FINAVIA
NOSS TRIAL REPORT

June 2007

Public Final Version

Project Manager: Manfred Barbarino, EUROCONTROL
Project Leader/Author: Ian Patterson, EUROCONTROL contractor

Contents

List of Tables in this report

List of Figures in this report

Acknowledgements

We would like to extend our personal thanks to everyone at FINAVIA who has contributed to this trial and made it a success. In particular thanks are due to the NOSS team for their hard work and assistance, particularly the Local Coordinators; without them this would not have been possible. Lastly to the NOSS observers who made a tremendous effort to learn new concepts and apply them in a very short period of time.

Manfred Barbarino, EUROCONTROL

Ian Patterson, EUROCONTROL contractor

Section 1: Executive summary

This report presents the results of a Normal Operations Safety Survey (NOSS) trial conducted at two sites within FINAVIA during August 2006. Sixty-three NOSS observations were made by six observers across ACC, Approach and Tower settings. The number of observations made during this trial is approximately a third[1] of what one would expect for a full NOSS study in an organisation like FINAVIA and as such the results may not reflect all aspects of the operation. Accordingly results and conclusions drawn from this trial must be treated with a degree of caution.

The reader should bear in mind that in NOSS we are dealing with events that in themselves do not have a high impact; they represent the routine and perhaps mundane aspect of operational performance. You will not find a list of near misses or catastrophic failures in this report to grab your attention. What you will find is an analysis of the types of events that could lead to such catastrophic events occurring. Additionally, NOSS does not aim to make safety recommendations; it aims merely to report on what it finds and highlight areas of potential safety related concern. It is therefore the task of the organisation, through its safety processes, to define the safety recommendations that may be required.

Threats in FINAVIA

The NOSS observers coded 511 threats in total. Within the ACC setting the most frequent threats were internally generated by the organisation (69%). Within the Tower setting the most frequent threats were generated by the airborne side of operational activity (41%). At a more detailed level (Level II) the Threat Types: 'Other controller/Flight data', 'Workspace/Materials', 'Equipment Threats', 'R/T Communication' and 'Aircraft Pilot Issue' represent the most frequently occurring types of threat. At the finest level of coding used within the trial, threats caused by other controllers were the most frequent. In particular, 'Controller Distraction' (Threat Code 205) presents as a relatively frequent threat that is, on occasion, not well managed.

Threats related to other controllers would also seem to be the biggest challenge facing controllers at handover.

Ninety-three percent of the observed threats were managed, leaving seven percent of threats less than optimally managed; which equates to around 0.7 mismanaged threats per hour of observation.

The data suggest that the Tower environment experiences the most difficulty in managing the threats faced. In particular, the threat of 'Blocked taxiway/stand' led directly to three undesired states.

As one would expect the different functional areas of the organisation have different threat profiles. For this reason future NOSS studies might best be run solely within each of these locations and tailored to local needs. Detailed analysis by the safety team of some of the more frequent threats is recommended and future NOSS studies should analyse these closely to detect trends.

Some areas to consider for further study or intervention are indicated in the body of the report.

Errors in FINAVIA

The NOSS observers coded 176 threats in total. The most frequently occurring errors are errors related to communication (52%) followed by errors related to procedures

[1] Recommendation based on findings of the ICAO NOSS Study Group.

(32%). Five percent of operational errors lead to another error or undesired state and can be considered to have been less than optimally managed.

Errors in communication would seem to be the biggest challenge facing controllers at handover.

The Error Code 813 ('Incomplete Briefing') was associated with 13 of the 29 errors related to Handover/ Opening and Closing of Position; this may have implications for looking at the ways in which briefings are conducted. In addition, seventeen percent of errors were related to position relief.

Areas for more detailed scrutiny include:

- A detailed analysis of the nature of the communication errors and errors related to procedures is indicated, the narrative reports that can provide an overview of these are available on separate CD.
- The execution of procedures and communication during position relief (handover) might be examined.

The following errors were relatively high in frequency and might be a target for intervention:

- 'Non-Operational conversation which distracts from principal controller tasks', 'Correct procedure not used' and 'Inappropriate coordination' within ACC.
- 'Inappropriate coordination' within Approach.
- Missed call', 'Correct procedure not used', within Tower.
- Subsequent NOSS studies should compare trends in the error codes used.

Undesired states in FINAVIA

Twenty-six undesired states were coded during the NOSS observation. The Tower environment accounted for a greater number of these than one would have expected based on the proportion of observations made in this environment.

The small numbers of undesired states observed is encouraging as these represent some of the precursors to reportable events, however, eleven undesired states relate to some form of reduction in safety for airborne separation. Action may be required to prevent an increase in such events that are clearly precursors to reportable incidents.

Some potential areas for future intervention include:

- Investigation of the ground traffic congestion; and possible solutions.
- All the undesired states should be reviewed by the safety team and manager (details are in the narratives available on separate CD).

The flow chart shown in Figure 1 shows some of the main results from the trial. However this chart can only be used as an aide-memoire as it does not contain the detailed explanations or context required to understand the figures.

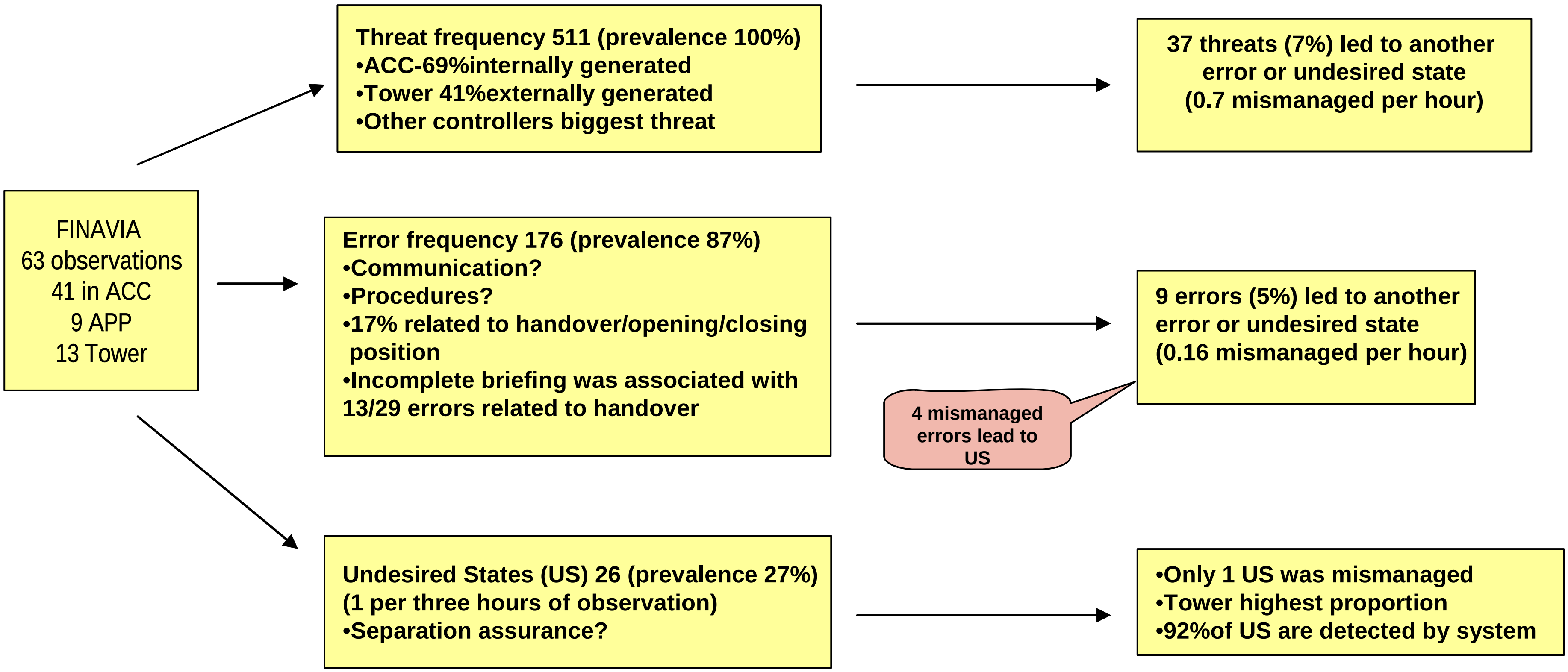

Figure 1: Main results from FINAVIA trial

In conclusion

The FINAVIA NOSS trial has demonstrated the utility of the NOSS approach and the data generated, whilst limited by the number of observations made, is encouraging. Refinements to the NOSS tool (observation form) and methodology were made through the course of the trial according to the local demands. It is likely that further customisation and refinements will be required when the NOSS methodology is applied in other settings.

The data provided by the trial has generated some interesting results and areas that might be considered for safety intervention. However, any conclusions based on this data must be treated with some caution due to the limited sample of observations obtained.

The real strength of NOSS lies in repeating the process over time using the same methodology and codes. In this way trends in the data should indicate if the organisation is moving in a direction that exposes it to a greater safety risk. For example, if subsequent data indicated an increase in the frequency of the undesired state 'Traffic congestion due to blocked taxiway' then action might be taken to resolve this issue.

The trial has met its objectives and thanks are due to the considerable efforts of the NOSS team within FINAVIA.

Section 2: Introduction and background

This report presents the results of the FINAVIA Normal Operations Safety Survey (NOSS) trial conducted in collaboration with EUROCONTROL in August 2006. The data was collected during the course of normal operations by controllers from FINAVIA who were trained in NOSS observation and recording methods. EUROCONTROL wishes to extend its thanks to all the staff at FINAVIA who made this project possible and, in particular, the operational staff who acted as NOSS observers and data verification specialists.

The trial had two aims:

1. To test the usability and applicability of the NOSS methods and ultimately the utility of the NOSS approach.
2. To provide a snapshot of the observable everyday Threats, Errors and Undesired States that FINAVIA experiences and to see how these are managed.

This NOSS trial was the first to be conducted in Europe and as such the scale of the NOSS is less than one would anticipate if NOSS data were being routinely collected in the organisation. The time frame for collecting the NOSS trial data was just over two weeks, restricting the number of NOSS observations to 63 in total, across three areas of functionality: ACC, Tower and Approach. If NOSS were run routinely in this organisation then more than twice this number of observations, (at least forty in each area of functionality) would be a minimum requirement. This would provide more data and give a more complete picture of the operation. <u>As it stands the results presented in this report must be treated with caution due to the small sample size obtained.</u>

NOSS background

Traditionally aviation safety has relied on incident analysis to provide the necessary information by which safety can be improved. Such analysis methods have great value but suffer certain limitations. Firstly, they are retrospective and tend to capture only events that by their nature come to the attention of the analysts. More significantly, the increasingly infrequent nature of such events, as aviation systems become progressively safer, means that this data is not easily obtained and new approaches are required.

Normal Operations Safety Survey (NOSS) is a method for the collection of safety data during normal Air Traffic Control (ATC) operations. A normal ATC operation is defined as: 'an operation during the course of which no accident, incident or event takes place that requires reporting and/or investigation under existing legislation or regulations'. With this in mind it is important to view NOSS as a tool that helps an organisation to see where everyday threats to the operation exist, and to acknowledge that NOSS is not intended to highlight dramatic and reportable events[2]. Rather NOSS looks for patterns or increased frequencies of events that may indicate safety related concerns for routine operations.

NOSS captures ATC system performance through the eyes of air traffic controllers using a series of 'over the shoulder' observations. NOSS identifies observable[3] Threats, Errors and Undesired States that are specific to an organisation's particular operational context, and sees how effectively those Threats, Errors, and Undesired States are managed by air traffic controllers during normal operations. The information obtained has the potential to assist the organisation to proactively make changes to its safety processes without having to experience the trauma of an incident or accident.

Once the NOSS data analysis is completed the information can be used by the organisation to propose safety adjustments to the operational processes. By conducting subsequent follow-up NOSS studies an organisation will get feedback on the effects of these changes.

It is important to understand that NOSS is a tool to provide an overview of the observable elements of operational performance and to identify overall areas of strength and weakness. It is not concerned with the performance of individuals, though it might identify areas where a number of individuals are having similar problems. In other words, NOSS is designed to take a systems view of the operation in which the everyday threats to the operation, and the ways in which the system responds to these are captured. The strength of NOSS is that it provides a context to threat, error and undesired state events and records the strategies that were employed to overcome potentially undesirable outcomes.

NOSS is based on the Line Operation Safety Audit (LOSA) method, designed to capture information about safety related events on the flight deck and their management during normal operations. The LOSA method was developed by The University of Texas Human Factors Research Project (UT) and is in use with a number of airlines around the world.

The relative success of the LOSA initiative prompted ICAO to form a study group to develop a similar method for air traffic control. This comprised air navigation service providers and aviation safety experts from around the globe. As a member of this group EUROCONTROL agreed to coordinate a pilot study of the NOSS method in Europe to add to the trials already being undertaken by The University of Texas Human Factors Research Project and other Air Navigation Service Providers (ANSPs) in the ICAO Study Group[4].

---

[2] NOSS is designed to ignore reportable events if they occur, as this is then no longer a normal operation. Other mechanisms for capturing the information from a reportable incident should then be activated.

[3] NOSS does not aim to capture the hidden or internal mental events that are part of normal operations, and whilst this could be considered a limitation of the NOSS method, experience suggests that the information obtained from the observable events alone is rich and useful.

[4] NAV Canada, AIRWAYS NEW ZEALAND and AIRSERVICES AUSTRALIA.

NOSS trial description and process

This was the first NOSS trial in Europe and the first applying the method in a setting where English was not the first language. Each observer made between nine and twelve observations. During each observation one controller position was observed for a period of between 25 and 75 minutes. Six observers were available for the duration of the trial, four ACC controllers and two tower/approach controllers. The four ACC controllers conducted observations in the ACC setting. The two tower/approach controllers conducted the tower observations and seven observations in the approach setting. Two additional approach observations were made by two of the ACC controllers who were familiar with the operational requirements of the approach positions.

To help ensure a successful trial the following steps were followed:

- An extensive marketing and promotional period preceded the NOSS trial. This involved many briefings and publications throughout the organisation and the appointment of a local coordinator for both Helsinki and Tampere.
- The controllers' association was involved from the beginning. An undertaking was given by the management of the organisation that persons providing the data be de-identified so that the source of the data remained confidential and would not be available or used for investigation or disciplinary purposes.
- The NOSS observers were recruited well in advance of the trial. Scheduling was arranged for a two-week period clear of other duties for the NOSS observers to make their observations. Additional time was made available so all observers would have the opportunity to attend part of the data verification process.
- Each observer received two days of classroom instruction in the Threat and Error Management Framework, NOSS methodology, and the data collection instrument. Following the training, observers conducted one observation then met with the training facilitator to receive feedback and further direction. Following completion of the second observation, at the request of the observers, feedback on individual observations was provided in a group setting. This proved very informative for the observers. Subsequent feedback on reports was provided by the facilitator as required, via phone and email.
- Data were collected during normal shifts and controllers had the right to refuse to be observed.
- All data were sent directly to EUROCONTROL for analysis. Preliminary data preparation (Data Verification) was carried out by the project coordinator (Data Analyst) from EUROCONTROL. Edits and questions were flagged in the narrative of the observers' reports and in the codes used. These pre-verified reports were used by the Data Verification Team.
- All data were considered by the Data Verification Team. The team were asked to read the complete observation and look for Threat, Error, and Undesired State events that might have been missed by the Observer or Data Analyst as well as critiquing existing data. The data was reviewed against the organisations' procedures to ensure that events had been properly coded. Analysis did not begin until this data integrity check had been completed.
- Data analysis and report preparation was undertaken by the EUROCONTROL Data Analyst (who was also the NOSS trainer and facilitator).

Description of the airspace under examination in this study

The trial was conducted at two ATC units within FINAVIA:

1) Air Navigation Services Centre for South Finland (Tampere FIR/ACC); and
2) Helsinki Airport, consisting of Tower and Approach Radar.

A total of 63 observations were made in the organisation, see Table 1.

Table 1: Number of observations by location

Location	Number of observations
Tampere ACC	41
Helsinki Approach	9
Helsinki Tower	13
Total	63

Air Navigation Services Centre for South Finland (Tampere FIR/ACC)

This covers Southern Finland and has the possibility of five sectors, some of which are combined at any one time. Up to three feeder sectors can also be opened.

Helsinki Airport (Tower and Approach Radar)

Helsinki tower has the possibility for four positions: TWR East, TWR West (which are sometimes combined), Ground Position and Clearance Delivery. Tower takes responsibility for aircraft from Approach at around four miles and up to 1300ft.

Within Helsinki Approach Radar there are five operational working positions: Radar East, Radar West, Arrivals East, Arrivals West (depending on traffic volumes, positions at Arrivals East and Arrivals West are sometimes combined) and a Radar Assistant position.

Duration of observations

A total of 54 hours and 25 minutes of observations were made representing an average of 52 minutes per observation.

Section 3: Presentation of results

The results are presented in three forms:

1) Executive Summary - Section 1 of this report.
2) Detailed report - Sections 3 – Section 11 of this report plus appendices. The results of the trial will be described according to the functional roles outlined above, i.e., ACC, Approach and Tower. This three-way split will provide the most meaningful picture of normal operations in the organisation as a whole. Where appropriate the combined data from these three functional groups will be reported.
3) Raw data CD - The de-identified raw data will be made available to the safety management team of the unit. This will be on a CD and will allow for a more detailed analysis of specific events where this is required. This is available in the form of:

a) A de-identified spread sheet in MS Excel, which shows the data associated with each observation and

b) The Narratives associated with each observation, in MS Word.

N.B. When reading these results it is important to remember that the small sample sizes involved in this study make forming definitive conclusions difficult. Care should be exercised in this regard and the results should be regarded as providing support for the process of NOSS rather than a definitive description of normal operations within FINAVIA. None the less, some useful indicators of safety performance are likely to be identified in the detail of the data and in this report.

Section 4: Threats in FINAVIA

Threat taxonomy

Under the NOSS frame work a Threat is defined as: ‘Events or errors (*by others than the observed controller*) that occur beyond the influence of the air traffic controller, increase operational complexity, and which must be managed to maintain the margins of safety’.

Threat events observed in the course of the NOSS observations are represented at three levels within the NOSS event taxonomy. Initially each event was allocated a Threat Code (Level III) that best described the event. This Threat Code in turn belongs within a Threat Type (Level II) and ultimately the Threat Category (Level I).

Where a code was not available to describe a threat or could not be developed, the missing data code 999 for ‘Other’ was used. This code was used four times only; these codes are not included in the results that follow.

For example, the Threat Code called Airspace Penetration (Code 518) represents the most detailed description of the threat (Level III). This code in turn belongs to the ‘Threat Type’ called ‘Aircraft Pilot Issue’ (code 1800, Level II), which in turn belongs to the Threat Category called Airborne Threats (code 3700, Level I). Table 2 shows a part of the threat taxonomy table used in coding the data. This is shown in greater detail in Appendix 4, the NOSS Radar, Tower & Approach Observation Form.

Table 2: Threat taxonomy example

Airborne Threats (3700)					
Aircraft Pilot Issue (1800)		R / T Communication (1900)		Traffic (2000)	
500	Flight plan – ATS system incongruence	630	Readback Error	650	Priority flight / VIP's
501	Heading Deviation	631	Non-standard phraseology	651	Military activity
502	Speed deviation	632	Language difficulty	652	Parachute activity
503	Altitude deviation	633	Similar call signs	653	Complex Sequencing Issue
504	Combo speed /altitude/heading deviation	634	Flight crew failure to respond to call	654	Non RVSM a/c in RVSM airspace
505	Slow to comply with command	635	Frequency congestion	655	Pop-up flight
506	Flight crew failure to report	636	Blocked frequency	656	Formation flight
507	Routing deviation	637	Clipped Transmission	657	Survey Flight
508	AC malfunction	638	Pilot communication difficulty	658	Training Flight
509	Rate of climb / descent	639	Pilot use of incorrect call sign	659	Minimum fuel
510	Pilot non-compliance w/ instruction	999	Other	660	Increasing traffic load
511	Closing speeds				
512	Emergency				
514	Airline Procedure				
515	Diversions				
516	Non-active RWY request				
517	Non-standard AC profile				
518	Airspace penetration				
519	Pilot request				
520	Other pilot error				
521	Uncorrelated target in class A airspace				
522	Aircraft calls on wrong frequency				
523	Non compliance with local procedure				
999	Other				

Table 3 shows the Threat Categories (Level I) and Threat Types (Level II), examples of Threat codes (Level III) are also shown.

Table 3: Threat taxonomy

Air Navigation Service Provider Internal Threats (3500), Level I	
Equipment, Level II	Maintenance, screen clutter, unserviceable equipment, Level III
Workspace / Materials, Level II	Noise, visitors, chart / manual error, lighting, Level III
Other Controllers, Level II	Controller error, controller distraction, coordination issue, Level III
Operational Performance, Level II	Combined sectors, flow control command, non-standard aircraft, Level, Level III
Air Navigation Service Provider External Threats (3600), Level I	
Airport layout (1500), Level II	Poor signage, Blocked taxiway/stand, Level III
Airspace Infrastructure/Design (1600), Level II	Restricted Airspace, Level III
External or Foreign Service Providers (1700), Level II	Nav Aid Reliability, Level III
Ground traffic (1750), Level II	Vehicle calls on wrong freq, Level III
Airborne Threats (3700), Level I	
Aircraft / Pilot Issue (1800), Level II	Heading deviation, AC malfunction, Airline Procedure, Level III
R / T Communication (1900), Level II	Similar call signs, read back error or non-standard phraseology from pilots, Level III
Traffic, Level II	Parachute activity, non RVSM aircraft in RVSM airspace, VIP / priority flight, Level III
Environmental Threats (3800), Level I	
Weather (2100), Level II	Thunderstorms, turbulence, visibility, winds, icing, Level III
Geographical Environment (2200), Level II	Terrain, obstacles, noise abatement, Level III

Threat profile

Threat definitions

- Events or errors, *by others than the observed controller*, that occur beyond the influence of the air traffic controller, increase operational complexity, and which must be managed to maintain the margins of safety.
- Mismanaged threat: A threat that is linked to or induces controller error or an undesired state.
- Threat Prevalence Index: The percentage of observations with one or more threats.
- Threat Mismanagement Index: The percentage of threats that were mismanaged.

NOSS observers recorded the threat events and documented how the controller handled them. The information obtained from this process has been coded and provides a threat profile for the area of the organisation being observed (ACC, Tower or Approach). This profile contains two main types of information:

1) The threat prevalence or frequency at which the threat was observed, and

2) Whether the threat was managed or not.

Mismanagement of a threat is defined by whether the threat leads to a separate controller error or undesired state. Mismanagement does not imply the controller was at fault in anyway but simply that the system failed to manage out the threat.

Threats were observed during all observations therefore the Threat Prevalence Index is 100%.

The total number of threats observed was 515, four of these were allocated the code 999 ('Other') and are not included in further analysis leaving 511 threats that were coded during the NOSS process. New codes were developed during the data verification process.

Threat Category (Level I) and Threat Types (Level II)

Table 4 shows the breakdown of the Threat Category and Threat Types by functional location: ACC, Approach and Tower.

Table 4: Threat Type by ATC function

Threat category (Level I)	Threat Type (Level II)	ACC	Approach	Tower	Total
Air Navigation Service Provider Internal Threats (3500)	Equipment Threats (1100)	41	7	13	61
	Workspace/Materials Threats (1200)	74	5	14	93
Total 300 (59%)	Other controller / Flight Data (1300)	90	15	19	124
	Operational Performance Threats (1400)	11	7	4	22
Air Navigation Service Provider External Threats (3600)	Airport Layout (1500)	0	1	23	24
	Airspace Infrastructure/Design (1600)	3	5	1	9
Total 53 (10%)	External or Foreign Service Providers (1700)	16	3	0	19
	Ground Traffic (1750)	0	0	1	1
Airborne Threats (3700)	Aircraft Pilot Issue (1800)	18	9	27	54
	R / T Communication (1900)	45	13	24	82
Total 148 (29%)	Traffic (2000)	10	1	1	12
Environmental Threats (3800)	Weather Threats (2100)	7	2	1	10
Total 10 (2%)	Total	315 61%	68 13%	128 25%	511[5]

A total of 511 threats were coded across the whole organisation. The most frequent Threat Types are shown in bold. It can also be seen from Table 4 that most threats (59%) experienced by the organisation are generated internally by the organisation. The next major Threat Category is Airborne Threats (29%). This information is shown graphically in Figure 2 which highlights that the Threat Types: 'Other controller/Flight

[5] The number of threats observed in each functional group is in proportion to the number of observations made in that group.

data', 'Workspace/Materials', 'Equipment Threats', 'R/T Communication' and 'Aircraft Pilot Issue' are the most common Threat Types facing controllers in the organisation.

The Threat Category 'Internal Threats (generated by the organisation) was the most frequent threat for the ACC environment. Two hundred and sixteen threats out of three hundred and fifteen (69%) were in this category.

The Threat Category 'Airborne Threats', threats generated externally to the organisation, was the most frequent threat in the Tower environment. Fifty three threats out of one hundred and twenty eight (41%) were in this category consisting mainly of Threat Types: 'Aircraft Pilot Issue' and 'R /T Communication' and Airport Layout'.

To interpret the threat results in more detail requires a little work on the reader's part. The reader needs to refer to Table 4 and Appendices 1 and 4. For example, let us consider, from the ACC column in, Table 4 and the relatively frequent Threat Type 'Other Controller/Flight Data' (frequency 90). From Appendix 4 it can be determined that this Threat Type contains the codes 'Controller distraction' (code 205) and 'Correct procedure not used or non-standard procedure used' (code 212). From Appendix 1 it can be seen that Code 'Controller distraction' scores a frequency of 29, and Code 'Correct procedure not used or non-standard procedure used' scores a frequency of 24. These are relatively high frequencies compared with other threat codes of this type. A safety manager might be interested in finding out more about the nature of the distraction or the nature of the threats caused by procedures. This information is available from a detailed examination of the narrative reports provided on a separate CD.

Alternatively the reader may wish to restrict themselves to the higher level of analysis merely noting that 'Other controller/Flight data', (Type Code 1300) seems to be a frequent threat. This might be noted and compared with subsequent NOSS studies. This highlights an important feature of NOSS in that it is the comparison of NOSS results over time that will provide the greatest information for safety management. Such comparisons allow the safety management to determine the way threats are trending.

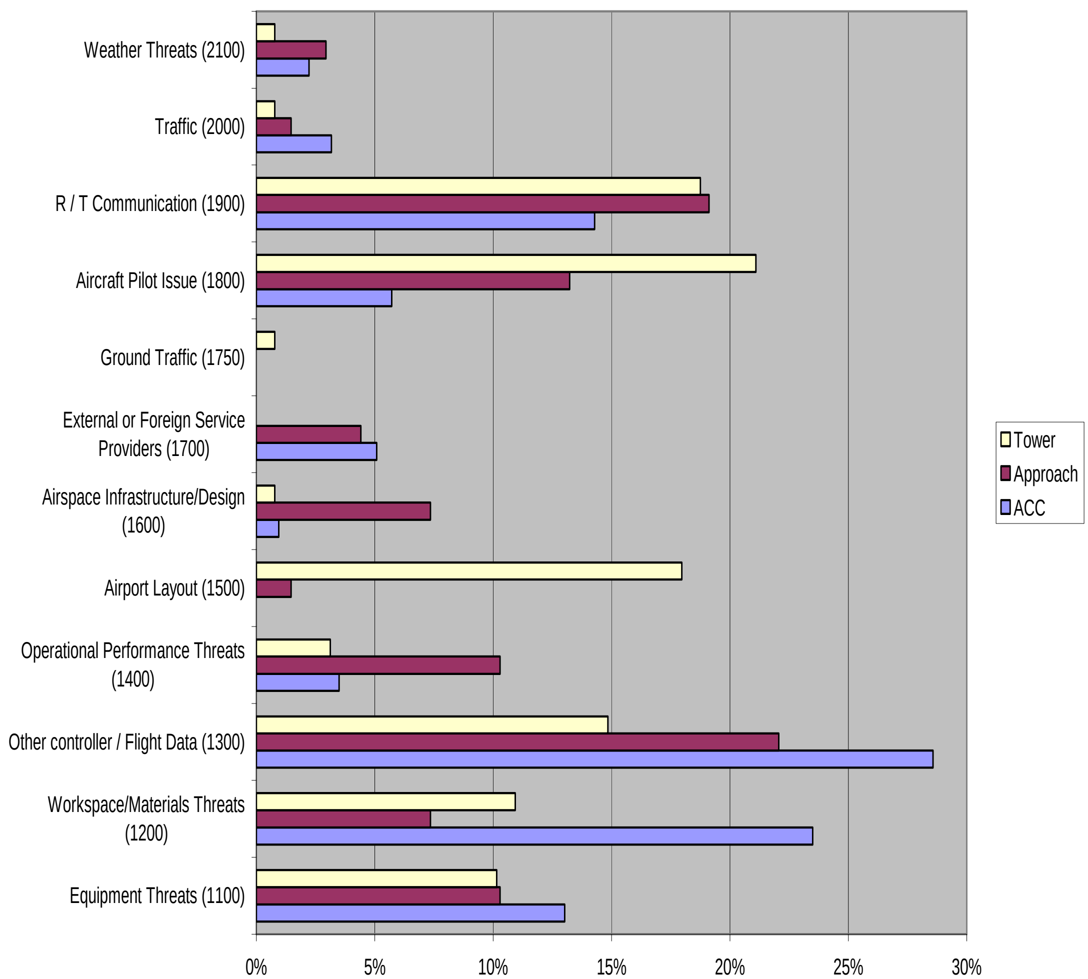

Figure 2: Threat Type by ATC function expressed as a percentage

Mismanaged threats

Mismanaged threats are defined as: 'threats that lead to a controller error or directly to an undesired state'. The total number of mismanaged threats was 37 out of 511; therefore the threat Mismanagement Index is 7%, representing 0.6 mismanaged threats per observation. This equates to 37 mismanaged threats in 54 hours and 25 minutes or 0.7 mismanaged threats per hour. The corollary of this is that the system is successfully managing 93% of all threats. The most frequent threats leading to mismanagement are shown in bold in Table 5.

The values shown in Table 5 show the percent of mismanaged threats out of the total number of threats observed (511).

Table 5: Mismanaged threats leading to Error or Undesired State

Threat Category mismanaged	Threat Type mismanaged	ACC	Approach	Tower	Total
Air Navigation Service Provider Internal Threats (3500) Total 25 (5%)	Equipment Threats (1100) (1%)	4	0	0	4
	Workspace / Materials Threats (1200) (>1%)	1	0	1	2
	Other controller / Flight Data (1300) (3%)	8	2	4	14
	Operational Performance Threats (1400) (1%)	0	2	3	5
Air Navigation Service Provider External Threats (3600) Total 5 (1%)	Airport Layout (1500) (1%)	0	0	4	4
	Airspace Infrastructure/Design (1600) (0%)	0	0	0	0
	External or Foreign Service Providers (1700) (>1%)	1	0	0	1
	Ground traffic (1750) (0%)	0	0	0	0
Airborne Threats (3700) Total 7 (1%)	Aircraft Pilot Issue (1800) (1%)	2	1	0	3
	R/T Communication (1900) (1%)	1	1	1	3
	Traffic (2000) (>1%)	1	0	0	1
Environmental Threats (3800) Total 0 (0%)	Weather Threats (2100) (0%)	0	0	0	0
Total mismanaged (7%)		18	6	13	37
Total threats coded		315	68	128	511
Percent mismanaged by ATC Function		6%	9%	10%	7%

Threats from ‘Other controllers’ represent the most frequent cause of threats likely to lead to further errors or undesired states. The role of Team Resource Management in mitigating such threats could be considered. Threats generated internally by the organisation account for more than half (68%) of the mismanaged threats.

The data suggest that the Tower environment experiences the most difficulty in managing the threats it faces[6].

[6] Because of the small numbers available for this analysis care must be exercised in interpreting these results, which should be considered only indicative of the true picture.

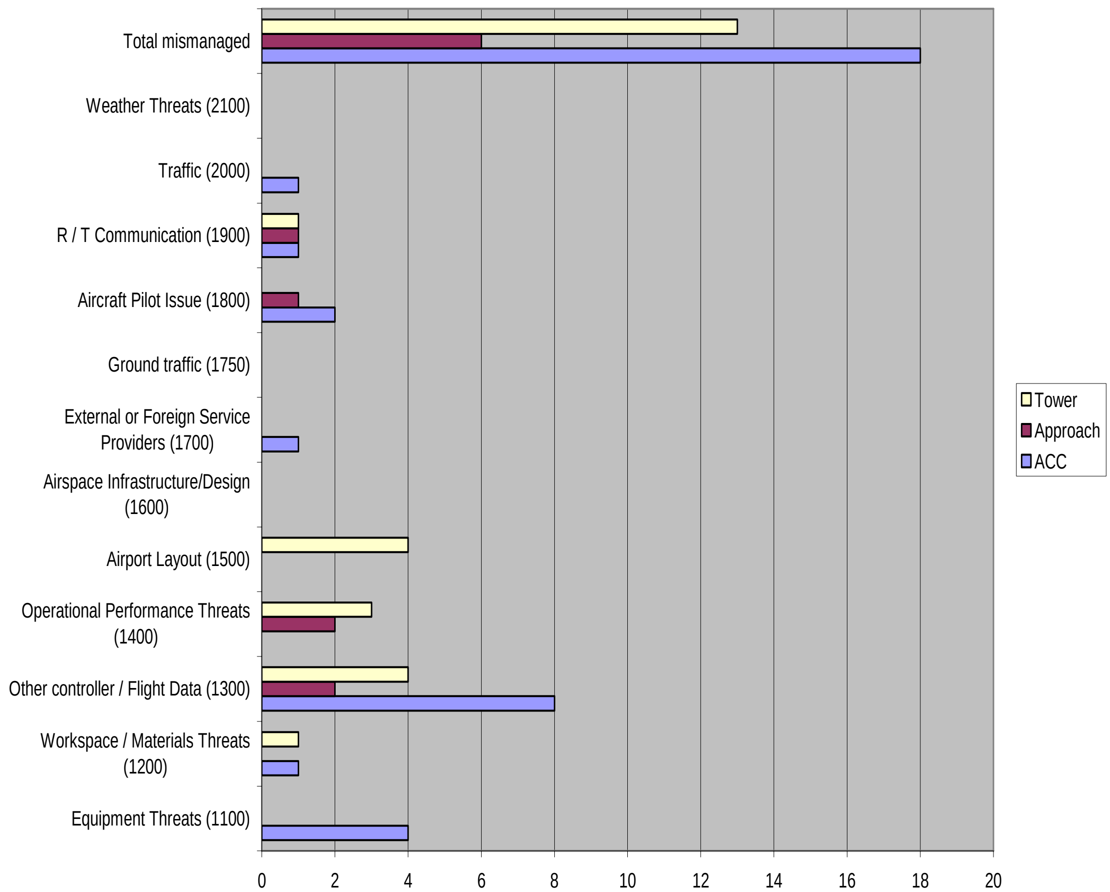

Figure 3: Number of mismanaged Threat Types leading to Error or Undesired State

Threats (Level III) and their management

Table 6 shows the ten most frequent threat codes by each ATC function and the frequency of mismanagement of these. This allows some impression of the threats that may be causing problems for controllers in each setting. For example, 'Noise' would appear to be very frequent threat in the ACC setting but in fact 'Controller Distraction' presents more of a management challenge.

For the Tower setting, 'Frequency Congestion' may be an issue that should be looked at, as this is not something that can always be managed at the time. Additionally, in the Tower, three of the ten threats coded as 'Blocked Taxiway' were mismanaged leading directly to Undesired States[7].

'Controller distraction' features in all three settings and is relatively frequently mismanaged[8]. 'Correct procedure not used or non standard procedure used' were coded as threats on 24 (8%) of occasions out of 315 in the ACC setting. Whilst all were successfully managed this might warrant further investigation to determine how the use of procedures might be changed so that they did not pose a threat.

[7] This data can be ascertained only by a detailed analysis of spreadsheet data, not included in this report.
[8] More detailed code descriptions are provided in Appendix 4, NOSS Radar, Tower and Approach Observation Form.

Table 6: Ten most frequent Threat Codes by ACC Function

ACC			Approach			Tower		
Threat Code	Freq	Mismanaged	Threat Code	Freq	Mismanaged	Threat Code	Freq	Mismanaged
Noise (150)	61	1	Controller distraction (205)	6	1	Frequency congestion (635)	18	0
Controller distraction (205)	29	3	Aircraft in conflict (258)	4	2	Runway/Taxiway configuration (302)	11	1
Correct procedure not used or non standard procedure used (212)	24	0	Read back Error (630)	4	1	Blocked taxiway/stand (305)	10	3
Read back Error (630)	13	0	Visitors (152)	3	0	Controller distraction (205)	8	2
Flight crew failure to respond to call (634)	13	0	Unspecified threat induced by other controller (210)	3	0	Pilot request (519)	8	0
Ex: Coordination issue(406)	11	1	High workload (259)	3	0	Poor Sight Lines (153)	7	1
False conflict alert, alarm (112)	9	1	Airspace design (352)	3	0	Non compliance with local procedure (523)	7	0
Visitors (206)	8	1	Ex: Coordination issue (406)	3	0	Data Incongruence (110)	4	0
Coordination Issue (210)	8	1	Frequency congestion (635)	3	0	Slow to comply with command (505)	4	0
Unspecified threat induced by other controller (152)	8	0	-	-	-	Equipment difficult to use (117)	3	0

Handover/Takeover - Opening and closing of position

The data in Table 7 shows that fifteen threats were linked to position relief and three were linked to the opening/closing of a position. This represents only 4% of all threats coded (511) indicating that threats are not particularly more prevalent at handover. Threats related to other controllers would seem to be the biggest challenge facing controllers at handover. This has implications for Team Resource Management

Training. Detailed examination of the Threat Codes reveals that the threat 'Controller Distraction' (Threat Code 205) was associated with five of the twenty links (25%).

Table 7: Threats linked to position relief or opening/closing position

Threat Type	Position Relief	Opening/closing of Position
Equipment Threats (1100)	0	1
Workspace / Materials Threats (1200)	1	1
Other controller / Flight Data (1300)	13	2
Operational Performance Threats (1400)	0	0
Airport Layout (1500)	0	0
Airspace Infrastructure/Design (1600)	0	0
External or Foreign Service Providers (1700)	1	0
Ground traffic (1750)	0	0
Aircraft Pilot Issue (1800)	0	1
R / T Communication (1900)	0	0
Traffic (2000)	0	0
Weather Threats (2100)	0	0
Total 20	15	5

Threat results summary

The NOSS observers coded 511 threats in total. Within the ACC setting the most frequent threats were internally generated by the organisation (69%). Within the Tower setting the most frequent threats were generated by the airborne side of operational activity (41%). At a more detailed level (Level II) the Threat Types: 'Other controller/Flight data', 'Workspace/Materials', 'Equipment Threats', 'R/T Communication' and 'Aircraft Pilot Issue' represent the most frequently occurring types of threat.

Threats caused by other controllers were the most frequent threats observed in FINAVIA. Threats related to other controllers would also seem to be the biggest challenge facing controllers at handover. Detailed examination of the Threat Codes reveals that the threat 'Controller Distraction' (Threat Code 205) presents as a relatively frequent threat and is on occasion not managed well.

Ninety-three percent of the observed threats were managed optimally leaving seven percent of threats less than optimally managed; around 0.7 mismanaged threats per hour of observation. Threats generated internally by the organisation account for more than half (68%) of the mismanaged threats.

The data suggest that the Tower environment experiences the most difficulty in managing the threats it faces.

The threat of 'Blocked taxiway/stand' led directly to three undesired states in the tower environment; this frequency is relatively high bearing in mind there were only 26 undesired states observed in total, (see Section 6).

As one would expect the different functional areas of the organisation have different threat profiles. For this reason future NOSS studies might be run solely within each of these locations and tailored to the local needs. Detailed analysis by the safety team of some of the more frequent threats is recommended and future NOSS studies should analyse these closely to detect trends.

Potential areas for future intervention

- Controller distraction might be investigated further. This is a frequent threat that is relatively frequently mismanaged. The nature of the Noise threat in the ACC environment might be related to this.
- The reasons for blocked taxiways and the relative importance of this might be investigated further.
- The nature of how procedures are generating threats might be investigated.
- Subsequent NOSS studies should compare trends in the threat codes used.

Section 5: Errors in FINAVIA

Error taxonomy

Under the NOSS framework an error is defined as: ‘actions or inactions by the air traffic controller that lead to deviations from organisational or controller intentions or expectations’. For the purposes of this study, the definition of error concerned only the person observed. Only events in their immediate control could be defined as errors and furthermore had to be against a procedure or accepted good practice[9].

Error events observed in the course of the NOSS observations are represented at two levels within the NOSS event taxonomy, these are called Error Type, Level I and Error Code, Level II. For example, the Error Code called ‘Incorrect read back given’ (Code 800) represents the most detailed description of the error (Level II). This code in turn belongs to the ‘Error Type’ called ‘Errors in the execution of communication/Communication Errors’ (Code 4100, Level I). Unlike threats there are no ‘Error Category’ codes.

Table 8 shows a part of the error taxonomy table used in coding the data. This is shown in greater detail in Appendix 4 the Amended NOSS Radar, Tower & Approach Observation Form.

Where a code was not available or could not be developed the missing data code 999 for ‘Other’ was used. This code was used eight times only; these missing data codes are not included in the results that follow.

[9] It is acknowledged that this involves a judgement by the observer and that this introduces an additional source of variability and subjectivity in the data.

Table 8: Error Taxonomy Error Codebook

Errors in the execution of communication/Communication Errors (4100)			
800	Incorrect read back given	810	No coordination
801	Incorrect read back not detected	811	A/C Transfer
802	Full read back not obtained	812	Non-Operational conversation which distracts from principal controller tasks
803	Wrong call sign used	813	Incomplete briefing or coordination
804	Non-standard phraseology	814	A/C type omitted in initial call
805	Missed call	815	Call sign omission
806	Late coordination	816	Clipped frequency
807	Incomplete / Inaccurate information given during coordination	817	Inappropriate coordination
808	Did not pass information (traffic, terrain, etc)	818	Frequency change error
809	Incomplete or incorrect information/instruction passed	999	Other

Table 9 shows the five Error Types (Level I) and examples of Error Codes (Level II) (There is no equivalent to the classification 'Threat Category' as in the threat results section).

Table 9: Error taxonomy

Error Type Errors in the execution of communication / Communication Errors (4100), Level I
Full read back not obtained, Level II
Missed call, Level II
Incomplete briefing or coordination, Level II
No coordination, Level II
Error Type Equipment / Automation Errors / Errors in the operation of equipment of automation (4200), Level I
Computer / Automation input error, Level II
Radar screen range selection, Level II
Data tag incomplete/inaccurate information, Level II
Error Type Flight Data Progress Strip Errors / Errors in the use of manipulation of flight strips or radar labels (4300), Level I
Label/FPS marking error, Level II
No update of flight label; Airspace not fully displayed, Level II
No strip on board, Level II
Error Type Error in the execution of procedures Procedural Errors (4400), Level I
Correct procedure not used, Level II
Error Type Aircraft Instruction Errors (4500), Level I
Late Descent, Level II
Sequencing judgment error

Error profile

Definitions

- Error: Actions or inactions by the air traffic controller that lead to deviations from organisational or controller intentions or expectations. For the purposes of this study, the definition of error concerned only the person observed. Only events in their immediate control could be defined as errors and furthermore had to be against a procedure or accepted good practice.
- Mismanaged Error: An error that is linked to or induces additional error or an undesired state.
- Error Prevalence Index: The percentage of observations with one or more errors.
- Error Mismanagement Index: The percentage of errors that were mismanaged.

NOSS observers recorded the error events and documented how they were handled by the controller. The information obtained from this process has been coded and provides an error profile for the area of the organisation being observed (ACC, Tower or Approach). This profile contains two main types of information:

1) The error prevalence or frequency at which the error was observed, and
2) Whether the error was managed or not.

Mismanagement of an error is defined by whether the error leads to an additional controller error or undesired state; mismanagement does not imply the controller was at fault in any way but simply that the system failed to successfully manage the error.

Errors were observed on 55 observations out of 63 therefore the Error Prevalence Index is 87%. The total number of errors observed was 184. Eight of these observations received the code 999 (‘Other’) and are not included in the further analysis leaving 176 errors that were successfully coded during the NOSS process. The error codes for the entire organisation are shown in Appendix 3.

Error Type (Level I)

Table 10 shows the breakdown of the Error Types by functional location: ACC, Approach and Tower. A total of 176 errors were observed across the whole organisation. The most frequent Error Types are shown in bold. This information is shown graphically in Figure 4. Errors related to communication (52%) followed by errors related to procedures (32%) are the most frequent.

It can be seen that ACC accounts for 150 errors out of 176 (85%). On the basis of the number of observations it contributed to the trial (41 out of 63) the percentage of errors attributed to ACC should be 65%. Therefore, ACC is accounting for larger proportion or errors than chance alone would predict. Such a comparison with the other two functional groups is of interest and might be used for comparison in future studies.

Table 10: Error Type by ATC function

Error Type (Level I)	ACC		Approach		Tower	
Errors in Communication (4100) Total 91(52%)	80	53%	3	30%	8	50%
Equipment / Automation Errors (4200) Total 17 (10%)	15	10%	1	10%	1	6%
Errors in the use of manipulation of flight strips or radar labels (4300) Total 6 (3%)	4	3%	1	10%	1	6%
Error in the execution of procedures Procedural Errors (4400) Total 56 (32%)	48	32%	4	40%	4	25%
Aircraft Instruction Errors (4500) Total 6 (3%)	3	2%	1	10%	2	13%
Total (176)	150	100%	10	100%	16	100%

Figure 4 shows the percentage of Error Types for each ATC functional location.

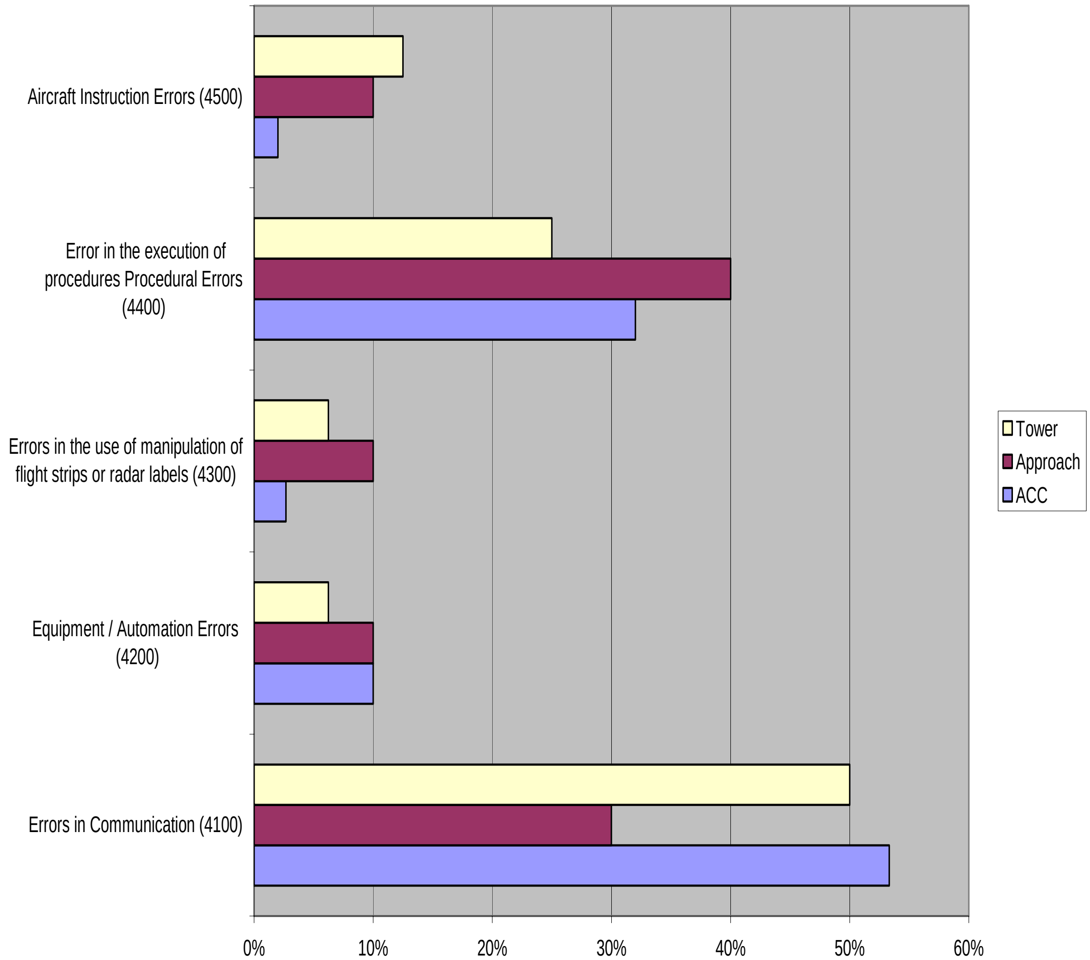

Figure 4: Error Type by ATC function expressed as a percentage

Table 11 shows the ten most frequent errors by ACC function. Whilst these are technically errors according to the NOSS taxonomy care must be taken in their interpretation. For example the code 'Non-Operational conversation which distracts from principal controller tasks' may technically be an error but in the context of the workload at the time, not troublesome. It is necessary to consider these errors in the context of the next section on error management to determine if these errors are consequential.

'Non-Operational conversation which distracts from principal controller tasks' (17% of errors in ACC), 'Correct procedure not used' (15% of errors in ACC) and 'Inappropriate coordination' (11% errors in ACC) are relatively frequent errors within the ACC environment. 'Inappropriate coordination' represents 20% of errors within Approach. 'Missed call' represents 31% of errors within Tower. Because these errors are relatively frequent, action might be taken to address these. However, care must be exercised in interpreting these results because of the relatively small sample sizes caused by the low number of observations.

Table 11: Ten most frequent Error Codes by ACC Function

ACC		Approach		Tower	
Error Code	Freq	Error Code	Freq	Error Code	Freq
Non-Operational conversation which distracts from principal controller tasks	25	Inappropriate coordination	2	Missed call	5
Correct procedure not used	23	Incorrect read back not detected	1	Correct procedure not used	3
Inappropriate coordination	17	Radar screen range selection	1	Taxi instruction error	2
Computer / Automation input error	11	Label/FPS manipulation	1	Non-standard phraseology	1
Reference document or checklist not used, equipment not checked	10	No / late issuance of heading restriction/ clearance	1	Incomplete or incorrect information/instruction passed	1
Incomplete or incorrect information/instruction passed	9	Early / Late transfer	1	Inappropriate coordination0	1
Missed call	8	Correct procedure not used	1	Computer / Automation input error	1
Inappropriate coordination	5	Prohibited clearance issued	1	No strip on board	1
Non-standard phraseology	4	Speed instruction error	1	No visual scan of airspace/runway/taxiway	1
Label/FPS manipulation	4	-	-		-

Mismanaged errors

Mismanaged errors are defined as: ‘errors that lead to a separate controller error or directly to an undesired state’. The total number of mismanaged errors was 9 out of 176 therefore the Error Mismanagement index is 5%, representing approximately 0.14 errors mismanaged per observation. This equates to nine mismanaged errors in 54 hours and 25 minutes or 0.16 mismanaged errors per hour.

The corollary of this is that the system is successfully managing 95% of all errors.

The percentage values shown Table 12 show the percentages of mismanaged errors out of the total number of errors observed (176).

Table 12: Mismanaged Error Types leading to additional error or undesired state

	ACC		Approach		Tower		
Error Type Mismanaged	Additional Error	Undesired State	Additional Error	Undesired State	Additional Error	Undesired State	Total
Errors in Communication (4100)	2	1	0	0	0	0	3 (2%)
Equipment / Automation Errors (4200)	0	0	0	0	0	0	0
Errors in the use of manipulation of flight strips or radar labels (4300)	0	0	0	0	0	0	0
Error in the execution of procedures Procedural Errors (4400)	3	1	0	0	0	0	4 (2%)
Aircraft Instruction Errors (4500)	0	0	0	1	0	1	2 (1%)
Total (9)	5	2	0	1	0	1	9 (5%)

Errors Types related to procedures represent the most frequent cause of error likely to lead to further errors or undesired states. The data suggest that errors, when they occur, are managed well throughout the organisation.

Errors (Level II) and their management

Table 13 shows the codes of the errors that were mismanaged. It is difficult to draw any conclusions from such a small sample of mismanaged errors. Again this is a limitation due to the number of observations carried out.

Table 13: Mismanaged Error Codes leading to additional error or undesired state

	ACC		Approach		Tower	
Error Code Mismanaged	Additional Error	Undesired State	Additional Error	Undesired State	Additional Error	Undesired State
(Non Operational Conversation (812)	1	1	0	0	0	0
Incomplete briefing or coordination (813)	1	0	0	0	0	0
Correct procedure not used (917)	3	1	0	0	0	0
Speed instruction error (953)	0	0	0	0	0	0
Taxi instruction error	0	0	0	0	0	0
Total (9)	5	2	0	1	0	1

Handover/Takeover - Opening and closing of position

The data in Table 14 shows that 26 errors were related to position relief and 3 were related to the opening/closing of a position. This represents 17% of all errors (176). Errors in communication would seem to be the biggest challenge facing controllers at handover. Detailed analysis has revealed that Error Code 813 (Incomplete Briefing) was associated with 13 of the 29 errors. This may have indications for looking at the ways in which briefings are conducted.

Table 14: Errors linked to position relief or opening/closing of position

Error Type	Position Relief	Opening/closing of Position
Errors in Communication (4100)	16	0
Equipment / Automation Errors (4200)	3	1
Errors in the use of manipulation of flight strips or radar labels (4300)	0	0
Error in the execution of procedures Procedural Errors (4400)	7	2
Aircraft Instruction Errors (4500)	0	0
Total 29	26	3

Error detection

Table 15 and Table 16 show the persons who appeared to detect each of the errors (where this could be determined). In some cases errors that are recorded as undetected ('Nobody' in table) may, in fact have been detected but ignored by the controllers as being insignificant, or missed by the observer. The tables show that: 96 (64%) of ACC errors, 6 (60%) of Approach errors and 7 (44%) of Tower errors appeared to go undetected. However, most errors are without consequence as seen from Table 12 and therefore may have been detected but simply evaluated and ignored. To understand further the nature of who detected which type of error refer to Table 17 which shows the position observed and who detected the error. Examination of this table indicates that the person most likely to detect an error made by the executive controller was the executive (Radar[10]) himself or herself.

[10] For Tower positions Radar means executive also.

Table 15: Error detection

ATC Function		Who detected error									
	Error Type	1 Nobody	2 Radar	3 Flight Data	5 Controller outside of sector	6 Pilot	7 Automated systems	8 Other	9 Planner	10. The controller observed	Total
ACC	Errors in Communication (4100)	59	14	0	0	0	1	0	5	0	79
	Equipment / Automation Errors (4200)	6	4	1	1	0	0	1	2	0	15
	Errors in the use of manipulation of flight strips or radar labels (4300)	0	2	0	0	0	1	1	0	0	4
	Error in the execution of procedures Procedural Errors (4400)	29	10	1	0	1	0	2	4	0	47
	Aircraft Instruction Errors (4500)	2	1	0	0	0	0	0	0	0	3
	Total	96	31	2	1	1	2	4	11	0	148
Approach	Errors in Communication (4100)	3	0	0	0	0	0	0	0	0	3
	Equipment / Automation Errors (4200)	1	0	0	0	0	0	0	0	0	1
	Errors in the use of manipulation of flight strips or radar labels (4300)	0	0	0	0	0	0	0	0	1	1
	Error in the execution of procedures Procedural Errors (4400)	2	1	0	0	1	0	0	0	0	4
	Aircraft Instruction Errors (4500)	0	1	0	0	0	0	0	0	0	1
	Total	6	2	0	0	1	0	0	0	1	10

Table 16: Error detection continued

ATC Function		Who detected error									
	Error Type	1 Nobody	2 Radar	3 Flight Data	5 Controller outside of sector	6 Pilot	7 Automated systems	8 Other	9 Planner	10. The controller observed	Total
Tower	Errors in Communication (4100)	2	0	0	0	1	0	5	0	0	8
	Equipment / Automation Errors (4200)	1	0	0	0	0	0	0	0	0	1
	Errors in the use of manipulation of flight strips or radar labels (4300)	0	0	0	0	0	0	1	0	0	1
	Error in the execution of procedures Procedural Errors (4400)	4	0	0	0	0	0	0	0	0	4
	Aircraft Instruction Errors (4500)	0	0	0	0	1	0	0	0	1	2
	Total	7	0	0	0	2	0	6	0	1	16

Table 17: Error detection by position observed

Position Observed	1 Nobody	2 Radar (EC)	3 Flight Data	5 Controller outside of sector	6 Pilot	7 Automated systems	8 Other	9 Planner (PLC)	10. The controller observed	Total
EC (Radar)	82	29	0	1	2	2	4	10	0	130
PLC (Planner)	20	5	2	0	0	0	0	1	0	28
Tower	5	0	0	0	1	0	2	0	0	8
GND	2	0	0	0	1	0	4	0	1	8
Total	109	34	2	1	4	2	10	11	1	174

Error results summary

The most frequently occurring errors are errors related to communication (52%) followed by errors related to procedures (32%).

Only 5% of errors are mismanaged.

Many errors that are made appear to go undetected or are otherwise ignored as being inconsequential. The NOSS process is not able to demonstrate which is the case as it is a behavioural observation tool only and not able to comment on what controllers' are thinking.

Errors in communication would seem to be the biggest challenge facing controllers at handover. Detailed analysis has revealed that Error Code 813 (Incomplete Briefing) was associated with 13 of the 29 errors related to Handover/Opening and closing of position. This may have indications for looking at the ways in which briefings are conducted.

Seventeen percent of errors were related to position relief or opening/closing of a position.

Areas for more detailed scrutiny include:

- A detailed analysis of the nature of the communication errors and errors related to procedures is indicated, the narrative reports that can provide an overview of these are available on separate CD.
- The execution of procedures and communication during position relief (handover) might be examined.

The following errors were relatively high in frequency and might be a target for intervention:

- 'Non-Operational conversation which distracts from principal controller tasks', 'Correct procedure not used' and 'Inappropriate coordination' within ACC.
- 'Inappropriate coordination' within Approach.
- Missed call', 'Correct procedure not used', within Tower.
- Subsequent NOSS studies should compare trends in the threat codes used.

Section 6: Undesired States in FINAVIA

Undesired States taxonomy

Under the NOSS framework an undesired state is defined as: 'operational conditions where an unintended traffic situation results in a reduction in margins of safety'. This section will draw together the information on undesired states placing them in the context of the threats and errors contributing to their development. This is important because the absolute frequency of threats and errors alone tells us merely how often they occur but not how much relevance they have to safety.

Undesired State profile

Definitions

- Undesired States: Operational conditions where an unintended traffic situation results in a reduction in margins of safety.

- Mismanaged Undesired State: An undesired state that is linked to or induces an additional error or an undesired state.
- Undesired State Prevalence Index: The percentage of observations with one or more undesired states.
- Undesired State Mismanagement Index: The percentage of undesired states that were mismanaged.

NOSS observers recorded the undesired state events and documented how the controller handled them. The information obtained from this process has been coded and provides an undesired state profile for the area of the organisation being observed (ACC, Tower or Approach). This profile contains two main types of information:

1) The undesired state prevalence or frequency at which the undesired state was observed, and
2) Whether the undesired state was managed or not.

Mismanagement of an undesired state is defined by whether the undesired state leads to separate controller errors. Mismanagement does not imply the controller was at fault in anyway but simply that the system failed to optimally manage the undesired state.

Undesired states were observed during 17 out of 63 observations; therefore the Undesired State Prevalence Index is 27%. This equates to approximately one undesired state per three hours of NOSS observation.

Table 18 shows the breakdown of Undesired States codes. In only one instance did an undesired state lead to a further ´forced´ error therefore the Undesired State Mismanagement Index was 4 % (1 out of 26) undesired states. The Undesired State code ‘Lack of Separation Assurance’ occurs on five occasions, one of which was directly linked to a threat and another directly linked to an error. This code is closely related to seven other instances of similar undesired states related to separation and identified in the ACC environment see the frequencies highlighted in red font in Table 18 (‘Deviation from route clearance’, ‘Airspace penetration’ and ‘Restricted airspace not protected´). This may indicate a problem in maintaining separation and should certainly be monitored.

The Tower environment contributes a relatively large number of undesired states for to the number of observations made in this environment, traffic congestion on the taxiway would appear to be a particular problem. However, care must be exercised in drawing conclusions due to the small number of undesired states observed in total.

On no occasion did an undesired state compromise safety or result in a reportable event. If this had happened the NOSS observation would have stopped.

Table 18: Undesired States

Undesired State	ACC	Approach	Tower
Inaccurate representation of traffic (1)	1	0	0
Unable to effectively monitor traffic on ground (8)	0	1	1
Incomplete HO / TO (2)	1	0	0
Traffic situation not being monitored (3)	1	0	0
Equipment failure (5)	1	0	0
Lack of separation assurance (50)	2	2 *	1
Deviation from route clearance (51)	4	0	0
RWY/TWY not verified to be clear for progress (53)	0	1	1
Airspace penetration (54)	2	0	0
Restricted airspace not protected (55)	1	0	0
Frequency congestion (56)	0	0	1
Aircraft is lined up on wrong runway/ wrong position (57)	0	0	2
Traffic congestion due to blocked taxi (58)	0	0	3
Total 26	13	4	9

* In one instance the Undesired State was mismanaged leading to a further error: 'No Conflict Check', (902)

Undesired State detection

Table 19 shows the persons who appeared to detect each of the undesired states where this could be determined. In some cases undesired states that are coded as undetected ('Nobody' in table) may, in fact have been detected but ignored by the controllers or missed by the observer.

The table shows that: 24 out of 26 (92%) of undesired states were detected by the system and as stated previously only one lead to an additional controller error. Indicating that, undesired states, when they occur, are generally well managed. Of course it is a rule of NOSS that if an event develops into a reportable incident the recording stops. The executive position (radar[11]) is the position most likely to detect the undesired state.

[11] For Tower positions Radar means executive also.

Table 19: Undesired State detection

		Who detected						
	Undesired State Type	1 Nobody	2 Radar	4 Supervisor	6 Pilot	8 Other	10. The controller observed	Total
ACC	Inaccurate representation of traffic (1)	0	0	1	0	0	0	1
	Incomplete HO / TO (2)	1	0	0	0	0	0	1
	Traffic situation not being monitored (3)	1	0	0	0	0	0	1
	Equipment failure (5)	1	0	0	0	0	0	1
	Lack of separation assurance (50)	0	2	0	0	0	0	2
	Deviation from route clearance (51)	0	4	0	0	0	0	4
	Airspace penetration (54)	0	2	0	0	0	0	2
	Restricted airspace not protected (55)	0	1	0	0	0	0	1
Total		3	9	1	0	0	0	13
Approach	Unable to effectively monitor traffic on ground (8)	0	0	0	0	1	0	1
	Lack of separation assurance (50)	0	2	0	0	0	0	2
	RWY/TWY not verified to be clear for progress (53)	0	0	0	0	1	0	1
Total		0	2	0	0	2	0	4
Tower	RWY/TWY not verified to be clear for progress (53)	1	0	0	0	1	0	1
	Frequency congestion (56)	0	0	0	0	1	0	1
	Aircraft is lined up on wrong runway/wrong position (57)	0	0	0	1	0	1	2
	Traffic congestion due to blocked taxi (58)	0	0	0	0	1	2	3
Total		0	0	0	1	3	3	7
Grand Total		3	11	1	1	5	3	24

Detailed analysis of selected Undesired States

This sub-section of the report presents in detail some of the undesired states that were coded during the NOSS trial. For details on other undesired states it is necessary to refer to the narratives and the data file available on a separate CD.

NOSS observation number A7

This is an example of a threat leading directly to an undesired state. The threat code causing the undesired state was 302, 'Taxi runway configuration'.

Undesired State description There are 25 runway crossings. 13 of these take place in front of landing aircraft, which has less than one minute to go over threshold. 7 crossings need to be ordered specifically to expedite. Accordingly there are several late landing clearances.	Undesired State Code 50 Lack of separation assurance	Controller used conditional crossing clearances as often as possible and few times advised arriving aircraft to expect late landing clearance. Mostly arriving aircraft are spaced well over 3 NM minima (practically 4-5 NM in final).

NOSS observation number B 9

This is an example of an error leading to an undesired state.

Error description FIN482 speed is reduced to 210 knots. The proceeding aircraft is very slow, so FIN482 speed should have been reduced more.	Error code 953 Speed instruction error	-
Undesired State description ARR says to FIN482: "you are 4 miles behind proceeding and 100 knots faster. Reduce to final approach speed."	US Code 50 Lack of separation assurance	RR calls to TWRE and asks whether he's able to see the arriving planes, so that there's no need for 3NM separation anymore. TWRE says that he sees both arriving aircraft, so the situation is ok.

NOSS observation number A 5

This is an example of a threat leading to an error then undesired state.

Threat description Blocked transmission in critical phase	Threat code 636 Blocked frequency	Unable to respond due to other tasks
Error description Controller fails to note the correct runway for departing flight and clears aircraft mistakenly to line up instead of crossing rwy.	Error code 960 Taxi instruction error	-
US description Aircraft is lining up wrong runway instead crossing it	US code 57 Aircraft is lined up on wrong runway/ aircraft in wrong position on runway/taxiway.	Controller managed to re clear crossing of a runway, just before aircraft turned to line up

NOSS observation number B 4

This is an example of a threat leading directly to an undesired state (arguably the threat need not have been coded as in E5 below).

Threat description Landed FIN334 vacates from the intersection ZG without clearance to do that, it's forbidden to vacate from it without permission.	Threat code 523 Non compliance with local procedure	TWR shouts to GND: "It didn't have permission to do that!" Luckily there was no incoming traffic to that intersection.
US description Landed FIN334 vacates from the intersection ZG without clearance to do that, it's forbidden to vacate from it without permission.	US code 57 Aircraft is lined up on wrong runway/ aircraft in wrong position on runway/taxiway.	No outcome

NOSS observation number E 5

This is an example where an undesired state was coded but no threat or error.

US description Russian military flying without ref to ACC in controlled airspace	Undesired State code 54 Airspace penetration	No outcome

NOSS observation number D 5

This is an example where an undesired state was coded but no threat or error.

US description GAO063T avoiding weather, heading towards active danger area.	US code 55 Restricted airspace not protected	Flight was cleared above weather

Undesired State results summary

Twenty-six undesired states were coded during the NOSS observation. The Tower environment accounted for a greater number of these than one would have expected based on the proportion of observations made in this environment. The small numbers of undesired states observed is encouraging as these represent some of the precursors to reportable events. However there are two features in the undesired sate data that should be highlighted. Eleven undesired states relate to some form of reduction in safety in relation to airborne separation.

Potential areas for future intervention

- Investigation of the issue of traffic congestion on the taxiway and possible solutions might be indicated.
- The undesired states contained in the narratives should be reviewed by the safety team/manager. These are available on separate CD.
- Subsequent NOSS studies should compare trends in the undesired state codes used.

Section 7: Identified good practices

The NOSS form used in this trial did not have a specific section to identify good practices that were observed. This should be considered for inclusion in future trials. It is not so easy to identify from the narratives, after the event, what represents a good practice. It is much easier for an observer to identify a good practice at the time of observation, when they have the full context of the event. Thus the NOSS form could usefully have a section for this that the observer could use at the time of writing up his/her report. Identified good practices could then be shared throughout the organisation.

The following represent good practices identified during data cleaning. There were probably more but these were not specifically identified.

Helsinki

"There are two runway crossings (via ZD and Y) and one intersection departure (ZG) at the same time. As ZG departing ATR is starting its take-off, second aircraft is cleared to cross runway. Controller did not specify this time the crossing intersection, which could alarm pilots in ATR as they are just departing. Generally controllers would be expected to specify intersection this represents a good practice."

"Updating the SMR display for departing flights by dragging identification from list to targets needs focusing and distracts from other more essential duties. Good practice to be able to do this is one has the time."

"The handover is dealt very well, all the affecting things are mentioned and the previous controller stays a while afterwards and asks then whether it's ok for him to leave."

Tampere

"Active use of dynamic short cuts at appropriate time to facilitate the traffic flow. For example, when military airspace became available, short cuts were issued in accordance with procedure. At times of high workload however, this is not an appropriate action."

Section 8: Threat and Error countermeasure markers

Table 20 shows the result of the ratings for performance made by the NOSS observers.

Scores were assigned to each countermeasure according to the following scale.

1	2	3	4
Poor	Marginal	Good	Outstanding
Observed performance had safety implications	Observed performance was barely adequate	Observed performance was effective	Observed performance was truly noteworthy

Countermeasures Markers that score less than 2 on average may represent a cause for concern as this represents Poor to Marginal performance. Scores of 3 or above are preferable as these indicate Good to Outstanding performance.

It can be seen from Table 20 that the countermeasure scanning received an average rating of 3.13, the highest value, whilst countermeasures related to 'Pre take over preparation' and 'Post Handover Support' scored the lowest at 2.79 and 2.86 respectively.

N.B. The results in Table 20 should be treated with extreme caution. The Countermeasure Marker Tool was included in the NOSS trial so that an impression of its utility could be investigated. The utility has not been supported by this initial trial and the author considers this part of the NOSS data collection tool as the least useful and perhaps the least reliable data source within the NOSS measure. It has not been psychometrically validated and suffers a number of shortcomings that are beyond the scope of this report. Additionally, there are no absolute reference points from which observers can make their judgements and the results provide very little information about how things are managed compared with what is available within the narrative reports and other NOSS data.

Table 20: Countermeasure markers

Countermeasure marker	Number of NOSS observations were rating was obtained	Minimum	Maximum	Mean	Std. Deviation
Pre Take over prep	52	1	4	2.79	0.595
Briefing	56	2	4	2.89	0.478
Plans started	60	2	4	3.00	0.504
Monitor Cross Check	61	2	4	3.05	0.574
Scanning	61	2	4	3.13	0.543
Workload Mngt	60	2	4	3.00	0.552
Equip/Automa Mgnt	58	2	4	2.91	0.431
Flight Strip Mngt	29	2	4	3.03	0.325
Adaptability	55	2	4	3.00	0.272
Post Handover Supp	49	2	4	2.86	0.500
Evaluation of Plans	53	2	4	3.00	0.277
Inquiry	54	2	4	3.04	0.272
Contingency Mngt	61	2	5	3.02	0.428
Route Consistency	48	2	3	2.98	0.144

Section 9: Lessons learnt from this trial and feedback from NOSS observers

An abridged version of the feedback provided orally by observers and from the feedback form provided, is summarised under the various following sub-headings.

General Comments

One observer commented about the very positive reception of the NOSS trial by employees in the organisation. The NOSS observers seemed very engaged and enthusiastic about the process and the potential value of NOSS. Three of the six observers even volunteered to do extra recordings to increase the sample size.

NOSS was well received by the workforce. No refusals were received from persons approached to be observed though one person indicated they did not wish to be observed prior to being approached. The marketing of NOSS was fairly intense, probably more so than other projects according to one observer.

Narratives were felt to be most useful at providing information. It was suggested that some sort of qualitative analysis of this data be might a good idea to draw out themes. Software could be sourced to do this in future.

Observation methods were considered clear and it was quite easy to detect threats and errors.

Language

English was not the first language for the participant NOSS observers in this trial. This did not present too much of a challenge for those concerned as the level of conversational English within this group was high. However, one comment made was that perhaps the narratives might be more useful if they could be written in the native tongue of the participants. This has implications for external support, coding and comparisons that might be made if benchmarking were to be considered across providers.

The taxonomy

Controllers did not like many of the codes available for the coding of events; many were not really appropriate to their setting. In addition many were considered ambiguous and could be interpreted in a variety of ways.

New Threat codes were introduced but the codes still require further expansion. For example new code 917, ‘Correct procedure not used’ could be usefully expanded into a number of other codes reflecting the type of procedure that was broken. This would require further work at a local level.

The Undesired States codes came under particular criticism. Many were not relevant and unclear. Codes that would have been useful did not exist. For example, CONGESTION ON THE GROUND FREQUENCY was considered an undesired state in the tower environment.

The Undesired State codes that had some value were very close to what this organisation considered a reportable event, technically this would end some NOSS observations even though safety was not significantly compromised. The question was asked, do we need these Undesired State codes?

The 'Who Detected' section of the form had some omissions that were corrected for this trial. This section should record if the observed person picked up their own error or if some other person did and, if so, who. Additionally, the ‘Who Detected’ sections could usefully apply to threats, errors and undesired states equally. This section of the coding needs to be simplified and customised to the local environment.

The layout of the form could be streamlined in places to make it easier to fill out and to aid data processing. The possibility of electronic data collection might be considered using appropriate technology such as a Palm Pilot.

Tower and Approach

Different working positions require different codes. Many of the codes were not relevant to ground operations according to the NOSS observers, and new codes were introduced.

ACC

Generally codes seemed more appropriate and easier to use. This was a strip-less environment; the codes had been developed in such an environment.

Philosophy on errors

Controllers did not always follow best working practices but they could not be coded as an error under NOSS because such instances were not against a published procedure.

A suggestion was made that code books are produced dedicated to the different environments: Tower, Approach and ACC.

The suggestion was made that the section of form entitled 'Traffic Picture As Observation Begins' is modified to capture the same information each time for each observations. For example: Weather, Traffic Load, Experience of controller, Activity in other sector airspace etc.

Comment on potential benchmarking

Given the challenges that coding presented it is likely that operators will want to use codes that a meaningful at a local level. This represents a challenge for benchmarking if this is envisaged for the future.

Countermeasure markers

The NOSS observers found this part of the tool a little too subjective and the countermeasures listed not intuitively the best ones. The data provided by this part of the tool might be useful where a large variation in scores between subsequent NOSS trials is observed on one or more of the countermeasures but this has yet to be proven.

Good Practices

The ability of NOSS to capture good practices was felt to be limited. A request was made for NOSS to log good practices directly from narratives. A space for this could be created on the form.

Section 10: Closing Comments

The preceding sections have described the data obtained from the NOSS trial conducted in FINAVIA and where appropriate some discussion and conclusions have been mentioned, within the relevant section, based on this data.

The utility of the NOSS approach has been demonstrated and the data generated, whilst limited by the number of observations made, is encouraging. Refinements to the NOSS tool (observation form) and methodology were made through the course of the trial as local demands required. It is likely that further customisation and refinements will be required the when the NOSS method is applied in other settings.

The real strength of NOSS is in repeating the process over time using the same methodology and codes. In this way trends in the data should indicate if the organisation is moving in a direction that exposes it to a greater safety risk. For example, if subsequent data indicated that an increase in the frequency of the undesired state 'Traffic congestion due to blocked taxiway' then action might be taken to resolve this issue.

Appendices

Appendix 1: Threat Frequency,

To interpret these codes use Appendix 4.

ACC		Approach		Tower	
Threat Code	Frequency	Threat Code	Frequency	Threat Code	Frequency
100.00	2	104.00	1	100.00	1
106.00	1	108.00	1	101.00	1
108.00	2	110.00	2	102.00	1
109.00	6	116.00	1	104.00	1
110.00	5	117.00	1	109.00	2
112.00	9	150.00	2	110.00	4
115.00	1	152.00	3	117.00	3
117.00	1	160.00	1	150.00	3
150.00	61	200.00	1	151.00	1
151.00	3	205.00	6	152.00	1
152.00	8	206.00	1	153.00	7
154.00	1	208.00	1	155.00	1
157.10	1	209.00	2	158.00	1
160.00	4	210.00	3	200.00	1
161.00	3	211.00	1	202.00	1
162.00	7	258.00	4	204.00	1
200.00	4	259.00	3	205.00	8
204.00	5	302.00	1	206.00	3
205.00	29	352.00	3	208.00	1
206.00	8	353.00	2	209.00	2
207.00	5	406.00	3	210.00	2
208.00	4	502.00	2	258.00	1
209.00	1	505.00	1	260.00	3
210.00	8	519.00	2	302.00	11
211.00	2	520.00	2	303.00	1
212.00	24	522.00	1	304.00	1
255.00	1	523.00	1	305.00	10
256.00	2	630.00	4	353.00	1
258.00	5	633.00	1	450.00	1
259.00	2	634.00	2	505.00	4
261.00	1	635.00	3	510.00	3

350.00	1	637.00	2	519.00	8
353.00	2	639.00	1	520.00	2
404.00	4	655.00	1	522.00	3
406.00	11	700.00	2	523.00	7
409.00	1	Total	68	630.00	1
500.00	1			631.00	2
506.00	2			635.00	18
507.00	2			636.00	1
510.00	1			638.00	2
518.00	2			653.00	1
519.00	4			704.00	1
520.00	1			Total	128
522.00	4				
523.00	1				
630.00	13				
631.00	2				
632.00	3				
633.00	2				
634.00	13				
635.00	6				
636.00	1				
637.00	1				
638.00	3				
639.00	1				
650.00	1				
651.00	1				
654.00	2				
655.00	2				
657.00	2				
660.00	2				
700.00	2				
701.00	4				
707.00	1				
Total	315				

Appendix 2: Threat Type frequency as percentage

	ACC %	Approach %	Tower %
Equipment Threats (1100)	13	10	10
Workspace/Materials Threats (1200)	23	7	11
Other controller / Flight Data (1300)	29	22	15
Operational Performance Threats (1400)	3	10	3
Airport Layout (1500)	0	1	18
Airspace Infrastructure/Design (1600)	1	7	1
External or Foreign Service Providers (1700)	5	4	0
Ground Traffic (1750)	0	0	1
Aircraft Pilot Issue (1800)	6	13	21
R / T Communication (1900)	14	19	19
Traffic (2000)	3	1	1
Weather Threats (2100)	2	3	1
	100	100	100

Appendix 3: Error Codes

To interpret these codes use Appendix 4.

Error Code	Frequency
801	1
803	2
804	5
805	13
806	1
807	3
808	3
809	10
810	6
812	25
813	17
817	5
850	12
851	2
852	3
870	5
875	1
902	3
905	1
906	3
907	1
909	10
910	1
911	4
912	1
917	27
918	1
919	2
921	2
953	1
955	1
956	1
960	2
961	1
Total	176

Appendix 4: Amended NOSS Radar, Tower & Approach Observation Form

Observer Information

Observer ID		**How many times have you observed this group?**	
Overall, how many observations have you conducted prior to this one?			

Observation Demographics

Radar /Tower App; indicate which		**Position Observed**		**Day of week**	
Observation Start Time (HH:MM) UTC		**End Time (HH:MM) UTC**			

Team Composition: What other positions are staffed?

Team Position

Traffic Picture as the Observation Begins

Narrative	Your Narrative should provide a context. Describe the traffic picture as you begin your observation. This description should provide a snapshot of the traffic flow and complexity.

The Story of the Observation

Narrative	Your Narrative should provide a context. Describe how the traffic flow changes during the course of the observation. What challenges had to be met? How did the controller/team manage threats, errors, and undesired states? How did the team/controller interact with: a) pilots b) other controllers c) their equipment? What did the team / controller do well? What did the team / controller do poorly? Also, be sure to justify your countermeasure markers. As you write your narrative remember to record the time stamp of each event (thing you observer) and when it represents a threat, error undesired state or countermeasure, for example 5T—13:40:28 is the 5th threat at time 13:40:28.

Position Relief

Narrative	Your narrative should provide a context. How did the controller prepare for the handover? Did the controller stay around the vicinity after unplugging? Were pertinent materials reviewed prior to handover? Were relevant issues covered in the brief? How did the controller get adjusted to the traffic situation? Also, be sure to justify your countermeasure markers. Record any threats / errors etc. associated with position relief or the opening/closing of a position. Use the same time stamp and code taken from the Narrative.		
Briefing #1	**Briefing Time Stamp**		
Briefing #2	**Briefing Time Stamp**		
Briefing #3	**Briefing Time Stamp**		

Overall Impressions

Use this section to provide an overall impression of what you observed and to raise issues that you consider the data cleaning team should consider. For example a threat or error that does not have an appropriate code.

Threat Management Worksheet

Threat Description						Threat Management
T ID	**Describe the threat**	**Threat code (See codebook)**	**Time Stamp (HH:MM) UTC**	**Link to Position Relief or opening / closing of position?** 1 No link 2 Position Relief 3 Opening 4 Closing	**Threat Outcome** 1 Inconsequential 2 Linked to Error 3 linked directly to US	**How did ATCO manage the threat?**
T1						
T2						
T3						
T4						
Threat Codes: See the NOSS Codebook for Threat Codes						

Error Management Worksheet

Error Description						Error Outcome		Error Management
E ID	**Describe the controller error**	**Error Code (See Code-book)**	**Time Stamp HH:MM UTC**	**Link to Position Relief or opening / closing of position?** 1 No link 2 Position Relief 3 Opening 4 Closing	**Link to threat? (if yes, enter threat ID)**	**Who detected error?** 1 Nobody 2 Radar 3 Flight Data 4 Supervisor 5 Controller outside of sector 6 Pilot 7 Automated systems 8 Other 9 Planner 10. The controller observed	**Error Outcome** 1 Inconsequential 2 Additional Error 3 Undesired State	**How did ATCO manage the error?**
E1								
E2								
E3								
Error Codes: See the NOSS Codebook for Error Codes								

Undesired State Management Worksheet

Undesired State Description					Undesired State response / outcome		Undesired State Management
US ID	**Describe the US**	**US Code**	**Error Link**	**Time Stamp HH:MM UTC**	**Who detected US?** 1 Nobody 2 Radar 3 Flight Data 4 Supervisor 5 Controller outside of Sector 6 Pilot 7 Automated systems 8 Other 9 Planner 10. The controller observed	**US Outcome** 1 Inconsequential 2 Additional Error	**How was the undesired state managed?**
US 1							
US 2							
US 3							
Undesired State Codes: See the NOSS Codebook for Undesired State Codes							

Threat and Error Countermeasures (one per observation)

1	2	3	4
Poor Observed performance had safety implications	**Marginal** Observed performance was barely adequate	**Good** Observed performance was effective	**Outstanding** Observed performance was truly noteworthy

			Rating
Pre-Takeover Preparation	Relevant materials were referenced prior to taking over a position.	*- Weather forecast reviewed* *- Operationally relevant materials reviewed*	
Briefing	Operationally thorough briefings were conducted.	*- Temporary agreements are briefed* *- Pending tasks are addressed*	
Plans Stated	Operational plans and decisions are acknowledged and communicated to other parties (e.g. other controllers, pilots)	*- Controllers communicate plans and decisions to other parties who may be affected*	
Monitor / Cross-Check	Controllers actively monitor and cross-check other controllers and pilots	*- Controllers monitor the work of other parties to detect threats to safety*	
Scanning	Controllers members utilize available resources to ensure traffic is conflict free and where it is intended to be	*- Radar monitored to verify aircraft parameters* *- Aircraft location compared to FPS*	
Workload Management	Operational tasks are prioritized and properly managed to handle primary ATC duties	*- Controller did not become fixated on tasks* *- Opening and closing of positions suitably handled.*	
Equipment / Automation Management	Equipment / Automation is properly managed to balance operational and / or workload requirements.	*- Automation setup was effective* *- Effective recovery techniques from anomalies*	
Flight Strip Management	Flight strips are properly organized and updated to keep track of traffic developments	*- Strips are promptly updated after issuing instructions* *- Strips are kept in appropriate order*	
Adaptability	Controller is able to recognize and adapt to changing conditions	*- News plans effectively executed when old plans are recognized to no longer be appropriate*	
Post - Handover Support	Support provided to new controller after transfer of responsibility has occurred.	*- Relieved controller monitors new controller to ensure smooth transfer*	
Evaluation of Plans	Existing plans are reviewed and modified when necessary	*- Decisions and actions were analyzed to make sure the existing plan was the best plan*	
Inquiry	Controllers are not afraid to ask questions to investigate and / or clarify current plans of action	*- Nothing taken for granted* *- Ambiguous statements / information investigated*	
Contingency management	Controller develops effective strategies to manage threats to safety	*- Problems and their consequences are anticipated* *- Uses all, Level of available resources to manage problems*	
Route consistency	Controller attempts to keep aircraft on their filed route when appropriate	*- Controller tries to avoid switching runway on descent* *- Controller tries to avoid taking aircraft of filed route for non operational matters*	

Threat Codebook

Air Traffic Service Provider Internal Threats (3500)							
Equipment Threats (1100)		Workspace / Materials Threats (1200)		Other controller / Flight Data (1300)		Operational Performance Threats (1400)	
100	Maintenance	150	Noise	200	Non-standard phraseology by other controller / flight data	250	Flow control command
101	Radios	151	Difficult to access reference materials	201	Readback Error by other controller / flight data	251	Combined sectors
102	Telephones	152	Visitors	202	Communication difficulty	252	Combining sectors
103	RSiT event Radar event	153	Poor Sight Lines	203	Communication channel used by other controller / flight data	253	De-combining sectors
104	RSiT Display Radar Display	154	Lighting	204	Controller System Input	254	Automated handoff failure
105	Radar coverage	155	Chart error	205	Controller distraction	255	STAR clearance variation
106	Frequency coverage	156	Manual error	206	Coordination Issue	256	Non-Standard, Level
107	Multiple input devices	157.1	Procedure not followed	207	Radar / Data controller interaction	257	Non-standard hold
108	Screen Clutter	157.2	Procedure correctly executed but not adequate	208	Supervisory action	999	Other
109	Unserviceable equip.	157.3	Procedure not correctly executed and not adequate.	209	AC transfer issue what is meant by this code?	258	Aircraft in conflict
110	Data Incongruence	158	Sun	210	Unspecified threat induced by other controller	259	High workload
		159	Windows (cleaning/spots)	211	Poor handover	260	Aircraft in conflict on ground
111	New Software/Equip.	999	Other	212	Correct procedure not used or non standard procedure used	261	Lack of knowledge
112	False conflict alert alarm						
113	AC Not identifying						
114	Equipment checks does this mean target of obs **did not check equipment**	163	No official procedure available				
115	Communication Interference						
116	Information missing from strip”						
117	Equipment difficult to use						
160 (could recode as 117.1)	Automation failure						
161 (could recode	Alert failure (MTCD etc)						

as 117.2)	
162 (could recode as 117.3	Lack of appropriate automation/equipment/software.

Air Traffic Service Provider External Threats (3600)					
Airport Layout (1500)		Airspace Infrastructure/Design (1600)		External or Foreign Service Providers (1700)	
300	Construction	350	Traffic load	400	Ex: N.S. phraseology
301	Runway contamination	351	Traffic mix (IFR/VFR, AC type)	401	Ex: Readback error
302	Runway/Taxiway configuration	352	Airspace design	402	Ex: Communication Difficulty
303	Poor signage	353	Restricted Airspace	403	Ex: Communication channel used
304	Change in active RWY	354	Nav Aid Maintenance	404	Ex: Controller system input
305	Blocked taxiway/stand	355	Nav Aid Reliability	406	Ex: Coordination issue
999	Other	999	Other	409	Ex: A/C transfer issue
				410	
Ground traffic					
450	Vehicle calls on wrong frequency				

Airborne Threats (3700)					
Aircraft Pilot Issue (1800)		R / T Communication (1900)		Traffic (2000)	
500	Flight plan – ATS system incongruence	630	Readback Error	650	Priority flight / VIP's
501	Heading Deviation	631	Non-standard phraseology	651	Military activity
502	Speed deviation	632	Language difficulty	652	Parachute activity
503	Altitude deviation	633	Similar call signs	653	Complex Sequencing Issue
504	Combo speed /altitude/heading deviation	634	Flight crew failure to respond to call	654	Non RVSM a/c in RVSM airspace
505	Slow to comply with command	635	Frequency congestion	655	Pop-up flight
506	Flight crew failure to report	636	Blocked frequency	656	Formation flight
507	Routing deviation	637	Clipped Transmission	657	Survey Flight
508	AC malfunction	638	Pilot communication difficulty	658	Training Flight
509	Rate of climb / descent	639	Pilot use of incorrect call sign	659	Minimum fuel
510	Pilot non-compliance w/ instruction	999	Other	660	Increasing traffic load
511	Closing speeds				
512	Emergency				

514	Airline Procedure		
515	Diversions		
516	Non-active RWY request		
517	Non-standard AC profile		
518	Airspace penetration		
519	Pilot request		
520	Other pilot error		
521	Uncorrelated target in class A airspace		
522	Aircraft calls on wrong frequency		
523	Non compliance with local procedure		
999	Other		

Environmental Threats (3800)			
Weather Threats (2100)		**Geographical Environment (2200)**	
700	Thunderstorms with turbulence	750	Terrain
701	Turbulence only	751	Obstacles
702	Icing	752	Noise abatement
703	Wind shear	999	Other
704	Winds (crosswind, tailwind, headwind)		
705	Visibility		
706	Cloudbase		
707	Combination / multiple weather threats		
999	Other		

Error Codebook

Errors in the execution of communication Communication Errors (4100)			
800	Incorrect readback given	810	No coordination
801	Incorrect readback not detected	811	A/C Transfer
802	Full readback not obtained	812	Non-Operational conversation which distracts from principal controller tasks
803	Wrong call sign used	813	Incomplete briefing or coordination
804	Non-standard phraseology	814	A/C type omitted in initial call
805	Missed call	815	Callsign omission
806	Late coordination	816	Clipped frequency
807	Incomplete / Inaccurate information given during coordination	817	Inappropriate coordination
808	Did not pass information (traffic, terrain, etc)	818	Frequency change error
809	Incomplete or incorrect information/instruction passed	999	Other

Equipment / Automation Errors Errors in the operation of equipment of automation (4200)			
850	Computer / Automation input error	854	Data tag incomplete/inaccurate information
851	Incomplete / Inaccurate info display	855	VSCS manipulation error
852	Radar screen range selection	999	Other
853	Aircraft label obscured information	856	

Flight Data Progress Strip Errors Errors in the use of manipulation of flight strips or radar labels (4300)			
870	Label/FPS manipulation	876	Flight Data Board out of sequence
871	Label/FPS marking error	877	No attitude written on strip
872	Assigned speed not noted on strip	878	Coordination not indicated on strip
873	Combined strip writing / manipulation	879	A/C verified, Level, not marked on strip
874	Times not written on strips	880	Strip not indicating required action
875	No strip on board	999	Other

Error in the execution of procedures Procedural Errors (4400)			
902	No conflict check	911	Early / Late transfer
903	No visual scan of RWY before takeoff clearance	912	No visual scan of radar
904	No / late response to alarms	913	No, Level verification
905	No / late issuance of speed restriction/clearance	914	No Identification of AC
906	No / late issuance of altitude restriction/ clearance	915	Wake turbulence application
907	No / late issuance of heading restriction/ clearance	916	Did not open position
908	Recorded line not used	999	Other
909	Reference document or checklist not used, equipment not checked	917 new code	Correct procedure not use
910	Flight plan not updated	918 new code	No visual scan of airspace/runway/taxiway
919	Prohibited clearance issued	922 new code	Procedure correctly executed but not adequate
		920 new code	Procedure not correctly executed and not adequate.
		921	Lack of knowledge

Aircraft Instruction Errors (4500)			
950	Late Descent	958	Inappropriate accommodation of request
951	Late Change	959	Incorrect joining instruction
952	Altitude instruction error	960	Taxi instruction error
953	Speed instruction error	961	Sequencing judgment error
954	Transponder/Altimeter instruction	962	MVA issued to A/C not on vectors
955	Heading instruction error	963	Radar services not terminated
956	Hold instruction error	999	Other
957	Clearance instruction error		

Undesired State Codebook

Controller Position Undesired States		Traffic Undesired States	
1	Inaccurate representation of traffic	50	Lack of separation assurance This is vague!!! Does it mean practical separation (keeping aircraft apart) or controller defined separation according to ICAO
2	Incomplete HO / TO	51	Deviation from route clearance
3	Traffic situation not being monitored	52	AC on incorrect frequency
4	Position not opened	53	RWY/TWY not verified to be clear for progress
5	Equipment failure	54	Airspace penetration
6	Unauthorized provision of services	55	Restricted airspace not protected
7	Incomplete coordination	99	Other
8	Unable to effectively monitor traffic on ground	56	Frequency congestion
99	Other	57	Aircraft is lined up on wrong runway/ aircraft in wrong position on runway/taxiway.
		58	Traffic congestion due to blocked taxi way leading to compromised safety and traffic flow problems.

- Threats: Events or errors that occur beyond the influence of the air traffic controller, increase operational complexity, and which must be managed to maintain the margins of safety.
- Errors: Actions or inactions by the air traffic controller that lead to deviations from organisational or controller intentions or expectations.
- Undesired States: operational conditions where an unintended traffic situation results in a reduction in margins of safety.

Appendix 5: NOSS observer feedback form

A) Think back to the introduction of NOSS into the organisation

1. **How well was the idea for NOSS communicated to the workforce? What was good about this? What could be improved?**

2. **Do you think enough was done to prepare the workforce for NOSS**

B) Think about the training you received as a NOSS observer

3. **Was there anything you found particularly useful in the training?**

4. **What would you improve in NOSS training?**

5. **Is there anything you would omit from the training you received?**

<u>C) Think back to your experience of taking part in the NOSS observations.</u>

6. **How did you find the NOSS process generally, any problems in observing, writing narrative, coding etc.**

7. **Was the support provided to you by the local coordinators (Kimmo Koivula, Erik Berg, Ian Patterson) good enough, how could it be improved?**

8. **Is there anything you would change in the way a NOSS is run?**

9. **Is there anything you would change on the NOSS forms?**

10. **Did you have any other difficulties in running the NOSS observations?**

11. **To what extent did the observational methods used in NOSS allow you to detect and understand the threats and errors occurring?**

12. **How were the threat and error codes what might be done to improve them?**

13. **Can you think of anything that you would change in the NOSS method to improve the quality of the data?**

We value any other comments you would like to make below. Thank you for helping!!
Ian Patterson (NOSS project manager)

Your observer ID _______________(OPTIONAL)

Appendix 6: Comments collected from the observer feedback forms

(Note: Where italics are used they have been added to improve context or a long phrase has been paraphrased to remove identifiers.)

Observer 1)

Full understanding *of NOSS process* for me came after 4-5 observations, so it's impossible to get full understanding for workforce.

At the beginning it was difficult to rewrite the narrative in English.

Codes weren't good. Maybe they should be checked in the training, or maybe someone should look at them before project begins.

Common feedback meetings were good. Team spirit doing observation was good.

Personally these observations gave a lot. Totally new sight to work. Some threats and errors can be discussed of. If joyful talk *of what* is an error or not in quiet situation.

Observer 2)

The Whole project was briefed better than usual **** projects. XX gave folks those leaflets about NOSS project and informed us about it. *Then the project manager from EUROCONTROL* made a hair rising briefing concerning NOSS. Just like this time best way *to prepare is* probably is to first send an info package and if people are interested then come over and make a face to face briefing about the subject.

The Project Manager from EUROCONTROL gave us complete training, but what I missed was an airtraffic controllers point of view for recording of events. Like what kind of information should be on the pretext or on the overall picture.

Codes were incomplete, but they are improving all the time so by the time if NOSS is part of our ANSPs everyday life the codes will be complete.

Support from coordinators (*project manager from EUROCONTROL*, was strong. It was great to get feedback from the EURCONTROL Project Manager after sent observations, to see which way we were going.

Too much effort and time is spent on the data cleaning ------*The* NOSS-team could make data cleaning while observations are done.

Should there be more specific boxes on Traffic Picture *as Observation begins*. For example Weather box, traffic load, what positions are occupied in ops.

The codebook should be divided to different sectors for ACC, APP and TOWER. *It would then be clear which codes could be used for which environment.*

Observation methods were clear and it was quite easy to detect threats and errors.

We have quite many suggestions for new codes, and the environment gives more those if NOSS is adopted in XXX. It is nice to notice that codes are changing all the time to improve them.

Observer 3)

Useful - brief background and NOSS principles which are reflected in several case exercises. Going through sample narratives.

Observing is usually quite intense and requires a lot of concentration to be able to capture what is really happening. Skill on doing notes which are later recognisable is very useful.

Due reasons above (*demanding to do NOSS obs*), it would be beneficial to do plenty of operational shifts in between NOSS –work.

Sometimes it seemed like a double effort to fill narrative and then repeat threats, errors and US´s in tables as well. Why couldn´t those issues be comprehensively mentioned in narrative only. It would save time and effort during writing as well as in data cleaning.

Controllers were extremely helpful and showed very positive attitude to the whole process.

Not useful - Coding. Codetables are somewhat confusing. Some codes refer to very specific occurrence and others are quite general. For single event there might be numerous codes which could be applied. This might lead to incorrect final data.

Observer 4)

The joint de-briefing of the first observations was by far the most useful experience

What would you improve in NOSS training? If possible, have an experienced observer do a couple of narratives in advance and have trainees code these, so the trainees are familiar with the observed unit. This of course is not possible with a pilot study.

Language issues naturally form an obstacle in writing the narrative.

Maybe put in a checklist for the 'traffic situation' section. Also the countermeasure doesn't seem very useful.

How where the threat and error codes what might be done to improve them?

I think this was covered quite well in the data cleaning process. Main issue that codes be more adapted to local environment & system.

Maybe further in the future narratives could be made in native language, and then only coded into English for the final analysis (requiring of course that also data cleaning be done exclusively by local staff; don't know if that's feasible).

Observer 5)

How did you find the NOSS process generally, any problems in observing, writing narrative, coding etc? You have to get use to write down things in English what is not our mother tongue. Codes have made in States and they are differ than what we would use in non-strips environment.

Useful - Making feedback *on first few observations* as teamwork to make it faster and more efficient

Not useful - Some of the codes were good but some needs to be changed and some modified to be more suitable for this environment

Observer 6)

Was there anything you found particularly useful in the training? Practising writing and reading the "old" reports. Also going through the first reports with everyone was a good thing to do.

What would you improve in NOSS training? Even more details how to write a report.

The codes aren't too good, but overall it's fine.

Is there anything you would change on the NOSS forms? Also a place for "good practices *to be recorded".*