. • Yellow on: PON is provisioned, PON admin state is up and there is no PON loss alarm on the PON, but there is no ONT provisioned or all ONTs are provisioned with bogus SN on the PON. • Green on: PON is provisioned, PON admin state is up, and at lease one non-bogus ONT is provisioned on the PON. • Red on: PON is provisioned, PON admin state is up and there is a PON loss alarm raised on the PON.
ACO	ACO (Alarm Cut-Off) LED indicates if the ACO switch has been used to disable external alarm output: • Green: when the ACO push-button switch is pushed less than 2 seconds to set the external critical alarm output contacts to the non-alarmed state, The LED is on.until the cut off alarm(s) are cleared or a new alarm condition is raised. • When the button is pressed more than two seconds, a lamp test starts. During a lamp test, all alarm LEDs and ACO LEDs are lit.External alarm relays are set to alarmed state.
GE Optical port	LED status: • Green: the Ethernet port is operational up • Flashing green: transmitting or receiving packet in link up state, traffic is OK • Off: the Ethernet port is not active

Table 10 **External LED behavior 7362 ISAM SF**

Interface	Status	Function
TEMP	Off	No power
	Solid red	Critical temperature reached
	Solid orange	One or more temperature sensor alarms raised
	Solid green	No temperature alarms
NTWK	Off	No power
	Solid red	All of the configured uplinks are operationally down
	Solid orange	One or more configured uplinks operationally down.
	Solid green	All of the configured uplinks operationally up.
PWR	Off	No power
	Solid orange	One Power Supply Unit (PSU) reported an alarm (not present, fault,…) - only applicable in case the 7362 ISAM SF-8GW is configured to use two PSUs. In case the 7362 ISAM SF-8GW is configured to use one PSU, then this status will never be shown.
	Solid green	All configured PSUs in service

4.6.2 Setting up OAM Connectivity

The *craftsman* has to perform the following procedure to set up the Operation, Administration and Maintenance (OAM) connectivity:

1 When the 7362 ISAM DF/SF becomes accessible, configure the basic parameters on the board to set up OAM connectivity with the *manager*.

- *The IP address*
- *The IP address of the default router:* Only needed in case the management system is located in another subnet with respect to the 7362 ISAM DF/SF.
- *The subnet mask* (if required)
- *The VLAN of the external management*

2 Configure SNMP authentication/authorization parameters when further configuration is only done via SNMP

3 The system stores this configuration in the database so that the changes take effect.

Note — From this step onwards it is recommended to backup the configuration in the local flash on a regular basis and to configure the flash restore operation to restore from flash on subsequent restarts.

4.6.3 Configuration

The *manager* has to perform the following procedure:

1 In case the factory SW differs from the target release, configure the IP address of the SFTP server which allows the system to retrieve the missing target SW OSWP files.

Specify the path name of the overall descriptor file and the OSWP file. The system downloads now the target SW OSWP.

Activate the target SW. If the DB version differs between factory and target release, an offline migration (i.e. database upload, database conversion and database download) is mandatory.

After the SW activation, the 7362 ISAM DF/SF will perform a WARM RESET and start up with the converted database.

2 Start configuring the ISAM (refer to the *“OAM Using CLI for 7362 ISAM DF/SF* for more information).

There are two options for the *manager* to provision a configuration:

- **Configuration via backup**
  If the configuration was backed up in a remote server, the configuration can be restored using a CLI command from a remote server to the NAND flash.
- **Configuration via command**
  In case of a first time installation, configure the 7362 ISAM DF/SF via separate commands.

Note — Refer to the *Operations and Maintenance Using CLI for 7362 ISAM DF/SF* for more information.

Backup of configuration

The *manager* has to perform the following procedure to make a backup of the configuration:

1 Perform a backup of the configuration in the local NAND flash of the system.

2 *OPTIONAL:* Perform a backup of the database to a remote server for backup purposes.

4.7 Troubleshooting

This section provides the most common problems during the installation of the system. If the problems remains contact Nokia.

4.7.1 xHub Subsystem Installation

Table 11 **Problem Solving xHub Subsystem Installation**

Problem	Proposed Action	Actor
The xHub subsystem is isolated.	The OAM connectivity parameters are wrongly configured (IP address can not be retrieved in dynamic mode, external management VLAN,...) Configure the correct parameters.	Craftsman
Related ports can not support the correct functionality.	Reconfiguration of the network ports is not successful.	Craftsman
Unpredictable behavior of the xHub subsystem.	Wrong database restored on the xHub subsystem (NT disk). The entire xHub subsystem shall be configured according to the contents of this database. Take the same basic actions as if the xHub subsystem starts up with no database.	Craftsman
Link alarms reported.	• **Wrong cabling of the IACM ports** By checking the MAC-table on the xHub subsystem detect any mismatches between the MAC address learnt by the xHub subsystem on a specific IACM subsystem port and the internal communication MAC address of the LT. Cabling has to be corrected according the port mapping. *Note:* The internal communication MAC addresses follow a fixed MAC address scheme. • **Ports are wrongly configured as administrative up while there is no LT equipped** Configure the administrative state of the related port correctly.	Craftsman
The uplink is operational down	Verify that an Nokia authorized SFP is inserted.	Craftsman

4.7.2 IACM Subsystem Installation

Table 12 **Problem Solving IACM Subsystem Installation**

Problem	Proposed Action	Actor
The NT does not restart properly and stays in boot.	Replace the NT by another NT.	Craftsman

(1 of 2)

Problem	Proposed Action	Actor
The NT can not read the remote inventory of the SMAS board.	Replace the SMAS board by another or fill in the remote inventory of the SMAS board correctly	Craftsman
The LT stays in boot.	• The LT SW as defined in the SWP is not present on the NT disk. • xHub subsystem is not reachable, reconfigure xHub subsystem.	Craftsman
Unpredictable behavior of the IACM subsystem.	The NT has already been used in a different NE and thus the configuration of this NE is stored persistently in its database. The NT shall configure the entire ISAM according to the planned configuration in this database. If this NT was formerly managed by a different manager, the correct manager shall not detect its presence. Take the same basic configuration actions as if the NT starts up with a default database.	Craftsman
The IACM subsystem is isolated.	Replace the NT board.	Craftsman
The NT is not detected by the manager and the NT remains isolated	Check and correct the OAM configuration parameters.	Craftsman and manager
The uplink is operational down	Verify that an Nokia authorized SFP is inserted.	Craftsman

(2 of 2)

4.7.3 7367 ISAM SX/DX or 7362 ISAM DF/SF Installation

Table 13 **Problem Solving 7367 ISAM SX/DX or 7362 ISAM DF/SF Installation**

Problem	Proposed Action	Actor
The system is isolated	The OAM connectivity parameters are wrongly configured (IP address, external management VLAN,...) Configure the correct parameters.	Craftsman
The uplink is operational down	Verify that an Nokia authorized SFP is inserted Verify the autonegotiation settings. Verify that the first uplink is used.	Craftsman

4.7.4 7363 ISAM MX Installation

Table 14 Problem Solving 7363 ISAM MX Installation

Problem	Proposed Action	Actor
The NT does not restart properly and stays in boot.	Replace the NT by another NT.	Craftsman
The LT stays in boot.	• The LT SW as defined in the SWP is not present on the NT disk. • Verify that LT's are planned correctly • Verify that LT SW has been downloaded to the system. If not do a re-download.	Craftsman / manager
Unpredictable behavior of the system	The NT has already been used in a different NE and thus the configuration of this NE is stored persistently in its database. The NT shall configure the entire ISAM according to the planned configuration in this database. If this NT was formerly managed by a different manager, the correct manager shall not detect its presence. Take the same basic configuration actions as if the NT starts up with a default database.	Craftsman
The system is isolated.	Verify via the serial line whether the system is up. If not reboot the system or finally replace the NT card.	Craftsman
The NT is not detected by the manager and the NT remains isolated	Check and correct the OAM configuration parameters.	Craftsman and manager
The uplink is operational down	Verify that an Nokia authorized SFP is inserted.	Craftsman

5 SWDB Processes

5.1 Introduction

This chapter describes the different SoftWare management and DataBase management (SWDB) processes.

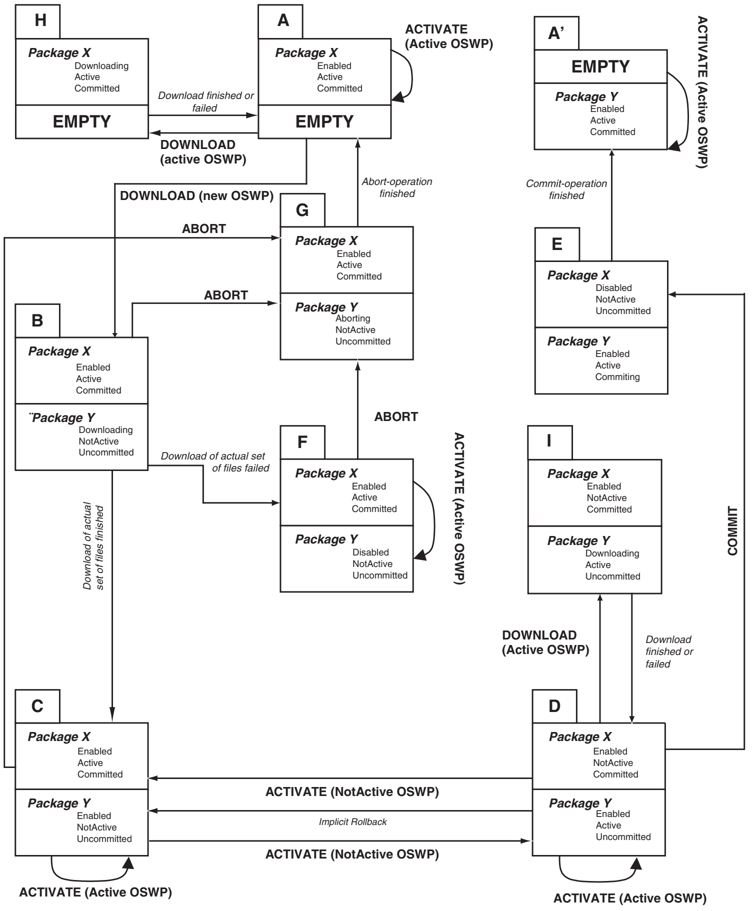
The following conditions must be established in order to complete one of the SWDB processes:

- The management channel between the system and the manager has been established.
- The system is not involved in another SWDB process.

5.2 Possible State Transitions of an OSWP

The system is able to handle two OSWPs simultaneously. The possible state transitions of these two OSWPs are shown in Figure 11.

Figure 11 **Possible State Transitions of an OSWP**



Note — The messages in bold correspond to requests from the management station, the messages in italic correspond to internal system events.

Table 15 gives a description of each of the possible OSWP state values.

Table 15 **OSWP State Values**

State Value	Description
Enabled	The OSWP is ready to become active or is already active. All the files of the considered OSWP are available on the system.
Disabled	The OSWP cannot become active since at least one of the files is not available on the system.
Downloading	The OSWP cannot become active since the download of the requested set of files is still going on.
Aborting	The system is still busy removing the files, not belonging to the current active OSWP, from the disk file.
Active	The OSWP is currently operational.
NotActive	The OSWP is not operational.

5.3 Download of a new OSWP

Note — For xHub-based systems only:

- From R4.3.02 onwards the download of a new OSWP (initiated by the manager) triggers the minimization of the currently active OSWP to make sure that sufficient space is available on the CF to store the new OSWP.
- The current active OSWP will be minimized up to the NT and the currently detected and/or planned LT boards. This automatic action is similar to a regular OSWP Download where also only files for the NT and planned and/or detected LTs are downloaded.
- Prior to R4.3.02, the manager had to manually remove redundant files from the currently active OSWP to make room for the new OSWP if insufficient space was available for the download (see section “Deletion of an Individual File”).

Note — For xHub-based systems only:

- From R5.3.01 onwards, a new overlay zone has been introduced for downloads. This extra storage limit will be used to store LT files. The NT files would still need to be stored in the default partition only. The new zone is under /data/Sw for SHUB Boards and /ONT/Sw for IHUB Boards.It is recommended that no manual operations must be performed in the overlay zone.

The following phases can be distinguished during the download process of an OSWP:

- Evaluation of the download request
- Download and interpretation of the files
- Interruption of the download
- Result of a new OSWP download.

5.3.1 Evaluation of the Download Request

The download of an OSWP is initiated by the manager. He will request the system to start a specific download session. The download request contains following information:

- The path name of the corresponding Overall Descriptor file.
- The IP address(es) of the SFTP-server(s) where the Overall Descriptor file can be found.
- The set of files the management station wants to have available on the system before activating the new OSWP.

Note — The download request will only be accepted in case only one OSWP is available in the system and the status of this OSWP is Enabled/Active/Committed. After acceptance of the download request (state A in Figure 11) the download process is started.

5.3.2 Download and Interpretation of the Files

The manager has the possibility to monitor the progress of the download process with granularity. The system is in state B of Figure 11:

- status first (current) OSWP: Enabled/Active/Committed
- status second (new) OSWP: Downloading/NotActive/Uncommitted.

Table 16 shows the different phases in a download process.

Table 16 **Download and Interpretation of the Files**

Phase	Description
1	After the acceptance of the download request, the system will download the Overall Descriptor file of the specified OSWP from the specified SFTP server. The location of this SFTP server is specified in the download request.
2	The Overall Descriptor file specifies the different SWPs that belong to the considered OSWP. Based on the specified SWPs the system downloads the different SWP descriptor files (via SFTP).

(1 of 2)

Phase	Description
3	Each SWP descriptor file specifies the different applicable SW file(s) and whether or not they belong to the minimum set of the OSWP. The system downloads the SW files that are specified in the downloaded SWP descriptor files on the following conditions: • Sufficient resources are available for their persistent storage. • The SW file is not yet available in the system. • The SW file belongs to the actual set of the new OSWP which means that the SW file belongs to the minimum set of the new OSWP or to a board type that is planned and/or detected in the system. The system downloads the selected SW files in the following order: 1: The SW files that belong to the minimum set of the new OSWP. 2: The SW files belonging to the actual set, but not to the minimum set of the OSWP (if requested by the manager). *Note:* The xHub SW file is part of a SWP and is handled as any other SW file.

(2 of 2)

5.3.3 Interruption of the Download

The download of a new OSWP can be interrupted by the system itself or by the manager.

5.3.3.1 Interruption by the System

The following cases are possible reasons for a interruption of the download process:

- The system has not enough resources to store the selected SW files.
- The system is not able to download the Overall Descriptor file.
- The system is not able to interpret the Overall Descriptor file because of a syntax error.
- The system is not able to download (one of) the (selected) SWP descriptor file(s).
- The system is not able to interpret (one of) the (selected) SWP descriptor file(s) because of a syntax error.
- The system is not able to download (one of) the (selected) SW file(s).
- The system restarts for some reason.

The manager will have the possibility to ask the system for the exact reason of interruption of the download process by the system.

The already downloaded files (SW files and/or SW descriptor files) are not removed by the system. The following situations are possible, depending on the already downloaded files:

- State C in Figure 11: All the files belonging to the actual set of files (that is, belonging to the minimum set or belonging to board types that are planned and/or detected in the system) of the new OSWP are available in the system.
  - status first (current) OSWP: Enabled/Active/Committed
  - status second (new) OSWP: Enabled/NotActive/Uncommitted
- State F in Figure 11: Some files belonging to the actual set of files of the new OSWP are not available in the system.
  - status first (current) OSWP: Enabled/Active/Committed
  - status second (new) OSWP: Disabled/NotActive/Uncommitted

5.3.3.2 Interruption by the manager

The manager requests the system to abort the ongoing download process. The system starts deleting all the files that do not belong to the current OSWP from the file disk. The system is in state G of Figure 11:

- status first (current) OSWP: Enabled/Active/Committed
- status second (new) OSWP: Aborting/NotActive/Uncommitted

When the deleting of all the files is done the system is in state A of Figure 11.

5.3.4 Result of a new OSWP Download

The system is in state C of Figure 11:

- status first (current) OSWP: Enabled/Active/Committed
- status second (new) OSWP: Enabled/NotActive/Uncommitted

5.4 Re-download of the Active OSWP (to add missing SW files)

- For xHub-based systems:
  In the system, one or more new board types have been planned and/or detected. These are present in an SWP descriptor file of the currently Active OSWP but at least one of the corresponding SW files is not yet present so they have to be downloaded again.

- For 7363 ISAM MX:

  In the system, one or more new board types have been planned and/or detected. These are present in an SWP descriptor file of the currently Active OSWP but at least one of the corresponding SW files is not yet present so they have to be downloaded again.
- For 7367 ISAM SX/DX and 7362 ISAM DF/SF:

  As the system is considered as a single unit, there is no optional SW to be re-downloaded.

Following phases can be distinguished during the download process of an OSWP:

- Evaluation of the download request
- Download and interpretation of the files
- Interruption of the download
- Result of a re-download of the Active OSWP.

5.4.1 Evaluation of the Download Request

A re-download of the Active OSWP can only be done if the system is either in “Operational” state (state A in Figure 11) or in “Activated” state (state D in Figure 11):

- State A:
  - status first (current) OSWP: Enabled/Active/Committed
  - status second (new) OSWP: EMPTY
- State D:
  - status first (current) OSWP: Enabled/NotActive/Committed
  - status second (new) OSWP: Enabled/Active/Uncommitted

The manager requests the system to re-download the currently active OSWP. He only specifies the name and index of the currently active OSWP.

5.4.2 Download and Interpretation of the Files

The manager has the possibility to monitor the progress of the download process with granularity. The system is in state H or I of Figure 11:

- State H:
  - status first (current) OSWP: Downloading/Active/Committed
  - status second (new) OSWP: EMPTY
- State I:
  - status first (current) OSWP: Enabled/NotActive/Committed
  - status second (new) OSWP: Downloading/Active/Uncommitted

Table 17 shows the different phases in a download process.

Table 17 **Download and Interpretation of the Files**

Phase	Description
1	The system reuses the existing (persistently stored) Overall descriptor file of the Active OSWP which contains a valid path name and a valid SFTP-server IP address for each SWP that belongs to this OSWP*. *Note:** If this is not the case, the manager has to download the Active OSWP again as a new OSWP with correct Overall descriptor file and activate that new OSWP first.
2	The system also reuses the existing (persistently stored) SWP descriptor file of each SWP, specified in the Overall descriptor file. Each existing SWP descriptor file contains for each supported board type the following information: the name, size and the format of the applicable SW file(s). For each SW file the SWP descriptor file also contains an indication whether the considered SW file belongs to the minimum set of the OSWP or not. The system downloads the SW files that are specified in the existing SWP descriptor files on the following conditions: • Sufficient resources are available for their persistent storage. • The SW file is not yet available in the system. • The SW file belongs to the actual set of the new OSWP which means that the SW file belongs to the minimum set of the new OSWP or to a board type that is planned and/or detected in the system.
3	• For xHub-based systems: As soon as the missing SW files for the new board types are present on the NT disk, the system will load them onto the corresponding detected boards that were waiting for them, if any. The corresponding “WaitingForSW” alarm(s) will be cleared by the system if no errors occur. • For 7362 ISAM DF/SF, 7363 ISAM MX and 7367 ISAM SX/DX: As soon as the missing SW files are present on the SEM disk, the system will load them. The corresponding “WaitingForSW” alarm(s) will be cleared by the system if no errors occur.

5.4.3 Interruption of the Download

The re-download of the Active OSWP can only implicitly be interrupted. Possible reasons for an implicit interruption are:

- The system has not enough resources to store the selected SW files.
- There is no valid path name or SFTP-server IP address in the Overall descriptor file for the SWP(s) corresponding with the selected SW files.
- The system is not able to download one of the selected SW files.
- The system restarts for some reason.

The manager has the possibility to ask the system for the exact reason of the implicit interruption of the download process.

The already downloaded SW files are not removed by the system. The status of the Active OSWP will not depend on the already downloaded files. It will always become the same as before the re-download process (state A or D in Figure 11).

5.4.4 Result of Re-download of the Active OSWP

The status of both OSWPs is the same as before the re-download process (state A or D in Figure 11):

- State A
  - status first (current) OSWP: Enabled/Active/Committed
  - status second (new) OSWP: EMPTY
- State D
  - status first (current) OSWP: Enabled/NotActive/Committed
  - status second (new) OSWP: Enabled/Active/Uncommitted

The previously missing SW files are now present on the NT disk an are now active on the detected boards that were waiting for them, if any.

5.5 Deletion of an OSWP

The download of a new OSWP is only possible when only one OSWP is available in the system. So in some cases the manager will first ask the system to delete one of the available OSWPs before it can initiate a new download process.

Following phases can be distinguished during the deletion of an OSWP:

- Evaluation of the deletion request
- Deletion process
- Result of the deletion process.

5.5.1 Evaluation of the Deletion Request

The deletion of a OSWP can only be initiated when the system is in state C or F of Figure 11:

- State C
  - status first (current) OSWP: Enabled/Active/Committed
  - status second (new) OSWP: Enabled/NotActive/Uncommitted
- State F
  - status first (current) OSWP: Enabled/Active/Committed
  - status second (new) OSWP: Disabled/NotActive/Uncommitted

5.5.2 Deletion Process

The system starts deleting all the persistent stored files (descriptor files and SW files) and databases that are related to the NotActive OSWP.

The system is in state G of Figure 11 during this process:

- status first (current) OSWP: Enabled/Active/Committed
- status second (new) OSWP: Aborting/NotActive/Uncommitted

5.5.3 Result of the Deletion Process

The system is in state A of Figure 11:

- status first (current) OSWP: Enabled/Active/Committed
- status second (new) OSWP: EMPTY

The Active OSWP is the only OSWP in the system. Only files (descriptor files and SW files) and databases related to this OSWP are stored persistently in the system.

5.6 Activation of an OSWP

The exact activation procedure depends on the status of the OSWP that must be activated. Following situations can be distinguished:

- activation of a NotActive OSWP
- activation of a Active OSWP

5.6.1 Activation of a NotActive OSWP

The following phases can be distinguished during the activation process of an NotActive OSWP:

- Evaluation of the activation request
- Activation with compatible database
- Activation with default database
- Result of the activation.

5.6.1.1 Evaluation of the Activation Request

The activation can only start when the current and new OSWP have the conditions as defined in state C or state D of Figure 11:

- State C
  - status first (current) OSWP: Enabled/Active/Committed
  - status second (new) OSWP: Enabled/NotActive/Uncommitted

- State D
  - status first (current) OSWP: Enabled/NotActive/Committed
  - status second (new) OSWP: Enabled/Active/Uncommitted

When the manager requests the system to activate the NotActive OSWP there are two possibilities concerning the used database:

- The manager requests that the NotActive OSWP is activated.
- The manager requests that the NotActive OSWP is activated with the default database.

5.6.1.2 Activation with Compatible Database

The system starts the activation process as shown in Table 18 (for xHub-based systems) or Table 19 (for 7367 ISAM SX/DX or 7362 ISAM DF/SF).

Note: In case the system does not find any compatible database linked to the Enabled/NotActive OSWP, the activation request with a compatible database is refused.

Table 18 **Activation with Compatible Database (xHub-based systems)**

Phase	Description
1	The system selects among the available databases the database that is compatible with and linked to the NotActive OSWP.
2	For each detected and not planned board belonging to a board type supported by the NotActive OSWP, the SW files of the NotActive OSWP become active.
3	For each detected and planned belonging to a board type supported by the NotActive OSWP, the SW files of the NotActive OSWP become active on condition that the board is not locked and no board-type mismatch alarm exists on this board.
4	For each detected board belonging to a board type that is not supported by the NotActive OSWP, the board goes in Boot. The system will report this to the manager.
5	The SW file for the xHub subsystem in the Enabled/NotActive OSWP will become active.
implicit SW rollback: If the system is not able to activate the NotActive OSWP, it immediately interrupts the activation process and reactivates the current Active OSWP (implicit SW rollback) on all the boards, even the boards for which an individual software upgrade was requested before the start of the activation procedure (see Section 5.10). The implicit SW rollback will be reported to the manager. If save actions are ongoing on the xHub subsystem or LT boards, the operator is informed. No new save actions are allowed for a certain time period.	

Table 19 **Activation with Compatible Database (7367 ISAM SX/DX or 7362 ISAM DF/SF)**

Phase	Description
1	The system selects among the available databases the database that is compatible with and linked to the NotActive OSWP.
2	The SW files of the NotActive OSWP become active.
implicit SW rollback: If the system is not able to activate the NotActive OSWP, it immediately interrupts the activation process and reactivates the current Active OSWP (implicit SW rollback). The implicit SW rollback will be reported to the manager.	

5.6.1.3 Activation with Default Database

The system starts the activation process as shown in Table 20 (for xHub-based systems) or Table 21 (for 7367 ISAM SX/DX or 7362 ISAM DF/SF).

Table 20 **Activation with Default Database (for xHub-based systems)**

Phase	Description
1	The system creates a default database based on the detected boards.
2	For each detected and not planned board belonging to a board type supported by the NotActive OSWP, the SW files of the NotActive OSWP become active.
3	For each detected and planned belonging to a board type supported by the NotActive OSWP, the SW files of the NotActive OSWP become active on condition that the board is not locked and no board-type mismatch alarm exists on this board.
4	For each detected board belonging to a board type that is not supported by the NotActive OSWP, the board goes in Boot. The system will report this to the manager.
5	The SW file for the xHub subsystem in the Enabled/NotActive OSWP will become active.
implicit SW rollback: If the system is not able to activate the NotActive OSWP, it immediately interrupts the activation process and reactivates the current Active OSWP (implicit SW rollback) on all the boards, even the boards for which an individual software upgrade was requested before the start of the activation procedure (see Section 5.10). The implicit SW rollback will be reported to the manager. If save actions are ongoing on the xHub subsystem or LT boards, the operator is informed. No new save actions are allowed for a certain time period.	

Table 21 **Activation with Default Database (for 7367 ISAM SX/DX or 7362 ISAM DF/SF)**

Phase	Description
1	The system creates a default database based on the detected boards.
2	The SW files of the NotActive OSWP become active.
implicit SW rollback: If the system is not able to activate the NotActive OSWP, it immediately interrupts the activation process and reactivates the current Active OSWP (implicit SW rollback).	

5.6.1.4 Result of the Activation

The system went from state C to D or from state D to C in Figure 11 together with the selected compatible database or the default database.

The system will not remove the files (descriptor files and SW files) and databases related to the NotActive OSWP. This makes it possible for the manager to return to the previous active OSWP in case he is not confident with the new activated OSWP.

5.6.2 Activation of an Active OSWP

The following phases can be distinguished during the activation process of an Active OSWP:

- Evaluation of the activation request
- Activation with compatible database
- Activation with default database
- Result of the activation.

5.6.2.1 Evaluation of the Activation Request

The activation can only start when the current and new OSWP have the conditions as defined in state A, A’, C, F or state D of Figure 11:

- State A
  - status first (current) OSWP: Enabled/Active/Committed
  - status second (new) OSWP: EMPTY
- State A’
  - status first (current) OSWP: EMPTY
  - status second (new) OSWP: Enabled/Active/Committed

- State C
  - status first (current) OSWP: Enabled/Active/Committed
  - status second (new) OSWP: Enabled/NotActive/Uncommitted
- State F
  - status first (current) OSWP: Enabled/Active/Committed
  - status second (new) OSWP: Disabled/NotActive/Uncommitted
- State D
  - status first (current) OSWP: Enabled/NotActive/Committed
  - status second (new) OSWP: Enabled/Active/Uncommitted

The activation process of an Active OSWP is less complex than the activation process of a NotActive OSWP because data checking is not needed. The system already contains a linked database that is compatible with the Active OSWP.

When the manager requests the system to activate the Active OSWP there are two possibilities concerning the used database:

- The system selects among the available databases the database that is compatible with and linked to the Active OSWP.
- The manager requests that the Active OSWP is activated with the default database. The system creates a default database based on the detected boards.

5.6.2.2 Activation with Compatible Database

The system starts the activation process as shown in Table 22 (for xHub-based systems).

Table 22 **Activation with compatible database**

Phase	Description
1	The system selects among the available databases the database that is compatible with and linked to the NotActive OSWP.
2	The SW files of the Active OSWP are not reloaded on the different boards. They keep running. Not applicable for 7367 ISAM SX/DX or 7362 ISAM DF/SF.
implicit DB rollback: If the system is not able interpret the linked database, it reactivates the Active OSWP together with the previous used database. The implicit DB rollback will be reported to the manager. If save actions are ongoing on the xHub subsystem or LT boards, the operator is informed. No new save actions are allowed for a certain time period.	

5.6.2.3 Activation with Default Database

The system starts the activation process as shown in Table 23 (for xHub-based systems).

Table 23 **Activation with the default database (for xHub-based systems)**

Phase	Description
1	The system creates a default database based on the detected boards.
2	The SW files of the Active OSWP are not reloaded on the different boards. They keep running. Not applicable for 7367 ISAM SX/DX or 7362 ISAM DF/SF.
Note: If save actions are ongoing on the xHub subsystem or LT boards, the operator is informed. No new save actions are allowed for a certain time period.	

5.6.2.4 Result of the Activation

After the activation the system is still in the same state as before the process but with the Active OSWP linked to another database (a compatible database or the default database).

The Activation of the Active OSWP is typically used during the backup/restore procedure of a database. After the restore operation at least two different databases are available:

- The current active database
- The new downloaded (restored) database.

Both databases have the same version number and are compatible with the Active OSWP. The restored database will be linked to the Active OSWP and selected during the activation of the Active OSWP.

5.6.3 Online database cloning

Online database cloning is introduced in R4.3 and only happens inside a major release (for example R4.3 -> R4.3.01).

R4.3 is compatible with database version A4.300.

R4.3.01 is compatible with B4.301 and is able to start up with an A4.300 database. To allow a rollback to R4.3, the A4.300 database will be copy/paste to a new database container and the database version will be changed to B4.301.

R4.3 can only start with A4.300 while R4.3.01 can start with B4.301 or A4.300 (after automatic database cloning to B4.301).

5.7 Commitment of an OSWP

Following phases can be distinguished during the activation process of an NotActive OSWP:

- Evaluation of the commitment request
- Commitment process
- Result of the commitment process.

5.7.1 Evaluation of the Commitment Request

The commitment can only start when the system is in state D of Figure 11:

- status first (current) OSWP: Enabled/NotActive/Committed
- status second (new) OSWP: Enabled/Active/Uncommitted

5.7.2 Commitment Process

After the acceptance of the commit request, the system will remove all persistent stored files (descriptor files and SW files) and databases that are not related to the Active OSWP.

The system is in state E of Figure 11 during this process:

- status first (current) OSWP: Disabled/NotActive/Uncommitted
- status second (new) OSWP: Enabled/Active/Committing

Note — The commit process only implies a status change of the Active OSWP and can never fail.

5.7.3 Result of the Commitment Process

The system is in state A’ of Figure 11:

- status first (current) OSWP: EMPTY
- status second (new) OSWP: Enabled/Active/Committed

The Active OSWP is the only OSWP in the system.

5.8 Download of an Individual File

In order to make testing easier, the manager has the possibility to download individual files (descriptor files and SW files) on the system via SFTP.

Note — The request from the manager to download an individual file will be refused when:

- No resources are available for the storage of the file.
- The file is already available in the system.

5.9 Deletion of an Individual File

It is possible for the manager to remove an individual file (descriptor file or SW file). All stored files can be removed individually, except the SWP/OSWP descriptor files or the files that belong to the NT file set.

5.10 Upgrade Software on a Individual Board

Note — This section is not applicable for 7367 ISAM SX/DX or 7362 ISAM DF/SF.

The concept of an OSWP implies that the system will upgrade at once. It is not possible to upgrade the software on an individual board, while the software on all the other boards of the same board type is not changed.

However for LT board types it is possible to upgrade the SW files on an individual board. The system will accept this request only if the system is in state C or D of Figure 11:

- State C:
  - status first OSWP: Enabled/Active/Committed
  - status second OSWP: Enabled/NotActive/Uncommitted
- State D:
  - status first OSWP: Enabled/NotActive/Committed
  - status second OSWP: Enabled/Active/Uncommitted

When the manager requests to upgrade the software on some individual boards, all these boards will be reloaded with the applicable SW files of the NotActive OSWP, even when these files do not differ from the current active files. The active SW on all other boards still belong to the Active OSWP. The status of the two available OSWPs in the system does not change.

Note 1 — The system will refuse the upgrade request in the following cases:

- The system detects that the selected board belongs to a board type that is not supported by the NotActive OSWP
- The selected board belongs to a supported NT board type.
- The selected board belongs to a supported LT board type, but the board is blocked or there exists a board type mismatch for the boards.
- The SW files of the NotActive OSWP on the selected board are not compatible with the current active NT board SW files and the current active database.

Note 2 — In case the selected board for a software upgrade runs in Boot the system will report the manager.

5.11 Save an SHub Database

When the save of an SHub database is initiated by the manager, the Shub subsystem will save its database in a temporary container. The SHub database is not saved on the NT disk if there was no change in the database since the previous save operation.

The system synchronizes the SHub database file in the temporary container from active NT board to standby NT board (redundancy).

When this synchronization is finished, the active and standby NT board replace their stored SHub database by those in the temporary containers. The standby SHub system is then triggered to reset.

Note — Besides the SHub database, the system also stores an updated version of the SHub minimal database.

5.12 Save an IHub Database

The save of an IHub database can be initiated by the manager or can be autonomous (every 10 minutes).

When the output of the Config Save request is stored on the Core0 CF (temporary directory) and the ConfigSaveComplete trap is received from core1, the files are synchronized to the standby NT board. When these files are successfully synchronized, the files in the temporary directory will be copied (on both the active NT and the standby NT) to the actual directory from which they can be retrieved when needed by Core1.

5.13 Save a 7362 ISAM DF/SF, 7363 ISAM MX or 7367 ISAM SX/DX Database

There is no explicit save command. The system decides itself which data is immediately stored on disk and which data is cached in persistent memory. When a power failure occurs it can therefore be that data stored in persistent memory is lost (because not yet flushed to disk). It's therefore recommended to wait a minute before shutting down the power of the system.

5.14 Upload a Database (SNMP based)

The upload of a database (database back-up) will always be initiated by the manager. The database upload can be part of a binary backup/restore procedure or a software migration procedure.

The manager requests the system to upload one of its available databases towards a SFTP server via SFTP. The database upload request contains following information:

- The identification of the database that needs to be uploaded.
- The identification of the SFTP server where the database must be sent to.
- The directory path on the selected SFTP server where the uploaded database must be stored.

The manager has the possibility to monitor the progress of the upload process.

Note 1 — The upload of the database will be aborted if:

- The system does not find the specified database.
- The system finds the specified database but is not able to transfer it faultless to the SFTP server.

Note 2 — For SHub-based systems only: If save actions are ongoing on the SHub subsystem or LT boards, the operator is informed. No new save actions are allowed for a certain time period.

5.15 Download a Database (SNMP based)

The download of a database (database restore) will always be initiated by the manager. The database download can be part of a binary backup/restore procedure or a software migration procedure.

The manager requests the system to download a database from a SFTP server via SFTP. The database download request contains following information:

- The identification of the database that needs to be downloaded.
- The identification of the SFTP server where the database is stored.

The system stores the complete database persistently and links it to the compatible OSWPs.

Note 1 — The download of the database will fail if:

- The system is not able to contact the SFTP server.
- The SFTP server is not able to download the requested database towards the system.

Note 2 — For more information on online database cloning see Section "Online database cloning".

5.16 Clear all Databases

The craftsman (CT) is able to send a request to the system to clear all databases. The intention of this action is to prepare the board (for xHub-based systems) or the system (for 7362 ISAM DF/SF, 7363 ISAM MX and 7367 ISAM SX/DX) for plug-out and make it behave as if it comes straight from the factory. Table 24 shows the different phases of the process to clear all databases.

Note — The system has to have on Active OSWP linked to one of the available (and compatible) databases an no second OSWP present in the system.

Table 24 **Process to Clear All Databases**

Phase	Description
1	The system first removes all the persistent stored files that do not belong to the Active OSWP.
2	The system also makes sure that all the files belonging to the complete set of the Active OSWP are stored persistently.
3	The system removes the links between the OSWP and the available databases and replace them by a link to the default database.

(1 of 2)

Phase	Description
4	The system goes into shutdown mode. The management channel between the system and the manager is not established anymore.

(2 of 2)

6 ISAM Hardware Upgrade from Simplex to Duplex

6.1 Introduction

NT redundancy is supported on the system. Refer to the *Product Information* of your system to see which NT boards support redundancy. The procedure to upgrade from a simplex to a duplex system is described below.

Note — This chapter is not applicable for 7362 ISAM DF/SF, 7363 ISAM MX and 7367 ISAM SX/DX.

6.2 Hardware Upgrade

The *Manager* and *Craftsman* must proceed as follows to perform a hardware upgrade:

Table 25 **Hardware Upgrade Procedure**

Actor	Action
Manager	Plans the new NT board. Locks the protection group in order to prevent an uncontrolled switch-over during the upgrade procedure.
Craftsman	Inserts the new NT board in slot B. The new NT is of the same type as the NT in slot A. The NT board will start up independently from the software present on its disk. The NT board will start a communication channel with the active NT board and both software and database will get synchronized autonomously.
Manager	Gets informed by the ISAM of the new standby NT board.
Manager	Enables the redundancy. Unlocks the protection group in order to use the redundancy functionality.

Note — If the operator wishes to install the second NT but prefers to activate the redundancy functionality at a later time, it is advised to keep the standby NT in the Locked state. The protection group should also be kept in the Locked state. No craftsman intervention is needed to activate the redundancy functionality. The operator will unlock the standby NT to start the synchronization and unlock the protection group to use the redundancy functionality.

6.3 Troubleshooting

Table 26 describes the most common problems which can be encountered during the hardware upgrade of the system, together with the corresponding troubleshooting action

Table 26 **Troubleshooting**

Problem	Proposed Action	Actor
The new NT board is not able to startup with the factory software.	Unplug the NT board, insert a new NT board and send the faulty NT board to Nokia.	Craftsman
Synchronization fails.	Redundancy does not function properly without synchronization. Abort the upgrade.	Craftsman/Manager

If the problem remains, contact Nokia.

6.4 Hardware Rollback

The operator can roll back the system to the situation before the hardware upgrade. The system rollback consists of the rollback of both the IACM and xHub subsystem.

The *Craftsman/Manager* must proceed as follows to perform a hardware rollback:

Table 27 **Hardware Rollback Procedure**

Actor	Action
Manager	Locks the standby NT board. This stops the peer-to-peer synchronization in order to prevent the flash disk getting corrupted due to disk write operations at the moment the standby NT board is extracted. The local craftsman is informed when the NT is locked by the front panel LEDs (refer to section LED Behavior on the NT).
Craftsman	Removes the standby NT board. The ISAM is now a simplex system again.
Manager	Since the standby NT board is still planned, a *"board missing"* alarm is reported to the manager.
Manager	Unplans the standby NT board. This clears the *"board missing"* alarm.

The system has performed a hardware rollback.

6.4.1 LED Behavior on the NT

Figure 12 shows the front panel LEDs on the NT.

Figure 12 **NT LEDs**

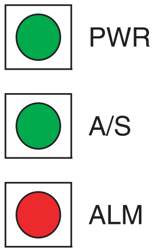


Table 28 describes the LED behavior on the NT.

Table 28 **NT LED Behavior**

LED	Color	State	Mode
ALM	RED	Failed	ON
A/S	GREEN	Active	ON
		Standby	OFF
		Synchronizing	1 pulse
PWR	GREEN	Power Off	OFF
		OSW running	3.5s ON, 0.5s OFF
		• Alive (boot SW) • Board locked	1s ON, 1s OFF
		SW loading	Flashing (load speed)
		• Database cleared • System shutdown	ON

7 Descriptor Files

7.1 Syntax

Both descriptor files and the Overall descriptor files are ASCII files. The same syntax (see Table 29) can be applied for Overall descriptor files and for descriptor files.

Table 29 **Syntax of Descriptor Files**

Syntax	Explanation
“BEGIN”	/*Token BEGIN*/;
“END”	/*Token END*/;
“DESCRIPTOR-FILE”	/*Token DESCRIPTOR-FILE*/;
“OVERALL-DESCRIPTOR-FILE”	/*Token OVERALL-DESCRIPTOR-FILE*/;
“SYNTAX-VERSION”	/*Token SYNTAX-VERSION*/;
“ASAM-CORE”	/*Token ASAM-CORE*/;
“VOX-GW“	/*Token VOX-GW*/;
“IP-SERVER”	/*Token IP-SERVER*/;
“TARGET”	/*Token TARGET*/;
“DBASE-VERSION”	/*Token DBASE-VERSION*/;
“DESCRIPTION”	/*Token DESCRIPTION*/;
“TYPE-x (x=A thru Z)”	/*Token TYPE-x (x = A thru Z)*/;
“DECOMPRESSION”	/*Token DECOMPRESSION*/;
“MINIMUMSET”	/*Token MINIMUMSET*/;
“YES”	/*Token YES*/;
“NO”	/*Token NO*/;
“TAR”	/*Token TAR*/;
“LZ77”	/*Token LZ77*/;
“ASCII”	/*Token ASCII*/;

(1 of 2)

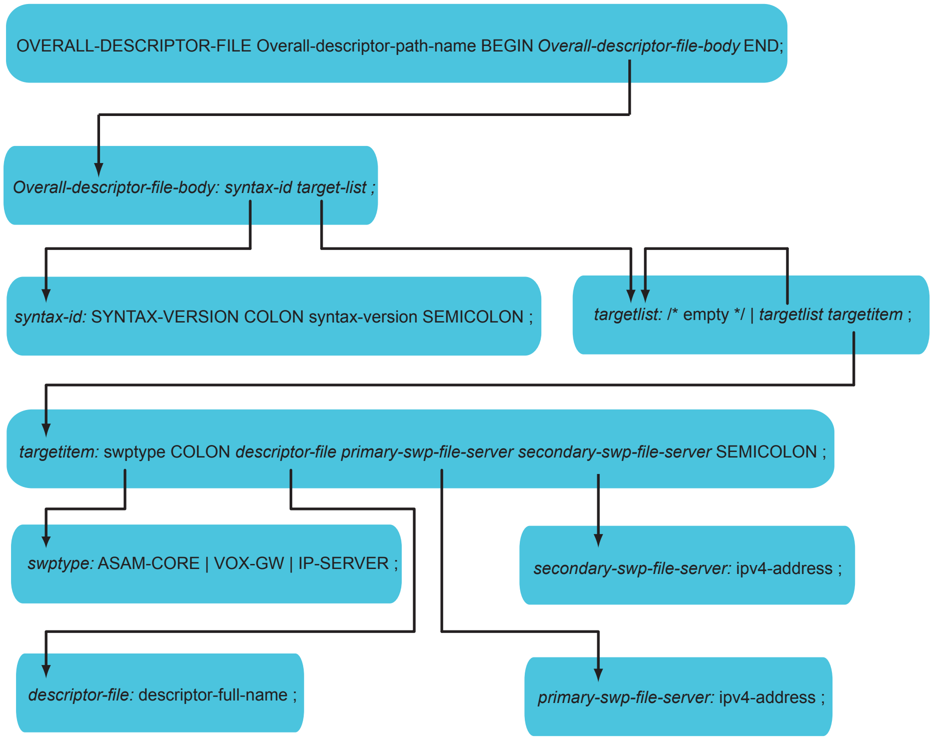
Syntax	Explanation
“EXE”	/*Token EXE*/;
“:”	/*Token COLON*/;
“;”	/*Token SEMICOLON*/;
[0-9]{2}”.”[0-9]{2}	/*Syntax version*/
“[A-Z]{4}”-”[A-Z]	/*Boardtype*/
((0 | [1-9][0-9]*)”.”){3}(0 | [1-9][0-9]*)	/*IPv4 address*/
[A-Za-z0-9]{8}”.”[0-9]{3}	/*Filename*/
[A-Za-z0-9._/]*”/”(L6GP)[A-Za-z0-9]{4}”.”[A-Za-z0-9]{3}	/*Overall-descriptor-path-name*/
[A-Za-z0-9._/]*”/” [A-Za-z0-9]{8}”.”[0-9]{3}	/*descriptor-path-name*/
[A-Za-z0-9]{2}”.”[0-9]{3}	/*database-version*/
(0 | [1-9][0-9]*)	/*Decimal number*/
“--”.*\n	/*Comment; ignore everything*/

(2 of 2)

7.2 Grammar

Figure 13 describes the grammar of an Overall descriptor file and Figure 14 describes the grammar of a descriptor file.

Figure 13 **Grammar of an Overall Descriptor File**



OVERALL-DESCRIPTOR-FILE Overall-descriptor-path-name BEGIN *Overall-descriptor-file-body* END;

Overall-descriptor-file-body: syntax-id target-list ;

syntax-id: SYNTAX-VERSION COLON syntax-version SEMICOLON ;

targetlist: /* empty */ | *targetlist targetitem* ;

targetitem: swptype COLON *descriptor-file primary-swp-file-server secondary-swp-file-server* SEMICOLON ;

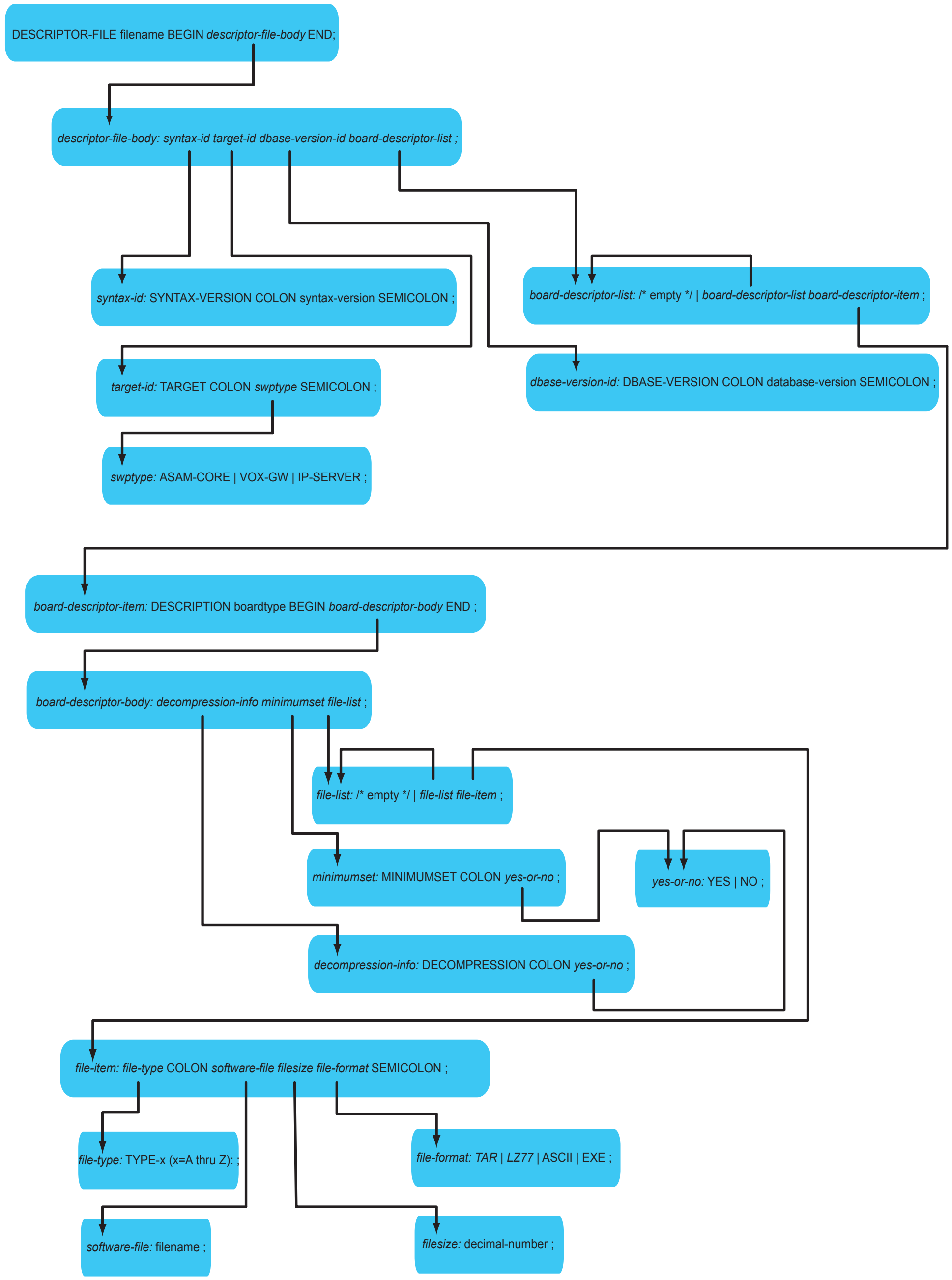
swptype: ASAM-CORE | VOX-GW | IP-SERVER ;

secondary-swp-file-server: ipv4-address ;

descriptor-file: descriptor-full-name ;

primary-swp-file-server: ipv4-address ;

Figure 14 Grammar of a Descriptor File


DESCRIPTOR-FILE filename BEGIN *descriptor-file-body* END;
descriptor-file-body: syntax-id target-id dbase-version-id board-descriptor-list ;
syntax-id: SYNTAX-VERSION COLON syntax-version SEMICOLON ;
board-descriptor-list: /* empty */ | *board-descriptor-list board-descriptor-item ;*
target-id: TARGET COLON *swptype* SEMICOLON ;
dbase-version-id: DBASE-VERSION COLON database-version SEMICOLON ;
swptype: ASAM-CORE | VOX-GW | IP-SERVER ;
board-descriptor-item: DESCRIPTION boardtype BEGIN *board-descriptor-body* END ;
board-descriptor-body: decompression-info minimumset file-list ;
file-list: /* empty */ | *file-list file-item ;*
minimumset: MINIMUMSET COLON *yes-or-no ;*
yes-or-no: YES | NO ;
decompression-info: DECOMPRESSION COLON *yes-or-no ;*
file-item: file-type COLON *software-file filesize file-format* SEMICOLON ;
file-type: TYPE-x (x=A thru Z): ;
file-format: TAR | *LZ77* | ASCII | EXE ;
software-file: filename ;
filesize: decimal-number ;

7.3 Examples

Example of an overall descriptor file:

```
OVERALL-DESCRIPTOR-FILE L6GPaa10.000 BEGIN
 SYNTAX-VERSION: 01.00 ;
 ASAM-CORE: /asamfiles/HHHDSAA1.002 123.65.1.2 123.65.1.4 ;
END
```

Example of a descriptor file:

```
DESCRIPTOR-FILE HHDHSAA1.002 BEGIN
 SYNTAX-VERSION: 01.00 ;
 -- Descriptor file for ASAM-CORE Release 1.0.00
 TARGET:ASAM-CORE ;
 DBASE-VERSION: A1.000 ;
DESCRIPTION EANT-A BEGIN
 DECOMPRESSION: NO ;
 MINIMUMSET: YES ;
 TYPE-A: <filename> 564786 ASCII ;
 TYPE-A: <filename> 1234567 EXE ;
 TYPE-B: <filename> 123456 EXE ;
END
DESCRIPTION EALT-A BEGIN
 DECOMPRESSION: YES;
 MINIMUMSET: NO ;
 TYPE-B: <filename> 7834893 LZ77 ;
END
DESCRIPTION EALT-B BEGIN
 DECOMPRESSION: NO ;
 MINIMUMSET: NO ;
 TYPE-A: <filename> 123456 TAR;
 TYPE-B: <filename> 8937613 TAR;
END
END
```

7.4 Nomenclature

The following nomenclature is used:

- Type-A: FPGA SW, startupfile, etc... for NT or LT
- Type-B: OSW for NT or LT
- Type-C: NT OSW selector file

- Type-D: FPGA selector file
- Type-E: OFLT selftest selector file (autonomous)
- Type-F: OFLT selftest selector file (interactive)
- Type-G: Data Driven ISAM Configuration file
- Type-H: LANX OSW file
- Type-I: Type-A file ODM boards
- Type-J: Type-B file for ODM boards
- Type_K file: Tar file used for debugging purposes.
- Type_L file: Ansi LT file to map a board’s FV to a specific Type A
- Type_M file: Ansi LT file to map a board’s FV to a specific Type B
- Type_N file: Bootpackage file. This file contains the FS/BSP for the NT
- Type_O file: Core 2&3 AI image
- Type_P file: file containing miscellaneous parameter options

Customer document and product support

Customer documentation

Customer Documentation Welcome Page

Technical Support

Product Support Portal

Documentation feedback

Customer Documentation Feedback