Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössische Flugunfallkommission
Commission fédérale sur les accidents d'aviation
Commissione federale sugli infortuni aeronautici
Federal Aircraft Accident Board

Final Report No. 1887 by the Federal Aircraft Accident Board

concerning the total failure of the radar air picture presentation

on all workstations of the Area Control Centre (ACC)
and the approach and departure control centre (APP)
in Zurich Air Traffic Control (ATC ZRH)
on 11 November 2003

This final report was drawn up by the Federal Aircraft Accident Board subsequent to an examination process in accordance with articles 22 to 24 of the Ordinance dated 23 November 1994 relating to the Investigation of Aircraft Accidents and Serious Incidents (VFU/SR 748.126.3). It is based on the investigation report of the Aircraft Accident Investigation Bureau dated 7 April 2006.

This report has been prepared solely for the purpose of accident prevention. The legal assessment of accident causes and circumstances is no concern of the investigation (art. 24 of the Air Navigation Law of 21.12.1948, LFG, SR 748.0).

General information regarding this report

In accordance with the agreement on International Civil Aviation (ICAO Annex 13) this report has been prepared solely for the purpose of accident/incident prevention. It is not the purpose of this investigation to ascertain a fault or to clarify questions of liability.

According to art. 24 of the Swiss Air Navigation Law the legal assessment of accident/incident causes and circumstances is no concern of the investigation.

The masculine form is used in this report regardless of gender for reasons of data protection.

If not otherwise stated, all times in this report are indicated in coordinated universal time (UTC). At the time of the accident the Central European Time (CET) was valid for the area of Switzerland. This CET was equal to the local time (LT). The relation between LT, CET and UTC is: LT = CET = UTC + 1 h.

The german-language version of this report is authoritative.

Anyone able to prove a legitimate interest in the result of the investigation may within 30 days of delivery of the investigation report request that it be verified for completeness and conclusiveness by the Federal Aircraft Accident Commission (Eidg. Flugunfallkommission – EFUK).

The Aircraft Accident Investigation Bureau thanks the authorities and organisations for the support given to it in the course of the investigation.

Contents

Final Report

System	Air traffic control of the area control centre and approach and departure control centre
Owner	skyguide – swiss air navigation services ltd
Location	Zurich Airport
Date and time	11 November 2003 18:35-18:55 UTC

General

Brief description

On 11 November 2003 at approximately 18:34 UTC, a total failure of the radar air picture presentation in the Zurich approach/departure control centre and area control centre was caused by an intervention in the radar system. As a result, it was only possible to handle air traffic subject to restrictions for approximately 20 minutes.

Investigation

Pursuant to attachment C "*List of examples of serious incidents"* of Annex 13 to the Convention on International Civil Aviation "*Aircraft Accident and Incident Investigation"* of the ICAO, the AAIB carried out an investigation. In this list of serious incidents, it is intended, among other things, that an investigation will be opened in the event of:

"Failures of more than one system in a redundancy system mandatory for flight guidance and navigation."

As a result of the failure of the radar display, the air traffic controllers in the area control centre and approach/departure control centre no longer had access to the necessary information from the following three redundant systems for processing radar data (cf. section 1.6.2.1):

- multi radar tracker (MRT) MV9800
- fallback radar data processing system (fbRDPS)
- individual radar display (front end processor – FEP)

These systems provide three different operating modes (MV, fallback and LR/SR) with different functions. The air traffic controller normally works in MV mode, as the other two modes have limited functionality.

The serious incident is attributable to the fact that the central monitoring and control computer terminated for unknown reasons all active processes relating to the radar air picture presentation, released after untested corrective interventions on the ADAPT system.

The following factors contributed to the development of the serious incident:

- Processes for corrective interventions were missing in the air navigation services company.
- To what extent the overall level of knowledge of the personnel involved which undertook corrective interventions on the technical systems of the air navigation services company was sufficient must remain open.
- The impending corrective intervention was not coordinated with air traffic control.
- The central monitoring and control computer's program had no safety precautions and warning systems.
- There was no redundant system for the presentation of the radar air picture.

I. Introductory remarks on the Zurich air traffic control system

I.I Radar system

I.I.I Primary surveillance radar

A primary surveillance radar (PSR) is a system for monitoring airspace. For this purpose, microwave pulses are emitted by a transmitter, via an antenna. These pulses are then partially reflected back to the antenna by the flying object. A receiver measures the time between transmission and the return of the pulses. This time period and the direction of incidence of the pulses make it possible to determine the position of the flying object.

Currently there are primary surveillance radar systems with two-dimensional (distance and azimuth) or three-dimensional (distance, azimuth and elevation) position finding.

Primary surveillance radar systems make it possible, within the monitored airspace, to detect and follow all flying objects which reflect sufficient radar radiation. Meteorological phenomena, flocks of birds, hang gliders, ground clutter, etc. are also detected in this way. The display of this additional information can partially be filtered out. This information is not necessary everywhere for control and management of air traffic. However, PSRs are indispensable for monitoring airspace.

A primary surveillance radar system has a power requirement of approximately 100 kW.

I.I.II Secondary surveillance radar

A secondary surveillance radar (SSR) is a system for air traffic surveillance and control. For this purpose, coded microwave pulses are sent from a transmitter to the aircraft. The aircraft responds to the SSR's interrogation by means of a transponder. The SSR's receiver interprets the information received in the response from the aircraft.

SSRs make it possible to display the positions, pressure altitude (mode C) and an assigned designation (mode A) from responding aircraft.

Mode S transponders additionally transmit an address squitter, which is specified for each individual aircraft. This address squitter enables the air traffic controller to interrogate aircraft individually. This allows a system overload to be avoided.

A secondary surveillance radar system has a power requirement of approximately 1 kW.

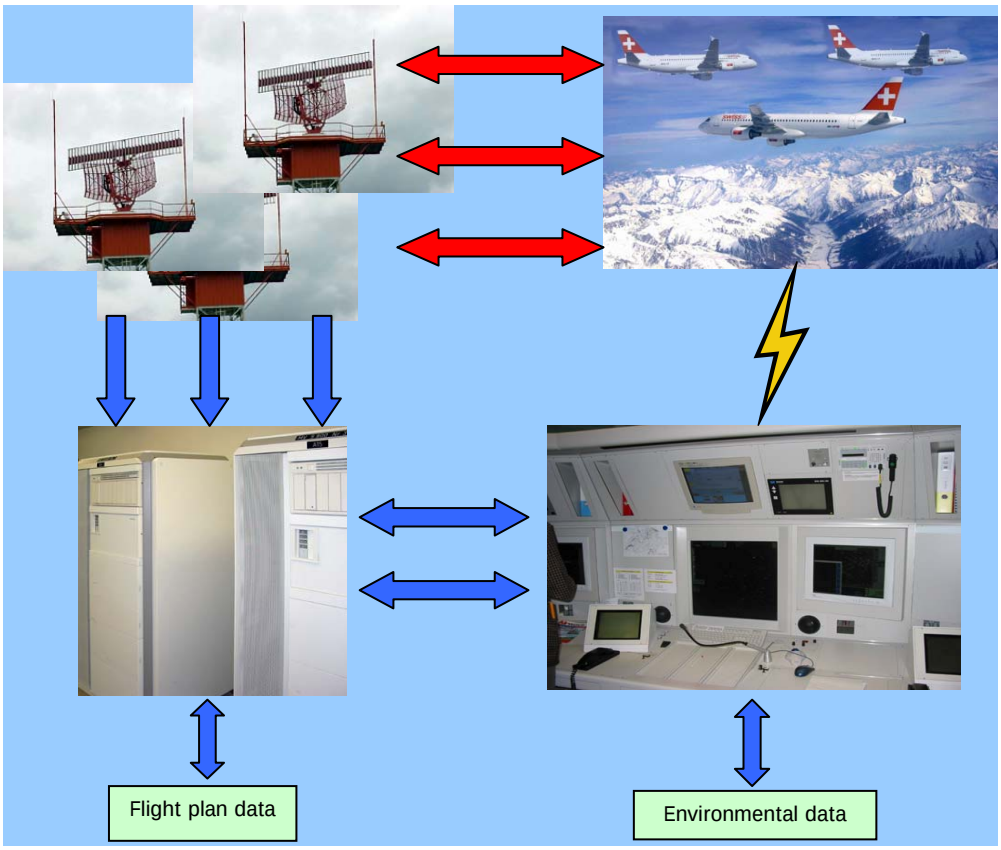
I.I.III Radar data processing

It is the task of civil air traffic control to manage air traffic safely and efficiently. In this task, the air traffic controller (ATCO) relies on complex, networked air traffic control techniques. These include, in particular:

- Radar air picture: secondary surveillance radar systems detect the current positions and collect data of aircraft. In approach control, primary surveillance radar systems are additionally used. A radar data processing system (multi radar tracker) compiles the information of radar systems into a current radar air picture.

This is termed a recognised air picture, because aircraft positions and data are detected concurrently by multiple radar systems. The section of the radar picture which is relevant for the corresponding sector is displayed for the appropriate ATCO on the radar screen of his integrated controller workstation (ICWS).

- Planned air picture: every flight requires prior planning: registration, callsign, flight route, flight times, etc. are registered centrally by the central flow management unit (CFMU) in Brussels, in order to allocate the necessary slots. In the normal case, the flight plan data are distributed to the air traffic control centres for processing. Flight plan data processing supplies the ATCO with the data for the flights which he has to control. The planned air picture and the radar air picture enable the ATCO to manage his airspace safely and efficiently. Automatic correlation of the planned air picture and the radar air picture facilitates the ATCO's job, because aircraft are displayed on the ICWS radar screens with their callsign, instead of the transponder code.
- Environmental data: dynamic environmental data (e.g. weather, airspace restrictions, aerodrome information) and static environmental information (airways, approach procedures, holding areas, beacons) complete the information which is essential for air traffic control.
- Workstations: ATCOs' ICWS serve on the one hand to provide a user-friendly display of information and on the other hand include the necessary means of communication (aircraft radio, telephone, intercom) for controlling air traffic and for coordination with other positions.

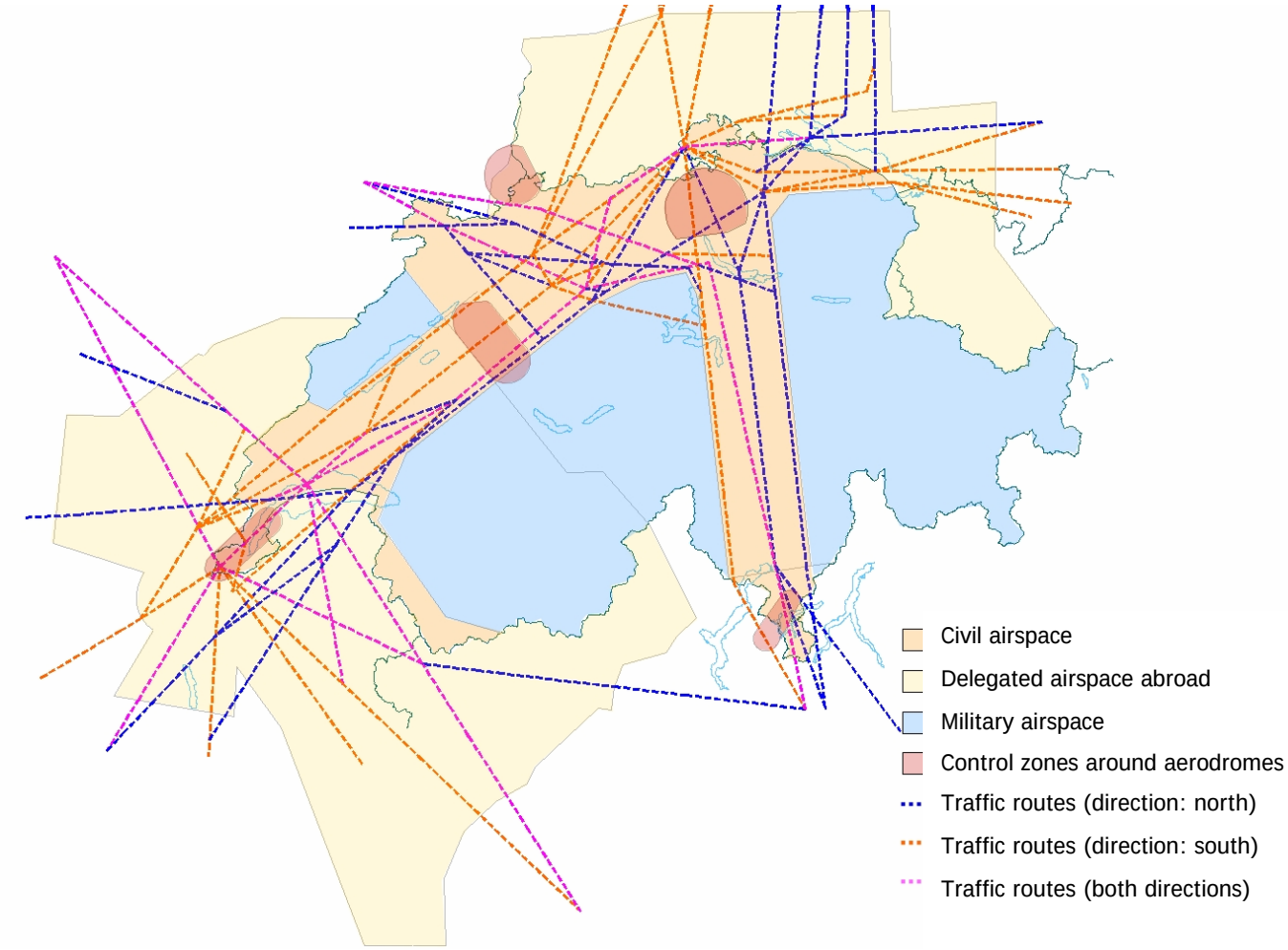


I.II Airspace structure in Switzerland

I.II.I Main traffic routes through Swiss airspace

The traffic handled by Zurich air traffic control is characterised by three different major traffic flows

- Arrivals at and departures from the airports of Zurich, Geneva, Bern-Belp, Grenchen and Lugano-Agno.
- Climbing and descending flights from and to airports in southern Germany, northern Italy and Basel-Mühlhausen.
- Transit flights as per the figure below.



I.II.II Responsibilities of Zurich air traffic control

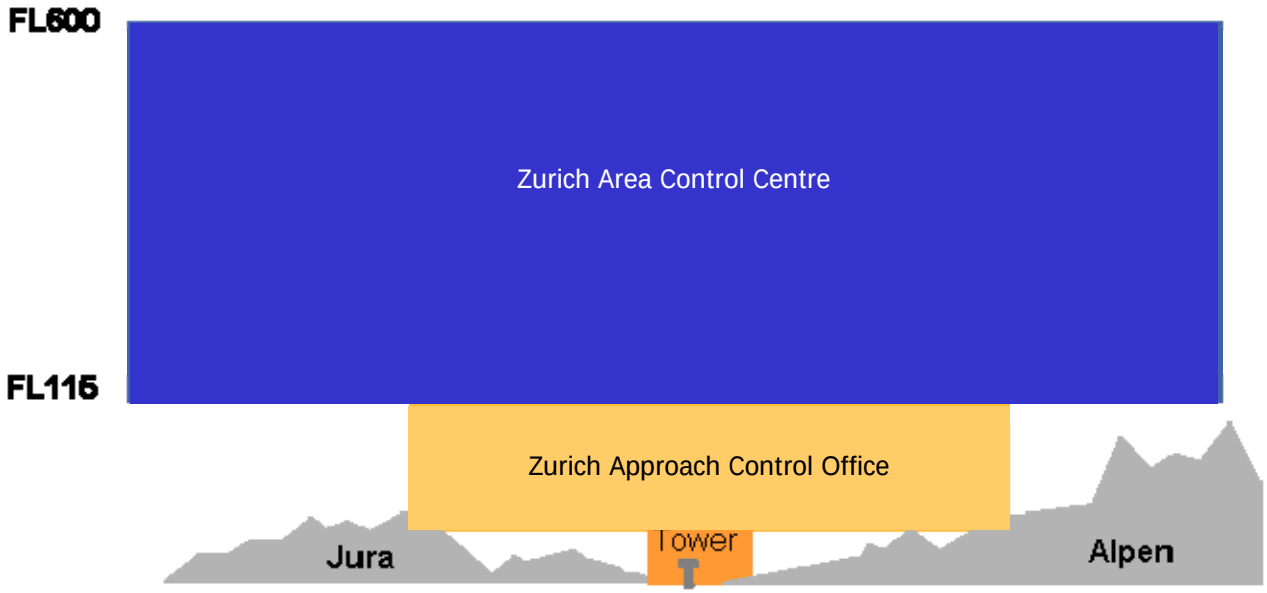
Zurich air traffic control is responsible for the airspace east of the line of separation from Geneva airspace.

In the Swiss part of the airspace extending from the ground to flight level (FL) 600, and in the delegated airspace, Zurich air traffic control provides air traffic control (ATC) services, flight information services (FIS) and alerting services (ALRS).

The air traffic control service is sub-divided as follows:

Competent service:	Controlled airspace:
Area Control Centre (ACC)	Airways (AWY) and Terminal Area (TMA)
Approach Control Office (APP / DEP)	Terminal Area (TMA) Controlled Traffic Region (CTR)
Aerodrome Control (ADC) (Tower – TWR)	Controlled Traffic Region (CTR)

I.II.III Airspace structure in Zurich



Sectorisation

The task of air traffic control is sub-divided by assigning logical sectors (predefined volumes of airspace) to physical sectors (grouping of 1-3 ICWS) in the common IFR room (CIR) for processing. Logical sectors for Zurich are:

ACC: ARFA, SOUTH, WEST, EAST, NORTH, UPPER1, UPPER2, UPPER3, UPPER4

APP: APW, APE, FINAL, DEP, TMA

The physical sectors are represented in the following layout of the CIR:

APP-W, APP-E, ARFA, NORTH, WEST, EAST, SOUTH, U3, U2, U4, U1.

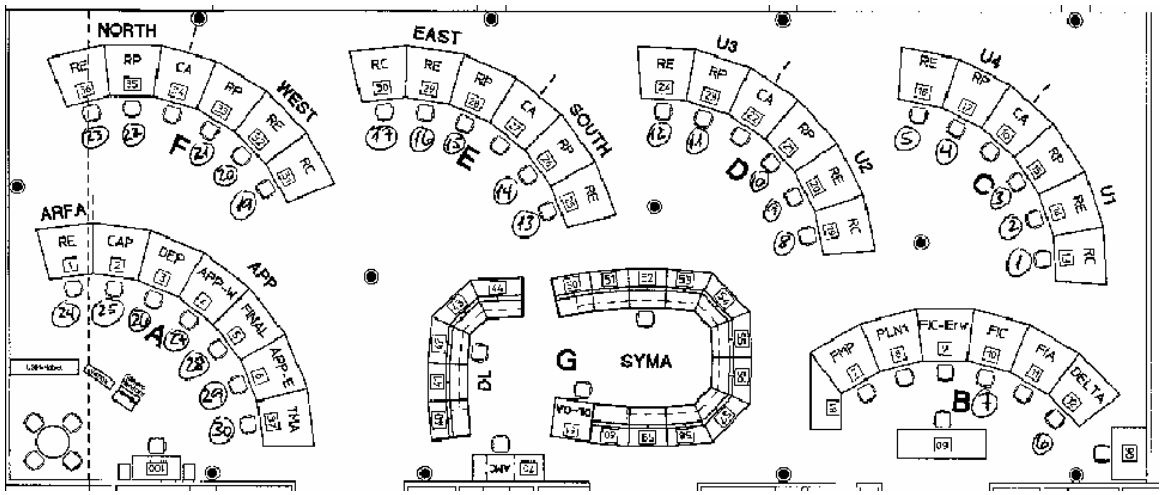


Figure 4: CIR layout (schematic)

Figure 5: ICWS in the CIR

Depending on the volume of air traffic, a different sectorisation is chosen, i.e. the allocation of the logical sectors to the physical sectors is adapted, or physical sectors are closed.

The presentation of the radar air picture on the ICSW is based on two main elements:

- an Xclient for preparation of the radar data,
- an Xserver for the graphical presentation on a large screen and the air traffic controller's user interface

The terms Xclient and Xserver are used both for the actual computers and for the processes which run on them.

In the CIR layout (cf. figures 4 and 5), the numbers of the Xservers which serve the respective radar screen of the ICWS are also entered. Every two Xservers receive the radar data from one Xclient. For every three operative Xclients, one Xclient is ready in standby mode.

Every six ICWS with the six Xservers and the four Xclients constitute one ICWS cluster. In addition, the cluster has an internal LAN, which can additionally receive data directly from the fbRDPS or an individual radar via a so-called radar switch and display it on the ICWS.

1 Factual information

1.1 Prior history and history of the serious incident

1.1.1 Prior history

1.1.1.1 Radar failure on 31 October 2003

On Friday 31 October 2003, according to a log entry by the system manager (SYMA), a radar track failure of a few seconds duration occurred at 09:32:15 UTC in the Zurich approach control centre. This meant that the display of all flight routes on the radar screens concerned suddenly failed. Only the map was displayed on these screens.

The screens at the approach sector west (APW) and terminal sector (TMA) workstations were affected by this failure. The TMA workstation was not occupied at this time. Despite the failure, traffic handling did not cause the APW ATCO difficulties of any kind. The volume of traffic was light and he was able in the short term to switch to the adjacent integrated controller workstation (ICWS) at the FINAL workstation. According to the ATCO's statement, the radar track failure lasted only 5-6 seconds.

All radar tracks and labels were cleared from the screen at the same time. After six seconds the first radar tracks reappeared on the screen. After the multi radar trackers' update time of four seconds, the presentation of the radar air picture was again complete. In all, the failure lasted approximately 10 seconds.

1.1.1.2 Handling of the radar track failure of 31.10.2003 by the technical services

The SYMA informed the competent duty service (actual situation processing – ASP) on the morning of 31 October 2003. At the instigation of the duty service, the radar processing technicians tried without success to find the cause in the area of the MV9800 multi radar tracking mainframe computer. Since the problem did not recur during the day, no immediate measures were taken.

The problem was passed on the "Zurich Platform Support" (TDZ) department. On Monday 3 November 2003, it was decided to pass the problem on to the technical service responsible for the Air Traffic Management Data Acquisition Processing and Transfer (ADAPT) system.

The head of TDZ decided to await the return of the ADAPT specialist. The latter was employed by a third-party company and was on holiday until Sunday 9 November 2003. The log files for this incident were not saved. Consequently, some of them had been overwritten with new data until 11 November 2003, the day of the serious incident.

1.1.2 History of the serious incident

On 10.11.2003, TDZ instructed the external ADAPT specialist to carry out an investigation of the 31 October 2003 incident the next day. The latter established in his investigation on the morning of 11.11.2003 that Xclient 28 had a greatly increased processor load. The operational Xclients are the control computers for the radar display of two each ICWS. For every three operative Xclients, one Xclient is available in standby mode. At the time of the 31 October radar track failure and on the morning of 11 November, Xclient 28 was configured as standby.

Konfiguration 11.11.2003	**before auto shutdown**			**after manual startup**		
X-Client	Modus	X-Server	ICWS	Modus	X-Server	ICWS
XC1	ops	1, 5	U1-RC, U4-RE	ops	2, 4	U1-RE, U4-RP
XC2	ops	2, 4	U1-RE, U4-RP	ops	3, 6	U1-RP, DELTA
XC3	ops	3, 6	U1-RP, DELTA	standby		
XC4	standby			ops	1, 5	U1-RC, U4-RE
XC7	ops	8, 12	U2-RC, U3-RE	ops	8, 12	U2-RC, U3-RE
XC8	ops	9, 11	U2-RE, U3-RP	ops	9, 11	U2-RE, U3-RP
XC9	ops	7, 10	FIC, U2-RP	ops	7, 10	FIC, U2-RP
XC10	standby			standby		
XC13	standby			ops	15	E-RP
XC14	ops	13, 17	S-RE, E-RC	ops	13, 17	S-RE, E-RC
XC15	ops	14, 16	S-RP, E-RE	standby		
XC16	ops	15	E-RP	ops	14, 16	S-RP, E-RE
XC19	ops	19, 23	W-RC, N-RE	ops	20, 22	W-RE, N-RP
XC20	ops	20, 22	W-RE, N-RP	ops	21, 24	W-RP, ARFA
XC21	ops	21, 24	W-RP, ARFA	standby		
XC22	standby			ops	19, 23	W-RC, N-RE
XC25	ops	25, 29	CAP, APE	ops	27, 30	APW, TMA
XC26	ops	27, 30	APW, TMA	ops	26, 28	DEP, FIN
XC27	ops	26, 28	DEP, FIN	ops	25, 29	CAP, APE
XC28	standby			standby		

Table 1: Configuration of the ADAPT system before and after the serious incident

By agreement with the SYMA, the ADAPT specialist carried out a restart of Xclient 28 at the system management position (SMP) workstation. This action was not entered in the SYMA log and the air traffic controllers were not informed.

At 12:12 UTC, the specialist informed TDZ, the SYMA and other persons in Technical Services (TS) by e-mail about the diagnosis and the intervention which had been undertaken to solve the problem by restarting Xclient 28. The problem was considered to have been solved and was placed on the agenda for the next coordination meeting between Operations and Technics (OPS-TEC meeting) on 17 November 2003.

In the course of the day, in the process of monitoring the ADAPT system, the specialist discovered two other Xclients (4 and 10) with a greatly increased load. By agreement with the SYMA, he restarted the two Xclients; at 18:31:16 UTC, a shutdown and startup of Xclient 4 took place at the SMP workstation. Even before completion of the restart of Xclient 4, shutdown of Xclient 10 took place at 18:34:26 UTC. During the shutdown of Xclient 10, at 18:34:31 UTC, the SMP computer issued automatic shutdown commands to all other Xclients and some other computers. As a result, all active programs (processes) and programs running in standby mode responsible for the display on the radar screens were stopped and cleared. Subsequently, within about 1 minute, total failure of the presentation of the radar air picture on all radar screens in the common IFR room (CIR) occurred.

Automatic Shutdown of Applications by SMP				
Node	**Action**	**Shutdown Start Time (UTC)**	**Xservers**	**Controller Positions**
SMP2	UNAS network status request	18:34:31		
COM2	shutdown	18:34:33		
XC1	shutdown	18:34:48	1, 5	U1-RC, U4-RE
XC2	shutdown	18:34:53	2, 4	U1-RE, U4-RP
XC3	shutdown	18:34:57	3, 6	U1-RP, DELTA
XC7	shutdown	18:35:02	8, 12	U2-RC, U3-RE
XC8	shutdown	18:35:08	9, 11	U2-RE, U3-RP
XC9	shutdown	18:35:10	7, 10	FIC, U2-RP
XC19	switchover	18:35:14	19, 23	W-RC, N-RE
XC20	shutdown	18:35:18	20, 22	W-RE, N-RP
XC21	shutdown	18:35:21	21, 24	W-RP, ARFA
XC22	shutdown	18:35:23		
XC25	switchover	18:35:25	25, 29	CAP, APE
XC26	shutdown	18:35:29	27, 30	APW, TMA
XC27	shutdown	18:35:31	26, 28	DEP, FIN
IPG1	shutdown	18:35:33		
IPG2	shutdown	18:35:38		
SUPV	shutdown	18:35:40		
XC15	shutdown	18:35:42	14, 16	S-RP, E-RE
XC16	shutdown	18:35:46	15	E-RP
XC14	shutdown	18:35:48	13, 17	S-RE, E-RC
XC13	shutdown	18:35:50		
XC28	shutdown	18:35:52		
XC4	shutdown	18:35:55		
SMP1	shutdown	18:35:57		

Table 2: Sequence of the automatic shutdown in the ADAPT system triggered by the SMP

1.1.2.1 Traffic situation at the beginning of the radar display failure

At the time of the radar display failure, 28 aircraft in the airspace under the control of Zurich ATC were on the air traffic controllers' screens (see annex 5.3).

1.1.2.2 Effects of the radar display failure of 11 November 2003 on air traffic control

Air traffic control was not informed in advance by the responsible technicians about the impending switchover work. There were no indications of an impending failure on the air traffic controllers' radar screens. The failure of the first radar console occurred at about 18:35 UTC. The display on all other radar screens then also failed in rapid succession.

The failure caused the radar screens to appear as if they had been switched off (black).

All 29 radar screens in the common IFR room (CIR) were affected by the failure.

Other systems at the air traffic controllers' workstations, such as telephone and radio communication, were not affected by the failure.

Approximately 20 minutes later, at about 18:55 UTC, radar data were again available to the air traffic controllers on all screens.

1.1.2.3 Effects on operation in the control tower

Aerodrome control (the control tower) monitors taxiing manoeuvres, take-offs and landings and guides traffic in the immediate vicinity of the airport.

Coordinator approach (CAP) informed the daily OPS manager (DOM) in the control tower of the screen failure in APP. At the time of the failure few departures were taking place. With regard to approaches, the volume of traffic was average. All the workstations in the control tower, except ADC2, were occupied. The radar screens in the control tower *(position radar de nuit à la Vigie* – PRN-Vigie) were fully functional. The DOM immediately stopped all departures and offered the CAP to take over the tasks of the approach sectors. To this end, two workstations in the control tower were set up as radar approach sectors. This meant that radar vectoring of individual approaches could be handled with the PRN-Vigie screens available there. Since the radar screens in APP were again functioning normally soon afterwards, the measures which had been taken were withdrawn in stages.

1.1.2.4 Effects on approach and departure control

The approach control office (APP) controls approaches and departures within a specific area of the control zone and the terminal area. This area normally extends up to a distance of approximately 50 km around the airport.

According to the statement of the CAP, the radar screen at his workstation in APP suddenly failed. Glancing at the screens to his left and right, he realised that all the APP radar screens had failed. During the failure, about 20 aircraft had to be controlled by APP. Four sectors were in operation. The volume of traffic was rather low and there was no complicated traffic situation. The CAP performed a series of measures to cope with the situation in accordance with the APP checklist in the emergency manual, “Radar Failure” section. These included, among others:

- informing the TWR DOM and suspending all departures
- clarifying whether the two approach sectors and the departure sector could transfer the current flight movements in a staggered manner to the next sector.
- implementing the offer by the TWR DOM to the effect that all approaching aircraft could be handed over directly by APP and ACC to aerodrome control 2 (ADC2). The radar screens in the control tower were not affected by the failure.

1.1.2.5 Effects on the area control centre

The area control centre (ACC) ensures flow of traffic within the airways and partly within the terminal area. The large horizontal and vertical extent of the areas to be controlled demands, depending on the volume of traffic, that they are sub-divided into various working sectors. This sub-division may be geographical or according to altitude ranges.

According to the ACC DOM's statement, all radar screens in the ACC failed one after the other within about 30 seconds. During the failure, about 35 aircraft had to be controlled by the ACC. Eight sectors were in operation. The volume of traffic was rather low and complexity was not very high. The DOM performed various measures to cope with the situation in accordance with his checklist in the emergency manual, section "Radar Failure". These included, among others:

- requesting the Brussels CFMU not to allow any more aircraft into Zurich airspace (zero rate)
- suspending all departures
- zero rate for all adjacent control centres
- informing skyguide management

he also arranged for the following:

- recalling the second DOM, who was on a break
- reinforcing individual workstations with personnel returning early from their breaks

Forty-five minutes after the failure occurred, the ACC DOM noted in the operating log that traffic handling was able to be carried out normally again.

1.1.2.6 Recommissioning sequence

The startup procedure in both the ACC and the APP took place in stages. The first radar screens were available again to air traffic controllers after a few minutes. All screens were in operation again after about 15 minutes. However, an actual hand-over of the restarted radar screens from the Technical Service (TD) to the air traffic controllers did not take place. The DOM ACC asked the SYMA about the operational functionality of the radar screens. The SYMA responded in the affirmative, but with the limitation that no standby was available for the time being. No further irregularities were discovered subsequently.

Manual System Recovery						
Node	**Primary / Standby**	**Start Time (UTC)**	**Controller Positions Ready**	**Action Completed**	**Xservers**	**Controller Positions**
		(confirm for manual command)	**Map Data Ready**			
XC13	primary	18:38:54	18:39:39		15	E-RP
XC19	primary	18:39:37	18:40:26		20, 22	W-RE, N-RP
XC1	primary	18:40:25	18:41:16	18:41:11	2, 4	U1-RE, U4-RP
XC7	primary	18:41:18	18:42:05		8, 12	U2-RC, U3-RE
XC25	primary	18:42:06	18:42:58		27, 30	APW, TMA
XC26	primary	18:43:03	18:43:53	18:43:41	26, 28	DEP, FIN
XC14	primary	18:43:49	18:44:39		13, 17	S-RE, E-RC
XC20	primary	18:44:23	18:45:16		21, 24	W-RP, ARFA
XC2	primary	18:44:55	18:45:48		3, 6	U1-RP, DELTA
XC8	primary	18:45:27	18:46:19		9, 11	U2-RE, U3-RP
XC16	primary	18:46:10	18:47:06		14, 16	S-RP, E-RE
XC27	primary	18:46:53	18:47:45		25, 29	CAP, APE
XC22	primary	18:47:35	18:48:29		19, 23	W-RC, N-RE
XC4	primary	18:48:16	18:49:09	18:48:51	1, 5	U1-RC, U4-RE
XC9	primary	18:49:03	18:49:56	18:50:04	7, 10	FIC, U2-RP
SUPV	primary	18:50:30		18:51:31		
COM2	standby	18:52:17		18:53:40		
COM1	primary	18:55:07		18:55:25		
IPG2	standby	18:55:48		18:57:00		
COM1	standby	18:57:25		18:59:34		
SMP1	standby	19:00:28				
XC28	standby	19:22:26		19:23:05		
XC15	standby	19:31:06		19:32:13		
XC21	standby	19:39:11		19:40:24		

Table 2: Sequence of manual recommissioning

The precise “action completed” time is not logged if the next command is initiated manually before the process is completed. The “controller position ready” time means that the maps are loaded onto the radar screen, the controls are functioning and the radar tracks are again displayed in their entirety after the next update time of 12 seconds for ACC and 4 seconds for APP.

1.2 Injuries to persons

Not applicable.

1.3 Damage to aircraft

Not applicable.

1.4 Traffic restrictions

1.4.1 General

The volume of traffic during the radar data failure was not very high in either approach and departure control (approximately 20 aircraft) or the area control centre (approximately 35 aircraft). The restrictions on traffic after the sudden radar data failure in the CIR had to be maintained only for a short time.

The majority of the flight crews who were in contact with Zurich air traffic control at the time of the radar data failure expressed themselves positively with regard to traffic handling by ATC during the failure. The information from the onboard traffic collision avoidance system (TCAS) was considered to be helpful in this situation. According to the information from the crews questioned, there were no TCAS alerts.

Since no aircraft had to wait in the holding patterns for longer than 10 minutes, there was no need to fly to alternative airports.

Three aircraft ready for take-off from Zurich experienced departure delays. The maximum take-off delay was 20 minutes.

1.4.2 Traffic restrictions in approach / departure control and control tower

After the coordinator approach (CAP) had informed the daily ops manager (DOM) in the control tower about the radar data failure in the CIR, the DOM realized that the radar data on the radar consoles in the control tower (PRN-Vigie) were available as normal.

Then, as an immediate measure, he suspended all departures without delay.

After the two workstations ADC2 and ground control (GRO) with the PRN-Vigie screens in the control tower had been set up as approach sectors, the aircraft on approach were handed over by approach control to these two approach sectors. These were able to guide the aircraft to the instrument landing system (ILS) with the two PRN-Vigie radar screens.

The following aircraft were instructed to join the holding patterns by approach control sectors West and East on their usual frequencies and workstations.

From there, it was possible for the approach sectors in the control tower to take over the aircraft in groups and guide them to the final approach. Aircraft just arriving in the area control centre were also handed over directly to the control tower.

Since, according to the approach and departure control's operations log, the data was available again on the radar monitors after approximately twelve minutes, the measures which had been taken could be withdrawn gradually and the approach control ATCOs took over radar vectoring again themselves.

1.4.3 Traffic restrictions in area control centre

The ACC DOM stayed in the area of sector U2 when he heard from sector North about the failure of the radar data there. He established that the other sectors were also affected within a short time.

The DOM subsequently reinforced the workstations with additional personnel who had returned early to the operations room from their breaks when the radar problems became known.

He then requested the adjacent control centres not to allow any more aircraft to fly into Zurich airspace. He additionally informed the CFMU in Brussels and asked them to control the traffic flow in such a way that no more aircraft were routed into the affected region.

On the basis of the measures taken and agreements, the ACC DOM was soon able once again to accept sporadic transit flights from the adjacent control centres.

The traffic restrictions had to be maintained in the area control centre only for a short time.

1.5 Personnel information

At the time of the incident, the following persons were on duty in the different areas.

ACC	2	daily ops manager (DOM)/air traffic controller
	15	air traffic controllers
	6	trainee air traffic controllers
	1	daily ops manager (DOM)/air traffic controller assistant
	5	air traffic controller assistants
APP	1	coordinator approach control (CAP)
	4	air traffic controllers
TWR	1	daily ops manager (DOM)/air traffic controller
	4	air traffic controllers
FTD	1	system manager (SYMA)
	1	ADAPT specialist (external company)

1.5.1 The system manager

The system manager (SYMA) has his workstation in the CIR; he monitors the installations and systems assigned to him with the aim of being able to provide air traffic control which is unaffected by malfunctions as far as possible. Based on the job description, he is entrusted with the following main tasks, among other things:

- monitoring the equipment and systems integrated in the SYMA.
- adapting the system configurations as a function of operational requirements.
- analysis of problems: classifying, analysing and assessing any technical problems which occur, taking into account the requirements of operational air traffic control (e.g. the volume of traffic, air traffic control procedures); coordinating measures to be taken with the DOM responsible for operational services.

- initial intervention/trouble-shooting: in the event of a malfunction, taking swift and appropriate countermeasures (e.g. activating redundant systems, carrying out reconfigurations), in order to re-establish operational functionality as quickly as possible.
- documenting incidents: recording all events and problems in the SYMA log and information by means of SYMA messages; briefing at shift changes.
- system documentation/checklists: updating the documentation on the systems for which he is responsible and on the networking of these. Drawing up checklists for "trouble-shooting" and for "system control" .
- TD support: support with preventive and corrective maintenance, and with system modifications, tests and analyses through coordination with the appropriate DOM of the operational services with regard to the operational release of the equipment concerned.
- periodically carrying out system switchovers (Xfers) of the operationally active systems in order to test system redundancies in practice and provide training in the switching procedures (OJT).
- supporting OPS personnel in the technical matters.
- informing management in the event of major system failures which have an effect on the capacity of the operational services.
- elaborating and implementing improvements in SYMA operation by participating in the evaluation, installation and commissioning of new air traffic control equipment, in so far as they affect the SYMA service.

The SYMA position is advertised. Candidates are selected and trained. No licence was required in Switzerland at the time of the serious incident.

1.5.2 The ADAPT specialist

The ADAPT specialist had concluded his basic education with a bachelor's degree in mathematics and had extensive additional training in computer technology. He worked for various companies as a programmer and software engineer. In the ADAPT project, he was employed by the supplier as Senior Systems Engineer. Among other things he was responsible for coordinating the integration of subsystems and software modifications, as well as for problem tracking reports (PTRs). Given his function, he had profound knowledge of the ADAPT system. As an external specialist, however, he was not trained systematically in specific operational requirements of air traffic control and the totality of the air traffic control systems technology.

1.6 Information on the Zurich air traffic control radar system

1.6.1 The ADAPT radar data processing system

ADAPT (air traffic management data acquisition processing and transfer) is the name of the project started by skyguide at the beginning of the 'nineties to replace the civil Swiss air traffic control systems with workstations which covered the totality of the technical functions.

1.6.2 System overview

The block diagram in figure 1 shows the main components of the skyguide radar system. The components of the implemented ADAPT system are included in the frame.

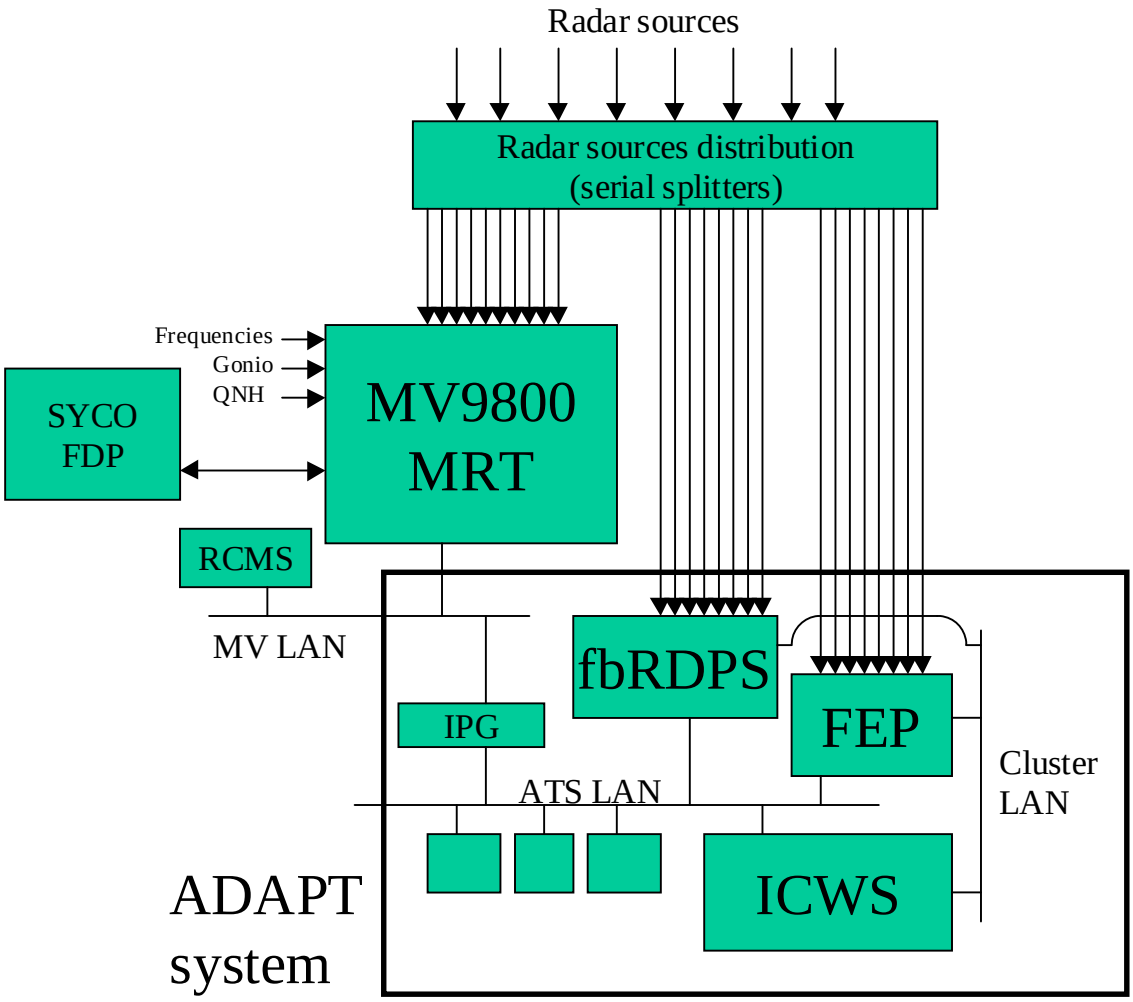


Figure 1: Block diagram with the main components of the skyguide radar system. Radar data can be processed and displayed in three different ways.

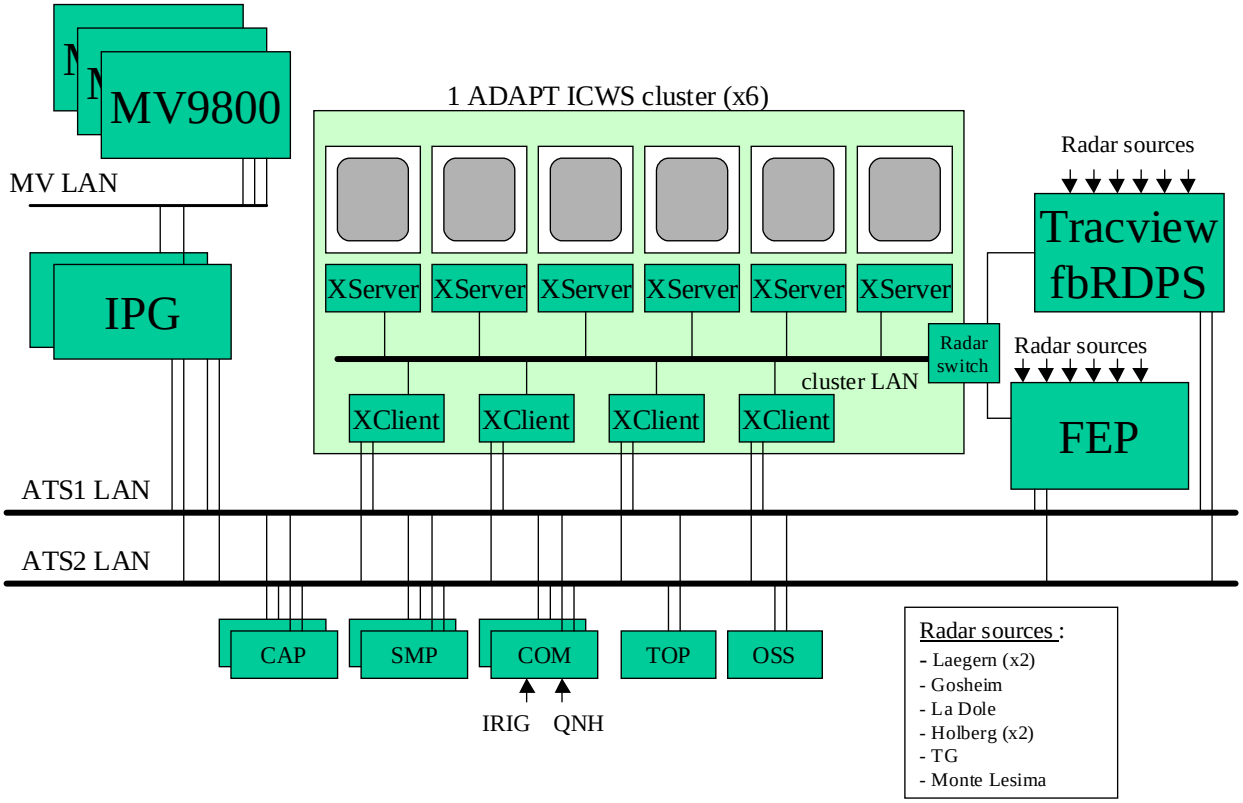
The three parallel MV9800 computers have direct access to other parts of the system, such as the processing of flight plan data by the *système de communication* (SYCO), the correction values for altitude information (QNH), the information on frequency assignment of the interface to the SWITCH-04 radio system, direction finding by GONIO or data recording by legal recording (REC01, not shown in figure 1). The system is controlled and monitored by the remote control and monitoring system (RCMS). The correlated radar data are forwarded by the MV9800 system via an IPS[1] processing gateway (IPG) to the ADAPT system.

[1] IPS – indicateur panoramique synthétique (synthetic panoramic indicator)

The air traffic services local area network (ATS LAN) provides the connection between the ADAPT subsystems. The ATS LAN appears logically as one network, but is duplicated physically on layer 1/2.

The cluster LAN, also termed the internal LAN, connects the elements of an ADAPT ICWS cluster. Data can be received direct from the fbRDPS or an individual radar via an Ethernet switch (radar switch) and displayed on the ICWS of an ADAPT cluster.

In the normal case, one Xclient serves the ICWS of two different physical sectors. Therefore, in the event of failure of one Xclient, the information in a physical sector is lost only partially.



1.6.2.1 Redundant systems

The radar system supports three modes of operation, which basically use the same data from the connected radars but are distinguished by different processing paths:

1. MV mode: this mode is used in normal operation. MV mode processes data as a multi radar tracker (MRT) on three MV9800 computers (MV1 to MV3), which have the following operating conditions:
   - one unit in operation (OPS)
   - one unit in hot standby (STBY) position
   - one unit in cold standby (TECH) position
2. fallback mode: this mode is designed for the case in which MV mode is not available. Fallback mode uses the multi radar tracker Trackview on a single HP748i computer (fbRDPS), which is part of ADAPT. The functions available in fallback mode are restricted compared with MV mode.

3. LR/SR mode: this mode is a backup system on a single HP748i computer (FEP, identical in construction to fbRDPS), which conveys the data from a long-range radar or a short-range radar directly to the ATCO's ICWS without a multi radar tracker. Zurich air traffic control uses Lägern en-route radar as long-range (LR) radar or Holberg approach radar as short-range (SR) radar.

Redundancy of radar data processing is achieved with the three operating modes in terms of:

- covering specific airspace with multiple radar stations
- processing the radar data using different hardware and software
- distributing the data using physically duplicated networks
- conditioning and displaying the radar data on a configurable system of Xclients and Xservers

No redundancy exists with regard to:

- the types of device used and the operating systems employed for distributing and displaying radar data, i.e. ICWS, ATS LAN, Xclient, Xserver
- software in the ADAPT system

1.7 Meteorological information

1.7.1 General weather situation

Switzerland was at the western edge of a high-pressure region, the centre of which was over eastern Europe. With only a light wind on the ground and at altitudes, the sky in Switzerland was practically cloudless. A layer of fog/low stratus lay over the valleys of the northern side of the Alps; its upper limit in the west was approximately 800 masl and in the east approximately 900 masl.

1.7.2 Weather conditions at Zurich airport

The following weather conditions prevailed at Zurich airport at 18:20 UTC:

Wind:	110 degrees, 3 knots
Visibility:	2000 m
Weather:	damp mist
Cloud:	1-2 eighths, base 200 ft
	8 eighths, base 500 ft
Temperature:	+ 05 °C
Dew point:	+ 04 °C
QNH:	1022 hPa
TREND:	NOSIG

The following weather conditions prevailed at Zurich airport at 18:50 UTC:

Wind:	120 degrees, 2 knots
Visibility:	2000 m
Weather:	damp mist
Cloud:	1-2 eighths, base 200 ft 8 eighths, base 500 ft
Temperature:	+ 05 °C
Dew point:	+ 04 °C
QNH:	1022 hPa
TREND:	NOSIG

1.7.3 Hazardous weather phenomena

None

1.8 Aids to navigation

There is no indication that the ground-based navigation aids such as VOR/DME or ILS were adversely affected at the time of the serious incident.

1.9 Communication

There is no indication of any restrictions in radio traffic or telephone links between the sectors and adjacent air traffic control centres.

1.10 Aerodrome information

Since this serious incident did indeed have effects on the operation of the airports in the area covered by ATC Zurich, but the individual airports were not involved in this investigation, the corresponding information is omitted.

1.11 Recording of events and data

There were four stages in the recording of events and data. These recordings are termed logs:

- the handwritten or electronic log of the DOM, the SYMA and the personnel of Technical Services.
- the log of the SMP, the ADAPT general monitoring and control system.
- the universal network architecture services log (UNAS log) of the ADAPT workstations which recorded incidents or messages on request.
- the classic UNIX log of the ADAPT workstations.

The ADAPT system used 62 UNIX workstations, of which 29 (Xservers) merely performed the function of simple graphics processors which supplied the IWCSs with display and user interface data.

Five UNIX workstations were not integrated into the UNAS: one for technical tasks (TOP), two for Trackview (FEP and fbRDPS) and two for operational support tasks (OSS).

Thus, 28 UNIX workstations (Xclients, SMP, COM, IPG and CAP) were actively involved in processing and displaying the radar air picture. Only on these workstations ran several important processes. All these workstations were interconnected via a redundant local area network, allowing management of all active processes and switching between the workstations using the UNAS software in case of failure. UNAS provided the basic functionalities for a distributed informatics system, such as, for example, communication between the processes, error detection and system status monitoring. All processes indicated their status with the aid of SNMP traps. SNMP is a classic protocol which is used under UNIX and by all TCP/IP networks (such as the internet). The SMP workstations collected the traps and events in order to update the graphics displays of the system status, and stored them. In addition commands such as reconfiguration, standby/primary switching, shutdown and start up were issued by the active SMP workstation. In the serious incident under investigation, the active SMP workstation issued the shutdown commands.

All events were provided with a time stamp using system time. The system time was synchronised to an accuracy of a few milliseconds by means of the network time protocol – NTP – and an absolute external reference (GPS or DCF77 time code transmitter in Mainflingen/D). Thus, an event which was stored in one or more logs at different workstations has the same time information. The log concerning the investigated serious incident can therefore be considered to be reliable on the basis of its redundancy and the time stamp.

1.11.1 Logbooks

Those parts of the following log book entries that originally were written in German, have been translated to English.

1.11.1.1 ACC operation log

Extract from the handwritten ACC operation log dated 11.11.2003:

"19:35 UTC: Radar failure in the CIR (both ACC and APP) from 18:35 – 18:55 UTC

Zero-Rate to central flow management unit (CFMU)

Reduced capacity accepted by adjacent sectors / adjacent control centres from 18:55 UTC

DL checklist carried out

Normal OPS 19:20 UTC"

1.11.1.2 APP operation log

Extract from the handwritten APP operation log dated 11.11.2003:

"18:38 UTC: complete radar failure APP + ACC!
all DEP stopped
INBND to control tower (ADC2)
18:50 UTC normal OPS, without backup"

1.11.1.3 Control tower operation log

Extract from the handwritten control tower operation log dated 11.11.2003:

"18:37 UTC: Failure of the ADAPT system
No radar data in the entire CIR.
Some aircraft lined-up by TWR with PRN-Vigie.
18:52 UTC ADAPT functioning normally again."

1.11.1.4 SYMA technical log

This is an electronic log, which is generated by the SYMA in the common IFR room (CIR). Printouts are available for 31.10.2003 and 11.11.2003:

Extract from logbook for Friday 31.10.2003 concerning message 820015082; names are replaced by the function and marked by underscores.

Start/end Date Time	Domain Text and reporter	System/ equipment	Status Action
31.10.2003 09:32:15 / 31.10.2003 11:49:01	Processing systems 31.10.2003 11:24:05 SYMA Brief track failure at APW, message from ATCO. Error message at MV: "*IPS APP 6 is failed*" and "*IPS APP 3 is failed*", 16 sec. later, at 09:32:31, ADAPT SMP1 reports following fault: "*zhxcc28:ICW_SIT_20 - MRIP-SO-CAUSE - Hardware failure on <zhxcc27>*". Note: zhxcc28 is SBY and DEP and FIN are connected to zhxcc27! According to information from Pikett and MV Engineer the two error messages may have nothing to do with each other. 31.10.2003 11:48:00 SYMA Since then, no more faults have occurred. 31.10.2003 11:49:01 SYMA message concluded	MV2 Hardware (ANC/MV9800)	Partial failure

Extract from logbook for Tuesday 11.11.2003 concerning message 820015139; names are replaced by the function and marked by underscores.

Comment: The shutdown and startup of Xclient 28 by the ADAPT specialist at 08:54 UTC was not recorded in the SYMA log.

Start/end Date Time	Domain Text and reporter	System/ equipment	Status Action
11.11.2003 18:30:00 / 11.11.2003 22:42:31	Processing systems 11.11.2003 21:45:09 SYMA ADAPT specialist has found further 2 standby-Xclients with the fault described in the morning. Shutdown and startup of Xclient 04. Then the shutdown at standby Xclient 10 was started. 18:37 All Xclients shut down. Total display failure in ACC and APP. OPS Restrictions: 18:37 Zero Rate 18:50 FLAS[2] Transit Accept Startup of the Xclients 18:56 In all clusters, all screens again display a picture. 19:04 SMS sent for ASP[3]. 19:20 no longer any restrictions. The stdby-Xclients will be run up one after the other by the ADAPT specialist. Engineering Manager called the desk. In the event of further problems, contact to be made directly with TD Manager. 20:15 All stdby-Xclients are run up , everything in order TZ Manager calls desk. 11.11.2003 22:42:31 SYMA – message concluded	Adapt systems	Total failure

1.11.1.5 SMP log

The two SMP workstations, primary and standby, at the SYMA workstation, make it possible to display the status of all ADAPT systems (activity of the workstations and processes) and to carry out reconfigurations, switching operations from standby to primary and shutdowns and startups. The commands issued by the SYMA, plus the events (process status messages) and the traps are saved to the local file “trapd.log”.

The SMP workstations' “trapd.log” file is the main source for documentation and analysis of events in the ADAPT system. It is saved every week to a DAT medium (magnetic tape cartridge) and conserved on the tape for between one and three months. The data are redundant, as they are saved at both SMP positions and permit a chronological reconstruction of events.

[2] FLAS: flight level allocation schemes

[3] ASP: actual situation processing

1.11.1.6 UNAS log (node log)

UNAS is a software program which runs on 28 of the 62 workstations on the ADAPT system, i.e. on all workstations which are actively involved in gathering data and which can be configured in primary or standby mode. UNAS is a message passing middleware, which allows the UNIX workstations to communicate with each other and to start and monitor processes (activated programs). The 28 UNAS workstations are therefore multiply networked, i.e. there are 378 connections in all[4]. Each UNAS transfer process (node-server – NSRVR) saves locally a series of predefined messages (incidents, configurations); the majority of these messages are local copies of the messages which are sent to the SMP workstation and saved to the "trapd.log" file.

These node logs are overwritten in a 7 day cycle. The node logs for 31 October 2003 were not backed up and were overwritten by the time of the fault analysis on 11 November 2003. The node logs for 11 November 2003 were backed up.

The same events, i.e. the networking of the workstations and process starts, were found as they were saved in the "trapd.log" file (see annexes 5.1 and 5.2).

1.11.1.7 UNIX log

Using the fprint () function each UNIX process (application program being executed) made it possible to display information on the system console or to save it to a local file. This function was basically called up after a return because of an error in a subroutine and to identify an important event. The scripts (series of system commands) could also save messages locally. The saved events were used in particular for debugging.

Any recordings in the UNIX log concerning the serious incident were not available for the investigation.

1.11.2 Reporting by the ADAPT specialist

One day after the serious incident, the ADAPT specialist sent TDZ the following report in an e-mail. Names have been replaced by functions and marked by underscores.

[4] The number of connections is determined by the formula N x (N-1)/2 where N=28

*"**From:** ADAPT specialist*

***Sent:** Wednesday, 12 November 2003 01:36*

***To:** TDZ; TD; T*

***Cc:** TDR; TDMX*

***Subject:** RE: Analysis - Message 820015082 - 31.10.2003 - IPS APP 3 & 6 failed*

Hi TDZ,

During the period from 22:45 to 23:45 (UTC) this evening, TDMX and I performed the same sequence of steps that led to the system failure as discussed during the telecon. The test was repeated 10 times with no problems encountered. So, the problem is NOT reproducible. (However, I will continue to perform tests in the STF and check for any type of degradation in system resources, performance or stability.)

Just to confirm the times when the corrective action was taken, and when the blank screen problem occurred:

08:54 (UTC)	*initial corrective action was taken with NO problems encountered (shutdown and restart of standby Xclient 28)*
~17:30 (UTC)	*observed that two more Xclients were running in a degraded mode, requiring further corrective action*
18:31 (UTC)	*second corrective action was taken (shutdown and restart of standby Xclients 4 and 10), resulting in the serious condition of all ICWS screens becoming blank* *- the shutdown and restart of Xclient 4 appeared normal* *- the problems started after the shutdown of Xclient 10*
~18:36 (UTC)	*- all Xclients (and a few other nodes) started shutting down, resulting in all screens being blank, with NO radar sources available (including fallback)*
~18:37 (UTC)	*the IPG (gateway to MV) and all Xclients were then started up one by one*
~18:39 to ~18:50	*situation display was restored to controllers, in a sequence to provide at least one display per sector as quickly as possible* *controllers were without a display for a period between roughly 3 and 14 minutes (based on the logging information)*

The reason for taking the corrective action during the day was for the following reasons. With the standby Xclients in a degraded state:

a reoccurrence of the 31.Oct problem could occur and the supply of track data to the ICWS displays could be interrupted

if a primary Xclient failed and switched over, the possibility existed that the standby would fail as well

I hope this helps to clarify the events and situation.

Regards,

ADAPT specialist"

1.12 Wreckage and impact information

Not applicable.

1.13 Medical and pathological information

Not applicable.

1.14 Fire

Not applicable.

1.15 Survival aspects

Not applicable.

1.16 Tests and research

Not applicable.

1.17 Organizational and management information

1.17.1 Air navigation services company skyguide

1.17.1.1 History

Radio Schweiz AG was founded in 1922 to meet requirements in the area of telegraphy and international telephony. This company introduced the first communication and location-finding systems (short-wave and telegraphic connections, radio direction finders) at Zurich and Geneva airports. However, it was not until 1931 that further developments in systems and procedures led to the introduction of actual air navigation services. In 1988, Radio Schweiz AG changed its name, first to swisscontrol and finally, after the amalgamation of military and civil air traffic control services to skyguide, on 1 January 2001.

At the end of 2003, skyguide employed 1326 personnel units; half of these were employed as air traffic controllers, a quarter worked as technicians (technical division) and a quarter consisted of the management, administration, trainees and temporary staff. Skyguide operates at various operational sites, such as the airports of Geneva, Zurich, Berne and Lugano, as well as at various regional aerodromes. In addition, it operates twenty exclusively technical sites (radar stations and stations for navigational aid or for VHF/UHF transmission/reception.

1.17.1.2 Technical Service

At the time of the serious incident, skyguide's technical service was mainly responsible for the procurement, installation, maintenance and development of air traffic control and navigation equipment. In November 2003, 303 personnel units were responsible for this task. Within the technical management and for technical services in the West region, 166 personnel units were employed in Geneva; 137 personnel units in Zurich were responsible for the East region. The technical service was split into five divisions, each with an area of technical responsibility

(TN, TC, TD, TZ and TG), and four support or development divisions (TA, TS, TB and TI):

TT (13) management and staff of the Technical Division

TN (46) navigation and surveillance: ILS, VOR, DME, radar stations, equipment for displaying and assessing the weather situation

TC (59) communication: ground/air communication systems, telephone, radio, data networks

TD (74) data processing: processing radar and flight plan data, display and exchange of flight data

TZ (31) SYMA & logistics Zurich: supervision and monitoring of the systems, general services: electricity, air-conditioning, power generation, safety, drawing office and construction workshop

TG (33) SYMA & logistics Geneva: supervision and monitoring of the systems, general services: electricity, air-conditioning, power generation, safety, planning office and construction workshop

TA (16) ATMAS Project

TS (7) system planning

TB (4) facility management: administration of buildings and structures

TI (20) management information system

The technical divisions TN, TC, TD, TZ and TG provided project management within their division as well as maintenance of the equipment for which they were responsible. Maintenance was provided by two specialist groups:

The first specialist group was responsible for preventive and corrective maintenance measures and for the installation of new systems. One member of this group provided a daytime on-site on-call service from 07:30 to 16:30 LT. At night and on holidays, the on-call service was provided from home.

The second specialist group handled difficult cases, made changes and carried out further developments. Technicians from the first group could also be drafted in for this work, if they specialised in a particular equipment type (courses in institutes, on manufacturers' premises or long-term practical experience) or if they were development engineers.

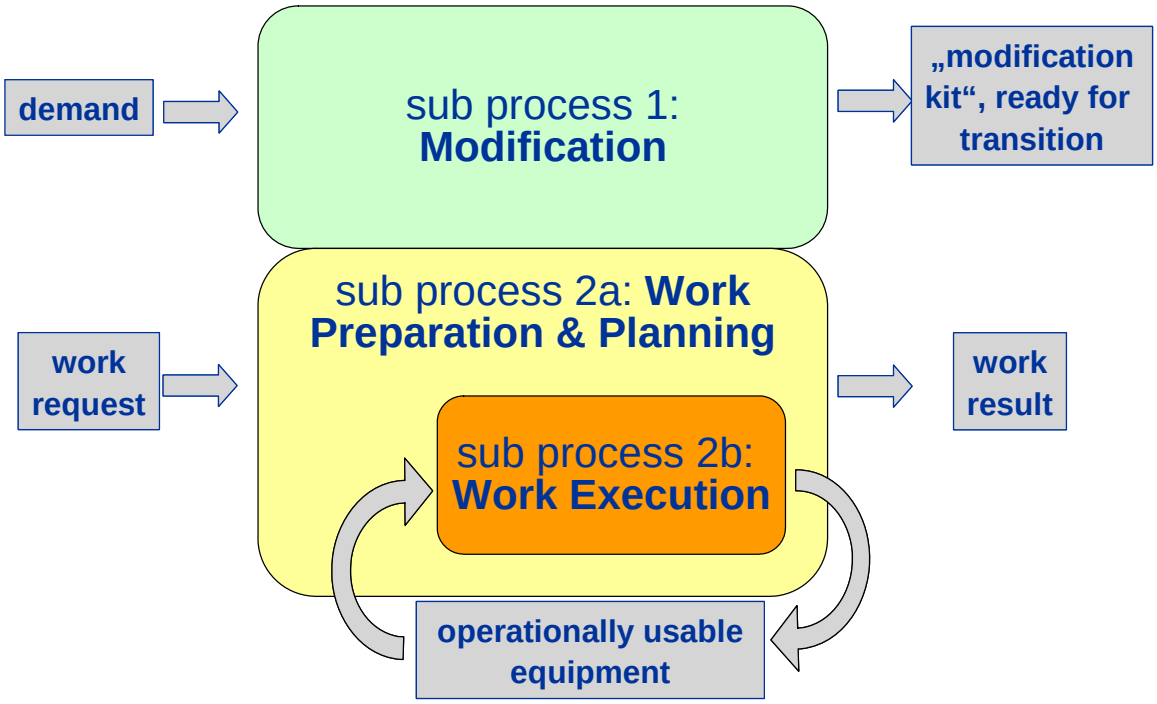
TG division was allocated air traffic control in Geneva and TZ division air traffic control in Zurich. Each of the divisions was responsible, among other things, for supervision of the aviation systems in the respective area control centre (SYMA workstation: system management).

The SYMA workstation was occupied on a daily basis from 05:00 LT to 23:30 LT. Outside these hours, an on-call service was available from home.

The SYMA had at his disposal numerous terminals and screens in order to be able to monitor and manage all the important technical air traffic control equipment. He coordinated his activities with the operational services and was able to reconfigure or switch over equipment in the event of deviations from the norm. Where appropriate, he had the technician from the technical service concerned (the first specialist group) make the intervention.

1.17.1.3 Coordination and processes between the technical services and the operational services

- OPS-TEC meeting in Zurich: monthly meetings took place, offering a platform for coordination of the respective requirements of the technical services and operational services or for an initial exchange of opinions on all interventions and modifications.
- planned work on ATM equipment (PWAE): This computer-assisted process served the administration of changes (adaptations, improvements and new software versions) and the installation of new equipment. It was introduced in Zurich at the end of 2002.



Two forms were used:

- process tracking form – PTF: this enabled the development of an intervention or a project to be monitored step by step; at the same time, traceability was guaranteed.
- degradation announcement – DA: this form contained all administrative data, i.e. the description, duration and commencement of the planned work as well as information on risk management and risk minimisation.

At the time of the serious incident, no procedures for preventive and corrective maintenance measures or for technical and operational training were yet in existence or had yet been introduced.

1.17.1.4 Information on the Technical Division TD (data processing)

The Technical Division TD comprised 74 personnel units, of which 39 at the Zurich site and 35 in Geneva. It was responsible for the maintenance and development of all equipment which displays radar data and flight plan data on the air traffic controllers' workstations. The TD division consisted of the groups TDR, TDE, TDA and TDP:

TD (G: 4) data processing division head

TDR (Z: 12) AIM & ADAPT

TDE (Z: 14) APP, DEP and airports

TDZ (Z: 13) platform support ZRH

TDG (G: 10) platform support GVA

TDA (G: 12) surveillance processing and ATM support

TDP (G: 9) en route traffic

List of the PWAEs which have been issued by the TD (data processing) division since their introduction in Zurich:

PWAE Completed"

- MV 9800
  Issued 15.01.2003
  Scheduled 22.01.2003 23:00 - 23.01.2003 02:00 LT
  Short Flightplan Message is modified and contains data in fields Callsign, SSR, EFL, EPT, SI, XPT, XFL, RNAV, 8.33, RVSM and the state of hold/lost
- ADAPT Display
  Issued 18.03.2003
  Scheduled 20.03.2003 22:00 - 04:00 LT
  Scheduled 27.03.2003 22:00 - 04:00 LT
  APP ICWS Main Display replacement by Barco LCD
- InfoNet AIS
  Issued 29.04.2003
  Scheduled 30.04.2003 08:00 - 17:00 LT
  Relocation of the InfoNet PCs in the app. room in AIS Zurich
- MSAW-zones for RWY 28
  Issued 19.05.2003
  Scheduled 11.06.2003 23:00 - 24:00 LT
  Minimum Safe Altitude Warning. Extension for Approach Runway 28 (3 additional zones, MSAW281,282 and 283)
- ADAPT New Software Real. 2.8
  Issued 16.06.2003
  Scheduled 17.06.2003 23:00 - 18.06.2003 05:00 LT
  Install and verify ADAPT software release 2.8. (All ADAPT equipment, except Trackview, fbRDPS and rFEP systems)
- MV 9800
  Issued 02.07.2003
  Scheduled 09.07.2003 21:00-23:00 LT
  Modification Sectorisation APP for TWR
- TACO/CALM New Release
  Issued 04.08.2003
  Scheduled 04.08.2003 23:00 - 05.08.2003 05:30 LT
  Installation of TACO Service-Release (technical enhancements) on all TACO workstations.

- IDM Patch Set
  Issued 05.09.2003
  Scheduled 06.11.2003 23:00 - 07.11.2003 02:00 LT
  Install Patchset 9.2.0.4 (Oracle) and OS Patches (HP)
- InfoNet
  Issued 16.09.2003
  Scheduled 24.09.2003 23:00 - 25.09.2003 02:00 LT
  Install Patchset 9.2.0.4 (Oracle) and OS Patches (HP)
- Primus compound tests
  Issued 30.09.2003
  Scheduled 16.10.2003 23:00 - 17.10.03 04:00 LT
  Scheduled 20.10.2003 23:00 - 21.10.03 04:00 LT
  This test will demonstrate that the RCMS can perform an MV switchover. All switchover combinations with the three local MVs will be tested 5 times. For each MV switchover, the temporary loss of MV output tracks (ACC and APP) is observed.
- INAS New Software release
  Issued 20.10.2003
  Scheduled 29.11.2003 ca. 13:30 LT
  Load new tables
- SPACK (x.25 international network)
  Issued 20.10.2003
  Scheduled 22.10.2003, 09:00 - 24.10.2003 16:00 LT
  - Test with P1 Munch
  - expand of the address range
- AFPS
  Issued 24.10.2003
  Scheduled 06.11.2003 23:00 – ca. 24:00 LT
  Monthly "chain change" (switch-over of operating and cold standby server)
- SYCO
  Issued 04.11.2003
  Scheduled 10.11.2003 23:00 - 11.11.2003 02:00 LT
  Supplement to DVO
  "PWAE in progress"
- SYCO
  Issued 17.11.2003
  Scheduled 26.11.2003 by agreement with operations
  Load new tables
- AFPS Bern
  Issued 17.11.2003
  Scheduled 19.11.2003 19:30 - 20.11.2003 21:00 LT
  Generate ghost of the software installation
- InfoNet Bern
  Issued 17.11.2003
  Scheduled 19.11.2003 23:00 - 20.11.2003 05:00 LT
  Generate ghost of the software installation
- ADAPT
  Issued 19.11.2003
  Scheduled 20.11.2003 23:30 - 21.11.2003 02:00 LT
  Software tool for CPU load monitoring

1.17.2 Technical Service TDZ

The TDZ service (**T**echnology - **D**ata Processing - Platform Support **Z**urich), consisting of 13 technicians, was responsible, among other things, for the ADAPT systems and in particular for the ICWS screens. The employees were divided into two sub-groups, which specialised in the ASP and PSP areas (first specialist group).

Actual Situation Processing – ASP (8 technicians):

MV9800	mainframe for processing radar/flight plan data
RCMS	monitoring system for the MV9800
ADAPT	**A**ir traffic management **D**ata **A**cquisition **P**rocessing and **T**ransfer - UNIX-workstations (Xclient/Xserver) - control screens (19" and 29" displays) - central servers (SMP, CAP, IPG and COM) - ADAPT's own LAN - redundant processing chains for radar data (Trackview FEP and fbRDPS)
PRN-Vigie	***P**osition **R**adar de **N**uit à la Vigie* (radar screens in the control tower)
TASD	**T**ower **A**ir **S**ituation **D**isplays for ZRH, Berne, Lugano, Altenrhein, Friedrichshafen, etc.
SAMAX	**S**wiss **A**irport **M**ovement **A**rea Control System (**X**: phonetic contraction of C and S)
ADR	**A**ll-purpose **D**ata Stream **R**eplicator to display meteorological data for the air traffic controllers
IDM	**I**ntegrated **D**ata **M**anagement, management of statistical aviation data

Planned Situation Processing - PSP (5 technicians):

SYCO ZRH	system for distribution and display of flight plans
SYCO MIL	system for distribution of flight plans to the military
COM Server	communications server for exchange of OLDI messages (Eurocontrol On-Line Data Interchange protocol) with neighbouring centres
TACO	**T**ower **A**pproach **Co**mmunication
CALM	**C**omputer-assisted **A**pproach and **L**anding **M**anagement
AFPS	**A**IS/ARO **F**light **P**lan **S**erver
STARS	**S**tatistical **T**raffic **A**nalysis **R**oute Charge and Flight Plan Data Processing **S**ystem
COPAIN	**Co**mputerized **P**reflight **A**eronautical **I**nformation and **N**OTAM: system for processing, verification and distribution of NOTAMs

ETFMS	**E**nhanced **T**actical **F**low **M**anagement **S**ystem: system for optimising traffic flow
CFMU	**C**entral **F**low **M**anagement **U**nit: central system for air traffic planning
AFTN	**A**eronautical **F**ixed **T**elecom **N**etwork
EAD	**E**uropean **A**eronautical Information Services **D**atabase
T-Boxes	interface between FLORAKO and ADAPT

Most of the TDZ technicians were also specialists in one or more installations. With the support of various engineers from the local development groups (TDR and TDE) they ensured maintenance.

At the time of the serious incident, an external ADAPT specialist was available to the TDR in Zurich. A second had been absent since June 2003. These ADAPT specialists originally belonged to the system supplier's foreign development team and were later contracted via an external company.

Since ADAPT had been taken out of service in Geneva in June 2003, there were no longer specialists available there for this system.

1.17.3 Technical training and education

The prerequisites for a position in the technical sector of skyguide were based on the basic educational grades of the Swiss education system with further qualifications at apprenticeship, advanced technical college or university level. Depending on the discipline, different educational grades were required.

At the time of the serious incident there was no technical college for aviation in Switzerland. For this reason, skyguide did not find any technical personnel on the local labour market that already had corresponding training. Consequently, skyguide drafted its own training concept, the aim of which was to train technical personnel with regard to performing their tasks.

This specialist technical training consisted of three consecutive phases:

1.17.3.1 Common Basic Training (CBT)

Thirty course days were available within the company for this training phase. It had to be completed by all new employees, in order to complete their professional knowledge in the area of aviation in general and the company in particular. It included the following subject areas:

- aviation (aircraft, flight rules, weather situation)
- air traffic control organisations (ICAO, FOCA, Eurocontrol)
- the organisation of airspace (FIR, CTA, CTR, TMA)
- the organisation of air traffic control (ACC, APP, TWR)
- technical methods for aviation (telephone, local area networks, RDP/FDP, navaids, introduction to radar)
- skyguide (task, organisation, infrastructure)

1.17.3.2 Qualification Training

This was a training phase which was particularly orientated towards the employee's future area of activity (communication, data processing, navigation and surveillance). The modules listed below lasted between one and several weeks and some were delegated to a foreign institution (ENAS in Toulouse, IANS in Luxembourg, DFS academy):

- HF technologies and radio communication
- primary surveillance radar
- secondary surveillance radar, MSSR and Mode S
- navigation aids: the fundamentals of ILS/VOR, ILS system, VOR system, DME system
- trends in air traffic control technology

1.17.3.3 System Training

In the final phase, the individual employees learned to operate equipment for which they would eventually be responsible (operation, maintenance, development, etc.). This often involved courses or practical sessions with a supplier or in a related aviation organisation (ENAC, Eurocontrol, NAV Canada):

- ASR10 (primary) / MSSR9600 (secondary) surveillance radars
- reformatting and distribution system for radar data RMCDE
- modelling of objects UML
- system administration HPUX-11.0
- multi-radar data processing ARTAS
- high-resolution radar screens
- weather radar

1.17.3.4 Training Organisation for Technical Equipment Management (TOTEM)

In order to meet the requirements of recommendation ESARR5 (Eurocontrol Safety Regulatory Requirement – ATM Services' Personnel) by 2005, skyguide developed a database application.

The initial phase in 2003 involved administration of the training courses offered (list and timetable for the courses).

In the subsequent phases, the following goals were targeted:

- analysis of requirements at equipment level
- determining the training courses according to disciplines
- inventory of existing knowledge and of the company's existing technical know-how

In practice, according to statements by skyguide employees, CBT was completed in only about 50% of cases. The schedule for the individual employees was so tight that they could not be released to attend the courses. In addition, the training content was not precisely defined and the choice of courses was left to the discretion of the individual employees.

The courses or practical sessions did not conclude with examinations. Hence an essential prerequisite for certification of training was lacking.

As already mentioned, the ADAPT specialists were not employed by skyguide but were under contract and had therefore not completed CBT.

1.17.4 International regulations on training and licenses in the area of aviation

1.17.4.1 International Civil Aviation Organization (ICAO)

Annex 1 of the ICAO's International Civil Aviation Agreement, "Personnel Licensing", contains the issuing of licences as well as the general requirements of all personnel working in aviation (pilots, aircraft maintenance personnel, air traffic controllers, maintenance technicians and flight dispatchers).

1.17.4.2 EUROCONTROL Safety Regulatory Requirement - ATM Services' Personnel (ESARR5)

Recommendation ESARR5, in the version dated 11.04.2002, is an addition to Annex 1 of the ICAO Agreement with regard to safety. It was issued to extend the requirements to all personnel of ATM services including those technical personnel whose function is related to flight safety. In this document, it is specified that on the one hand air traffic controllers must be qualified to exercise their profession and must possess a valid licence and on the other hand that air navigation services companies must ensure that technical personnel have the training and corresponding capabilities to perform the duties assigned to them. This recommendation was not yet in force in Switzerland at the time of the serious incident.

1.17.5 Specialist international associations

The associations of technical personnel in air navigation services (Air Traffic Safety Electronics Personnel – ATSEP) of various countries came together in 1972 and founded the International Federation of Air Traffic Safety Electronics Associations (IFATSEA). This organisation set itself the goal of promoting safety, efficiency and regulatory compliance in aviation and protecting the professional interests of technical personnel (ATSEP).

Fifty-four countries, including Switzerland, are represented in IFATSEA. In Switzerland, professional technical personnel of air navigation services came together in the Swiss Air Traffic Control Technical Association – SATTA.

The IFATSEA has achieved that the International Labour Organisation (ILO) of the UNO has recognised the profession of air traffic safety technicians in the same way as air traffic controllers.

1.17.6 Implementation of ICAO Annex 1 and ESARR5

Qualification and the issuing of licences[5] are described in greater detail in the above-mentioned ICAO documentation and by Eurocontrol. In it, no licence is required for technical personnel.

It is the responsibility of the air navigation services company to ensure that technical personnel have corresponding training and adequate qualifications to perform the duties assigned to them.

The requirement for technical personnel to also be issued with licences has arisen only in recent years, because the electronic equipment and informatics systems in handling and monitoring air traffic have become more and more important.

In the early days of commercial aviation, air traffic control equipment was limited to stand-alone electronic devices, such as HF and VHF transmitters/receivers, non-directional radio beacons, radio direction finders and the instrument landing system (ILS). Nowadays, air navigation technology systems are networked and in addition to electronic devices also include information and communication systems. The multidisciplinary character of air traffic control systems led the IFATSEA to propose, on 5 April 2000, that Annex 1 of the ICAO Agreement be amended in the area of ATSEP qualifications and licences.

In addition, in 2000, the IFATSEA, in conjunction with the ICAO, initiated the development of a training manual for technical personnel. This document was published by the ICAO in 2004 (Doc 7192-AN/857 Part E-2); it describes the goals, phases and knowledge which are required for basic training as well as the qualification in the main areas of air navigation services.

- communication systems
- navigation equipment
- surveillance systems
- data processing systems
- safety and risk management

In the third phase of training, technical personnel should be provided with the capability to master the equipment for which they are responsible. Only the goals are described for this training phase (rating). However, it must always be passed before technical personnel start work on operational systems. In the process, special weight is accorded to the following tasks:

- systems control and monitoring
- preventive maintenance measures
- corrective maintenance measures for defect rectification
- modifying and upgrading operational systems
- calibration and validation of systems with regard to compliance with specifications
- certification and recertification

[5] A licence is an authorisation issued by a higher authority to exercise a regulated activity.

This training manual is based largely on the work of the IFATSEA and the ICAO, as well as on the contributions of different states or international organisations.

At the end of 2002, Eurocontrol amended Recommendation ESARR5 and inserted section 5.3 as an addition. This contains the requirements put on technical personnel performing air navigation services duties which are relevant to safety.

Together with the ICAO, on 06.10.2003 Eurocontrol published a guide to Qualification Training of ATSEP and on 02.04.2004 a similar guide on Common Base Training.

2 Analysis

2.1 Technical aspects

2.1.1 System concept

The ADAPT system is controlled by a central monitoring and control computer (SMP). A computer of identical construction is on hot standby for this SMP. All Xclients and workstations (IPG, CAP, COM) in the CIR are controlled by the active SMP. Consequently, for radar data display by the ADAPT system, redundancy exists only with regard to the workstations, but not with regard to the central control function. A fault in the control function may therefore, as in the serious incident, lead to a total failure of the radar air picture presentation. Independent distribution of the control function or the provision of an independent display system was omitted during the design of the ADAPT system.

2.1.2 The incident on 31 October 2003

The incident was correctly recorded in the SYMA log and the responsible on-call service was informed by telephone. The SYMA log contains error messages from the MV and from the ADAPT SMP. For fault analysis, MV engineering was consulted by the on-call service. After the procedure which was described in the log as “some MV investigations” produced no results and the fault did not recur, it was decided not to take any immediate measures. The SYMA concluded the notification.

Although it was stated in the SYMA log that the ADAPT SMP error message might have had nothing to do with the MV error message, ADAPT engineering was not included in the analysis of the cause. Primarily on the basis of the symptoms having been eliminated, i.e. no further track failure could be observed; no further clarifications and measures were sought. It cannot be understood why, with the exception of the SYMA log, no data for the analysis of the incident were backed up. Consequently the log files of the ADAPT SMP monitoring and control computer, as well as those for the Xclient 27, 28 and the Xserver 27, 30 involved, were lost.

On the following Monday 3 November 2003, TDZ decided, on the basis of the telephone enquiry from the SYMA and a discussion with the on-call service and MV engineering, to forward the incident to ADAPT engineering for investigation. Immediately after the incident on 31 October 2003, insufficient qualified personnel were available for a detailed analysis. This is why TDZ decided to await the return of the ADAPT specialist from holiday on the following Monday, 10 November 2003. At this point, it would still have been possible to back up the data on the incident, but this was not done. Furthermore, no risk analysis was carried out and no operational precautions were taken.

The analysis of the incident on 31.10.2003, the assessment of the situation and the decision to defer actions were inappropriate. A total failure of the radar tracks on two ICWS should have required a thorough and profound analysis of the causes.

There was no process with work instructions and checklists to handle system malfunction. Only a planned work on ATM equipment (PWAE) process existed. Hence new installations and system upgrades or modifications were covered, but not preventive or corrective maintenance interventions in the system.

2.1.3 The serious incident of 11 November 2003

The ADAPT specialist, who was entrusted on 10 November 2003, with the investigation of the failure of 31 October 2003, found the anomaly of an unusually high CPU load on standby Xclient 28 from the affected cluster. A shutdown/startup of Xclient 28 was carried out at 08:54 UTC on a trial and error basis.

The handling of the incident by the air navigation services company included the following deficiencies:

- A causal connection with the incident on 31 October 2003 was not sought and is also not documented.
- After an analysis of the cited incident had been deferred for 10 days, it was decided on the presumed reduced functionality of standby Xclient 28 to make an immediate corrective intervention in the operational system, without making any further preparations for this.
- The procedure on the operational system was discussed with the SYMA, but was neither assessed for operational risks nor entered in the SYMA log.
- The corrective intervention was carried out at a time when there was traffic and when operational precautions should urgently have been taken in the event of a failure of the intervention.
- The corrective intervention included an untested operation on a system in operational use. This operation was not documented in the system manual and its effects were not described. This is why the present report refers to an untested intervention.
- No process existed for such corrective interventions, which would have regulated the sequences, responsibilities or coordination with air traffic control.

2.1.3.1 Additional corrective interventions on 11 November 2003

After the shutdown/startup of Xclient 28, the system was checked for other Xclients with an increased CPU load. In the process, an increased CPU load was detected on Xclients 4 and 10, which were working in standby mode. After the corrective intervention on Xclient 28 in the morning appeared to have been successful in terms of the problem of CPU load, the same corrective interventions were also made on these computers at 18:31:17 UTC and 18:34:28 UTC according to the SMP log. In addition to the deficiencies already mentioned, this procedure exhibited the following deficiencies:

- No clarification of the cause and effects of the increased Xclient CPU load was carried out.
- The second corrective intervention on Xclient 10 was started before the first intervention on Xclient 4 was fully completed.

The sequence of the corrective intervention in the morning on Xclient 28 began at 08:54:18 UTC with the shutdown command:

Tue Nov 11 08:54:18 2003 zhsuc01 - zhsuc02:SMC2 - SMC NSRVR NODE SHUTDOWN - Node zhxcc28 shut down.

After just 2 minutes, the process was active again, i.e. green on the screen:

Tue Nov 11 08:56:10 2003 zhsuc01 - Process State: zhxcc28 ICW_SIT_20 State= ACTIVE, Mode= Standby

However, the SMP log shows that the "standby sit 5" process was not ready for operation until a good nine minutes later:

068541404 7 Tue Nov 11 09:03:24 2003 zhsuc01 - zhxcc28:ICW_SIT_20 - ICW-STANDBY-READY - Standby sit 5 process ready for operation;1 .1.3.6.1.4.1.9999.0.10003 0

The corrective intervention on Xclient 10 took place a good three minutes after the shutdown command for Xclient 4 and about two minutes after the process on Xclient 4 was active again, but not yet ready for operation.

Nov 11 18:32:25 2003 zhsuc01 - Process State: zhxcc04 ICW_SIT_04 State= ACTIVE, Mode= Standby

Tue Nov 11 18:34:28 2003 zhsuc01 - zhsuc02:SMC2 - SMC NSRVR NODE SHUTDOWN - Node zhxcc10 shut down.

The messages concerning "...*process ready for operation*..." were not logged, since the total failure occurred before. Three seconds after the shutdown command for Xclient 10 and one second after the network links to the other computers went down, control over the state of the network was lost:

Tue Nov 11 18:34:30 2003 zhsuc01 - Network State: DISCONNECT_NODE zhxcc04 zhxcc10

Tue Nov 11 18:34:31 2003 zhsuc01 - zhsuc02:SMC2 - SMC CFG SYNC ACTIVE PROCESS ER - zhgwm02 is not active in the list of NSRVR processes, shutting down zhgwm02.

If the computers for the central monitoring and control computer (SMC) can no longer be controlled, the SMC program issues shutdown commands without any prior warning. Thus in the same second shutdown commands were issued to all Xclients automatically. This then led to the rapid failure of the radar display on the ICWS.

During the following night, a vain attempt was made to reproduce the incident by performing the operations made in the evening in accordance with the new system configuration on standby Xclients 3 and 10.

The chronological coincidence between the corrective intervention and the instability of the network configuration which led to the shutdown of all Xclients by the SMC allows the conclusion to be drawn that the said intervention in the operational system triggered the total failure.

2.1.4 Training, certification and maintenance

2.1.4.1 Training and certification

The training and in particular the certification of technical personnel and the certification of the air traffic control equipment constitute a complex task. The systems in use, such as SYCO, MRT or ADAPT, use different technologies and in addition were manufactured in very small series or even were custom built. For a long time this circumstance served as an argument for designating such systems and the personnel responsible for their maintenance as non-certifiable.

2.1.4.2 Eurocontrol safety requirements

With regard to both the maintenance of equipment and the training of technical personnel, skyguide, according to its own statements, refers to recommendations ESARR4 and ESARR5 and intended to apply these.

These recommendations were not yet in force at the time of the serious incident; the technical personnel involved did not have the training and qualifications which would have been required according to the recommendation in ESARR5.

2.2 Operational aspects

This total failure of the radar air picture presentation represented a considerable potential hazard for air traffic.

The measures taken after the failure by the air traffic controllers concerned were thoroughly appropriate. The mutual agreements proved to be correct.

It was also fortunate that at the time of the incident the volume of traffic was fairly light and that the DOM control tower, DOM area control centre, and approach and departure control were occupied by experienced personnel.

3 Conclusions

3.1 Findings

3.1.1 Prior history and sequence of the serious incident

- On 31 October 2003, at approximately 09:30 UTC, a sudden failure of all radar tracks of several seconds duration occurred on two ICWS in approach control in the CIR.
- TDZ decided to await the return of the absent specialist before analysing and rectifying the problem.
- The log files for this incident were not backed up and had been overwritten by the time of the fault analysis on 11 November 2003.
- On 11 November 2003 it was established that Xclient 28 had a greatly increased processor load.
- At 08:54 UTC on the same day, a shutdown/startup of Xclient 28 took place. This corrective intervention in the operational system was not entered in the SYMA log.
- In the course of the day, two further standby Xclients (4 and 10) were found with an increased processor load.
- At 18:31:17 UTC a shutdown/startup command was sent to Xclient 4.
- At 18:34:28 UTC a shutdown command was sent to Xclient 10.
- During the shutdown of Xclient 10 the central monitoring and control computer (SMP) issued shutdown commands to the active ADAPT processes.

3.1.2 Technical aspects

- There were three redundant systems for processing radar data.
- No real redundancy existed in the system for displaying the radar air picture, as the same types of equipment, operating systems and software were used.
- A causal connection between the increased CPU load and the incident on 31 October 2003 was not sought and is also not documented.
- The corrective intervention included an untested operation on a system in operational use.
- The corrective intervention was made without a detailed and documented risk assessment.
- No processes, procedural or working instructions were defined or introduced for corrective interventions on systems in operational use.

3.1.3 Operational aspects

- Air traffic control was not informed of the corrective intervention in the system.
- There were no indications of an impending failure of the radar air picture presentation on the air traffic controllers' radar screens.
- From 18:34:48 UTC, all radar screens of the area control centre and approach and departure control were affected by the failure.
- Within one minute the failure spread to all 29 radar screens and lasted for about 15 minutes.
- After the failure all departures from Zurich were suspended for a period of approximately 20 minutes.
- The radar screens in the tower were not affected by the failure. These were used to vector aircraft which were already in the vicinity. Following aircraft were instructed to fly into holding patterns, from where they were taken over by the approach sectors in the control tower.
- The measures taken by the air traffic controllers concerned were thoroughly appropriate.

3.1.4 General conditions

- skyguide's technical personnel involved in the serious incident did not have the training and qualifications which would have been required according to the recommendation in ESARR5. This recommendation was not yet in force at the time of the serious incident.

3.2 Causes

The serious incident is attributable to the fact that the central monitoring and control computer terminated for unknown reasons all active processes relating to the radar air picture presentation, released after untested corrective interventions on the ADAPT system.

The following factors contributed to the origin of the serious incident:

- Processes for corrective interventions were lacking in the air traffic control company.
- To what extent the overall level of knowledge of the personnel involved which undertook corrective interventions on the technical systems of the air navigation services company was sufficient must remain open.
- The impending corrective intervention was not coordinated with air traffic control.
- The central monitoring and control computer's program had no safety precautions and warning systems.
- There was no redundant system for the presentation of the radar air picture.

4 Safety recommendations and measures taken since the serious incident

4.1 Procedures after technical failures

4.1.1 Safety deficit

The incident on 31 October 2003 was incompletely documented:

- The data were not backed up.
- The cause was not systematically clarified.
- Prior to initiating corrective measures, no thorough risk assessment was carried out.

On the basis of the symptoms having been eliminated, by restarting Xclient 28, the problem was considered to have been solved.

4.1.2 Safety recommendation No. 320 (formerly No. 90)

The Federal Office for Civil Aviation should arrange for all technical incidents and failures to be treated in accordance with a uniform and defined process and systematically documented in a technical logbook. In particular the description of the incident, the backed-up data, the causal analysis and the measures taken must form part of such documentation.

4.2 Interventions in systems in use

4.2.1 Safety deficit

In connection with the investigation of the collision of two airline aircraft over Überlingen, the Aircraft Accident Investigation Bureau in Germany issued the following safety recommendation:

Safety Recommendation No. 01/2003 of the German Aircraft Accident Investigation Bureau (SE draft Überlingen):

The Federal Office for Civil Aviation (FOCA) should ensure that the air traffic control service provider issues and implements procedure to undertake maintenance work on the ATC Systems stipulating operational effects and available redundancies. The procedure shall include the following aspects:

- *Stipulating the detailed responsibilities of the Operational Division and the Technical Division.*
- *Personnel reserve planning of the operational staff for maintenance work on the ATC Systems.*
- *Timely dissemination of procedure to the controllers, in order to prepare them to deal with the situations.*
- *Establish and implement the checklists for the maintenance as well operational staff, when maintenance work on the ATC Systems is undertaken, to enhance the safety net.*
- *Selection of best possible time from operational aspects for the maintenance work on the ATC Systems.*

In view of the long delay between the incident on 31 October 2003 and the associated intervention on 11 November 2003, the intervention should have been made in accordance with the process for planned work on ATC equipment (PWAE). Instead, the technical expert decided on a spontaneous corrective action. No defined and introduced sequence of processes existed for this type of intervention in an operational system. Thus, a flow of information to the operational services in particular was not guaranteed.

Already at the time of the Überlingen collision the air traffic controller had only been partially informed of the planned technical work and was therefore able only to make an incomplete assessment of the operational consequences.

4.2.2 Safety recommendation No. 321 (formerly No. 91)

The Federal Office for Civil Aviation should arrange for the safety recommendation of the German Aircraft Accident Investigation Bureau to be amended as follows:

All interventions in operational systems should take place in accordance with a defined and introduced process sequence. In addition, this process must include the following measures:

- informing the operational services of all interventions
- assessing the possible operational effects
- planning any operational and technical preventive measures

Moreover, the Federal Office for Civil Aviation should examine which interventions in the technical systems in use for air traffic control must be strictly limited to the times between 24:00 and 05:00 LT.

4.3 Certification of air traffic control equipment

4.3.1 Safety deficit

The investigation has shown that important technical equipment for air traffic control does not have any effective redundancy and that no adequate safety precautions and warning systems existed.

On the occasion of an Air Navigation Conference the ICAO produced the following document:

"REF: AN-Conf/11-WP/197 29/9/03

2.3 SAFETY CERTIFICATION OF ATM SYSTEMS

2.3.1 The meeting discussed a number of issues concerning the need for certification of ATM service providers and systems, and the need for coordination and cooperation between safety regulatory authorities with regard to certification standards and procedures. The meeting recalled that certification requirements existed for aircraft and aircraft equipment. Provisions requiring certification of aerodromes had become applicable on 1 November 2001. However, there were no existing ICAO requirements for certification of ATM systems, or ATM service providers.

....

2.3.3 The meeting expressed strong support for the concept of certification. It was recognized that there was more than one way in which this could be approached. Certification requirements could be introduced for ATM equipment, or for ATM service providers, or for both.

2.3.4 The meeting noted that safety of ATM system operations depended on a great number of criteria including, inter alia, the competency of personnel, the quality and reliability of the aeronautical data, operational procedures, navigation communications and surveillance equipment, and the interactions between these elements. It was further noted that in modern ATM systems, it was possible that ATS providers could be relying on facilities or services, such as satellite navigation and communications, which were outside the jurisdiction of the State concerned. All these factors would need to be taken into account in the development of certification criteria.

....

Recommendation 2/6 — Safety certification of ATM systems: That ICAO investigates the need for the development of provisions for safety certification of ATM systems and service providers."

4.3.2 Safety recommendation No. 322

The Federal Office for Civil Aviation should arrange for technical air traffic control personnel and air traffic control equipment to be certificated.

4.4 Measures taken since the serious incident

According to a letter from skyguide dated 22 March 2006, the following measures have been taken to improve air safety (the following seven points are a translation from the original letter that was written in German):

1. Directly after the incident, skyguide immediately banned all manual switchovers and shutdown/startup interventions using the SMP until revocation; in the days after the incident, the readiness of the maintenance team was increased in order to be able to react immediately to any further faults.
2. In December 2003, as an immediate measure, the software of the SMC application was modified so that not more than 3 nodes can be shutdown together automatically.
3. The reason for the increased CPU load was investigated and could be clearly identified. Appropriately adapted software, which eliminates the problem first detected on 10 November, was put into service on 19 February 2004.
4. skyguide has made efforts to reproduce the incident on the ADAPT test platform in order to obtain further information on its cause. A comparable fault occurred only after three months of testing and after 120,000 automatically implemented shutdown/startups (corresponding to about 500 years of operation).
5. The maintenance procedures were revised from the ground up. In particular, a procedure was defined for so-called "unexpected situations". The full package of all new maintenance procedures was checked by an independent agency in September 2005 as part of an ISO audit.

6. In April 2004, a second air picture presentation system, independent of the main system, was brought into operation. Since then, the possibility exists at each air traffic controller workstation, to display the current air picture on an auxiliary screen in the event of a main system failure.

7. In May 2004, as part of a system renovation phase decided upon on 10 June 2003, the entire ADAPT display system was replaced by a newly developed system.

Comments by the AAIB

On point 3: during the investigation the AAIB requested written information on the reason for the increased CPU load. This question had not been answered before the investigation was concluded.

On point 4: skyguide does not specify the software version under which the three-month test was carried out.

Berne, 26 August 2008

Federal Aircraft Accident Board

André Piller, President

Tiziano Ponti, Vice-President

Ines Villalaz-Frick, Member

Annexes

Annex 1: Extract from file "trapd.log"

The "Node Startup" command is given and the confirmation "Node Confirm" is accepted, in order to restart all the processes on the station Xclient 13:

....
....
....
Tue Nov 11 18:38:52 2003 zhsuc02 E UNASMap : INFORMATION : User at SMP performed action "Node Startup" on object Zurich/Zurich_ACC/ACC/zhxcc13
Tue Nov 11 18:38:53 2003 zhsuc02 - Interface Info: 1;1 .1.3.6.1.4.1.19.5.1.34.1.1.100.0.2 0
Tue Nov 11 18:38:54 2003 zhsuc02 E UNASMap : INFORMATION : User at SMP performed action "Node Confirm" on object Zurich/Zurich_ACC/ACC/zhxcc13;
Tue Nov 11 18:39:07 2003 zhsuc02 - Interface Info: 0 zhsuc02;1 .1.3.6.1.4.1.19.5.1.34.1.1.31.0.2 0
Tue Nov 11 18:39:07 2003 zhsuc02 - Interface Info: 0 zhsuc02;1 .1.3.6.1.4.1.19.5.1.34.1.1.32.0.2 0
Tue Nov 11 18:39:10 2003 zhsuc02 - zhsuc02:SMC2 - SMC NSRVR NODE REINTRO - Node zhxcc13 reintroduction in progress.;1 .1.3.6.1.4.1.9999.0.10003 0
Tue Nov 11 18:39:11 2003 zhsuc02 - Network State: CONNECT_NODE zhgwm01 zhxcc13;1 .1.3.6.1.4.1.19.0.64 0
Tue Nov 11 18:39:11 2003 zhsuc02 - Network State: CONNECT_NODE zhcsm02 zhxcc13;1 .1.3.6.1.4.1.19.0.64 0
Tue Nov 11 18:39:11 2003 zhsuc02 - Network State: CONNECT_NODE zhsuc02 zhxcc13;1 .1.3.6.1.4.1.19.0.64 0
Tue Nov 11 18:39:11 2003 zhsuc02 - Network State: CONNECT_NODE zhxcc13 zhcsm01;1 .1.3.6.1.4.1.19.0.64 0
Tue Nov 11 18:39:11 2003 zhsuc02 - Network State: CONNECT_NODE zhcsm01 zhxcc13;1 .1.3.6.1.4.1.19.0.64 0
Tue Nov 11 18:39:12 2003 zhsuc02 - Network State: CONNECT_NODE zhxcc13 zhgwm03;1 .1.3.6.1.4.1.19.0.64 0
Tue Nov 11 18:39:12 2003 zhsuc02 - Network State: CONNECT_NODE zhgwm03 zhxcc13;1 .1.3.6.1.4.1.19.0.64 0
Tue Nov 11 18:39:12 2003 zhsuc02 - Process State: zhxcc13 ICW_SIT_09 CREATE_PROCESS;1 .1.3.6.1.4.1.19.0.65 0
Tue Nov 11 18:39:12 2003 zhsuc02 - Process State: zhxcc13 ICWS_09_BRDRCVR CREATE_PROCESS;1 .1.3.6.1.4.1.19.0.65 0
Tue Nov 11 18:39:12 2003 zhsuc02 - Process State: zhxcc13 ICWS_09_SAIL_1 CREATE_PROCESS;1 .1.3.6.1.4.1.19.0.65 0
Tue Nov 11 18:39:12 2003 zhsuc02 - Process State: zhxcc13 ICWS_09_SAIL_2 CREATE_PROCESS;1 .1.3.6.1.4.1.19.0.65 0
Tue Nov 11 18:39:12 2003 zhsuc02 - Process State: zhxcc13 ICWS_09_BRDRCVR State= COLD_START, Mode=;1 .1.3.6.1.4.1.19.0.65 0
Tue Nov 11 18:39:12 2003 zhsuc02 - Process State: zhxcc13 ICWS_09_SAIL_1 State= COLD_START, Mode=;1 .1.3.6.1.4.1.19.0.65 0
Tue Nov 11 18:39:12 2003 zhsuc02 - Process State: zhxcc13 ICWS_09_SAIL_2 State= COLD_START, Mode=;1 .1.3.6.1.4.1.19.0.65 0
Tue Nov 11 18:39:12 2003 zhsuc02 - Process State: zhxcc13 SMC19 CREATE_PROCESS;1 .1.3.6.1.4.1.19.0.65 0
Tue Nov 11 18:39:12 2003 zhsuc02 - Process State: zhxcc13 SMC19 State= COLD_START, Mode=;1 .1.3.6.1.4.1.19.0.65 0
Tue Nov 11 18:39:13 2003 zhsuc02 - Process State: zhxcc13 ICW_SIT_09 State= COLD_START, Mode=;1 .1.3.6.1.4.1.19.0.65 0

Annex 2: Extract from file ZHXCC13_NSRVR_INFO_11 31/10/03 08:28

INFORMATION 1839:11 Process_Client_Message reported NSRVR_INFORMATION

Connected to client: zhgwm01 NSRVR

INFORMATION 1839:11 Process_Client_Message reported NSRVR_INFORMATION

Connected to client: zhcsm02 NSRVR

INFORMATION 1839:11 Process_Gac_Response reported NSRVR_INFORMATION
Connected to GAC NSRVR

INFORMATION 1839:11 Process_Privileged_Status reported NSRVR_INFORMATION
Connected to NSRVR_PROCESS on zhsuc02

INFORMATION 1839:11 Process_Client_Message reported NSRVR_INFORMATION
Connected to client: zhsuc02 NSRVR

INFORMATION 1839:11 Process_Privileged_Status reported NSRVR_INFORMATION
Connected to NSRVR_PROCESS on zhcsm01

INFORMATION 1839:11 Process_Client_Message reported NSRVR_INFORMATION

Connected to client: zhcsm01 NSRVR

INFORMATION 1839:12 Process_Privileged_Status reported NSRVR_INFORMATION

Connected to NSRVR_PROCESS on zhgwm03

INFORMATION 1839:12 Process_Client_Message reported NSRVR_INFORMATION
Connected to client: zhgwm03 NSRVR

INFORMATION 1839:12 Process_Gac_Response reported NSRVR_INFORMATION
Connected to new GAC ICWS_09_BRDRCVR

INFORMATION 1839:12 Process_Gac_Response reported NSRVR_INFORMATION
Connected to new GAC ICWS_09_SAIL_1

INFORMATION 1839:12 Process_Gac_Response reported NSRVR_INFORMATION
Connected to new GAC ICWS_09_SAIL_2

INFORMATION 1839:12 Process_Gac_Response reported NSRVR_INFORMATION
Connected to new GAC SMC19

INFORMATION 1839:13 Process_Gac_Response reported NSRVR_INFORMATION
Connected to new GAC ICW_SIT_09
....
....
....

Annex 3: Radar air picture at the beginning of the serious incident