THALES

NORGIL

SkyView Link 1 Interface
Security Target

Written by:	**Jens Helge RYPESTØL**	Checked by:	**O.J. PEDERSEN**
Position:	**Systems Engineer**	Position:	**QA Manager**
Signature:		Signature:	
Approved by:	**Erik JØRGENSEN**		
Position:	**Technical Manager**		
Signature:			

DOCUMENT REFERENCES						CLASSIFICATION	PAGE
Identification	Variant	Document Code	Volume	Revision Index	Language		
3AQ 23805	**AAAA**	**SC**	**-**	**D**	**EN**	**THALES Approved**	**1**/26

SUCCESSIVE CHANGES

REVISION INDEX	DATE	CHANGED BY	DESCRIPTION
A	2008-12-17	Jens Helge Rypestøl	First Edition
B	2010-10-26	Roar Jacobsen	General: • I.L1Msg -> I.L1MsgTx Ch 1.3: • Figure 1.3-3 updated • SF.SPI_filter -> SF.SPI_Filter • 4 x Link1_filter -> Link1_Mgmn • SF.Link1_enc -> SF.Link1_Enc • Link1_dec -> Link1_Dec Ch 3.1: • Added subject ACD • Added object I.L1MsgRx • Added object I.GL1Rec Ch 4.2 and 4.3: • Added security objective OE.OS and updated corresponding rationale. Ch 7: • SF.L1_ENC -> SF.Link1_Enc
C	2010-11-29	Roar Jacobsen	Ch 1.1: • Table 1.1-1: TOE version added Ch 1.2: • (3): TOE type “none” confirmed Ch 4.3: • Table 4.3-1: Mapping between OE.PHYSICAL and T.RELEASE removed Ch 6.3.2: • Table 6.3-2: FMT_MSA included. Note added.
D	2011-05-10	Roar Jacobsen	General: • The text “UNNTATT OFFENTLIGHET jf § 5a og fvl. § 13(1) 2. alternative” removed from header and footer • Misprints of “I.STrack” corrected Succesive Changes: • Change log for revision C updated

Contents

List of figures

List of tables

1. ST INTRODUCTION (ASE_INT)

1.1 ST and TOE References

(1) The following table identifies the Security Target (ST) and the Target of Evaluation (TOE):

Item	Identification
ST title	SkyView Link 1 Interface, Security Target
ST reference	3AQ 23805 AAAA SC
ST version	See Revision Index in footer
ST authors	See front page
ST date	See page 2.
TOE developer	ThalesRaytheonSystems
TOE name	GL1 Computer Software Component of SkyView
TOE version	2.0.9-i2
EAL	EAL4

Table 1.1-1 Identification of ST and TOE

1.2 TOE Overview

(1) GL1 TOE is a Computer Software Component of the TRT Computer Software Configuration Item of the SkyView subsystem of NORGIL.

(a) NORGIL is the Norwegian Ground Infrastructure for Link 16

(b) SkyView is the NORGIL C2 application.

(c) TRT (TRaiTement) includes all the C2 applications in charge of operational processing within SkyView.

(d) GL1 (Gestionnaire de Liaison 1) is the Link 1 interface processor.

(2) TOE Usage and Major Security Features:

(a) GL1 shall ensure that it transmits only Link 1 formatted messages to the Link 1 interfaces.

(b) GL1 shall prevent air tracks protected by the SPI (Special Processing Indicator) to be transmitted on Link 1 interfaces, unless authorised by Emergency indicator or Force Tell indicator.

(3) The TOE type is “none”, i.e. GL1 is not of a readily available general type TOE.

(4) Required non-TOE hardware/software/firmware:

(a) GL1 is a Computer Software Component of SkyView.

(b) GL1 is running on HP-UX 11i

1.3 TOE Description

(1) SkyView is a component of MIU, which in turn is a component of NORGIL. SkyView is the NORGIL C2 application, processing radar inputs, Link 1 and Link 16 messages.

(2) NORGIL shall communicate with MASE over Link 1. MASE operates at NATO CONFIDENTIAL level, while NORGIL handles information classified up to NATO SECRET. SkyView shall prevent NATO SECRET information to be transmitted over Link 1 to MASE.

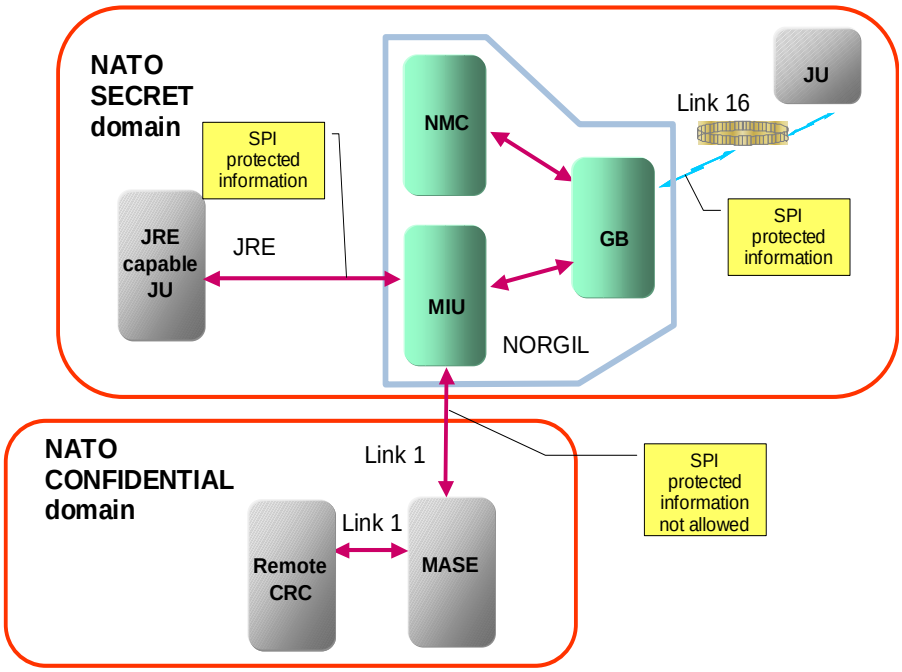
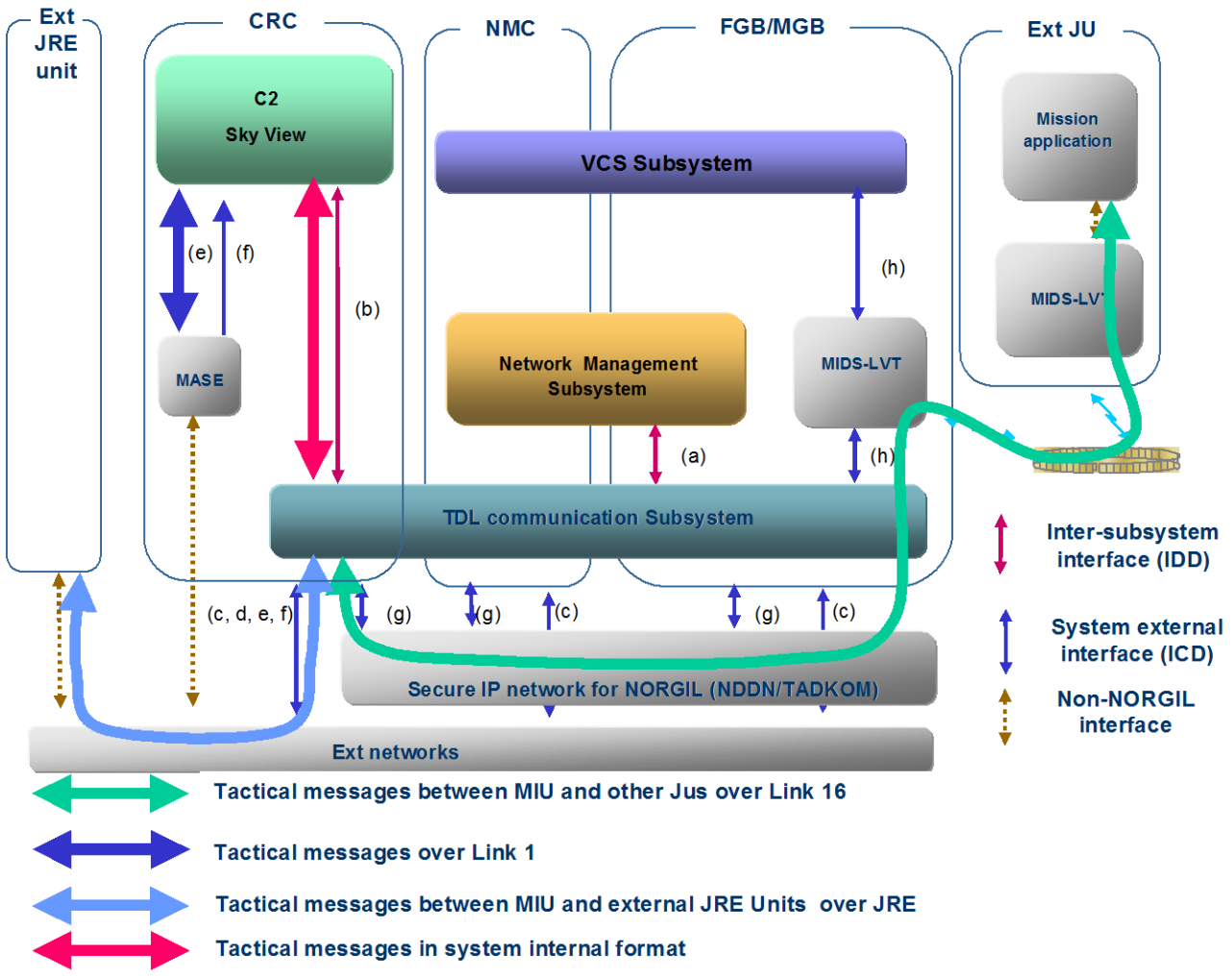


Figure 1.3-1 Data Flow for SPI Protected Information

(3) All surveillance, warning, and amplification data in Link 16 messages in which the SPI is set to value 1 shall be classified NATO SECRET, and on reception shall be afforded the protection commensurate with that classification. (Ref. [4] STANAG 5516 §1.1.6.1.a.). SkyView is processing such information.



(a) Interface between TDL subsystem and NMS subsystem

(b) Interface between TDL subsystem and SkyView subsystem

(c) JRE interface, MIL-STD 3011

(d) SIMPLE Interface, STANAG 5602

(e) Link 1 Interface

(f) Radar plots

(g) NDDN interface

(h) Interface to MIDS terminal

Figure 1.3-2 Data Flow for Air Tracks

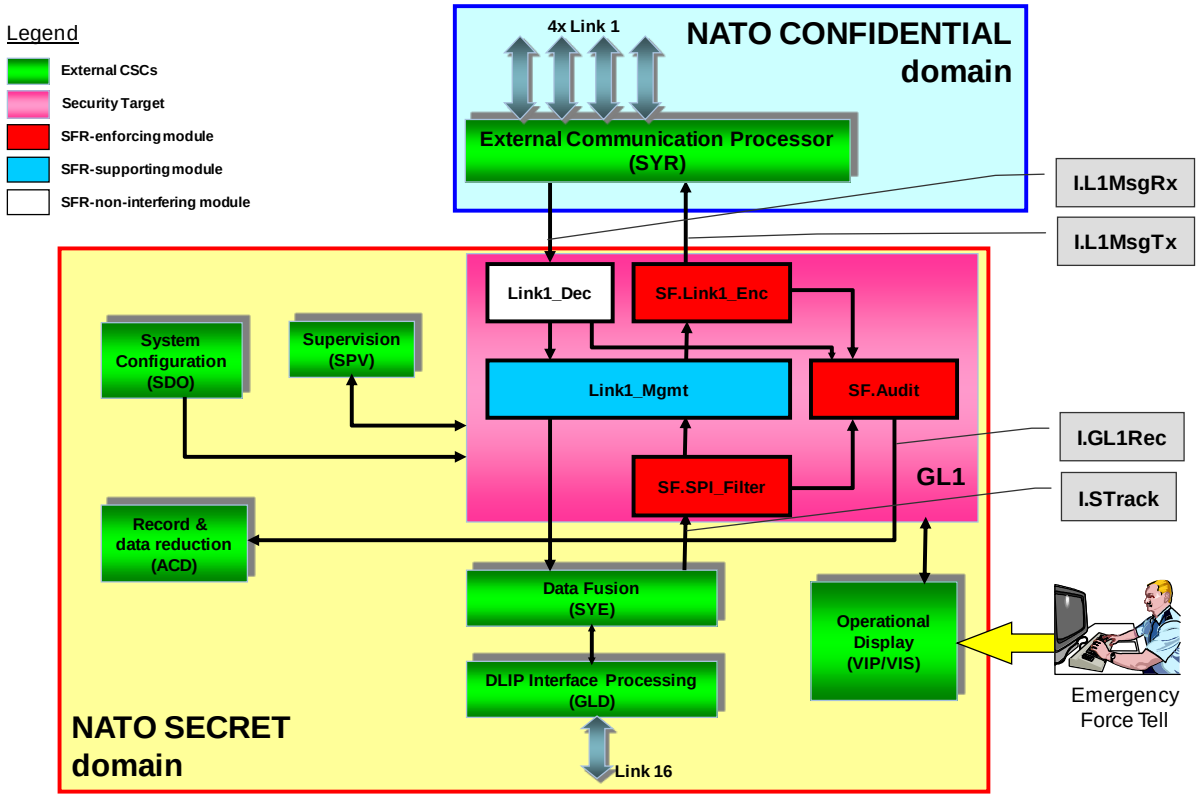


Figure 1.3-3 Information Flow for SkyView Link 1 Handling

(4) The Data Fusion (**SYE**) component submits the complete set of system tracks (**I.STrack**) to **GL1**. GL1 will filter the system tracks (i.e. prevent them being transmitted on Link 1) in two steps:

(a) The SPI filter (**SF.SPI_Filter**) will remove all system tracks that are not granted access according to the security policy for transmission of SPI protected information: all air tracks with SPI indicator = 0 will be granted access. Air tracks with SPI = 1 will only be granted access if Emergency indicator = 1 or Force Tell indicator = 1.

(b) GL1 has one set of Link 1 filters (**Link1_Mgmn**) for each of the four links. This set is composed of geographical filters plus start tell and stop tell on individual tracks or track identity. The Link 1 filters have no security functionality.

(5) System tracks (**I.STrack**) with SPI = 1 will be recorded (**SF.Audit, I.GL1Rec, ACD**).

(6) GL1 will encode (**SF.Link1_Enc**) the air tracks according to the Link 1 encoding rules. Link 1 messages (**I.L1MsgTx**) do not contain SPI bit or Force Tell bit, but may carry the Emergency bit. The transmitted Link 1 messages will be recorded (**SF.Audit, I.GL1Rec, ACD**).

(7) GL1 will decode (**Link1_Dec**) received Link 1 messages (**I.L1MsgRx**). The Link 1 decoding has no security functionality. The received Link 1 messages will be recorded (**SF.Audit, I.GL1Rec, ACD**). The recording of the received Link1 messages is not security related.

(8) The External communication processor (**SYR**) and the channel between SYR and GL1 will ensure that only Link 1 messages filtered by GL1 are transmitted on the Link 1 interfaces.

2. CONFORMANCE CLAIMS (ASE_CCL)

(1) This TOE and ST are conformant with the following specifications:

CC Part 2 [2]: Security functional requirements, September 2007, Version 3.1, Revision 2, conformant.

CC Part 3 [3]: Security assurance requirements, September 2007, Version 3.1, Revision 2, conformant, EAL4.

3. SECURITY PROBLEM DEFINITION (ASE_SPD)

3.1 Definitions of Subjects, Objects, and Security Attributes

(1) The Subjects, Objects and Security Attributes are defined in the following tables.

Subjects	Description
SYE	The Data Fusion (SYE) subject submits system tracks (I.STrack) to TOE.
SYR	The external communication processor (SYR) is the subject receiving filtered Link 1 messages (I.L1MsgTx) from TOE to be transmitted on Link 1.
ACD	The Record and data reduction (ACD) is the subject receiving messages (I.GL1Rec) from SF.Audit to be recorded in the ACD.

Table 3.1-1 Subjects

Objects	Description
I.L1MsgTx	Information object containing a transmitted Link 1 message. A given instance of a transmitted Link 1 message is denoted $I.L1MsgTx_i$ and is derived from a corresponding system track $I.STrack_i$.
I.L1MsgRx	Information object containing a received Link 1 message.
I.STrack	Information object containing a system track. A given instance of a system track is denoted $I.STrack_i$.
I.GL1Rec	Information objects containing audit records from GL1 to be recorded in the ACD.

Table 3.1-2 Objects

Security attributes	Description
SA.Em	Security attribute Emergency indicator of an I.STrack. A given instance of a system track $I.STrack_i$ has a corresponding $SA.Em_i$.
SA.FT	Security attribute Force Tell indicator of an I.STrack. A given instance of a system track $I.STrack_i$ has a corresponding $SA.FT_i$.
SA.SPI	Security attribute SPI indicator of an I.STrack. A given instance of a system track $I.STrack_i$ has a corresponding $SA.SPI_i$.

Table 3.1-3 Security Attributes

3.2 Threats

3.2.1 Assets

(1) All surveillance, warning, and amplification data in messages in which the SPI is set to value 1 shall be classified NATO SECRET, and on reception shall be afforded the protection commensurate with that classification. (Ref. [4] STANAG 5516 §1.1.6.1.a.).

(2) The TOE will not receive any NATO SECRET information except for SPI protected information. However Skyview and the rest of NORGIL may handle other NATO SECRET information e.g. voice and Link 16 messages containing free text.

(3) The assets to be protected by TOE are defined in the following table.

Asset	Description
AS.NS	NATO SECRET information

Table 3.2-1 Assets

3.2.2 Threat Agents

(1) The threats to assets are defined in the following table.

Threat agents	Description
TA.EXTERNAL	Personnel with no authorized access to the TOE environment. These threat agents may try to access the NATO SECRET (AS.NS) information and may have “unlimited” resources supporting them.
TA.USER	Authenticated authorized users of the TOE. These threat agents may intentionally or unintentionally perform unauthorized actions.

Table 3.2-2 Threat Agents

3.2.3 Identification of Threats

(1) The threats to assets are defined in the following table.

Threats	Description
T.RELEASE	A TOE user (TA.USER) may release SPI protected tracks (AS.NS) to systems operating at lower security level without authorization.

Table 3.2-3 Threats

3.3 Organisational Security Policies (OSPs)

(1) The TOE is compliant with the policy for handling SPI protected information as outlined in [4] STANAG 5516.

OSP	Description
P.SPI_L1	An air track shall not be transmitted on Link 1 when a source is marking this track with SPI = 1, unless the track is marked as Emergency or Force Tell.

Table 3.3-1 Organisational Security Policies

3.4 Assumptions

(1) The assumptions to TOE environment are defined in the following table.

Assumptions	Description
A.LOCATE	The processing resources of the TOE are assumed to be located within controlled access facilities that will prevent unauthorised physical access.

Table 3.4-1 Assumptions

4. SECURITY OBJECTIVES (ASE_OBJ)

4.1 Security Objectives for the TOE

(1) The security objectives for the TOE are defined in the following table.

Security objectives	Description
O.AUDIT	The TOE will initiate recording of security relevant events, to assist a security officer in the detection of potential violations of the security policy for protection of SPI protected information.
O.SPI_L1_FILTER	The TOE will prevent information to be transmitted to Link 1 according to P.SPI_L1 policy.

Table 4.1-1 Security Objectives for the TOE

4.2 Security Objectives for the Operational Environment

(1) The security objectives for the TOE environment are defined in the following table.

Security objectives	Description
OE.ACCESS	The TOE environment will provide the means of controlling and limiting access to the TOE IT environment to authorized users.
OE.AUDIT	The TOE environment will provide the means of recording security relevant events, so as to assist a security officer in the detection of potential violations of the security policy for protection of SPI protected information, and also to hold users accountable for any actions they perform that are relevant to this security policy.
OE.AUDITLOG	Administrators of the TOE must ensure that audit facilities are used and managed effectively. In particular: a) Appropriate action must be taken to ensure continued audit logging, e.g. by regular archiving of logs before audit trail exhaustion to ensure sufficient free space. b) Audit logs should be inspected on a regular basis, and appropriate action should be taken on the detection of breaches of security.
OE.L1_CHANNEL	The TOE environment will provide the means to ensure that only messages from the TOE are transmitted on Link 1 interfaces.
OE.OS	The operating system will provide process isolation capability including isolation of data with respect to any other process running on the same computer.
OE.PHYSICAL	Those responsible for the TOE and its IT environment must ensure that the hardware components of the IT environment is protected from physical attack which might compromise IT security, and that the physical protection for the hardware components is sufficient for protection of the information handled by the hardware components.

Table 4.2-1 Security Objectives for the TOE Environment

4.3 Security Objectives Rationale

(1) The mapping of security objectives for the TOE and TOE environment to threats, OSPs, and assumptions are defined in the following table.

Threats/Assumptions/Policies Objectives	T.RELEASE	P.SPI_L1	A.LOCATE
O.AUDIT	X	X	
O.SPI_L1_FILTER		X	
OE.ACCESS			X
OE.AUDIT	X		
OE.AUDITLOG	X	X	
OE.L1_CHANNEL		X	
OE.OS	X	X	
OE.PHYSICAL			X

Table 4.3-1 Mapping of Security Objectives to Threats, Assumptions and Policies

A.LOCATE
The TOE is located within physically protected areas (OE.PHYSICAL) with access control measures (OE.ACCESS) that will prevent unauthorised users (TA.EXTERNAL) access to the TOE IT environment.

P.SPI_L1
The TOE will perform filtering of system tracks (O.SPI_L1_FILTER) to be transmitted as Link 1 according to P.SPI_L1 policy. The TOE will perform the Link 1 encoding (O.SPI_L1_FILTER) according to the P.SPI_L1 policy. The environment will ensure that only Link 1 messages from the TOE are transmitted on the Link 1 interfaces (OE.L1_CHANNEL). The audit of SPI protected tracks (O.AUDIT) will register when SPI protected tracks (AS.NS) are forwarded to Link 1. The audit review (OE.AUDITLOG) will reveal violations of the policy. The operating system (OE.OS) will provide process isolation to support the integrity of the TOE functionality.

T.RELEASE
The environment audit mechanisms (OE.AUDIT) will register when Emergency indicator or Force Tell indicator is set for a track and will identify which user (TA.USER) has performed this operation. The audit of SPI protected tracks (O.AUDIT) will register when SPI protected tracks (AS.NS) are forwarded to Link 1. The audit review (OE.AUDITLOG) will reveal unauthorized release of SPI protected tracks and which user has performed this action. The operating system (OE.OS) will provide process isolation to support the integrity of the TOE functionality.

5. EXTENDED COMPONENTS DEFINITION (ASE_ECD)

(1) Not applicable.

6. SECURITY REQUIREMENTS (ASE_REQ)

6.1 Security Functional Requirements (SFRs)

6.1.1 Class FAU: Security Audit

6.1.1.1 Security audit data generation (FAU_GEN)

FAU_GEN.1 AUDIT DATA GENERATION

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps. (included (environment))

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*not specified*] level of audit; and
c) [*All system tracks I.STrack with SA.SPI indicator set; and all Link 1 messages I.L1MsgTx*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*none*].

6.1.2 Class FDP: User Data Protection

6.1.2.1 Export to outside TSF control (FDP_ETC)

FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control (included hierarchical component FDP_IFC.2 Complete information flow control)]

FDP_ETC.1.1 The TSF shall enforce the [*P.SPI_L1 policy*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.
Note: Emergency indicator is included in the Link 1 message, but is then not regarded as a security attribute.

Note: This export refers to the transmission of user data from GL1 to SYR.

6.1.2.2 Information flow control policy (FDP_IFC)

FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes (included)

FDP_IFC.2.1 The TSF shall enforce the [*P.SPI_L1 policy*] on [*the information I.STrack and I.L1MsgTx for the subjects SYE and SYR*] and all operations that cause that information to flow to and from subjects covered by the SFP.

Note: The policy state the rules for preventing information received from SYE to be transmitted to SYR. The information received from SYE is denoted I.STrack, and the information transmitted to SYR is denoted I.L1MsgTx.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.1.2.3 Information flow control functions (FDP_IFF)

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control (included hierarchical component FDP_IFC.2 Complete information flow control).
FMT_MSA.3 Static attribute initialization (not included).

FDP_IFF.1.1 The TSF shall enforce the [*P.SPI_L1 policy*] based on the following types of subject and information security attributes: [*the subjects SYE and SYR, on the information I.STrack and I.L1MsgTx, using the security attributes SA.SPI, SA.Em, SA.FT*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*Information $I.L1MsgTx_i$ extracted from a system track $I.STrack_i$ flows from SYE to SYR if the following is TRUE: $(NOT\ SA.SPI_i) + SA.Em_i + SA.FT_i$*].

FDP_IFF.1.3 The TSF shall enforce the [removal of tracks not granted access by the SPI_filter and ensure that the information is encoded according to Link 1 encoding rules].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.3 Class FPT: Protection of the TSF

6.1.3.1 Time stamps (FPT_STM)

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2 Security Assurance Requirements (SARs)

(1) The assurance level of the TOE is EAL4.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing: security enforcing modules
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Table 6.2-1 EAL4 Assurance Requirements.

6.3 Security Requirements Rationale

6.3.1 Relation Between SFRs and Security Objectives

Objective / SFR	O.SPI_L1_FILTER	O.AUDIT
FAU_GEN.1		X
FDP_ETC.1	X	
FDP_IFC.2	X	
FDP_IFF.1	X	
FPT_STM.1		X

Table 6.3-1 Mapping of SFRs to Security Objectives

O.SPI_L1_FILTER
The O.SPI_L1_FILTER is the basic security handling objective implementing the P.SPI_L1 policy. The objective ensures that the P.SPI_L1 policy applies to all data that flows between SYE and SYR (FDP_IFC.2), and that the policy rules are based on a set of security attributes (FDP_IFF.1). The filtered data are exported outside TOE as Link 1 messages that do not have fields for the SPI and Force Tell flags (FDP_ETC.1).

O.AUDIT
The TOE will generate the required audit records (FAU_GEN.1) with reliable time stamps (FPT_STM.1). (The records are tracks that are already time-stamped).

6.3.2 SFR Dependencies

The TOE fulfils all SFR dependencies as shown in the table below.

SFR	Dependency	Fulfilled by SFR
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FDP_ETC.1	FDP_IFC.1	Hierarchical FDP_IFC.2
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3 (*)	Hierarchical FDP_IFC.2
FPT_STM.1	None	Not applicable

(*) Note:
All security attributes are included in I.STracks, hence there are no static attributes.

Table 6.3-2 SFR dependencies

6.3.3 SAR Rationale

The SARs specified in this ST are according to EAL4 as selected by NSM.

7. TOE SUMMARY SPECIFICATION (ASE_TSS)

7.1 TOE Security Functions Specification

(1) Please use Figure 1.3-3 as a reference for the following TOE Security Functions Specification.

7.1.2 SF.Audit

The SF.Audit generates audit records for the following events:

- All messages received by SF.SPI_Filter from SYE (I.STrack) with SA.SPI = 1.
- All Link 1 messages (I.L1MsgTx) sent from SF.Link1_Enc to SYR outside TOE.

(The SF.Audit will also generate some audit records which are not security related.)

7.1.3 SF.Link1_Enc

The SF.Link1_Enc receives messages from SF.SPI_Filter (except those discarded by the Link 1 filters) and encodes the information in Link 1 messages. The Link 1 messages (I.L1MsgTx) are transmitted to SYR outside the TOE.

7.1.4 SF.SPI_Filter

The SF.SPI_Filter performs a filtering of messages received from SYE (I.STrack) according to P.SPI_L1.

Messages that are not granted access according P.SPI_L1 are discarded.

7.2 TOE Security Functions Rationale

The table below shows the mapping between the SFRs and the implementing security function, and a description is given in the following subsections.

Security Functions SFR	SF.SPI_Filter	SF.Link1_Enc	SF.Audit
FAU_GEN.1			X
FDP_ETC.1		X	
FDP_IFC.2	X		
FDP_IFF.1	X	X	
FPT_STM.1			X

Table 7.2-1 Mapping of SFRs to TOE Security Functions

7.2.1 FAU_GEN.1

FAU_GEN.1 is directly implemented by SF.Audit that generates the audit records.

7.2.2 FDP_ETC.1

FDP_ETC.1 is implemented by SF.Link1_Enc, which performs the Link 1 encoding and transmission to outside the TOE.

7.2.3 FDP_IFC.2

FDP_IFC.2 is directly implemented by SF.SPI_Filter

7.2.4 FDP_IFF.1

FDP_IFF.1 is implemented by SF.SPI_Filter using the security attributes for the flow control, and the SF.Link1_Enc which that has no encoding field for the SA.SPI and SA.FT attributes.

7.2.5 FPT_STM.1

FPT_STM.1 is indirectly implemented by SF.Audit that receives the timestamp together with the audit information

APPENDIX A Glossary

A.1 Abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
GL1	Gestionnaire Liaison 1
MASE	Multi Aegis Site Emulator
MIU	MASE Interface Units
NORGIL	Norwegian Ground Infrastructure for Link 16
NSM	Nasjonal sikkerhetsmyndighet
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SPI	Special Processing Indicator
ST	Security Target
STANAG	NATO Standardisation Agreement
SYE	SYnfoniE
SYR	SYRes
TOE	Target of Evaluation
TSF	TOE Security Function
TRT	TRaiTement
TSF	TOE Security Functionality

A.2 Definitions

See [1] CC Part 1 for definition of Common Criteria terminology.

APPENDIX B Referenced Documents

Document id	Document abbreviation	Document name
[1] CCMB-2006-09-001	CC part 1	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 1, September 2006
[2] CCMB-2007-09-002	CC part 2	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 2, September 2007,
[3] CCMB-2007-09-003	CC part 3	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 2, September 2007
[4] STANAG 5516 Ed 3	STANAG 5516	STANAG 5516 Ed 3