Final OSED for Madrid TMA (Annex Security Assessment)

Document information	
Project title	Full Implementation of P-RNAV in TMA
Project N°	05.07.04
Project Manager	AENA
Deliverable Name	N/A
Deliverable ID	N/A
Edition	00.01.00

Please complete the advanced properties of the document

Authoring & Approval

Prepared By		
Name & company	Position / Title	Date
<Name> / <company>	<Position / Title>	<Date>
[redacted] ISDEFE	[redacted]	19/12/2011

Reviewed By		
Name & company	Position / Title	Date
<Name> / <company>	<Position / Title>	<Date>
[redacted]	[redacted]	20/12/2011

Approved By		
Name & company	Position / Title	Date
<Name> / <company>	<Position / Title>	<Date>
[redacted]	[redacted]	22/12/2011

Document History

Edition	Date	Status	Author	Justification
00.00.01	07/09/2011	Draft	[redacted]	Doc. edition
00.01.00	25/11/2011	Final		Doc. edition

Intellectual Property Rights (foreground)

The foreground of this deliverable is owned by the SJU.

Table of Contents

List of tables

List of figures

1 Scoping the Security Assessment

P05.07.04 project is mainly focused on SESAR main goal of increasing Capacity of the ATM system, in particular by improving capacity in complex TMA's via reduction of ATCO workload per flight and achievement of better airspace efficiency. This is to be achieved by new airspace and routes design together with new procedures.

Another SESAR main goal, the improvement on Environmental Impact, is also one of the focuses of the project by determining feasibility of concepts to address noise nuisance in transition from conventional to P-RNAV procedures. Furthermore the remaining SESAR main goals, Safety and ATM Costs, are impacted as a consequence of the change in procedures and in capacity, respectively. The indirect impacts on such areas are also assessed, although they are not the primary focus of the project.

Although not as a main goal of the SESAR programme, the KPA Security is also addressed in the SESAR JU projects. This section deals with identifying the possible security aspects impacted by P05.07.04 project and with building the basis for deciding whether a detailed security assessment is need or not.

1.1 System scope

One of the initial steps when performing a security assessment is to clearly identify the scope of the system being addressed by the project. Moreover the context of the system, namely the part of the environment with a direct link to the system, needs to be identified as well.

The system under the scope of P5.7.4 work stream 1 (Full implementation of P-RNAV in Madrid TMA) consists of **new procedures and route structures for Madrid TMA airspace**.

Generally speaking, ATC procedures are supported by infrastructure, facilities and technological systems. However, none of these elements are within the scope of P5.7.4 project; however they belong to the context.

The following figure illustrates the system under the scope of P5.7.4 work stream 1, namely the system scope, the context of the system, and the boundary separating both scope and context.

Figure 1: System scope and context of the project's work stream 1.

1.2 Security Assessment Scope

The preliminary analysis on the need for performing a detailed security assessment for P05.07.04 work stream 1 (P-RNAV in Madrid TMA) by WP16 come out with a few, non-critical security related items to be considered in this operational project. Further analysis would be necessary once the OSED was mature enough to get to understand what the exact scope of the security assessment could be.

As a result of the 'Application of 16.06.0x Reference Material to 05.07.04' workshop held in Madrid on May 4th 2011, three milestones were identified as a reference for the security assessment process. The milestones were related with:

- The availability of the initial project documentation (OSED, SPR, INTEROP), which analysis would allow producing detailed scope and planning for the security assessment.
- The initiation of the validation process, which might include security objectives.
- The final project documentation (OSED, SPR, INTEROP), which would include security recommendations.

Figure 1 shows the overall process of the security assessment against the P5.7.4 project lifecycle.

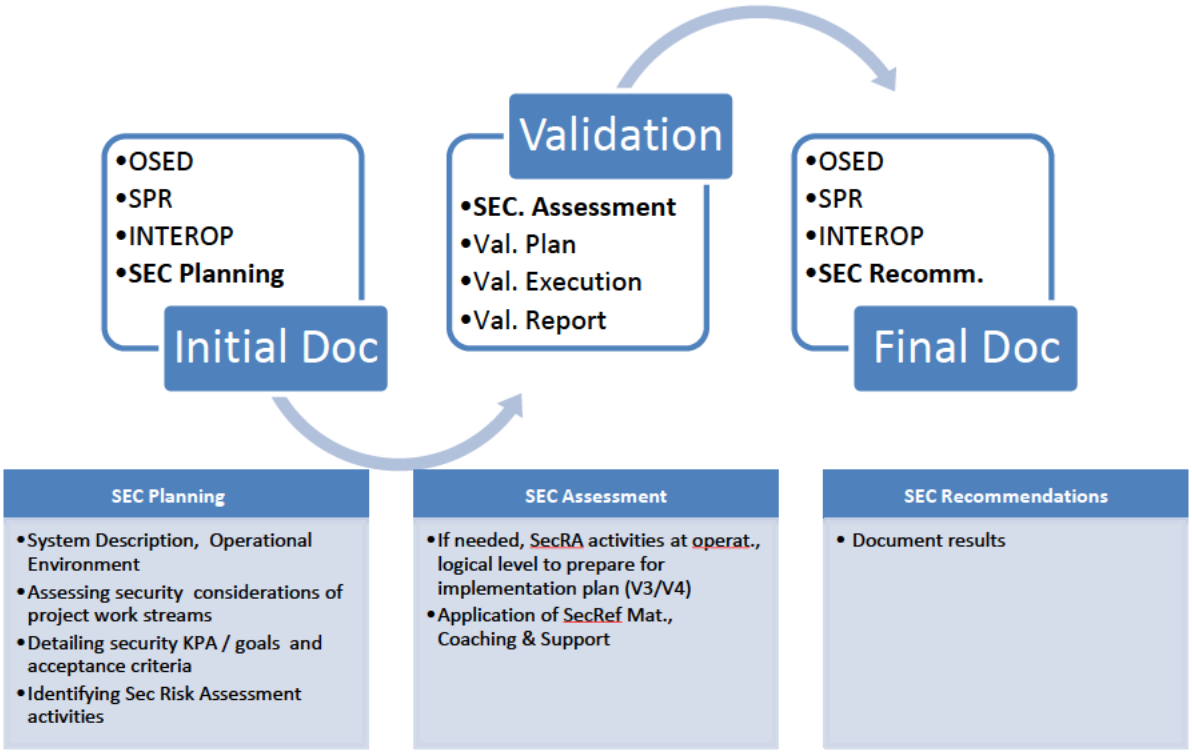

Figure 2: Security Assessment vs. Project Lifecycle

Once a mature enough work stream 1 OSED (P05.07.04 D02 - Updated Draft Initial Operational Service and Environment Definition for Madrid TMA – Madrid TMA) has been made available, it has been analysed against the security criteria provided by P16.06.02 project (see 5.7.4 Scoping & Change Assessment Questionnaire).

TA table shows the results of the above mentioned preliminary analysis[1].

[1] The original table is partially shown. The columns under the title 'Reasoning', 'Implications of answer', 'Source of information' and 'Comments' have been omitted.

TA Topic	Question	Answer
48. Security	System Factors • Are design specifications available for the concept? • Does the project use standardised designs consistent with other systems? • Does the design take into account requirements for business continuity and preventive maintenance? In particular, what is the contingency to maintain ATM services in the event of a complete failure? • Has the design taken into account possible failure modes of the system and the requirement to recover services and/or data? • Has provision been made for access controls, and are adequate authentication mechanisms in place? • Can system maintenance be carried out without operational impact? • Are mechanisms in place to ensure accountability for actions (by people or machines), and are appropriate records maintained and audited? • Are there appropriate mechanisms to ensure system and data integrity?	• YES (P-RNAV guidance material by EUROCONTROL) • YES (airspace structure, routes and procedures follow international standards and are consistent with the surrounding airspace structure). • YES, conventional procedures and modes of operations. Yes, business continuity and preventive maintenance as of current procedures. (Fall-back, redundancy, etc.) *FOLLOWING RESPONSES ARE SYSTEMS ORIENTED. RESPONSE IS GIVEN BUT IT SHOULD BE CHECKED WITH SYSTEMS' PROJECTS* • YES, from an ACC point of view, following normal procedures. • Yes, following applicable security procedures (out of the scope of this project). • Yes (out of the scope of this project). • Yes (voice and radar records are seamlessly active). (Out of the scope of this project). • Yes, already in place. (Out of the scope of this project)
49. Security	Independence • Does the system interact with other systems, which may result in interdependent failures? • Is there a system diagram or similar document showing the interdependence of this system with other ATM or connected systems? • Are there appropriate mechanisms in place to ensure security protection at the boundaries with connected systems (e.g. firewalls, anti-virus, routing protection, intruder detection)?	This is an operational project focused on airspace structures and operational procedures, with no impact on technical systems. (Out of the scope of this project)
50. Security	Physical & Environmental Factors • Are system assets protected against physical intrusions or environmental failures? • Will system changes negate current physical security measures? (e.g. remote access possible from insecure sites to capabilities currently secured physically) • Has the effect of the system on infrastructure or externally provided services been evaluated and necessary adjustments made? (e.g. Utilities, networking, contracted-out services, insurance) • Are there any features that will be affected by environmental conditions that might violate current assumptions and need special attention?	*FOLLOWING RESPONSES ARE SYSTEMS ORIENTED. RESPONSE IS GIVEN BUT IT SHOULD BE CHECKED WITH SYSTEMS' PROJECTS* • Assets related with this project like ACC centre, antennas, etc. are out of the scope of the project. • No, since there is no change to the infrastructure or externally provided services • No.
51. Security	Human Factors • Will the system require changes to operational roles and responsibilities? (e.g. between pilots, ATCOs, planners) • Will the system need more, better or changed	• No, in fact roles and responsibilities will keep the same. • Yes, there will be a need for

	training and development? • Will the system change workload, workload variability or task complexity? • Will the system change the potential to identify and manage security incidents, and have such changes been reflected in procedures and training? • Will the system change security roles or responsibilities, and is the change reflected in the security management system.	training in the new procedures and routes structures. • Yes, there is a potential improvement of workload, workload variability and task complexity, which will be validated within the project. • No, there is no impact in identification and management of security incidents. • No, there is no impact on roles and responsibilities.
51. Security	Human-system Interaction • Will the nature of human-system interactions change? • Will the balance between reliance on humans and machines change? • Is increased reliance on machines expected to result in a loss of professional skills by human operators?	• No. • No. • YES, conventional procedures are supposed to be less used than today. The skills of human operators must be ensured as such procedures will be used in case of contingency and in mixed mode operations only.
52. Security	Airspace Security • Will the system change flight identification or the processing of incident-related information in situations such as hi-jack, COMLOSS, or renegade aircraft. • Will the system change the interface between the ATM system and military or national airspace security systems.	• No • No

Table 1: Screening-scoping reference for the security assessment

2 Preliminary Security Risk Assessment

This section describes an assessment of the security elements within the scope of the project work stream 1 (WS 1). This preliminary security assessment is focused on identifying the security related aspects which may be relevant for the project scope and addresses the definition of treatment actions. However, as the project nature is purely operational, it is assumed from the first instance that no system or infrastructure element will be directly influenced by the project.

As an added value, the assessment has gone further and includes a list of assets beyond that scope. These assets have been identified as being closely related with the ability to operate under the procedures defined in the project. Following the rationale of section 1.1 (see figure *Figure 1*), such assets fit in the system context, but not in the system scope.

The EUROCONTROL guidelines (D06-001 – SESAR ATM Security Reference material) have been followed to realize a security Assessment on project 5.7.4 – Full implementation of P-RNAV in TMA (Work Stream 1 – Madrid TMA case).

Although SESAR addresses all eleven ICAO Key Performance Areas (KPA), the programme goals refer to four out of those areas, namely: Capacity, Safety, Environment, and Cost-Efficiency. As no specific goal has been allocated to the KPA Security, the following goal has been assumed in this project:

Security Goal – "To improve, or at least maintain, TMA Airspace security levels as they are today." –

2.1 Step 1: Identify Assets

As stated in section 1.1, the system addressed in this project consists of three main items:

- Madrid TMA airspace;
- P-RNAV routes in Madrid TMA; and
- ATC Operational Procedures in Madrid TMA.

The assets identification in this preliminary assessment has been extended to the 'system context', namely:

- Air Navigation infrastructure (ACC Building incl. access control)
- CNS systems & facilities (Radar, ILS, Radio-beacons, etc.)
- Back-up CNS systems
- Aircraft (using the TMA)
- ATCO HMI (at Madrid ACC)
- Airports within the TMA (Madrid-Barajas, Torrejón and Getafe)
- Madrid TMA surrounding En-route sectors

It must be noted that all the **assets within the 'system context' are out of the scope of this project.** However it is recognized that a close relation with the continuity and resilience of the operational service addressed by the project exists.

Table 2 shows the assets identified by the project team under the work stream 1 of the P5.7.4 project (full implementation of P-RNAV in the Madrid TMA). The impact of possible asset failures on the elements under the scope of P5.7.4 work stream 1 (TMA airspace, route structures and operational procedures) has been qualitatively categorized as either critical or relevant.

Asset type	Domain	Rationale for P5.7.4 work stream 1
Physical	Control Centres	The P-RNAV procedures in the Madrid TMA are fully dependent on the quality of service provided by the Madrid ACC. The TMA could suffer a decrease in capacity or even be closed until

		minimum service levels are resumed due to possible shortfall in the ATC service. Hence the Madrid ACC premises have been identified as critical assets regarding the P-RNAV operation in the TMA; however they are **out of the scope** of P5.7.4 project work stream 1.
	Radar Facilities	The P-RNAV procedures in the Madrid TMA are fully dependent on the availability of the radar service in the TMA airspace. Without the radar service, it would not be possible to operate in the TMA under safe conditions. Hence the radar facilities, which are essential for the radar service provision, have been identified as a critical asset regarding the TMA operation; however they are **out of the scope** of P5.7.4 project work stream 1.
	Navigation aids	The P-RNAV route structure in the Madrid TMA is supported by navigation aids, namely: • Aircraft altimeter (airborne); • DME-DME (ground); and • GPS – and other GNSS. However none of those aids in isolation are considered essential for aircraft to comply with P-RNAV navigation requirements in the TMA. Actually it is assumed that radio beacons and GNSS are redundant systems. In fact the radio beacons have become kind of back-up systems since almost all commercial aircraft are GPS equipped. For non-GPS equipped aircraft, radio beacons are still the main navigation aids under IFR. Hence the navigation aids have been identified as relevant assets regarding the P-RNAV operation in the TMA; however they are **out of the scope** of P5.7.4 project work stream 1.
	Aircraft	The aircraft need to be compliant with P-RNAV procedures. The airborne navigation equipment, such as the Flight Management System (FMS), need to: • comply with the P-RNAV standards; and • contain all the flight information required (flight plan) Aircraft either non P-RNAV compliant or without the required flight information will fly under conventional procedures. Hence the aircraft have been identified as relevant assets regarding the P-RNAV operation in the TMA; however they are **out of the scope** of P5.7.4 project work stream 1.
	Runways	One of the main TMA design criteria is based upon the existing runways at the served airports and their configurations. Any change in runway availability has a critical impact on the operation within the TMA. Thus the TMA design must consider all cases in which any runway of those airports is temporarily closed. Some examples of such cases are: • runway under maintenance processes; • runway accidentally blocked by an aircraft; • runway incursion. For service continuity reasons, the TMA design must comprise a generic contingency case yielding runway closure. It is necessary to assess the feasibility of maintaining the P-RNAV routes and procedures when a runway has been closed. Hence the runways at the airports within the Madrid TMA have been identified as relevant assets regarding the P-RNAV operation in the TMA; they are addressed within the P5.7.4 project work stream 1. In particular, the 'runway closure case' is

		within the scope of the project.
Human	Staff (operational)	The ATC operators in the Madrid ACC dealing with the Madrid TMA should be trained accordingly to the new procedures and routes structure. Furthermore increased reliance on machines could result in a loss of professional skills by human operators. Thus conventional procedures, i.e. radar vectoring, should be addressed from the safety perspective for both non P-RNAV equipped aircraft and contingency situations. Hence the operational staffs belonging to the Madrid TMA have been identified as critical assets regarding the P-RNAV TMA operation, thus falling **within the scope** of P05.07.04 project.
Communication Systems	Ground Networks A/G voice/datalinks SATCOM A/A communication	The communication systems security is already covered by the current Madrid TMA contingency plan The implementation of P-RNAV would have no effect on them. In any case, the communication systems are considered as critical assets regarding the TMA operation; however they are **out of the scope** of P5.7.4 project work stream 1.
Information and data	Corporate knowledge (design)	The corporate knowledge concerning the Madrid TMA is under Aena's corporate knowledge policy, which comprises a set of security measures for self-protection. In any case, the corporate knowledge is considered as a critical asset regarding the TMA operation; however they are **out of the scope** of P5.7.4 project work stream 1.
Operating procedures and routines	Operating procedures	The P-RNAV operating procedures are considered as a critical asset regarding the TMA operation; they are fully addressed by P5.7.4 project work stream 1.

Table 2: Assets identification

2.2 Steps 2 to 5

The following steps of the EUROCONTROL's security assessment process have been omitted:

- Step 2: Identify Vulnerabilities
- Step 3: Identify Threads / Threads Conditions
- Step 4: Risk Evaluation
- Step 5: Select Treatment Options

The Spanish contingency protocol fully describes the ATM system vulnerabilities, the threads. It also makes a risk evaluation and defines treatment options in detail. Any vulnerability of or threat performed against the Madrid TMA will be dealt with by following the protocol.

Regarding the vulnerabilities identification, the radar facilities deserve special attention as they are the most critical assets. Without radar service, there would be no possibility to operate in the TMA, but with non-radar based procedures. In the current situation (real operations), such procedures are considered obsolete and are not in use anymore, so if the radar service is not available, the current contingency procedure is to close the airspace.

For P05.07.04 project, when designing new procedures, the measure of closing the airspace in case of radar service not available has also been embraced, as it is the case for current, real procedures. The actual justification for such decision is twofold:

- on the one hand, it is absolutely questionable that such a failure in the system preventing radar service from being used occurs, since the redundancy is high and statistically it is proven that this has not occurred for many years;
- on the other hand, keeping the operational staff trained for non-radar procedures is not justified due to the high costs of the training and the extremely low likelihood of real need for such procedures.

The solution implemented for this project is thus closing the Madrid TMA airspace in case the radar service is not available.

2.3 Step 6: Preliminary conclusions

At the beginning of a project it must be clarified whether a complete security assessment is necessary or not. This section intends to document justification to the project related management layers (P5.7.4, P16.6.6, and the SJU) as to why a detailed security assessment should be performed or not.

The conclusions are:

1. It is NOT necessary to perform a detailed security assessment in P5.7.4 work stream 1 due to its purely operational nature.
2. It has been demonstrated that the project has NO relevant impact on ATM Security. Only two minor risks have been identified in the preliminary security risk assessment and the corresponding treatment actions have been defined. Such risks are related with the following assets: runway and staff. The treatment actions are described in section 3 as recommendations.
3. Several ‘security related assets’ have been identified in the context of the system addressed by the project. However all of them fall outside its scope (see section 2). Among the assets identified, the most critical one concerning the operation in the TMA is the radar, namely the radar service not being available for any cause.

3 Recommendations

From the security perspective, the following recommendations are made on the basis of the two security risks (SEC Risks) identified when scoping the security assessment (sections 1 and 2):

1. SEC Risk 1 – The system will need changed training and development.

   Treatment action – Training in new procedures and airspace structure should be addressed in the project.

2. SEC Risk 2 – There is an increased reliance on machines that could result in a loss of professional skills by human operators.

   Treatment action – Conventional procedures, i.e. radar vectoring, should be addressed from the safety perspective for both non P-RNAV equipped aircraft and contingency situations.

It is recommended that these two risks be included in the RIO management of the project.

4 References

Name of project,Title of document, Identification number, Edition, Date

4.1 Applicable Documents

This Annex complies with the requirements set out in the following documents:

[1] SESAR SEMP v2.0

[2] B4.2 Initial Service Taxonomy document

[3] Template Toolbox 02.00.00

[4] Requirements and V&V Guidelines 02.00.00

[5] Toolbox User Manual 02.00.00

4.2 Reference Documents

The following documents were used to provide input/guidance/further information/other:

[6] SJU P05.07.04, Initial OSED – Madrid TMA (main body), 05.07.04.D02.

[7] SJU P16.06.06, 05.07.04-16.06-TA-Support-ATMSecurity.ppt

[8] SJU P16.06.02, SESAR ATM Security Management Plan, 16.06.02.D03, Edition 00.01.00.

[9] SJU P16.06.02, SESAR ATM Security Reference Material, 16.06.02.D06, Edition 00.01.00.

[10] EUROCONTROL, ATM Security Risk Management Toolkit – Guidance Material, Edition 1.01, Edition date: December 2010.

[11] EUROCONTROL, Security Management Handbook – A Framework, Edition 1.0, Edition date: May 2008.

[12] EUROCONTROL, Critical Asset Identification for ATM, Edition 0.4, Edition date: May 2008 (draft).

- **END OF DOCUMENT -**