06.03.01 Remote and Virtual Tower Security Risk Assessment

Document information	
Project Title	06.03.01 Remote and Virtual Tower Security Risk Assessment
Project Number	16.06.02
Project Manager	EUROCONTROL
Deliverable Name	06.03.01 Remote and Virtual Tower Security Risk Assessment
Deliverable ID	
Edition	00.00.02
Template Version	03.00.00
Task contributors	
EUROCONTROL, NORACON/LFV	

Please complete the advanced properties of the document

Abstract

This document reports on a security risk assessment of OFA 06.09.03, Remote and Virtual Tower. The risk assessment is one of the earlier assessments carried out by 16.06.02 and has also been used to test the risk assessment methodology and other components of the security reference material.

Authoring & Approval

Prepared By - *Authors of the document.*		
Name & Company	Position & Title	Date
[redacted] EUROCONTROL	[redacted]	09/12/2013
[redacted] EUROCONTROL	[redacted]	09/12/2013

Reviewed By - *Reviewers internal to the project.*		
Name & Company	Position & Title	Date
[redacted] EUROCONTROL	[redacted]	09/12/2013

Reviewed By - *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date
<Name / Company>	<Position / Title>	<DD/MM/YYYY>

Approved for submission to the SJU By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
<Name / Company>	<Position / Title>	<DD/MM/YYYY>

Rejected By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date
<Name / Company>	<Position / Title>	<DD/MM/YYYY>

Rational for rejection
None.

Document History

Edition	Date	Status	Author	Justification
00.00.01	16/11/2012		[redacted]	New Document
00.00.02	09/12/2013		[redacted]	Revised risk assessment

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Table of Contents

EXECUTIVE SUMMARY 5
1 INTRODUCTION 6
1.1 CHANGES FROM THE PREVIOUS VERSION 6
1.2 CONTEXT OF THE ASSESSMENT 6
1.2.1 Expertise of the assessors 6
1.2.2 Sources of information 6
1.2.3 Scope 6
1.2.4 Dependencies 8
1.2.5 Assumptions 8
2 IDENTIFICATION OF PRIMARY ASSETS 9
2.1 IMPACT OF COMPROMISED CIA ON PRIMARY ASSETS 11
2.2 IDENTIFICATION OF SUPPORTING ASSETS 13
3 THREAT SCENARIOS 17
3.1 THREATS 17
3.2 THREAT SCENARIOS 19
4 RISK EVALUATION 20
4.1 IMPACT EVALUATION 20
4.2 LIKELIHOOD EVALUATION 20
4.3 RISK LEVEL EVALUATION 20
1 RISK TREATMENT 30
4.4 INTRODUCTION 30
5 CONTROL SELECTION 31
6 CONTROL REFINEMENT AND DESIGN 47
6.1 OVERVIEW 47
6.2 CONTROL CONSIDERATIONS FOR DEVELOPMENT PHASE 47
6.3 FURTHER WORK 48
7 REFERENCES 49

List of tables

Table 1: ATM service and application matrix 8

List of figures

Figure 1: Models for connecting the Tower to the Supporting Assets 7
Figure 2: Mapping of controls to supporting assets (1 of 2)........ 32
Figure 3: Mapping of controls to supporting assets (2 of 2)........ 33

Executive summary

A security risk assessment of Operational Focus Area (OFA) 06.03.01 has been carried out as this was previously identified as a security 'hotspot'. The assessment followed the SESAR Security Risk Assessment Methodology. This version of the document builds on a first pass analysis and goes to a greater depth of analysis of the primary and supporting assets. The version also includes further development of the techniques to manage the assessment. The assessment has been used in part to gain familiarity with the SESAR ATM Security Risk Assessment Methodology (SecRAM) and develop techniques to manage the assessment.

The assessment covers the following key aspects:

1. Identification of Primary Assets for the different instantiations of remote operated towers (single, multiple, AFIS and contingency operations).
2. An impact assessment of the loss of a security attribute (confidentiality, availability or integrity) to ATM operations/business and societal outcomes.
3. Identification of Supporting Assets, noting that the methodology focuses primarily on supporting assets that are central to the operational focus area.
4. Applicable threats to the supporting assets, identified from a long list of threats by the authors.
5. Threat scenarios, matching threats to supporting assets.
6. The likelihood of threat scenarios being executed by an attacker.
7. The risk of each threat scenario, calculated by combining impact and likelihood.
8. Controls, for each threat scenario, identified from a long list of controls with the aim of provisioning for a 'defence in depth'. The document also attempts group the findings in a way that reduces duplication of control recommendations.

The assessment was carried out before the Minimum Set of Security Controls (MSSCs) were finalised and these have not therefore been included in the analysis, although it is likely that many of the controls identified will also feature within the set of MSSCs.

Of the recommended controls, most of those identified will be standard to ANSP security management. However, two categories of control stand out for particular attention in the SESAR development phase:

Encoding/Encryption of data within and between the following supporting assets:

- Wide-Area Network link - RTC unit
- A/D visualisation system - Camera "N" - Local unit

Bespoke 'Technical' controls to address some specific security risks to the following supporting assets:

- ATC and voice data recording - RTC unit
- Binocular View - Local unit
- PTZ Unit - Local unit
- Aerodrome equipment communications network - Local unit
- Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit
- A/D visualisation system - Camera "N" - Local unit

1 Introduction

This document records the security assessment of the Remote Operated Tower OFA 06.03.01.

The risk assessment has been carried out on the Remote Operated Tower (ROT) concept in accordance with the SESAR Security Reference Material (In particular 16.02.03 D02 SESAR ATM Security Risk Assessment Methodology 00.01.04).

The assessment was carried out on spreadsheet from which the tables in this report have been generated. The spreadsheet is available from the authors for inspection/validation.

1.1 Changes from the previous version

This is the second assessment of the ROT OFA and is based on a greater depth of analysis of the primary and supporting assets. This version also attempts group the findings in a way that reduces duplication of control recommendations. The version also includes further development of the techniques to manage the assessment. The assessment has been used in part to gain familiarity with the SESAR ATM Security Risk Assessment Methodology (SecRAM) and develop techniques to manage the assessment.

1.2 Context of the assessment

1.2.1 Expertise of the assessors

The assessment was carried out by members of the EUROCONTROL SESAR Security Team in the scope of WP16.6.2. The team is experienced in safety and security risk assessment for ATM operations.

1.2.2 Sources of information

The assessors have used a variety of operational and technical documents associated with the ROT OFA as well as the SESAR Security Reference Material for guidance on how to carry out the risk assessment.

1.2.3 Scope

The ROT OFA is sufficiently mature that the full SESAR ATM Security Risk Assessment Methodology can be applied. The assessment covers the following Operational Improvements (OIs) that are described in the Remote Tower OSED:

- OI SDM-0201 “Remotely Provided ATS for Single Aerodromes” falls under SESAR Operational Step 1 (ATM Service Level 2).
- OI SDM-0205 “Remotely Provided ATS for Multiple Aerodromes” falls under SESAR Operational Step 3 (ATM Service Level 4).
- OI SDM-0204 “Remotely Provided ATS for Contingency at Aerodromes”

The OSED essentially describes the OFA as applicable to two different environments:

- Aerodrome Control Service (covering a control service provided by a qualified Air Traffic Control Officer (TWR) and/or an Approach/departure Control Service for Arriving and Departing aircraft (APP))
- Aerodrome Flight Information Service (AFIS) provided by a suitably qualified AFIS Officer.

The application areas identified are:

- Single remote tower - for low to medium density rural airports
- Multiple remote tower - for low to medium density rural airports
- Contingency tower - for medium to high density airports, where the primary tower is unusable (planned or unplanned).

The assessment considers two main sites for the implementation of the concept:

- Local site (aerodrome), assumed to have a level of security commensurate with a low-medium density airport.
- Remote Tower Centre, assumed to be within an existing enroute or approach unit and with corresponding security controls.

In addition, a wide area connection is required to link the local sites with the remote tower centre.

In making the assessment the scope of the work is somewhat driven by the need to understand whether the Remote Tower facility will be created by simply connecting existing data services termination points to a new facility and adding in new necessary services (e.g. CCTV to replace tower views), or by routeing all data services to the new tower directly from the data source.

The first option potentially offers the lowest capital cost since for existing services, the only need is for data message re-routeing. The second option may need all data services to be rerouted and might need new cable ducts etc.

Figure 1 below shows the options. If option 1 is the implemented model, then in principle since the aerodrome will have needed to undertake a security risk assessment, this assessment should be limited to only new services and the re-routeing element of existing services. The second option requires this assessment to essentially go back to the data generation level. To ensure maximum security assurance this assessment has assumed model 2.

Figure 1: Models for connecting the Tower to the Supporting Assets

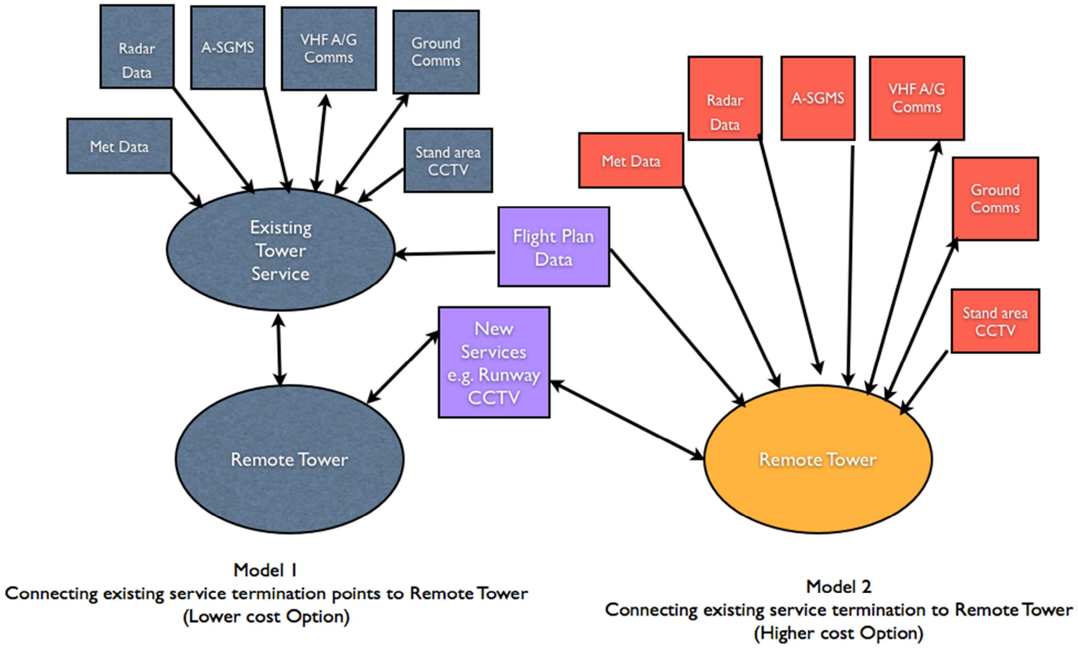


Table 1 below identifies the ATM service and application matrix that has been evaluated.

Table 1: ATM service and application matrix

Application Areas	Aerodrome Control Service	AFIS Service
Single Remote Tower	Yes	Yes
Multiple Remote Tower	Yes	No
Contingency Tower	Yes	Not in OSED

1.2.4 Dependencies

The assessment has identified that the ROT OFA is not materially dependent on other ATM modernisation projects. However, additional analysis is recommended in the case of implementation of the following OFAs:

- OFA 01.03.01 Time based separation, noting that this concept may not be required in the aerodromes of interest for ROT operations.
-

1.2.5 Assumptions

A number of assumptions have been made in this analysis:

- The Remote Tower Centre is external to the Airfield, if not the majority of the risk assessment would be coherent with the Security Assessment for the Aerodrome itself.
- A certain level of security is assumed for existing airport and remote centre assets. This means that security risks to these assets have not been assessed. The Common Requirements regulation (EU) 1035/2011 requires ANSPs to establish a Security Management System. The risk assessment therefore assumes that ANSPs will maintain a Security Management System that meets these requirements and will assure the security of existing ATC units.
- All Supporting Assets provide status monitoring information, if not they are unlikely to be able to support JAR/FAR 25 operations.
- The medium size airports provide services to JAR/FAR 25 and General Aviation (including commercial helicopter) flights, but not pleasure flyers such as microlights or gliders: this latter assumption simplifies the ATCOs' data requirements.
- The small size airports have a larger proportion of non JAR/FAR 25 flights.
- The Remote Tower Centre has the capability to "move" aerodrome service displays to different control stations.
- ATCOs hold appropriate qualifications i.e. Aerodrome certifications are still necessary (This is an implicit security control). *Check this is still valid.*

2 Identification of primary assets

Primary assets are either services or information necessary for the operational concept. The following table lists the primary assets identified for the ROT concept. A wide approach has been taken, including conventional primary assets. The new primary assets introduced by the ROT concept are marked with an asterix in the reference column.

			ROT Primary Assets (*indicates new PA)
Primary Asset reference	**Description**	**Type (information/ service)**	**Rationale for considering PA**
A1*	Visual reproduction of aerodrome (+ taxiways & apron)	Information	Gives the 'out the window' view to remote CWP and other units / airport partners.
A2	Aeronautical mobile service	Service	Air-ground communications
A3	Aeronautical fixed service	Service	Ground-ground communications
A4	Surveillance position and identity (if required for operational declaration)	Information	Where available used to augment the visual reproduction through a position and identity overlay.
A5	Precision runway approach guidance (ILS/MLS)	Information	Provides guidance signals (information) to aircraft flight director system for manual or autopilot coupled flight.
A6	Visual approach slope /path indicator (VASI / PAPI)	Information	Provides visual information of slope and lateral position for pilots.
A7	Runway and Taxiway lighting, control and monitoring data	Information	Provides visual guidance for aircraft on the aerodrome
A8	Runway Visual Range data	Information	Measurements to determine type of operation (VMC / IMC)
A9*	Aerodrome (airport) sound reproduction	Information	Supplements the 'out the window view'
A10	Flight Plan Data and ATS messages e.g. airborne activation messages	Information	Information used and updated by local controllers / CWP systems. RVT shall enable access to and handling of ATS messages (as described in ICAO Doc 4444 Chapter 11)
A11	ASMGCS position information and control and monitoring data	Information	Will be available at larger airports, possibly using ROT as a contingency TWR.
A12*	Binocular view reproduction	Information	Binoculars used by controllers - noted that this may also support

ROT Primary Assets (*indicates new PA)

Primary Asset reference	Description	Type (information/ service)	Rationale for considering PA
			signalling lamps.
A13	Meteorological information	Information	May currently be performed by local ATCO/AFISO but this is not assumed for the RVT (ROT) concept. E.g. an external source is needed and / or automated met equipment.
A14*	Aerodrome Identifier Tag	Information	Sanity check that control actions are applied to the correct aerodrome.
A15*	Data distribution within ROT	Service	
A16	Aircraft taxi and apron guidance systems (If fitted)	Service	Typically lighting systems that indicate taxiway direction to follow.
A17	Direct signalling lamp towards aircraft	Service	The means of directing the signalling lamp towards the applicable aircraft may be combined with the binocular function.
A18*	Airfield equipment control and condition monitoring information	Information	A general catch all - essential for controllers to know availability of equipment**.
A19	Transmit information between aerodrome and ROT	Service	Catch-all to ensure transmission of data is covered.
A20	Surface movement control service	Service	Communications for the control of vehicles other than aircraft on manoeuvring areas at controlled aerodromes) for the aerodrome and its vicinity.
A21	ATS Messages	Information	
A22	Time in UTC	Information	All operations synchronised to UTC
A23	Safety performance monitoring	Service	Recording incidents, non-nominal situations, supporting data etc.

*** "RVT shall enable the ATCO/AFISO to adjust and monitor percentage and on/off status of visual navigational aids (runway and field lighting systems as applicable to the aerodrome, such as approach, PAPI, runway, taxiway, RGL, stopway and obstacle lighting).","RVT shall enable monitoring of the technical status of systems that can affect the safety or efficiency of flight operations and/or the provision of air traffic service. Note I: This corresponds to requirements on local tower operations, with the addition of systems that are specific to remote tower operation, such as detecting corrupt/delayed visual presentation. Note II: For multiple tower operations, there will be additional requirements on monitoring systems for more than one aerodrome in parallel."*

2.1 Impact of compromised CIA on primary assets

Each primary asset has been assessed as to the impact that would occur on an airport's operations should the primary asset be compromised in terms of its confidentiality, integrity or availability. The analysis has considered whether other criteria merit analysis such as 'authenticity', 'non-repudiation', 'traceability', 'provability'. It was decided that these are either not relevant to the operations or would be covered by CIA. It should also be noted that the highest impact only is carried through to the next stage of the analysis, hence additional criteria are unlikely to change the impact assessment.

			Impact							
Primary Asset	Description	Potential compromise of C, I or A:	Personnel	Capacity	Performance	Economic	Branding	Regulatory	Environment	Overall impact
A1	Visual reproduction of aerodrome (+ taxiways & apron)	C	0	4	3	0	4	4	0	4
		I	0	5	4	0	5	4	0	5
		A	0	5	4	0	5	4	0	5
A2	Aeronautical mobile service	C	0	0	0	0	2	0	0	2
		I	0	0	4	0	0	0	0	4
		A	0	5	4	0	0	0	0	5
A3	Aeronautical fixed service	C	0	0	3	0	4	4	0	4
		I	0	3	4	0	4	4	0	4
		A	0	3	4	0	4	4	0	4
A4	Surveillance position and identity (if required for operational declaration)	C	0	0	3	0	4	4	0	4
		I	0	3	4	0	4	4	0	4
		A	0	3	4	0	4	4	0	4
A5	Precision runway approach guidance (ILS/MLS)	C	0	3	0	0	0	0	0	3
		I	0	3	3	0	3	0	0	3
		A	0	3	3	0	3	0	0	3
A6	Visual approach slope /path indicator (VASI / PAPI)	C	0	0	0	0	0	0	0	0
		I	0	5	3	0	3	0	0	5
		A	0	5	3	0	3	0	0	5
A7	Runway and Taxiway lighting, control and monitoring data	C	0	0	0	0	0	0	0	0
		I	0	3	3	0	3	0	0	3
		A	0	3	3	0	3	0	0	3
A8	Runway Visual Range data	C	0	0	0	0	0	0	0	0
		I	0	3	3	0	3	0	0	3
		A	0	3	3	0	3	0	0	3
A9	Aerodrome (airport) sound reproduction	C	0	0	0	0	0	0	0	0
		I	0	3	0	0	3	0	0	3
		A	0	3	0	0	3	0	0	3
A10	Flight Plan Data and ATS messages e.g. airborne activitation messages	C	0	3	4	0	4	4	0	4
		I	0	3	5	0	5	4	0	5
		A	0	3	5	0	5	4	0	5
A11	ASMGCS position	C	0	0	3	0	4	4	0	4

			Impact							
Primary Asset	**Description**	**Potential compromise of C, I or A:**	**Personnel**	**Capacity**	**Performance**	**Economic**	**Branding**	**Regulatory**	**Environment**	**Overall impact**
	information and control and monitoring data	I	0	3	4	0	4	4	0	4
		A	0	3	4	0	4	4	0	4
A12	Binocular view reproduction	C	0	4	3	0	4	4	0	4
		I	0	5	4	0	5	4	0	5
		A	0	5	4	0	5	4	0	5
A13	Meteorological information	C	0	0	3	0	3	3	0	3
		I	0	3	3	0	3	3	0	3
		A	0	3	3	0	3	3	0	3
A14	Aerodrome Identifier Tag	C	0	0	0	0	0	0	0	0
		I	0	4	3	0	3	3	0	4
		A	0	4	3	0	3	3	0	4
A15	Data distribution within ROT	C	0	3	4	0	4	4	0	4
		I	0	5	4	0	5	4	0	5
		A	0	5	4	0	5	4	0	5
A16	Aircraft taxi and apron guidance systems (If fitted)	C	0	0	3	0	3	3	0	3
		I	0	3	3	0	3	3	0	3
		A	0	3	3	0	3	3	0	3
A17	Direct signalling lamp towards aircraft	C	0	0	3	0	3	3	0	3
		I	0	0	3	0	3	3	0	3
		A	0	0	3	0	3	3	0	3
A18	Airfield equipment control and condition monitoring information	C	0	3	3	0	3	3	0	3
		I	0	5	4	0	4	4	0	5
		A	0	5	4	0	4	4	0	5
A19	Transmit information between aerodrome and ROT	C	0	3	4	0	4	4	0	4
		I	0	5	4	0	5	4	0	5
		A	0	5	4	0	5	4	0	5
A20	Surface movement control service	C	0	0	3	0	3	3	0	3
		I	0	3	3	0	3	3	0	3
		A	0	3	3	0	3	3	0	3
A21	ATS Messages	C	0	3	4	0	4	4	0	4
		I	0	3	5	0	5	4	0	5
		A	0	3	5	0	5	4	0	5
A22	Time in UTC	C	0	3	0	0	3	3	0	3
		I	0	3	4	0	4	4	0	4
		A	0	3	4	0	4	4	0	4
A23	Safety performance monitoring	C	0	0	0	0	3	3	0	3
		I	0	0	4	0	4	4	0	4
		A	0	0	4	0	4	4	0	4

2.2 Identification of Supporting Assets

Supporting assets have been identified from a variety of documents and the team's own knowledge of airport equipment and systems. The table below designates a hierarchical reference to each Supporting Asset (SA), its location, description, 16.6.2 Asset Catalogue Reference. This approach led to around 70 supporting assets being identified. Therefore to simplify the assessment a further two columns were added to include or exclude supporting assets on the following grounds:

1. Whether the supporting asset should be considered a sub-component of another equipment or sub-system.
2. Whether the supporting asset would be already included in the ATC unit's existing security management processes.

Point 1 implies that the supporting asset could be vulnerable to a distinct attack on it, rather than an attack on its 'parent' component or sub-system. However, this may be difficult to determine when considering cyber attacks.

Ref.	Location	Description	IN/OUT	IN/OUT Rationale
SA1	RTC unit	Remote Tower Building and facilities (HLP) - RTC unit	OUT	Existing controls / MSSCs likely to be sufficient
SA1.1	RTC unit	Client (Controller) Working Position - RTC unit	IN	
SA1.1.1	RTC unit	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit	IN	
SA1.1.1.1	RTC unit	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit	IN	Existing controls may not be sufficient
SA1.1.1.2	RTC unit	Servers for visualization - RTC unit	IN	
SA1.1.1.3	RTC unit	ATC and voice data recording - RTC unit	IN	The existing tower may or may not have this recording function. It is classed as IN for the following reasons: first it will be in a new facility, second it is likely that during, at least the early deployments of ROT all facilities will need recording to add to the assurance of the safety of the methodology.
SA1.1.2	RTC unit	OTW display - RTC unit	IN	
SA1.1.2.1A	RTC unit	Multi Display System - RTC unit	OUT	Sub-component or option
SA1.1.2.1A.1	RTC unit	Display "N" - RTC unit	OUT	Sub-component or option
SA1.1.2.1B	RTC unit	Circular Video Wall - RTC unit	OUT	Sub-component or option
SA1.1.2.1B.1	RTC unit	Projector "N" - RTC unit	OUT	Sub-component or option
SA1.1.2.2	Local unit	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit	IN	

Ref.	Location	Description	IN/OUT	IN/OUT Rationale
SA1.1.2.3	RTC unit	Central tracking unit CTU (common gateway for all site sensors) - RTC unit	IN	
SA1.1.3	RTC unit	OTW audio presentation - RTC unit	IN	
SA1.1.4	RTC unit	CWP computers / control systems / local network tools - RTC unit	OUT	Existing controls / MSSCs likely to be sufficient
SA1.1.5	RTC unit	Display screens other than OTW - RTC unit	IN	
SA1.2	RTC unit	Wide-Area Network link - RTC unit	IN	
SA1.3	RTC unit	FDP interface - RTC unit	OUT	Existing controls / MSSCs likely to be sufficient
SA1.4	RTC unit	Aircraft track monitoring display (radar, A-SMGCS etc.) - RTC unit	OUT	Existing controls / MSSCs likely to be sufficient
SA2	Local unit	FIS for display and update of met and operational flight information - Local unit	IN	
SA3	Local unit	A/G Transmit/Receive aerial stations - Local unit	OUT	Existing controls / MSSCs likely to be sufficient
SA4	Local unit	AFTN Ground/Ground Coms and relay stations - Local unit	OUT	Existing controls / MSSCs likely to be sufficient
SA5	RTC unit	Personnel - RTC unit	IN	
SA5.1	RTC unit	RTC personel - RTC unit	OUT	Sub-component or option
SA5.1.1	RTC unit	ATCO - RTC unit	OUT	Sub-component or option
SA5.1.2	RTC unit	AFISO - RTC unit	OUT	Sub-component or option
SA5.1.3	RTC unit	Watch Supervisor - RTC unit	OUT	Sub-component or option
SA5.1.4	RTC unit	Technician/Engineers - RTC unit	OUT	Sub-component or option
SA5.2	Local unit	Airport personnel (dedicated to ROT operations) - Local unit	IN	
SA5.2.1	Local unit	Technician/Engineers - Local unit	IN	Kept in as increased importance c.f. current ops.
SA6	Local unit	Runway Visual Range Equipment - Local unit	OUT	Connection to airport network in SA28
SA7	Local unit	Visual navigation aids - Local unit	OUT	Connection to airport network in SA28
SA7.1	Local unit	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit	IN	Especially connection to ROT. Whilst airfields may have already addressed the security controls, as part of the overall safety/security assurance it has been classified as IN.

Ref.	Location	Description	IN/OUT	IN/OUT Rationale
SA8	Local unit	Instrument Landing System (localiser and glide path) including status monitoring to ATCO - Local unit	OUT	Connection to airport network in SA28
SA8.1	RTC unit	ILS control panel - RTC unit	OUT	Sub-component or option
SA9.1	Local unit	A/D visualisation system - Camera "N" - Local unit	IN	
SA9.1.1	Local unit	A/D visualisation system - Encoder "N" - Local unit	OUT	Sub-component or option
SA9.1.2	RTC unit	A/D visualisation system - Decoder "N" - RTC unit	OUT	Sub-component or option
SA9.4	RTC unit	WAN connection - RTC unit	OUT	Already covered as WAN link
SA10	Local unit	Binocular View - Local unit	IN	
SA10.1	Local unit	PTZ Unit - Local unit	IN	
SA10.1.1	Local unit	Pan-Tilt head inc. signalling lamps (signal light gun) - Local unit	OUT	Sub-component or option
SA10.1.2	Local unit	Zoom Camera - Local unit	OUT	Sub-component or option
SA10.1.3	Local unit	Infra-red Camera - Local unit	OUT	Sub-component or option
SA10.2.1	Local unit	PTZ Server - Local unit	OUT	Sub-component or option
SA10.2.2	Local unit	API Infra-red Camera - Local unit	OUT	Sub-component or option
SA10.2.3	Local unit	API Zoom Camera - Local unit	OUT	Sub-component or option
SA10.2.4	Local unit	Digital Encoder (for IR camera) - Local unit	OUT	Sub-component or option
SA10.2.5	Local unit	Analog Encoder (for Zoom Camera) - Local unit	OUT	Sub-component or option
SA10.3	RTC unit	Remote tower Centre Software (should be also HW) - RTC unit	IN	
SA10.3.3	RTC unit	HMI - RTC unit	OUT	Sub-component or option
SA11.1	Local unit	Telephone landlines (not AFTN) - Local unit	IN	Kept in as increased importance c.f. current ops.
SA11.2	Local unit	Microwave links if used - Local unit	OUT	Assume not used
SA11.3	RTC unit	Sat and mobile comms technology - RTC unit	OUT	Assume not used
SA12	Local unit	Radar Stations - Local unit	OUT	
SA13	Local unit	Surveillance sensors other than radar (A-SMGCS) - Local unit	OUT	
SA14	Local unit	Airport Sound System (audio monitors around aerodrome and on TWR) - Local unit. NB, this is different to Noise and Track Keeping monitors.	IN	
SA15	Local unit	Met station (likely to be automated) inc. anemometer - Local unit	OUT	Connection to airport network in SA28

Ref.	Location	Description	IN/OUT	IN/OUT Rationale
SA16	Local unit	Aerodrome Identifier Tags for Visualisation data - Local unit	IN	
SA17	Local unit	Data Concentrator (APT) - Local unit	IN	
SA18	Local unit	Radio Gateway (APT) - Local unit	IN	
SA19	Local unit	Contingency VCS (APT) - Local unit	IN	
SA20	Local unit	Specific Protocol converters (APT) - Local unit	IN	
SA21	Local unit	Local Network infrastructure (APT) - Local unit	IN	NB, this may be a duplicate of SA 28.
SA22	Local unit	Monitoring proxy/node (APT) - Local unit	IN	
SA24	RTC unit	VCS Switch (core element) - RTC unit	OUT	
SA25	RTC unit	Technical supervision (s/w) tool - RTC unit	IN	
SA26	Local unit	Tower Building and facilities (HLP) - Local unit	OUT	
SA27	Local unit	Other navaids (NDB, DME, VOR) - Local unit	OUT	
SA28	Local unit	Aerodrome equipment communications network - Local unit	IN	
SA1.2.1	Local unit	WAN connection - Local unit	IN	
SA30	RTC unit	UTC timing signal - RTC unit	OUT	

3 Threat scenarios

3.1 Threats

A list of possible threats to the ROT OFA has been derived from:

- (A) the SecRA Methodology Annex A, which itself refers to ISO 27005.
- (B) The EUROCONTROL Draft EATM Threat Catalogue, created as part of a Security Management Toolkit in 2009.

These are shown in the table below with a reference to the source of the threat description (A or B above) and the type of threat. Where there was overlap in the threat descriptions, the SecRA methodology description has taken precedence. Further descriptions of the threats may be found from ISO27005 and the Draft EATM Threat Catalogue.

Source	Ref	Type of Threat
A	CoF	Compromise of functions
A	CoI	Compromise of Information
A	TEC	Technical failure
A	PHD	Physical damage
A	UA	Unauthorized action
A	LoES	Loss of essential services
A	Rad	Disturbance due to radiation
B	INF	Information
B	PRO	Procedural
B	PHY	Physical

The Risk Assessors decided that the list of threats was sufficiently comprehensive for the risk assessment, but advise that future risk assessments review the list. Not all threats were selected for the assessment as they were deemed out of scope in accordance with the Security Reference Material. The threats included are as follows:

	Threats included in the assessment
REF	**Attack method / threat**
CoF1	Abuse of rights
PHY2	Blockade of Facilities
CoF4	Breach of personnel availability
CoI7	Data from untrustworthy sources
INFF9	Data Manipulation
CoF3	Denial of actions
INF19	Denial of Service Attack
Rad3	Electromagnetic pulses
Rad1	Electromagnetic radiation
LoES3	Failure of telecommunication equipment
PRO2	Failure of Third Party Service Provision
CoF2	Forging of rights
INFF6	Hackers / Social Engineering
PHY3	Indirect Disruptive Events
CoI1	Interception of compromising interference signals
INFF10	Network/VPN Separation Corruption

INFF12	Radio Spoofing
CoI8	Tampering with hardware
CoI9	Tampering with software
PHY4	Theft/Fraud and Criminal Damage
Rad2	Thermal radiation
INFF8	Viruses Malware Trojans etc.

Threats were excluded from the analysis if they were from natural causes (water damage), extreme events (IED, major disasters) or not felt to be relevant to the concept (disclosure, eavesdropping). Whilst these threats are relevant in the eventual deployment of the concept, assessment of them was not thought to add greatly to the concept requirements at this stage of development (SESAR development phase).

It is however recommended that the excluded threats are taken into consideration in deployment risk assessments in accordance with operators' Security Management System processes.

	Threats excluded in the assessment
REF	**Attack method / threat**
TEC2	Breach of information system maintainability
UA4	Corruption of data
PHD5	Destruction of equipment or media
CoI6	Disclosure
CoI3	Eavesdropping
LoES1	Failure of air-conditioning or water supply system
PHD1	Fire
UA2	Fraudulent copying of software
UA5	Illegal processing of data
PHY1	Improvised Explosive Devices (IED)
PRO6	Inadequate Contingency Arrangements
PHY6	Kidnapping / Hostage Taking
PHY9	Legislative / Regulatory Non Compliance
LoES2	Loss of power supply
PHY12	Major Disasters
CoI10	Position detection
CoI2	Remote spying
CoI5	Retrieval of recycled or discarded media
TEC1	Saturation of the information system
PHY5	Standoff Attack
CoI4	Theft of equipment
CoI3	Theft of media or documents
UA1	Unauthorized use of equipment
UA3	Use of counterfeit or copied software
PHD2	Water damage

3.2 Threat scenarios

The threats identified in the previous section have been applied to the supporting assets to create threat scenarios. These link threats to supporting assets, and thereby primary assets, and whether the threat may cause a loss of C,I or A. As the threat scenarios table is large and is an interim step in defining the risks it is not shown in this document.

4 Risk evaluation

Risk comprises the likelihood and impact of a potential threat.

4.1 Impact evaluation

In accordance with the Security Risk Assessment Methodology, the impact of a loss of Confidentiality, Integrity or Availability is inherited by the supporting assets of each primary asset. There is also the facility to revise the inherited impact through a 'reviewed impact'. In this assessment the reviewed impact has been made equal to the inherited impact. It is notable that the threat scenarios generally have the highest level of impact, as the impact is predominantly inherited from safety and capacity impact areas.

To avoid duplication in this report, the threat scenarios are shown in section 4.3 as part of the risk table.

4.2 Likelihood evaluation

Each threat scenario has been assessed according to its likelihood of occurrence, based on a qualitative scale of 1 – 5, where 5 is 'certain' and '1' is 'very unlikely'.

4.3 Risk level evaluation

Combining impact and likelihood results in the following table of risks:

Ref.	Supporting Assets	Threats	Reviewed Impact	Likelihood	Risk level
SA1.1	Client (Controller) Working Position - RTC unit	Abuse of rights	5	2	High
SA1.1	Client (Controller) Working Position - RTC unit	Electromagnetic pulses	5	1	Medium
SA1.1	Client (Controller) Working Position - RTC unit	Forging of rights	5	3	High
SA1.1	Client (Controller) Working Position - RTC unit	Hackers / Social Engineering	5	3	High
SA1.1	Client (Controller) Working Position - RTC unit	Indirect Disruptive Events	5	2	High
SA1.1	Client (Controller) Working Position - RTC unit	Tampering with hardware	5	2	High
SA1.1	Client (Controller) Working Position - RTC unit	Tampering with software	5	3	High
SA1.1	Client (Controller) Working Position - RTC unit	Theft/Fraud and Criminal Damage	5	1	Medium
SA1.1	Client (Controller) Working Position - RTC unit	Viruses Malware Trojans etc.	5	3	High
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit	Abuse of rights	5	2	High
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit	Electromagnetic pulses	5	1	Medium

Ref.	Supporting Assets	Threats	Reviewed Impact	Likelihood	Risk level
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit	Forging of rights	5	3	High
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit	Hackers / Social Engineering	5	3	High
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit	Indirect Disruptive Events	5	2	High
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit	Tampering with software	5	3	High
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit	Theft/Fraud and Criminal Damage	5	1	Medium
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit	Viruses Malware Trojans etc.	5	3	High
SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit	Electromagnetic pulses	5	1	Medium
SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit	Failure of telecommunication equipment	5	3	High
SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit	Failure of Third Party Service Provision	5	4	High
SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit	Indirect Disruptive Events	5	2	High

Ref.	Supporting Assets	Threats	Reviewed Impact	Likelihood	Risk level
SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit	Tampering with hardware	5	2	High
SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit	Theft/Fraud and Criminal Damage	5	1	Medium
SA1.1.1.2	Servers for visualization - RTC unit	Abuse of rights	5	2	High
SA1.1.1.2	Servers for visualization - RTC unit	Electromagnetic pulses	5	1	Medium
SA1.1.1.2	Servers for visualization - RTC unit	Forging of rights	5	2	High
SA1.1.1.2	Servers for visualization - RTC unit	Hackers / Social Engineering	5	3	High
SA1.1.1.2	Servers for visualization - RTC unit	Indirect Disruptive Events	5	2	High
SA1.1.1.2	Servers for visualization - RTC unit	Tampering with software	5	3	High
SA1.1.1.2	Servers for visualization - RTC unit	Theft/Fraud and Criminal Damage	5	1	Medium
SA1.1.1.2	Servers for visualization - RTC unit	Viruses Malware Trojans etc.	5	3	High
SA1.1.1.3	ATC and voice data recording - RTC unit	Abuse of rights	4	2	Medium
SA1.1.1.3	ATC and voice data recording - RTC unit	Electromagnetic pulses	4	1	Medium
SA1.1.1.3	ATC and voice data recording - RTC unit	Electromagnetic radiation	4	2	Medium
SA1.1.1.3	ATC and voice data recording - RTC unit	Forging of rights	4	2	Medium
SA1.1.1.3	ATC and voice data recording - RTC unit	Hackers / Social Engineering	4	3	High
SA1.1.1.3	ATC and voice data recording - RTC unit	Indirect Disruptive Events	4	2	Medium
SA1.1.1.3	ATC and voice data recording - RTC unit	Tampering with hardware	4	2	Medium
SA1.1.1.3	ATC and voice data recording - RTC unit	Tampering with software	4	3	High
SA1.1.1.3	ATC and voice data recording - RTC unit	Theft/Fraud and Criminal Damage	4	1	Medium
SA1.1.1.3	ATC and voice data recording - RTC unit	Viruses Malware Trojans etc.	4	3	High
SA1.1.2	OTW display - RTC unit	Electromagnetic pulses	5	1	Medium
SA1.1.2	OTW display - RTC unit	Indirect Disruptive Events	5	2	High
SA1.1.2	OTW display - RTC unit	Tampering with hardware	5	2	High
SA1.1.2	OTW display - RTC unit	Tampering with software	5	2	High
SA1.1.2	OTW display - RTC unit	Theft/Fraud and Criminal Damage	5	1	Medium

Ref.	Supporting Assets	Threats	Reviewed Impact	Likelihood	Risk level
SA1.1.2	OTW display - RTC unit	Viruses Malware Trojans etc.	5	3	High
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit	Abuse of rights	5	2	High
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit	Electromagnetic pulses	5	1	Medium
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit	Forging of rights	5	2	High
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit	Hackers / Social Engineering	5	3	High
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit	Indirect Disruptive Events	5	3	High
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit	Tampering with software	5	3	High
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit	Viruses Malware Trojans etc.	5	3	High
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit	Abuse of rights	5	2	High
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit	Electromagnetic pulses	5	1	Medium
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit	Forging of rights	5	3	High
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit	Hackers / Social Engineering	5	3	High
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit	Indirect Disruptive Events	5	2	High
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit	Tampering with hardware	5	2	High
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit	Tampering with software	5	3	High

Ref.	Supporting Assets	Threats	Reviewed Impact	Likelihood	Risk level
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit	Theft/Fraud and Criminal Damage	5	1	Medium
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit	Viruses Malware Trojans etc.	5	3	High
SA1.1.3	OTW audio presentation - RTC unit	Electromagnetic pulses	3	1	Low
SA1.1.3	OTW audio presentation - RTC unit	Indirect Disruptive Events	3	2	Low
SA1.1.3	OTW audio presentation - RTC unit	Tampering with hardware	3	2	Low
SA1.1.3	OTW audio presentation - RTC unit	Tampering with software	3	3	Medium
SA1.1.3	OTW audio presentation - RTC unit	Theft/Fraud and Criminal Damage	3	1	Low
SA1.1.3	OTW audio presentation - RTC unit	Viruses Malware Trojans etc.	3	3	Medium
SA1.1.5	Display screens other than OTW - RTC unit	Electromagnetic pulses	5	1	Medium
SA1.1.5	Display screens other than OTW - RTC unit	Indirect Disruptive Events	5	2	High
SA1.1.5	Display screens other than OTW - RTC unit	Tampering with hardware	5	2	High
SA1.1.5	Display screens other than OTW - RTC unit	Theft/Fraud and Criminal Damage	5	1	Medium
SA1.2	Wide-Area Network link - RTC unit	Electromagnetic pulses	5	1	Medium
SA1.2	Wide-Area Network link - RTC unit	Failure of telecommunication equipment	5	3	High
SA1.2	Wide-Area Network link - RTC unit	Failure of Third Party Service Provision	5	4	High
SA1.2	Wide-Area Network link - RTC unit	Hackers / Social Engineering	5	3	High
SA1.2	Wide-Area Network link - RTC unit	Indirect Disruptive Events	5	2	High
SA1.2	Wide-Area Network link - RTC unit	Network/VPN Separation Corruption	5	3	High
SA1.2	Wide-Area Network link - RTC unit	Theft/Fraud and Criminal Damage	5	1	Medium
SA2	FIS for display and update of met and operational flight information - Local unit	Abuse of rights	5	2	High
SA2	FIS for display and update of met and operational flight information - Local unit	Electromagnetic pulses	5	1	Medium
SA2	FIS for display and update of met and operational flight information - Local unit	Forging of rights	5	3	High
SA2	FIS for display and update of met and operational flight information - Local unit	Hackers / Social Engineering	5	3	High
SA2	FIS for display and update of met and operational flight	Indirect Disruptive Events	5	3	High

Ref.	Supporting Assets	Threats	Reviewed Impact	Likelihood	Risk level
	information - Local unit				
SA2	FIS for display and update of met and operational flight information - Local unit	Tampering with hardware	5	3	High
SA2	FIS for display and update of met and operational flight information - Local unit	Tampering with software	5	3	High
SA2	FIS for display and update of met and operational flight information - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA2	FIS for display and update of met and operational flight information - Local unit	Viruses Malware Trojans etc.	5	3	High
SA5	Personnel - RTC unit	Blockade of Facilities	5	2	High
SA5	Personnel - RTC unit	Breach of personnel availability	5	3	High
SA5	Personnel - RTC unit	Hackers / Social Engineering	5	3	High
SA5	Personnel - RTC unit	Theft/Fraud and Criminal Damage	5	1	Medium
SA5.2	Airport personnel (dedicated to ROT operations) - Local unit	Blockade of Facilities	5	2	High
SA5.2	Airport personnel (dedicated to ROT operations) - Local unit	Breach of personnel availability	5	3	High
SA5.2	Airport personnel (dedicated to ROT operations) - Local unit	Hackers / Social Engineering	5	3	High
SA5.2	Airport personnel (dedicated to ROT operations) - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA5.2.1	Technician/Engineers - Local unit	Blockade of Facilities	5	2	High
SA5.2.1	Technician/Engineers - Local unit	Breach of personnel availability	5	3	High
SA5.2.1	Technician/Engineers - Local unit	Hackers / Social Engineering	5	3	High
SA5.2.1	Technician/Engineers - Local unit	Indirect Disruptive Events	5	1	Medium
SA5.2.1	Technician/Engineers - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit	Electromagnetic pulses	3	1	Low
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit	Indirect Disruptive Events	3	3	Medium
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit	Tampering with hardware	3	3	Medium

Ref.	Supporting Assets	Threats	Reviewed Impact	Likelihood	Risk level
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit	Tampering with software	3	3	Medium
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit	Theft/Fraud and Criminal Damage	3	2	Low
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit	Viruses Malware Trojans etc.	3	3	Medium
SA9.1	A/D visualisation system - Camera "N" - Local unit	Abuse of rights	5	2	High
SA9.1	A/D visualisation system - Camera "N" - Local unit	Data from untrustworthy sources	5	3	High
SA9.1	A/D visualisation system - Camera "N" - Local unit	Denial of Service Attack	5	3	High
SA9.1	A/D visualisation system - Camera "N" - Local unit	Electromagnetic pulses	5	1	Medium
SA9.1	A/D visualisation system - Camera "N" - Local unit	Electromagnetic radiation	5	3	High
SA9.1	A/D visualisation system - Camera "N" - Local unit	Hackers / Social Engineering	5	3	High
SA9.1	A/D visualisation system - Camera "N" - Local unit	Indirect Disruptive Events	5	3	High
SA9.1	A/D visualisation system - Camera "N" - Local unit	Tampering with hardware	5	3	High
SA9.1	A/D visualisation system - Camera "N" - Local unit	Tampering with software	5	3	High
SA9.1	A/D visualisation system - Camera "N" - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA9.1	A/D visualisation system - Camera "N" - Local unit	Viruses Malware Trojans etc.	5	3	High
SA10	Binocular View - Local unit	Abuse of rights	5	2	High
SA10	Binocular View - Local unit	Electromagnetic pulses	5	1	Medium
SA10	Binocular View - Local unit	Electromagnetic radiation	5	3	High
SA10	Binocular View - Local unit	Hackers / Social Engineering	5	3	High
SA10	Binocular View - Local unit	Indirect Disruptive Events	5	3	High
SA10	Binocular View - Local unit	Tampering with hardware	5	3	High
SA10	Binocular View - Local unit	Tampering with software	5	3	High
SA10	Binocular View - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA10	Binocular View - Local unit	Viruses Malware Trojans etc.	5	3	High
SA10.1	PTZ Unit - Local unit	Abuse of rights	5	2	High
SA10.1	PTZ Unit - Local unit	Electromagnetic	5	1	Medium

Ref.	Supporting Assets	Threats	Reviewed Impact	Likelihood	Risk level
		pulses			
SA10.1	PTZ Unit - Local unit	Hackers / Social Engineering	5	3	High
SA10.1	PTZ Unit - Local unit	Indirect Disruptive Events	5	3	High
SA10.1	PTZ Unit - Local unit	Tampering with hardware	5	3	High
SA10.1	PTZ Unit - Local unit	Tampering with software	5	3	High
SA10.1	PTZ Unit - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA10.1	PTZ Unit - Local unit	Viruses Malware Trojans etc.	5	3	High
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit	Abuse of rights	5	2	High
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit	Electromagnetic pulses	5	1	Medium
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit	Forging of rights	5	3	High
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit	Hackers / Social Engineering	5	3	High
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit	Indirect Disruptive Events	5	2	High
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit	Tampering with software	5	3	High
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit	Theft/Fraud and Criminal Damage	5	1	Medium
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit	Viruses Malware Trojans etc.	5	3	High
SA11.1	Telephone landlines (not AFTN) - Local unit	Electromagnetic pulses	5	1	Medium
SA11.1	Telephone landlines (not AFTN) - Local unit	Failure of telecommunication equipment	5	3	High
SA11.1	Telephone landlines (not AFTN) - Local unit	Indirect Disruptive Events	5	3	High
SA11.1	Telephone landlines (not AFTN) - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA17	Data Concentrator (APT) - Local unit	Abuse of rights	5	2	High
SA17	Data Concentrator (APT) - Local unit	Electromagnetic pulses	5	1	Medium
SA17	Data Concentrator (APT) - Local unit	Hackers / Social Engineering	5	3	High
SA17	Data Concentrator (APT) - Local unit	Indirect Disruptive Events	5	3	High

Ref.	Supporting Assets	Threats	Reviewed Impact	Likelihood	Risk level
SA17	Data Concentrator (APT) - Local unit	Tampering with hardware	5	3	High
SA17	Data Concentrator (APT) - Local unit	Tampering with software	5	3	High
SA17	Data Concentrator (APT) - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA17	Data Concentrator (APT) - Local unit	Viruses Malware Trojans etc.	5	3	High
SA18	Radio Gateway (APT) - Local unit	Abuse of rights	5	2	High
SA18	Radio Gateway (APT) - Local unit	Electromagnetic pulses	5	1	Medium
SA18	Radio Gateway (APT) - Local unit	Failure of telecommunication equipment	5	3	High
SA18	Radio Gateway (APT) - Local unit	Hackers / Social Engineering	5	3	High
SA18	Radio Gateway (APT) - Local unit	Indirect Disruptive Events	5	3	High
SA18	Radio Gateway (APT) - Local unit	Tampering with hardware	5	3	High
SA18	Radio Gateway (APT) - Local unit	Tampering with software	5	3	High
SA18	Radio Gateway (APT) - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA18	Radio Gateway (APT) - Local unit	Viruses Malware Trojans etc.	5	3	High
SA19	Contingency VCS (APT) - Local unit	Abuse of rights	5	2	High
SA19	Contingency VCS (APT) - Local unit	Electromagnetic pulses	5	1	Medium
SA19	Contingency VCS (APT) - Local unit	Hackers / Social Engineering	5	3	High
SA19	Contingency VCS (APT) - Local unit	Indirect Disruptive Events	5	3	High
SA19	Contingency VCS (APT) - Local unit	Tampering with hardware	5	3	High
SA19	Contingency VCS (APT) - Local unit	Tampering with software	5	3	High
SA19	Contingency VCS (APT) - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA19	Contingency VCS (APT) - Local unit	Viruses Malware Trojans etc.	5	3	High
SA20	Specific Protocol converters (APT) - Local unit	Abuse of rights	5	2	High
SA20	Specific Protocol converters (APT) - Local unit	Electromagnetic pulses	5	1	Medium
SA20	Specific Protocol converters (APT) - Local unit	Hackers / Social Engineering	5	3	High
SA20	Specific Protocol converters (APT) - Local unit	Indirect Disruptive Events	5	3	High

Ref.	Supporting Assets	Threats	Reviewed Impact	Likelihood	Risk level
SA20	Specific Protocol converters (APT) - Local unit	Tampering with software	5	3	High
SA20	Specific Protocol converters (APT) - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA20	Specific Protocol converters (APT) - Local unit	Viruses Malware Trojans etc.	5	3	High
SA21	Local Network infrastructure (APT) - Local unit	Electromagnetic pulses	5	1	Medium
SA21	Local Network infrastructure (APT) - Local unit	Failure of telecommunication equipment	5	3	High
SA21	Local Network infrastructure (APT) - Local unit	Indirect Disruptive Events	5	3	High
SA21	Local Network infrastructure (APT) - Local unit	Tampering with hardware	5	3	High
SA21	Local Network infrastructure (APT) - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA22	Monitoring proxy/node (APT) - Local unit	Abuse of rights	5	2	High
SA22	Monitoring proxy/node (APT) - Local unit	Electromagnetic pulses	5	1	Medium
SA22	Monitoring proxy/node (APT) - Local unit	Hackers / Social Engineering	5	3	High
SA22	Monitoring proxy/node (APT) - Local unit	Indirect Disruptive Events	5	3	High
SA22	Monitoring proxy/node (APT) - Local unit	Tampering with hardware	5	3	High
SA22	Monitoring proxy/node (APT) - Local unit	Tampering with software	5	3	High
SA22	Monitoring proxy/node (APT) - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA22	Monitoring proxy/node (APT) - Local unit	Viruses Malware Trojans etc.	5	3	High
SA25	Technical supervision (s/w) tool - RTC unit	Abuse of rights	5	2	High
SA25	Technical supervision (s/w) tool - RTC unit	Electromagnetic pulses	5	1	Medium
SA25	Technical supervision (s/w) tool - RTC unit	Forging of rights	5	3	High
SA25	Technical supervision (s/w) tool - RTC unit	Hackers / Social Engineering	5	3	High
SA25	Technical supervision (s/w) tool - RTC unit	Indirect Disruptive Events	5	2	High
SA25	Technical supervision (s/w) tool - RTC unit	Tampering with software	5	3	High
SA25	Technical supervision (s/w) tool - RTC unit	Theft/Fraud and Criminal Damage	5	1	Medium
SA25	Technical supervision (s/w) tool - RTC unit	Viruses Malware Trojans etc.	5	3	High

Ref.	Supporting Assets	Threats	Reviewed Impact	Likelihood	Risk level
SA28	Aerodrome equipment communications network - Local unit	Abuse of rights	5	2	High
SA28	Aerodrome equipment communications network - Local unit	Electromagnetic pulses	5	1	Medium
SA28	Aerodrome equipment communications network - Local unit	Electromagnetic radiation	5	3	High
SA28	Aerodrome equipment communications network - Local unit	Failure of telecommunication equipment	5	3	High
SA28	Aerodrome equipment communications network - Local unit	Forging of rights	5	3	High
SA28	Aerodrome equipment communications network - Local unit	Hackers / Social Engineering	5	3	High
SA28	Aerodrome equipment communications network - Local unit	Indirect Disruptive Events	5	3	High
SA28	Aerodrome equipment communications network - Local unit	Tampering with hardware	5	3	High
SA28	Aerodrome equipment communications network - Local unit	Theft/Fraud and Criminal Damage	5	2	High
SA1.2.1	WAN connection - Local unit	Electromagnetic pulses	5	1	Medium
SA1.2.1	WAN connection - Local unit	Failure of telecommunication equipment	5	3	High
SA1.2.1	WAN connection - Local unit	Indirect Disruptive Events	5	3	High
SA1.2.1	WAN connection - Local unit	Theft/Fraud and Criminal Damage	5	2	High

1 Risk treatment

4.4 Introduction

The risk treatment options are (a) accept/tolerate, (b) reduce/treat, (c) avoid/terminate, (d) transfer. The risk assessors consider that the identified risks are too great to be tolerated and cannot be transferred. Furthermore, validation work to date has shown a viable concept without unmanageable security concerns. The conclusion is that all of the risks identified should be treated through the application of controls.

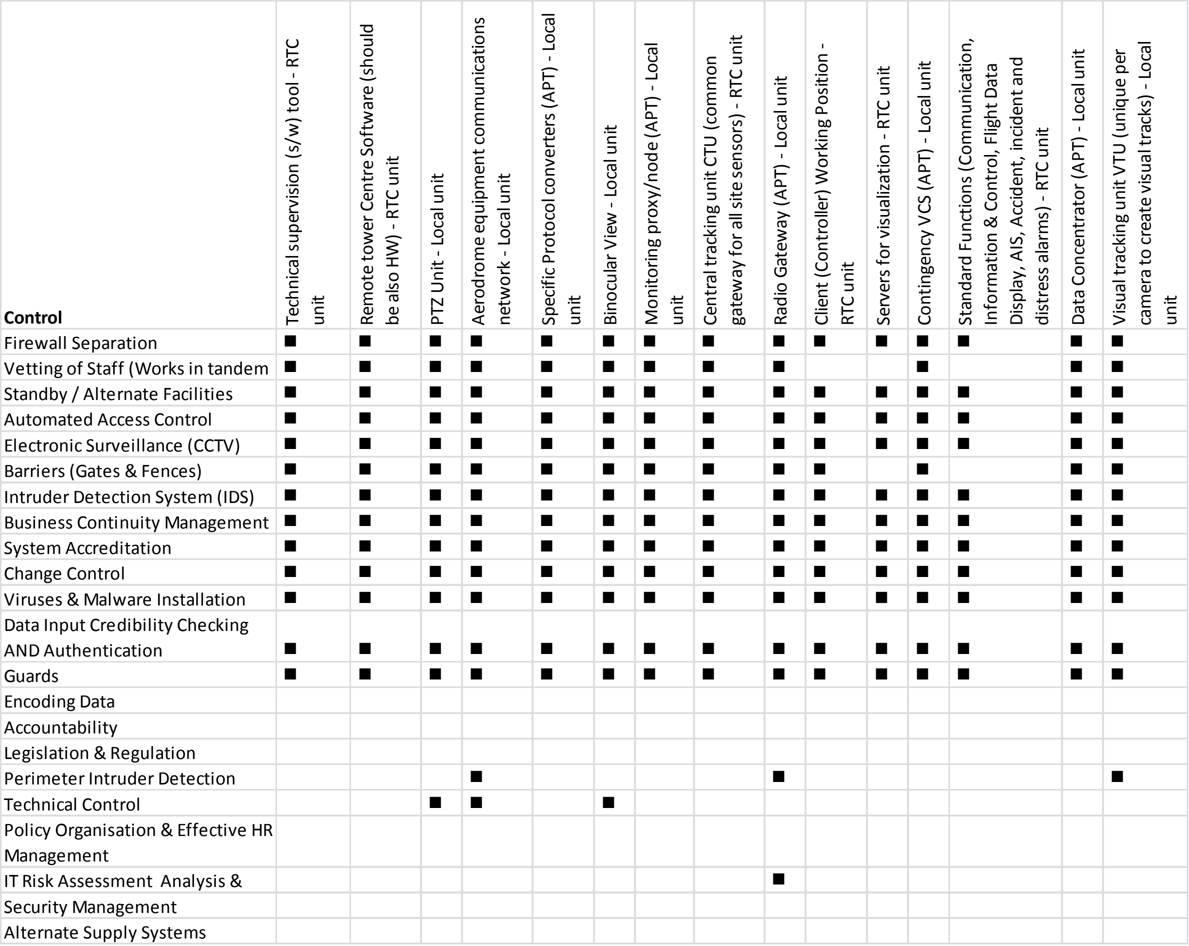
5 Control selection

The detailed approach of this assessment has led to a large set of threat scenarios and possible control strategies. A ‘defence in depth’ approach has been taken, with each threat scenario having multiple controls applied as determined by the assessors. It should be noted that as the SecRAM produces a qualitative assessment, there is not mechanism for estimating the likely decrease in risk following the application of a control. Therefore the assessors have made their own judgements as to how the risks should be reduced to ‘low’ from ‘medium’ or ‘high’.

The following figure shows a mapping of controls to supporting assets, where it can be seen that many of the controls apply across the range of assets analysed. This is to be expected as many of the threats concern access to an asset, with control options centred around restricting access to authentic persons only. Thus the assessment establishes the controls needed for each supporting asset, however in many cases the same control applied at the Unit (Aerodrome or ROT facility) level provides sufficient protection. For example a perimeter fence with effective access control, staff vetting, segregated IT systems and controlled system access would protect a wide range of supporting assets. Thus the approach is one of detailed asset analysis followed by ‘rolling up’ to find common controls that can be applied at the Unit or system level, followed by a check against the detailed assessment to establish remaining supporting asset specific controls.

Due to the large number of control-supporting asset pairs, the results of the assessment have been organised as which controls should be applied to which assets. In this sense, the two following figures show that 22 controls have been recommended to be applied to sub-sets of 30 assets in total.

Figure 2: Mapping of controls to supporting assets (1 of 2)



Control	Technical supervision (s/w) tool - RTC unit	Remote tower Centre Software (should be also HW) - RTC unit	PTZ Unit - Local unit	Aerodrome equipment communications network - Local unit	Specific Protocol converters (APT) - Local unit	Binocular View - Local unit	Monitoring proxy/node (APT) - Local unit	Central tracking unit CTU (common gateway for all site sensors) - RTC unit	Radio Gateway (APT) - Local unit	Client (Controller) Working Position - RTC unit	Servers for visualization - RTC unit	Contingency VCS (APT) - Local unit	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit	Data Concentrator (APT) - Local unit	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
Firewall Separation	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Vetting of Staff (Works in tandem	■	■	■	■	■	■	■	■	■			■		■	■
Standby / Alternate Facilities	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Automated Access Control	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Electronic Surveillance (CCTV)	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Barriers (Gates & Fences)	■	■	■	■	■	■	■	■	■	■		■		■	■
Intruder Detection System (IDS)	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Business Continuity Management	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
System Accreditation	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Change Control	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Viruses & Malware Installation	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Data Input Credibility Checking AND Authentication	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Guards	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Encoding Data															
Accountability															
Legislation & Regulation															
Perimeter Intruder Detection				■					■						■
Technical Control			■	■		■									
Policy Organisation & Effective HR Management															
IT Risk Assessment Analysis &									■						
Security Management															
Alternate Supply Systems															

Figure 3: Mapping of controls to supporting assets (2 of 2)

Control	FIS for display and update of met and operational flight information - Local unit	A/D visualisation system - Camera "N" - Local unit	ATC and voice data recording - RTC unit	Telephone landlines (not AFTN) - Local unit	Personnel - RTC unit	WAN connection - Local unit	Wide-Area Network link - RTC unit	Local Network infrastructure (APT) - Local unit	Technician/Engineers - Local unit	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit	Airport personnel (dedicated to ROT operations) - Local unit	Display screens other than OTW - RTC unit	OTW audio presentation - RTC unit	OTW display - RTC unit
Firewall Separation	■	■	■				■								
Vetting of Staff (Works in tandem with PE22)	■	■		■	■	■	■	■	■	■		■	■	■	
Standby / Alternate Facilities	■	■	■	■		■	■	■		■	■		■	■	■
Automated Access Control System (AACS)	■	■	■	■		■	■	■		■	■		■	■	■
Electronic Surveillance (CCTV)	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Barriers (Gates & Fences)	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Intruder Detection System (IDS)	■	■	■		■	■	■	■		■	■		■	■	■
Business Continuity Management	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
System Accreditation	■	■	■				■				■				
Change Control	■	■	■												
Viruses & Malware Installation and Patches	■	■	■	■		■	■	■		■	■		■	■	■
Data Input Credibility Checking AND Authentication	■	■	■												
Guards	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Encoding Data		■					■								
Accountability							■				■				
Legislation & Regulation					■				■			■			
Perimeter Intruder Detection System (PIDS)		■		■		■	■	■	■	■	■	■			
Technical Control		■	■							■					
Policy Organisation & Effective HR Management					■				■			■			
IT Risk Assessment Analysis & Application															
Security Management		■													
Alternate Supply Systems				■	■		■	■	■		■	■			

The recommended controls have been organised in the following format for each sub-section:

"[control X] to be applied to the following supporting assets".

Following the list of controls below, section 6 proposes some refinements to the list to simplify the requirements specification.

1.1 Accountability to be applied to the following supporting assets

SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit
SA1.2	Wide-Area Network link - RTC unit

1.2 Alternate Supply Systems to be applied to the following supporting assets

SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit
SA1.2	Wide-Area Network link - RTC unit
SA11.1	Telephone landlines (not AFTN) - Local unit
SA21	Local Network infrastructure (APT) - Local unit
SA5	Personnel - RTC unit
SA5.2	Airport personnel (dedicated to ROT operations) - Local unit
SA5.2.1	Technician/Engineers - Local unit

1.3 Automated Access Control System (AACS) to be applied to the following supporting assets

SA1.1	Client (Controller) Working Position - RTC unit
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit
SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit
SA1.1.1.2	Servers for visualization - RTC unit
SA1.1.1.3	ATC and voice data recording - RTC unit
SA1.1.2	OTW display - RTC unit
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit
SA1.1.3	OTW audio presentation - RTC unit
SA1.1.5	Display screens other than OTW - RTC unit

SA1.2	Wide-Area Network link - RTC unit
SA1.2.1	WAN connection - Local unit
SA10	Binocular View - Local unit
SA10.1	PTZ Unit - Local unit
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit
SA11.1	Telephone landlines (not AFTN) - Local unit
SA17	Data Concentrator (APT) - Local unit
SA18	Radio Gateway (APT) - Local unit
SA19	Contingency VCS (APT) - Local unit
SA2	FIS for display and update of met and operational flight information - Local unit
SA20	Specific Protocol converters (APT) - Local unit
SA21	Local Network infrastructure (APT) - Local unit
SA22	Monitoring proxy/node (APT) - Local unit
SA25	Technical supervision (s/w) tool - RTC unit
SA28	Aerodrome equipment communications network - Local unit
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.4 Barriers (Gates & Fences) to be applied to the following supporting assets

SA1.1	Client (Controller) Working Position - RTC unit
SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit
SA1.1.1.3	ATC and voice data recording - RTC unit
SA1.1.2	OTW display - RTC unit
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit
SA1.1.3	OTW audio presentation - RTC unit
SA1.1.5	Display screens other than OTW - RTC unit
SA1.2	Wide-Area Network link - RTC unit
SA1.2.1	WAN connection - Local unit
SA10	Binocular View - Local unit
SA10.1	PTZ Unit - Local unit
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit
SA11.1	Telephone landlines (not AFTN) - Local unit
SA17	Data Concentrator (APT) - Local unit
SA18	Radio Gateway (APT) - Local unit
SA19	Contingency VCS (APT) - Local unit
SA2	FIS for display and update of met and operational flight information - Local unit

SA20	Specific Protocol converters (APT) - Local unit
SA21	Local Network infrastructure (APT) - Local unit
SA22	Monitoring proxy/node (APT) - Local unit
SA25	Technical supervision (s/w) tool - RTC unit
SA28	Aerodrome equipment communications network - Local unit
SA5	Personnel - RTC unit
SA5.2	Airport personnel (dedicated to ROT operations) - Local unit
SA5.2.1	Technician/Engineers - Local unit
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.5 Business Continuity Management to be applied to the following supporting assets

SA1.1	Client (Controller) Working Position - RTC unit
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit
SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit
SA1.1.1.2	Servers for visualization - RTC unit
SA1.1.1.3	ATC and voice data recording - RTC unit
SA1.1.2	OTW display - RTC unit
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit
SA1.1.3	OTW audio presentation - RTC unit
SA1.1.5	Display screens other than OTW - RTC unit
SA1.2	Wide-Area Network link - RTC unit
SA1.2.1	WAN connection - Local unit
SA10	Binocular View - Local unit
SA10.1	PTZ Unit - Local unit
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit
SA11.1	Telephone landlines (not AFTN) - Local unit
SA17	Data Concentrator (APT) - Local unit
SA18	Radio Gateway (APT) - Local unit
SA19	Contingency VCS (APT) - Local unit
SA2	FIS for display and update of met and operational flight information - Local unit
SA20	Specific Protocol converters (APT) - Local unit
SA21	Local Network infrastructure (APT) - Local unit
SA22	Monitoring proxy/node (APT) - Local unit
SA25	Technical supervision (s/w) tool - RTC unit

SA28	Aerodrome equipment communications network - Local unit
SA5	Personnel - RTC unit
SA5.2	Airport personnel (dedicated to ROT operations) - Local unit
SA5.2.1	Technician/Engineers - Local unit
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.6 Change Control to be applied to the following supporting assets

SA1.1	Client (Controller) Working Position - RTC unit
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit
SA1.1.1.2	Servers for visualization - RTC unit
SA1.1.1.3	ATC and voice data recording - RTC unit
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit
SA10	Binocular View - Local unit
SA10.1	PTZ Unit - Local unit
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit
SA17	Data Concentrator (APT) - Local unit
SA18	Radio Gateway (APT) - Local unit
SA19	Contingency VCS (APT) - Local unit
SA2	FIS for display and update of met and operational flight information - Local unit
SA20	Specific Protocol converters (APT) - Local unit
SA22	Monitoring proxy/node (APT) - Local unit
SA25	Technical supervision (s/w) tool - RTC unit
SA28	Aerodrome equipment communications network - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.7 Data Input Credibility Checking AND Authentication to be applied to the following supporting assets

SA1.1	Client (Controller) Working Position - RTC unit
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit
SA1.1.1.2	Servers for visualization - RTC unit
SA1.1.1.3	ATC and voice data recording - RTC unit
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit

SA10	Binocular View - Local unit
SA10.1	PTZ Unit - Local unit
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit
SA17	Data Concentrator (APT) - Local unit
SA18	Radio Gateway (APT) - Local unit
SA19	Contingency VCS (APT) - Local unit
SA2	FIS for display and update of met and operational flight information - Local unit
SA20	Specific Protocol converters (APT) - Local unit
SA22	Monitoring proxy/node (APT) - Local unit
SA25	Technical supervision (s/w) tool - RTC unit
SA28	Aerodrome equipment communications network - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.8 Electronic Surveillance (CCTV) to be applied to the following supporting assets

SA1.1	Client (Controller) Working Position - RTC unit
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit
SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit
SA1.1.1.2	Servers for visualization - RTC unit
SA1.1.1.3	ATC and voice data recording - RTC unit
SA1.1.2	OTW display - RTC unit
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit
SA1.1.3	OTW audio presentation - RTC unit
SA1.1.5	Display screens other than OTW - RTC unit
SA1.2	Wide-Area Network link - RTC unit
SA1.2.1	WAN connection - Local unit
SA10	Binocular View - Local unit
SA10.1	PTZ Unit - Local unit
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit
SA11.1	Telephone landlines (not AFTN) - Local unit
SA17	Data Concentrator (APT) - Local unit
SA18	Radio Gateway (APT) - Local unit
SA19	Contingency VCS (APT) - Local unit
SA2	FIS for display and update of met and operational flight information - Local unit
SA20	Specific Protocol converters (APT) - Local unit
SA21	Local Network infrastructure (APT) - Local unit

SA22	Monitoring proxy/node (APT) - Local unit
SA25	Technical supervision (s/w) tool - RTC unit
SA28	Aerodrome equipment communications network - Local unit
SA5	Personnel - RTC unit
SA5.2	Airport personnel (dedicated to ROT operations) - Local unit
SA5.2.1	Technician/Engineers - Local unit
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.9 Encoding Data to be applied to the following supporting assets

SA1.2	Wide-Area Network link - RTC unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.10 Firewall Separation to be applied to the following supporting assets

SA1.1	Client (Controller) Working Position - RTC unit
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit
SA1.1.1.2	Servers for visualization - RTC unit
SA1.1.1.3	ATC and voice data recording - RTC unit
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit
SA1.2	Wide-Area Network link - RTC unit
SA10	Binocular View - Local unit
SA10.1	PTZ Unit - Local unit
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit
SA17	Data Concentrator (APT) - Local unit
SA18	Radio Gateway (APT) - Local unit
SA19	Contingency VCS (APT) - Local unit
SA2	FIS for display and update of met and operational flight information - Local unit
SA20	Specific Protocol converters (APT) - Local unit
SA22	Monitoring proxy/node (APT) - Local unit
SA25	Technical supervision (s/w) tool - RTC unit
SA28	Aerodrome equipment communications network - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.11 Guards to be applied to the following supporting assets

SA1.1	Client (Controller) Working Position - RTC unit
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit
SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit
SA1.1.1.2	Servers for visualization - RTC unit
SA1.1.1.3	ATC and voice data recording - RTC unit
SA1.1.2	OTW display - RTC unit
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit
SA1.1.3	OTW audio presentation - RTC unit
SA1.1.5	Display screens other than OTW - RTC unit
SA1.2	Wide-Area Network link - RTC unit
SA1.2.1	WAN connection - Local unit
SA10	Binocular View - Local unit
SA10.1	PTZ Unit - Local unit
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit
SA11.1	Telephone landlines (not AFTN) - Local unit
SA17	Data Concentrator (APT) - Local unit
SA18	Radio Gateway (APT) - Local unit
SA19	Contingency VCS (APT) - Local unit
SA2	FIS for display and update of met and operational flight information - Local unit
SA20	Specific Protocol converters (APT) - Local unit
SA21	Local Network infrastructure (APT) - Local unit
SA22	Monitoring proxy/node (APT) - Local unit
SA25	Technical supervision (s/w) tool - RTC unit
SA28	Aerodrome equipment communications network - Local unit
SA5	Personnel - RTC unit
SA5.2	Airport personnel (dedicated to ROT operations) - Local unit
SA5.2.1	Technician/Engineers - Local unit
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.12 Intruder Detection System (IDS) to be applied to the following supporting assets

SA1.1	Client (Controller) Working Position - RTC unit

SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit
SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit
SA1.1.1.2	Servers for visualization - RTC unit
SA1.1.1.3	ATC and voice data recording - RTC unit
SA1.1.2	OTW display - RTC unit
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit
SA1.1.3	OTW audio presentation - RTC unit
SA1.1.5	Display screens other than OTW - RTC unit
SA1.2	Wide-Area Network link - RTC unit
SA1.2.1	WAN connection - Local unit
SA10	Binocular View - Local unit
SA10.1	PTZ Unit - Local unit
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit
SA17	Data Concentrator (APT) - Local unit
SA18	Radio Gateway (APT) - Local unit
SA19	Contingency VCS (APT) - Local unit
SA2	FIS for display and update of met and operational flight information - Local unit
SA20	Specific Protocol converters (APT) - Local unit
SA21	Local Network infrastructure (APT) - Local unit
SA22	Monitoring proxy/node (APT) - Local unit
SA25	Technical supervision (s/w) tool - RTC unit
SA28	Aerodrome equipment communications network - Local unit
SA5	Personnel - RTC unit
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.13 IT Risk Assessment Analysis & Application to be applied to the following supporting assets

SA18	Radio Gateway (APT) - Local unit

1.14 Legislation & Regulation to be applied to the following supporting assets

SA5	Personnel - RTC unit
SA5.2	Airport personnel (dedicated to ROT operations) - Local unit

SA5.2.1	Technician/Engineers - Local unit

1.15 Perimeter Intruder Detection System (PIDS) to be applied to the following supporting assets

SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
SA1.2	Wide-Area Network link - RTC unit
SA1.2.1	WAN connection - Local unit
SA11.1	Telephone landlines (not AFTN) - Local unit
SA18	Radio Gateway (APT) - Local unit
SA21	Local Network infrastructure (APT) - Local unit
SA28	Aerodrome equipment communications network - Local unit
SA5.2	Airport personnel (dedicated to ROT operations) - Local unit
SA5.2.1	Technician/Engineers - Local unit
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.16 Policy Organisation & Effective HR Management to be applied to the following supporting assets

SA5	Personnel - RTC unit
SA5.2	Airport personnel (dedicated to ROT operations) - Local unit
SA5.2.1	Technician/Engineers - Local unit

1.17 Security Management to be applied to the following supporting assets

SA9.1	A/D visualisation system - Camera "N" - Local unit

1.18 Standby / Alternate Facilities to be applied to the following supporting assets

SA1.1	Client (Controller) Working Position - RTC unit
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit

SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit
SA1.1.1.2	Servers for visualization - RTC unit
SA1.1.1.3	ATC and voice data recording - RTC unit
SA1.1.2	OTW display - RTC unit
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit
SA1.1.3	OTW audio presentation - RTC unit
SA1.1.5	Display screens other than OTW - RTC unit
SA1.2	Wide-Area Network link - RTC unit
SA1.2.1	WAN connection - Local unit
SA10	Binocular View - Local unit
SA10.1	PTZ Unit - Local unit
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit
SA11.1	Telephone landlines (not AFTN) - Local unit
SA17	Data Concentrator (APT) - Local unit
SA18	Radio Gateway (APT) - Local unit
SA19	Contingency VCS (APT) - Local unit
SA2	FIS for display and update of met and operational flight information - Local unit
SA20	Specific Protocol converters (APT) - Local unit
SA21	Local Network infrastructure (APT) - Local unit
SA22	Monitoring proxy/node (APT) - Local unit
SA25	Technical supervision (s/w) tool - RTC unit
SA28	Aerodrome equipment communications network - Local unit
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.19 System Accreditation to be applied to the following supporting assets

SA1.1	Client (Controller) Working Position - RTC unit
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit
SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit
SA1.1.1.2	Servers for visualization - RTC unit
SA1.1.1.3	ATC and voice data recording - RTC unit
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit
SA1.2	Wide-Area Network link - RTC unit

SA10	Binocular View - Local unit
SA10.1	PTZ Unit - Local unit
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit
SA17	Data Concentrator (APT) - Local unit
SA18	Radio Gateway (APT) - Local unit
SA19	Contingency VCS (APT) - Local unit
SA2	FIS for display and update of met and operational flight information - Local unit
SA20	Specific Protocol converters (APT) - Local unit
SA22	Monitoring proxy/node (APT) - Local unit
SA25	Technical supervision (s/w) tool - RTC unit
SA28	Aerodrome equipment communications network - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.20 Technical Control to be applied to the following supporting assets

SA1.1.1.3	ATC and voice data recording - RTC unit
SA10	Binocular View - Local unit
SA10.1	PTZ Unit - Local unit
SA28	Aerodrome equipment communications network - Local unit
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.21 Vetting of Staff (Works in tandem with PE22) to be applied to the following supporting assets

SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit
SA1.1.3	OTW audio presentation - RTC unit
SA1.1.5	Display screens other than OTW - RTC unit
SA1.2	Wide-Area Network link - RTC unit
SA1.2.1	WAN connection - Local unit
SA10	Binocular View - Local unit
SA10.1	PTZ Unit - Local unit
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit
SA11.1	Telephone landlines (not AFTN) - Local unit
SA17	Data Concentrator (APT) - Local unit
SA18	Radio Gateway (APT) - Local unit

SA19	Contingency VCS (APT) - Local unit
SA2	FIS for display and update of met and operational flight information - Local unit
SA20	Specific Protocol converters (APT) - Local unit
SA21	Local Network infrastructure (APT) - Local unit
SA22	Monitoring proxy/node (APT) - Local unit
SA25	Technical supervision (s/w) tool - RTC unit
SA28	Aerodrome equipment communications network - Local unit
SA5	Personnel - RTC unit
SA5.2	Airport personnel (dedicated to ROT operations) - Local unit
SA5.2.1	Technician/Engineers - Local unit
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

1.22 Viruses & Malware Installation and Patches to be applied to the following supporting assets

SA1.1	Client (Controller) Working Position - RTC unit
SA1.1.1	Standard Functions (Communication, Information & Control, Flight Data Display, AIS, Accident, incident and distress alarms) - RTC unit
SA1.1.1.1	Phone communications between ATCO/AFISO in RTF and remotely controlled tower/airport - RTC unit
SA1.1.1.2	Servers for visualization - RTC unit
SA1.1.1.3	ATC and voice data recording - RTC unit
SA1.1.2	OTW display - RTC unit
SA1.1.2.2	Visual tracking unit VTU (unique per camera to create visual tracks) - Local unit
SA1.1.2.3	Central tracking unit CTU (common gateway for all site sensors) - RTC unit
SA1.1.3	OTW audio presentation - RTC unit
SA1.1.5	Display screens other than OTW - RTC unit
SA1.2	Wide-Area Network link - RTC unit
SA1.2.1	WAN connection - Local unit
SA10	Binocular View - Local unit
SA10.1	PTZ Unit - Local unit
SA10.3	Remote tower Centre Software (should be also HW) - RTC unit
SA11.1	Telephone landlines (not AFTN) - Local unit
SA17	Data Concentrator (APT) - Local unit
SA18	Radio Gateway (APT) - Local unit
SA19	Contingency VCS (APT) - Local unit
SA2	FIS for display and update of met and operational flight information - Local unit
SA20	Specific Protocol converters (APT) - Local unit
SA21	Local Network infrastructure (APT) - Local unit

SA22	Monitoring proxy/node (APT) - Local unit
SA25	Technical supervision (s/w) tool - RTC unit
SA28	Aerodrome equipment communications network - Local unit
SA7.1	Runway Approach Lights, Centre line, taxiway and stand route lighting - Local unit
SA9.1	A/D visualisation system - Camera "N" - Local unit

6 Control refinement and design

6.1 Overview

In this section the assessors review the list of controls to help refine them into security requirements for the OFA. This is achieved by considering the controls that apply to most supporting assets and are therefore likely to be applied at the ATC unit level. These are:

- Firewall Separation
- Vetting of Staff (Works in tandem with PE22)
- Standby / Alternate Facilities
- Automated Access Control System (AACS)
- Electronic Surveillance (CCTV)
- Barriers (Gates & Fences)
- Intruder Detection System (IDS)
- Business Continuity Management
- System Accreditation
- Change Control
- Viruses & Malware Installation and Patches
- Data Input Credibility Checking AND Authentication
- Guards

This leaves the following 2 controls that are recommended for application to a smaller set of supporting assets:

- Encoding Data
- Technical Control

Several controls have been defined for a smaller set of assets but are by their nature more widely applicable:

- Security Management, *which is anyway applicable at the organisation level and a regulatory requirement on ANSPs*
- IT Risk Assessment Analysis & Application
- Perimeter Intruder Detection System (PIDS)
- Accountability
- Legislation & Regulation – *this has been defined to address the threat of 'Blockade of Facilities', although the feasibility of this as a control requires investigation.*
- Policy Organisation & Effective HR Management
- Alternate Supply Systems

6.2 Control considerations for development phase

Two categories of control may require particular design thought during the development phase: encoding data and 'technical' controls.

Encryption of data is proposed to mitigate against attacks that might seek to manipulate the data feeds within and between the local and remote unit. Hence encryption may be necessary between each camera at the local unit and the remote tower centre, spanning the wide area network link.

'Technical' controls refer to bespoke solutions to different threats and the principal concerns are:

- Runway Approach Lights, Centre line, taxiway and stand route lighting, which when connected by remote networks may become vulnerable to viruses, malware, trojans etc.
- A/D visualisation system - Camera "N", which is vulnerable to laser beam interference. This would also apply to the Binocular View.
- PTZ Unit, which may be vulnerable to malware.
- Aerodrome equipment communications network, which may be vulnerable to electromagnetic interference as a form of attack.

The controls for the above may be straight-forward (such as appropriate cable screening) but the process of examining them in further detail will likely yield further insight into the risks and appropriate controls.

6.3 Further work

This risk assessment requires further input by OFA 06.03.01 to validate the various choices made in identifying primary and supporting assets, relevant risks and controls. As an example, the assessment has not included the risk of ‘stand-off attack’, although variations of this may be worthwhile addressing, such as a UAV threat to the camera and PTZ unit. Of primary concern, however, would seem to be risks to the integrity of data feeds, as loss of availability will most likely be addressed through safety protocols.

7 References

[1] 06.09.03 D04 Functional Specification - Single AD 00.00.04_Delta, Project 06.09.03, D25, Edition 00.00.04, February 2011

[2] Availability Note Single Trial AFIS prototype V3 - 01 00 00, Project 12.04.07, D12, Edition 01.00.00, March 2013

[3] DEL - 12 04 06 - D04 - Target Tracking Technology Prototyping V2 - 01 00 00, Project WP 12.04.06, D03, Edition 01.00.00, Jun 2012

[4] DEL - 12.04.06 - D03 - Visual Reproduction Technology Prototyping V2, Project 12.04.06, D03, Edition 01.00.00, March 2012

[5] DEL - 12.04.06 - D06 Part 1 - Technical Supervision-V2, Project 12.04.06, D06 Part 1, Edition 01.00.00, March 2012

[6] DEL - 12.04.06 - D06 Part 2 - Technical Supervision-V2, Project 12.04.06, D06 Part 2, Edition 01.00.00, March 2012

[7] DEL - 12.04.06 - D07 - Camera Positioning Prototyping V2, Project 12.04.06, D07, Edition 01.00.00, September 2012

[8] DEL-06 09 03-D04-OSED updated 24 aug 2012, Project 06.09.03, D04, Edition 00.03.02, August 2012

[9] DEL-06 09 03-D07-VALR-00 02 01, Project 06.09.03, D07, Edition 00.02.01, September 2012

[10] DEL12 04 07-Technical Specifications 00 01 00, Project 12.04.07, D05, Edition 00.01.00, Jun 2012

[11] DEL12.04.07-D10 NATMIG single remote TWR prototype - step 1-12.4.6 D03 Visual rep technology prototype V2-VP, Project 12.04.06 / 12.04.07, 12.4.7-D10 12.4.6-D03, Edition 01.02.00, March 2012

[12] DEL12.04.07-D10 NATMIG single remote TWR prototype - step 1-12.4.6 D03 Visual rep technology prototype V2-VR, Project 12.04.06 / 12.04.07, 12.4.7-D10 12.4.6-D03, Edition 01.02.00, September 2012

[13] DEL-12.4.6-D08-Voice and Data Distribution V2, Project 12.04.06, D08, Edition 01.00.00, February 2012

[14] Release 2 SE Review 3-Guidance-V01 00 00, Project , D, Edition 01.00.00, January 2013

[15] WP6 9 3_Preliminary SAR for RVT_00 00 02-111125, Project 06.09.03, D , Edition 00.00.02, November 2011

-END OF DOCUMENT-