



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

# **Schlussbericht Nr. 1887**

## **der Eidg. Flugunfallkommission**

### **über den Totalausfall der Darstellung der Radarluftlage**

an sämtlichen Arbeitsstationen der Bezirksleitstelle (ACC)  
und der An- und Abflugleitstelle (APP)

in der Flugverkehrsleitung Zürich (ATC ZRH)

vom 11. November 2003

Dieser Schlussbericht wurde von der Eidgenössischen Flugunfallkommission nach einem Überprüfungsverfahren gemäss Art. 22 – 24 der Verordnung vom 23. November 1994 über die Untersuchung von Flugunfällen und schweren Vorfällen erstellt (VFU/SR 748.126.3). Er basiert auf dem Untersuchungsbericht des Büros für Flugunfalluntersuchungen vom 7. April 2006.

Der Bericht wurde ausschliesslich zum Zwecke der Flugunfallverhütung erstellt. Die rechtliche Würdigung der Umstände und Ursachen von Flugunfällen ist nicht Gegenstand der Flugunfalluntersuchung (Art. 24 des Luftfahrtgesetzes vom 21.12.1948, LFG, SR 748.0).

### Allgemeine Hinweise zu diesem Bericht

Entsprechend dem Abkommen über die internationale Zivilluftfahrt (ICAO Annex 13) ist das alleinige Ziel der Untersuchung eines Flugunfalles oder eines schweren Vorfalles die Verhütung künftiger Unfälle oder schwerer Vorfälle. Es ist nicht Zweck dieser Untersuchung, ein Verschulden festzustellen oder Haftungsfragen zu klären.

Gemäss Art. 24 des Schweizer Luftfahrtgesetzes ist die rechtliche Würdigung der Umstände und Ursachen von Flugunfällen und schweren Vorfällen nicht Gegenstand der Flugunfalluntersuchung.

Geschlechtsunabhängig wird in diesem Bericht aus Datenschutzgründen ausschliesslich die männliche Form verwendet.

Alle Zeiten in diesem Bericht sind, wo nicht anders angegeben, in koordinierter Weltzeit (*coordinated universal time* – UTC) angegeben, die im Unfallzeitpunkt der mitteleuropäischen Sommerzeit (MESZ) als Normalzeit (*local time* – LT) entsprach. Die Beziehung zwischen LT, MESZ und UTC lautet:  $LT = MESZ = UTC + 1 \text{ h}$ .

Der Wortlaut des deutschsprachigen Berichtes ist massgebend.

## Inhaltsverzeichnis

<b>Allgemeines</b> .....	<b>6</b>
<b>Kurzdarstellung</b> .....	<b>6</b>
<b>Untersuchung</b> .....	<b>6</b>
<b>I. Einleitende Bemerkungen zum System der Flugsicherung Zürich</b> .....	<b>8</b>
<b>I.I Radarsystem</b> .....	<b>8</b>
I.I.I Primärradar .....	8
I.I.II Sekundärradar .....	8
I.I.III Radardatenverarbeitung .....	8
<b>I.II Luftraumstruktur Schweiz</b> .....	<b>10</b>
I.II.I Hauptverkehrsachsen durch den Luftraum der Schweiz .....	10
I.II.II Zuständigkeiten der Flugsicherung Zürich.....	10
I.II.III Luftraumstruktur Zürich .....	11
<b>1 Sachverhalt</b> .....	<b>14</b>
<b>1.1 Vorgeschichte und Verlauf des Vorfalles</b> .....	<b>14</b>
1.1.1 Vorgeschichte .....	14
1.1.1.1 Radarausfall vom 31. Oktober 2003.....	14
1.1.1.2 Bearbeitung des Radarspurenausfalls vom 31.10.2003 durch die technischen Dienste .....	14
1.1.2 Verlauf des schweren Vorfalles.....	14
1.1.2.1 Verkehrslage zu Beginn des Ausfalls der Radardarstellung .....	16
1.1.2.2 Auswirkungen des Ausfalls der Radardarstellung vom 11. November 2003 auf die Flugverkehrsleitung .....	16
1.1.2.3 Auswirkungen auf den Betrieb im Kontrollturm .....	17
1.1.2.4 Auswirkungen auf die An- und Abflugleitstelle .....	17
1.1.2.5 Auswirkungen auf die Bezirksleitstelle .....	18
1.1.2.6 Ablauf der Wiederinbetriebnahme .....	18
<b>1.2 Personenschäden</b> .....	<b>19</b>
<b>1.3 Schaden am Luftfahrzeug</b> .....	<b>19</b>
<b>1.4 Verkehrseinschränkungen</b> .....	<b>20</b>
1.4.1 Allgemeines .....	20
1.4.2 Verkehrseinschränkungen An-/Abflugleitstelle und Kontrollturm.....	20
1.4.3 Verkehrseinschränkungen Bezirksleitstelle .....	20
<b>1.5 Angaben zu Personen</b> .....	<b>21</b>
1.5.1 Der Systemmanager .....	21
1.5.2 Der ADAPT Spezialist .....	22
<b>1.6 Angaben zum Radarsystem der Flugsicherung Zürich</b> .....	<b>22</b>
1.6.1 Radardatenverarbeitungssystem ADAPT .....	22
1.6.2 Systemübersicht.....	23
1.6.2.1 Redundante Systeme .....	24

<b>1.7</b>	<b>Meteorologische Angaben .....</b>	<b>25</b>
1.7.1	Allgemeine Wetterlage.....	25
1.7.2	Wetterbedingungen auf dem Flughafen Zürich.....	25
1.7.3	Gefährliche Wettererscheinungen .....	26
<b>1.8</b>	<b>Navigationshilfen.....</b>	<b>26</b>
<b>1.9</b>	<b>Kommunikation .....</b>	<b>26</b>
<b>1.10</b>	<b>Angaben zum Flughafen .....</b>	<b>26</b>
<b>1.11</b>	<b>Aufzeichnung von Ereignissen und Daten .....</b>	<b>26</b>
1.11.1	Logbücher .....	27
1.11.1.1	Betriebslog ACC .....	27
1.11.1.2	Betriebslog APP .....	28
1.11.1.3	Betriebslog Kontrollturm .....	28
1.11.1.4	Technisches Log SYMA .....	28
1.11.1.5	SMP-log .....	29
1.11.1.6	UNAS-log (node log) .....	30
1.11.1.7	UNIX-log .....	30
1.11.2	Berichterstattung des ADAPT Spezialisten.....	30
<b>1.12</b>	<b>Angaben über den Aufprall, das Wrack und die Unfallstelle .....</b>	<b>32</b>
<b>1.13</b>	<b>Medizinische und pathologische Angaben .....</b>	<b>32</b>
<b>1.14</b>	<b>Feuer .....</b>	<b>32</b>
<b>1.15</b>	<b>Überlebensmöglichkeiten .....</b>	<b>32</b>
<b>1.16</b>	<b>Versuche und Forschungsergebnisse .....</b>	<b>32</b>
<b>1.17</b>	<b>Angaben zu verschiedenen Organisationen und deren Führung .....</b>	<b>32</b>
1.17.1	Flugsicherungsunternehmen skyguide .....	32
1.17.1.1	Geschichte .....	32
1.17.1.2	Technischer Dienst.....	32
1.17.1.3	Koordination und Prozesse zwischen den technischen Diensten und den Betriebsdiensten.....	34
1.17.1.4	Angaben zum Bereich Technik TD (Datenverarbeitung) .....	35
1.17.2	Technischer Dienst TDZ.....	37
1.17.3	Technische Aus- und Weiterbildung .....	38
1.17.3.1	Common Basic Training (CBT).....	38
1.17.3.2	Qualification Training .....	39
1.17.3.3	System Training.....	39
1.17.3.4	Training Organisation for Technical Equipment Management (TOTEM).....	39
1.17.4	Internationale Richtlinien bezüglich Ausbildung und Lizenzen im Bereich der Luftfahrt .....	40
1.17.4.1	International Civil Aviation Organization (ICAO) .....	40
1.17.4.2	EUROCONTROL Safety Regulatory Requirement - ATM Services' Personnel (ESARR5).....	40
1.17.5	Internationale Fachverbände.....	41
1.17.6	Umsetzung von ICAO-Anhang 1 und ESARR5.....	41

<b>2</b>	<b>Analyse .....</b>	<b>43</b>
<b>2.1</b>	<b>Technische Aspekte .....</b>	<b>43</b>
2.1.1	Konzept des Systems.....	43
2.1.2	Vorfall vom 31. Oktober 2003.....	43
2.1.3	Schwerer Vorfall vom 11. November 2003 .....	44
2.1.3.1	Zusätzliche korrigierende Eingriffe vom 11. November 2003 .....	44
2.1.4	Ausbildung, Zertifizierung und Unterhalt.....	46
2.1.4.1	Ausbildung und Zertifizierung.....	46
2.1.4.2	Sicherheitsanforderungen von Eurocontrol .....	46
<b>2.2</b>	<b>Betriebliche Aspekte.....</b>	<b>46</b>
<b>3</b>	<b>Schlussfolgerungen .....</b>	<b>47</b>
<b>3.1</b>	<b>Befunde.....</b>	<b>47</b>
3.1.1	Vorgeschichte und Verlauf des schweren Vorfalls .....	47
3.1.2	Technische Aspekte.....	47
3.1.3	Betriebliche Aspekte .....	48
3.1.4	Rahmenbedingungen.....	48
<b>3.2</b>	<b>Ursachen .....</b>	<b>49</b>
<b>4</b>	<b>Sicherheitsempfehlungen und seit dem schweren Vorfall getroffene Massnahmen .....</b>	<b>50</b>
<b>4.1</b>	<b>Vorgehen nach technischen Ausfällen.....</b>	<b>50</b>
4.1.1	Sicherheitsdefizit .....	50
4.1.2	Sicherheitsempfehlung Nr. 320 (vormals Nr. 90) .....	50
<b>4.2</b>	<b>Eingriffe in im Einsatz stehende Systeme .....</b>	<b>50</b>
4.2.1	Sicherheitsdefizit .....	50
4.2.2	Sicherheitsempfehlung Nr. 321 (vormals Nr. 91) .....	51
<b>4.3</b>	<b>Zertifizierung von Anlagen der Flugsicherung .....</b>	<b>51</b>
4.3.1	Sicherheitsdefizit .....	51
4.3.2	Sicherheitsempfehlung Nr. 322.....	52
<b>4.4</b>	<b>Seit dem schweren Vorfall getroffene Massnahmen.....</b>	<b>52</b>
<b>Anlagen</b>	<b>.....</b>	<b>54</b>
<b>Anlage 1:</b>	<b>Auszug aus der Datei "trapd.log" .....</b>	<b>54</b>
<b>Anlage 2:</b>	<b>Auszug aus der Datei ZHXCC13_NSRVR_INFO_11 31/10/03 08:28.....</b>	<b>55</b>
<b>Anlage 3:</b>	<b>Radarluftlage bei Beginn des schweren Vorfalls.....</b>	<b>56</b>

## Schlussbericht

System	Flugverkehrsleitung der Bezirksleitstelle sowie der An- und Abflugleitstelle
Eigentümer	skyguide - Schweizerische AG für Flugsicherung
Ort	Flughafen Zürich
Datum und Zeit	11. November 2003, 18:35-18:55 UTC

### Allgemeines

#### Kurzdarstellung

Am 11. November 2003 um ca. 18:34 UTC wurde durch einen Eingriff in das Radarsystem ein Totalausfall der Darstellung der Radarluftlage in der An-/Abflugleitstelle und der Bezirksleitstelle Zürich verursacht. Als Folge davon konnte der Flugverkehr während ungefähr 20 Minuten nur noch mit Einschränkungen abgewickelt werden.

#### Untersuchung

In Anwendung des *attachment C "list of examples of serious incidents"* des *Annex 13 to the Convention on International Civil Aviation "Aircraft Accident and Incident Investigation"* der ICAO hat das BFU eine Untersuchung durchgeführt. In dieser Liste schwerer Vorfälle ist unter anderem vorgesehen, dass eine Untersuchung eröffnet wird bei:

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

Durch den Ausfall der Radarbildschirmdarstellung hatten die Flugverkehrsleiter der Bezirksleitstelle sowie der An- und Abflugleitstelle keinen Zugang mehr zu den notwendigen Informationen der folgenden drei redundanten Systeme zur Verarbeitung der Radardaten (vgl. Ziffer 1.6.2.1):

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

Diese Systeme stellen drei verschiedene Betriebsmodi (MV, *fallback*, LR/SR) mit unterschiedlichen Funktionen zur Verfügung. Der Flugverkehrsleiter arbeitet normalerweise im MV *mode*, da die beiden anderen *mode* bezüglich Funktionen eingeschränkt sind.

Der schwere Vorfall ist darauf zurückzuführen, dass der zentrale Überwachungs- und Steuerungsrechner aus unbekanntem Gründen alle aktiven Prozesse zur Darstellung der Radarluftlage beendete, ausgelöst durch ungeprüfte korrigierende Eingriffe ins ADAPT System.

Folgende Faktoren haben zur Entstehung des schweren Vorfalls beigetragen:

- Im Flugsicherungsunternehmen fehlten Prozesse für korrigierende Eingriffe.
- Inwieweit der übergreifende Kenntnisstand des beteiligten Personals, welches an den technischen Anlagen des Flugsicherungsunternehmens korrigierende Eingriffe vorgenommen hat, genügend war, muss offen bleiben.
- Der bevorstehende korrigierende Eingriff wurde mit der Flugverkehrsleitung nicht koordiniert.
- Das Programm des zentralen Überwachungs- und Steuerungsrechners verfügte über keine Sicherheitsvorkehrungen und Warnsysteme.
- Ein redundantes System zur Darstellung der Radarluftlage war nicht vorhanden.

## I. Einleitende Bemerkungen zum System der Flugsicherung Zürich

### I.1 Radarsystem

#### I.1.1 Primärradar

Ein Primärradar (*primary surveillance radar* – PSR) ist ein System zur Überwachung des Luftraumes. Dazu werden von einem Sender über eine Antenne Mikrowellenpulse ausgesandt, welche vom Flugobjekt teilweise zur Antenne zurück reflektiert werden. Ein Empfänger misst die Zeit zwischen dem Aussenden und der Rückkehr der Pulse. Diese Laufzeit und die Einfallsrichtung der Pulse ermöglichen die Berechnung der Position des Flugobjekts.

Heute gibt es Primärradarsysteme mit zweidimensionaler (Distanz und Azimut) oder mit dreidimensionaler (Distanz, Azimut, Elevation) Positionsbestimmung.

Primärradarsysteme erlauben es, im überwachten Luftraum alle Flugobjekte, welche genügend Radarstrahlung reflektieren, zu detektieren und zu verfolgen. Auch meteorologische Erscheinungen, Vogelschwärme, Hängegleiter, Bodenreflexionen (*ground clutter*), etc. werden so erfasst. Die Anzeige dieser zusätzlichen Informationen kann zum Teil ausgefiltert werden. Für die Kontrolle bzw. die Führung des Flugverkehrs sind diese Informationen nicht überall nötig. Für die Überwachung des Luftraumes sind die PSR hingegen unabdingbar.

Ein Primärradar hat einen Leistungsbedarf von ca. 100 kW.

#### I.1.11 Sekundärradar

Ein Sekundärradar (*secondary surveillance radar* – SSR) ist ein System zur Kontrolle und Führung des Flugverkehrs. Dazu werden von einem Sender codierte Mikrowellenpulse zum Luftfahrzeug gesandt. Das Luftfahrzeug beantwortet die Anfrage des SSR mittels eines *transponders*. Der Empfänger des SSR wertet die in der Antwort des Luftfahrzeugs enthaltene Information aus.

SSR erlauben es, die Positionen, die Druckhöhe (*mode C*) und eine zugeordnete Bezeichnung (*mode A*) der antwortenden Luftfahrzeuge darzustellen.

*Mode S transponder* übermitteln zusätzlich einen Code (*address squitter*), welcher für jedes einzelne Luftfahrzeug festgelegt wird. Dank diesem Code wird es dem Flugverkehrsleiter ermöglicht, Luftfahrzeuge individuell abzufragen. Damit kann einer Überlastung des Systems vorgebeugt werden.

Ein SSR hat einen Leistungsbedarf von ca. 1 kW.

#### I.1.111 Radardatenverarbeitung

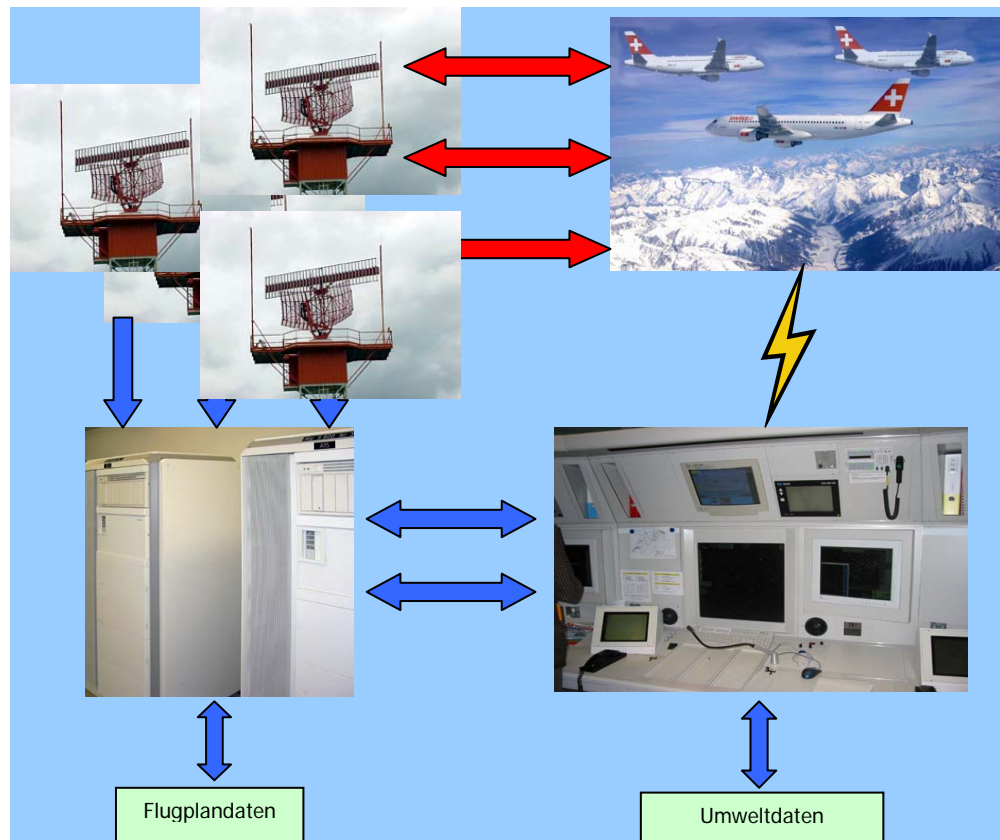
Die Aufgabe der zivilen Flugsicherung besteht darin, den Flugverkehr sicher und effizient zu leiten. Dabei stützt sich der Flugverkehrsleiter (FVL) auf komplexe vernetzte Systeme der Flugsicherungstechnik. Diese umfassen insbesondere:

- Radarluftlage: Sekundärradarsysteme erfassen die aktuellen Positionen und Daten der Luftfahrzeuge. In der Anflugleitung werden zusätzlich Primärradarsysteme eingesetzt. Eine Radardatenverarbeitungsanlage (*multi radar tracker*) fügt die Informationen der Radarsysteme zu einer aktuellen Radarluftlage zusammen.



Man spricht von einem *recognised air picture*, weil Position und Daten der Luftfahrzeuge durch mehrere Radarsysteme übereinstimmend erfasst werden. Der für den entsprechenden Sektor relevante Ausschnitt der Radarluftlage wird dem zuständigen FVL auf dem Radarbildschirm seiner Arbeitsstation (*integrated controller workstation - ICWS*) dargestellt.

- Planluftlage: Jeder Flug bedingt eine vorgängige Planung: Immatriculation, Rufzeichen, Flugweg, Flugzeiten, etc. werden zentral durch die *central flow management unit* – CFMU in Brüssel erfasst, um die erforderlichen Zeitfenster (*slots*) zuzuteilen. Im Normalfall werden die Flugplandaten von der CFMU zur Verarbeitung an die Flugsicherungen verteilt. Die Flugplandatenverarbeitung versorgt den FVL mit den Daten der Flüge, welche er zu leiten hat. Plan- und Radarluftlage ermöglichen es dem FVL, den Luftraum sicher und effizient zu bewirtschaften. Die automatische Korrelation von Plan- und Radarluftlage erleichtert die Aufgabe des FVL, indem auf den Radarbildschirmen der ICWS die Luftfahrzeuge mit dem Rufzeichen anstelle des *transpondercodes* dargestellt werden.
- Umweltdaten: Dynamische Umweltdaten (z.B. Wetter, Luftraumeinschränkungen, Flugplatzinformationen) und statische Umweltinformationen (z.B. Luftstrassen, Anflugverfahren, Warteräume, Funkfeuer) vervollständigen die Informationen, die zur Flugverkehrsleitung notwendig sind.
- Arbeitsstationen: Die ICWS der FVL dienen einerseits der benutzergerechten Darstellung der Informationen und umfassen andererseits die notwendigen Kommunikationsmittel (Flugfunk, Telefon, Intercom) zur Leitung des Flugverkehrs und zur Koordination mit anderen Stellen.

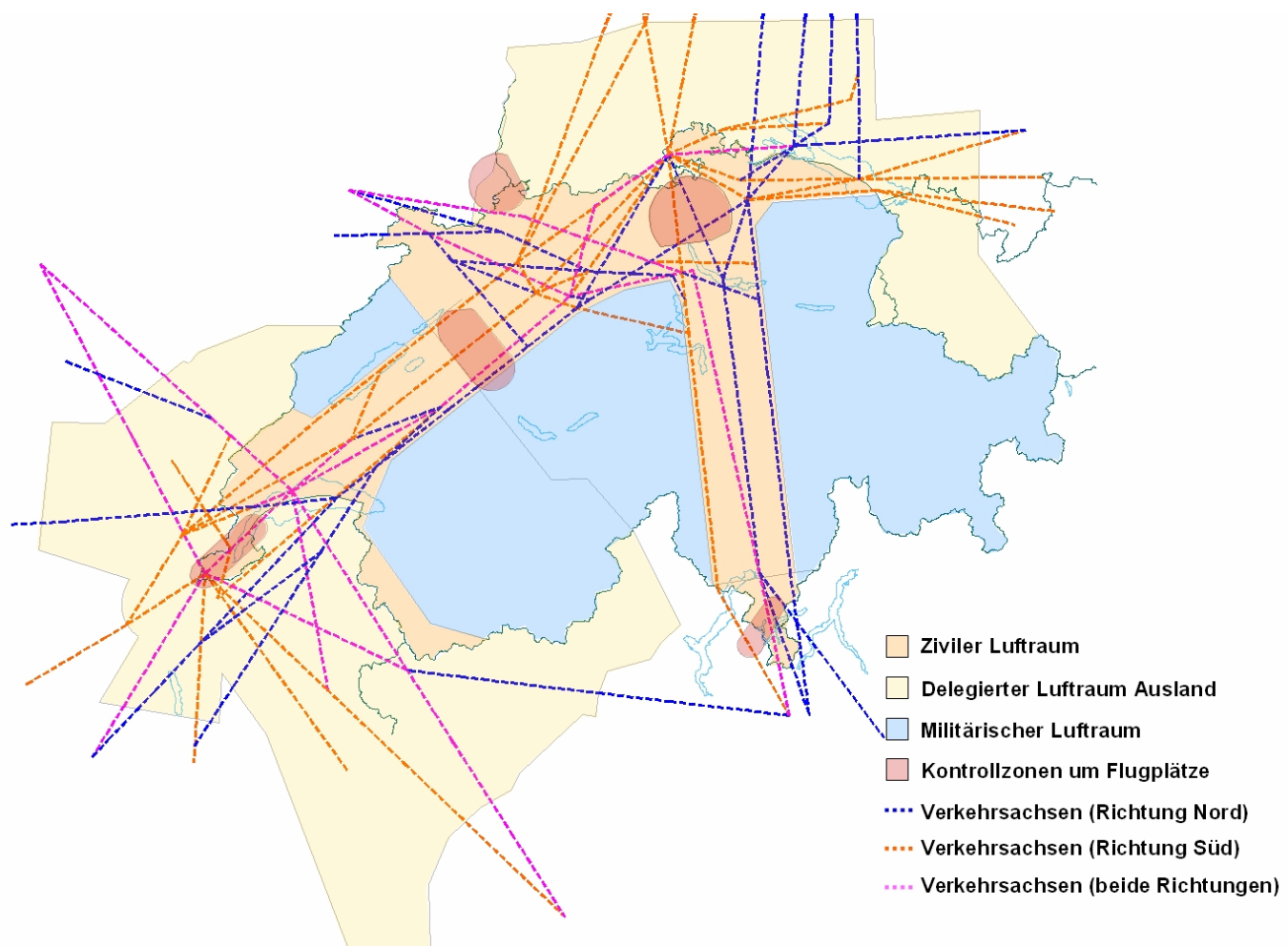


## I.II Luftraumstruktur Schweiz

### I.II.I Hauptverkehrsachsen durch den Luftraum der Schweiz

Das Verkehrsaufkommen der Flugsicherung Zürich ist durch drei unterschiedliche Hauptverkehrsströme gekennzeichnet:

- An- und Abflüge zu und von den Flughäfen Zürich, Genf, Bern-Belp, Grenchen und Lugano-Agno.
- Steig- und Sinkflüge von und zu den Flughäfen in Süddeutschland, in Norditalien und Basel-Mühlhausen.
- Transitflüge gemäss untenstehender Darstellung.



### I.II.II Zuständigkeiten der Flugsicherung Zürich

Die Flugsicherung Zürich ist zuständig für den Luftraum östlich der Trennlinie zum Luftraum Genf.

Die Flugsicherung Zürich leistet im schweizerischen Teil des Luftraumes, der sich vom Boden bis nach Flugfläche 600 (*flight level* – FL) erstreckt, sowie im delegierten Luftraum Flugverkehrsleitdienst (*air traffic control* – ATC), Fluginformationssdienst (*flight information service* – FIS) und Alarmdienst (*alerting service* – ALRS).

Der Flugverkehrsleitdienst gliedert sich wie folgt:

Zuständiger Dienst	Englischer Fachbegriff	Kontrollierter Luftraum
Bezirksleitdienst	<i>area control centre</i> – ACC	Luftstrassen (AWY) und Nahkontrollbezirk (TMA)
An- und Abflugleitdienst	<i>approach control office</i> – APP / DEP	Nahkontrollbezirk (TMA) Kontrollzone (CTR)
Platzverkehrsleitdienst	<i>aerodrome control</i> – ADC ( <i>tower</i> – TWR)	Kontrollzone (CTR)

I.II.III Luftraumstruktur Zürich

**FL600**



**FL115**



### Sektorisierung

Die Aufgabe der Flugverkehrsleitung wird aufgeteilt, indem logische Sektoren (vordefinierte Volumina des Luftraums) physikalischen Sektoren (Gruppierung von 1-3 ICWS) im *common IFR room* (CIR) zur Bearbeitung zugewiesen werden. Logische Sektoren für Zürich sind:

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

APP: APW, APE, FINAL, DEP, TMA

Die physikalischen Sektoren sind im nachfolgenden Layout des CIR dargestellt: APP-W, APP-E, ARFA, NORTH, WEST, EAST, SOUTH, U3, U2, U4, U1.

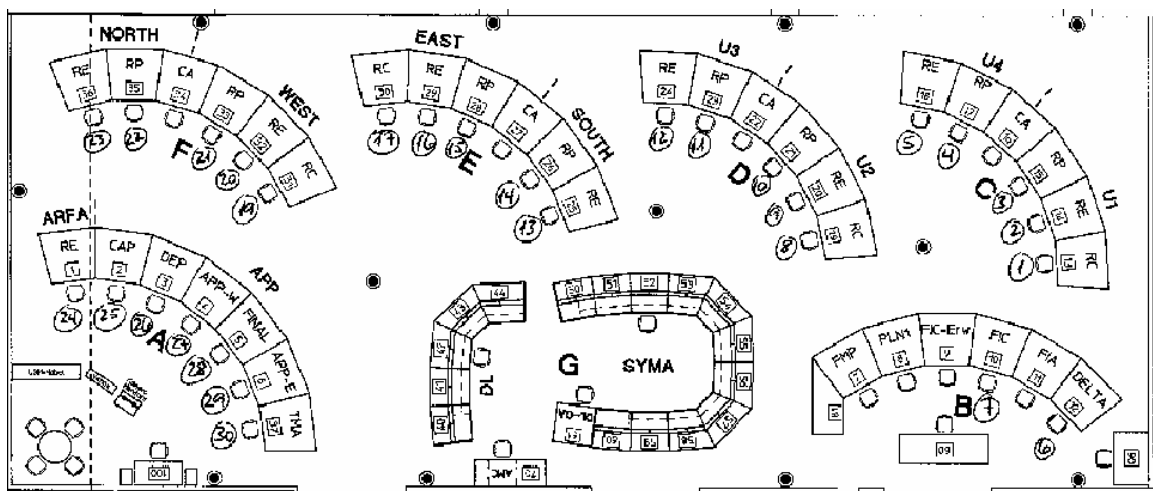


Bild 4: CIR Layout (schematisch)



Bild 5: ICWS im CIR

Je nach Intensität des Flugverkehrs wird eine unterschiedliche Sektorisierung gewählt, d.h. die Zuordnung der logischen auf die physikalischen Sektoren angepasst, bzw. physikalische Sektoren werden geschlossen.

Die Darstellung der Radarluftlage auf den ICWS basiert auf zwei Hauptelementen:

- einem *X-client* für die Aufbereitung der Radardaten,
- einem *X-server* für die Grafikdarstellung auf einem Grossbildschirm und das Benutzerinterface des FVL

Der Begriff *X-client* bzw. *X-server* wird sowohl für die eigentlichen Computer wie auch für die darauf laufenden Prozesse verwendet.

Im CIR Layout (vgl. Bild 4 und 5) sind zudem die Nummern der *X-server* eingetragen, welche jeweils den Radarbildschirm der ICWS bedienen. Je zwei *X-server* erhalten die Radardaten von einem *X-client*. Für je drei operative *X-client* steht ein *X-client* im *standby* Modus bereit.

Jeweils sechs ICWS mit den sechs *X-server* und den vier *X-client* bilden einen ICWS *cluster*. Der *cluster* hat zudem ein internes LAN, welches zusätzlich über einen sogenannten *radar switch* direkt Daten vom fbRDPS, bzw. einem einzelnen Radar empfangen und zur Darstellung auf den ICWS bringen kann.

## 1 Sachverhalt

### 1.1 Vorgeschichte und Verlauf des Vorfalls

#### 1.1.1 Vorgeschichte

##### 1.1.1.1 Radarausfall vom 31. Oktober 2003

Am Freitag, 31. Oktober 2003, trat gemäss dem Protokoll des Systemmanagers (SYMA) um 09:32:15 UTC in der Anflugleitstelle Zürich ein Radarspurenausfall von einigen Sekunden Dauer auf. Das bedeutete, dass die Darstellung aller Flugwege auf den betroffenen Radarbildschirmen plötzlich ausfiel. Auf diesen Bildschirmen wurde nur noch die Kartendarstellung (*map*) angezeigt.

Von diesem Ausfall waren die Bildschirme an den Arbeitsplätzen *approach sector west* (APW) und *terminal sector* (TMA) betroffen. Der Arbeitsplatz TMA war zu dieser Zeit nicht besetzt. Die Verkehrsabwicklung bereitete dem betroffenen FVL am APW trotz des Ausfalls keinerlei Schwierigkeiten. Das Verkehrsaufkommen war gering und er konnte kurzfristig auf die benachbarte *integrated controller workstation* (ICWS) am Arbeitsplatz FINAL ausweichen. Gemäss der Aussage des FVL dauerte der Radarspurenausfall lediglich 5-6 Sekunden.

Alle *radar tracks* und *labels* wurden gleichzeitig vom Bildschirm gelöscht. Nach sechs Sekunden erschienen die ersten Radarspuren wieder auf dem Bildschirm. Nach einer Aufdatierungszeit des *multi radar trackers* von vier Sekunden war die Darstellung der Radarluftlage wieder vollständig. Der Ausfall dauerte insgesamt ungefähr 10 Sekunden.

##### 1.1.1.2 Bearbeitung des Radarspurenausfalls vom 31.10.2003 durch die technischen Dienste

Der SYMA informierte den zuständigen Bereitschaftsdienst (*actual situation processing* – ASP) am Morgen des 31. Oktober 2003. Auf Veranlassung des Bereitschaftsdienstes wurde von den Technikern der Radardatenverarbeitung im Bereich des Hauptrechners MV9800 des *multi radar tracking* erfolglos versucht, die Ursache zu finden. Da das Problem während des Tages nicht mehr auftrat, wurden keine Sofortmassnahmen eingeleitet.

Das Problem wurde der Abteilung „Plattform Support Zürich“ (TDZ) übergeben. Am Montag, 3. November 2003, wurde beschlossen, das Problem dem zuständigen technischen Dienst für das System des *Air traffic management Data Acquisition Processing and Transfer* (ADAPT) zu übergeben.

Der Chef des Bereichs TDZ entschied, die Rückkehr des ADAPT Spezialisten abzuwarten. Dieser war bei einer Drittfirma angestellt und weilte bis Sonntag, 9. November 2003, in den Ferien. Die *log files* (Protokolldateien) dieses Vorfalls wurden nicht gesichert. Deshalb wurden sie bis zum 11.11.2003, dem Tag des schweren Vorfalls, zum Teil durch neue Daten überschrieben.

#### 1.1.2 Verlauf des schweren Vorfalls

Am 10.11.2003 beauftragte der TDZ den externen ADAPT-Spezialisten, am nächsten Tag die Untersuchung des Vorfalls vom 31. Oktober 2003 aufzunehmen. Dieser stellte in seiner Untersuchung am Morgen des 11.11.2003 eine stark erhöhte Prozessorlast des *X-client* 28 fest. Die operationellen *X-client* sind die Steuerungsrechner für die Radardarstellung von je zwei ICWS. Für je drei operationelle *X-client* steht ein *standby X-client* zur Verfügung. Zur Zeit des Radarspurenausfalls vom 31. Oktober und am Morgen des 11. November war der *X-client* 28 als *standby* konfiguriert.

Konfiguration 11.11.2003	vor dem automatischen Abschalten			nach dem manuellen Aufstarten		
	X-Client	Modus	X-Server	ICWS	Modus	X-Server
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		

Tabelle 1: Konfiguration des ADAPT System vor und nach dem schweren Vorfall

Nach Absprache mit dem SYMA nahm der ADAPT-Spezialist am SMP Arbeitsplatz (*system management position*) einen *restart* des *X-client* 28 vor. Diese Aktion wurde nicht im SYMA *log* eingetragen und die Flugverkehrsleiter wurden nicht informiert.

Um 12:12 UTC informierte der Fachspezialist mittels E-Mail den TDZ, den SYMA und weitere Personen der Technischen Dienste (TD) über die Diagnose und die erfolgte Intervention zur Lösung des Problems mittels *restart* des *X-client* 28. Das Problem wurde als gelöst erachtet und für die nächste Koordinationssitzung zwischen Betrieb und Technik (*OPS-TEC meeting*) vom 17. November 2003 traktandiert.

Bei der Überwachung des ADAPT entdeckte der Fachspezialist im Verlaufe des Tages zwei weitere *X-client* (4 und 10) mit stark erhöhter Last. Im Einverständnis mit dem SYMA nahm er einen *restart* der beiden *X-client* vor; um 18:31:16 UTC erfolgte am SMP Arbeitsplatz ein *shutdown* und *startup* des *X-client* 4. Noch vor Abschluss des *restart* des *X-client* 4 erfolgte um 18:34:26 UTC der *shutdown* des *X-client* 10. Während des *shutdown* des *X-client* 10 erteilte der SMP Rechner um 18:34:31 UTC automatische Abschaltbefehle an alle übrigen *X-client* und einige weitere Rechner. Dadurch wurden alle aktiven und im *standby mode* laufenden Programme (Prozesse), welche für die Darstellung auf den Radarbildschirmen zuständig waren, gestoppt und gelöscht. In der Folge kam es innert etwa 1 Minute zum Totalausfall der Darstellung der Radarluftlage an allen Radarbildschirmen im *common IFR room* (CIR).

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		

Tabelle 2: Verlauf des durch den SMP ausgelösten automatischen *shutdown* im ADAPT System

#### 1.1.2.1 Verkehrslage zu Beginn des Ausfalls der Radardarstellung

Zur Zeit des Ausfalls der Radardarstellung befanden sich auf den Bildschirmen der Flugverkehrsleiter 28 Flugzeuge im von Zürich ATC kontrollierten Luftraum (siehe Anlage 5.3).

#### 1.1.2.2 Auswirkungen des Ausfalls der Radardarstellung vom 11. November 2003 auf die Flugverkehrsleitung

Die Flugverkehrsleitung war vorgängig von den zuständigen Technikern über die bevorstehenden Umschaltarbeiten nicht informiert worden. Auf den Radarbildschirmen der FVL waren keine Anzeichen für einen bevorstehenden Ausfall zu erkennen. Der Ausfall der ersten Radarkonsole ereignete sich etwa um 18:35 UTC. In schneller Folge fiel daraufhin die Darstellung auch auf allen anderen Radarbildschirmen aus.

Der Ausfall stellte sich so dar, als wären die Radarbildschirme ausgeschaltet worden (schwarz).



Alle 29 Radarbildschirme im *common IFR room* (CIR) waren vom Ausfall betroffen.

Andere Systeme an den Arbeitsplätzen der FVL, wie z.B. Telefon- und Funkverbindungen, waren vom Ausfall nicht betroffen.

Ungefähr 20 Minuten später, gegen 18:55 UTC, standen den FVL die Radardaten auf sämtlichen Bildschirmen wieder zur Verfügung.

#### 1.1.2.3 Auswirkungen auf den Betrieb im Kontrollturm

Der Platzverkehrsleitdienst (Kontrollturm, *aerodrome control*) überwacht Rollmanöver, Starts und Landungen und leitet den Verkehr in der unmittelbaren Umgebung des Flughafens.

Der Koordinator Anflugleitstelle (*coordinator approach – CAP*) informierte den *daily OPS manager* (DOM) im Kontrollturm über den Bildschirmausfall in der APP. Zum Zeitpunkt des Ausfalls fanden wenige Abflüge statt. Bezüglich Anflüge herrschte ein mittleres Verkehrsaufkommen. Alle Arbeitsplätze im Kontrollturm, mit Ausnahme des ADC2, waren besetzt. Die Radarbildschirme im Kontrollturm (*position radar de nuit à la Vigie – PRN-Vigie*) waren voll funktionstüchtig. Der DOM liess sofort alle Abflüge stoppen und bot dem CAP an, die Aufgaben der Anflugsektoren zu übernehmen. Zu diesem Zweck wurden im Kontrollturm zwei Arbeitsplätze als Radaranflugsektoren eingerichtet. Damit konnte die Radarführung (*radar vectoring*) einzelner Anflüge mit den hier vorhandenen PRN-Vigie Bildschirmen übernommen werden. Da bald darauf die Radarbildschirme in der APP wieder normal funktionierten, wurden die getroffenen Massnahmen schrittweise rückgängig gemacht.

#### 1.1.2.4 Auswirkungen auf die An- und Abflugleitstelle

Die An- und Abflugleitstelle (*approach control office - APP*) leitet die An- und Abflüge innerhalb eines bestimmten Bereichs der Kontrollzone und des Nahkontrollbezirks. Dieser Bereich reicht normalerweise bis zu einer Entfernung von ca. 50 km um den Flughafen.

In der APP fiel gemäss Aussage des CAP der Radarbildschirm an seinem Arbeitsplatz plötzlich aus. Bei einem Blick auf die Bildschirme links und rechts von ihm stellte er fest, dass sämtliche Radarbildschirme in der APP ausgefallen waren. Während des Ausfalls mussten etwa 20 Flugzeuge von der APP geleitet werden. Es waren vier Sektoren in Betrieb. Die Verkehrsmenge war eher gering und es lag keine komplizierte Verkehrslage vor. Der CAP ergriff gemäss der APP-Checkliste im *emergency manual*, Kapitel „Radarausfall“, eine Reihe von Massnahmen zur Bewältigung der Situation. Unter anderem waren dies:

- Information des DOM TWR und Sistierung aller Abflüge
- Abklärung, ob die beiden Anflugsektoren und der Abflugsektor die laufenden Flugbewegungen gestaffelt an den nächsten Sektor übergeben könnten
- Umsetzung des Angebotes des DOM TWR, dass alle anfliegenden Flugzeuge von der APP und der ACC direkt an die Platzverkehrsleitung (*aerodrome control 2 – ADC2*) übergeben werden können (die Radarbildschirme im Kontrollturm waren vom Ausfall nicht betroffen)

#### 1.1.2.5 Auswirkungen auf die Bezirksleitstelle

Die Bezirksleitstelle (*area control centre* – ACC) gewährleistet den Verkehrsablauf innerhalb der Luftstrassen und teilweise im Nahkontrollbezirk. Die grosse horizontale und vertikale Ausdehnung der zu kontrollierenden Gebiete erfordert, je nach Verkehrsdichte, eine Aufteilung in verschiedene Arbeitssektoren. Diese Unterteilung kann geografisch sein oder nach Höhenbereichen erfolgen.

In der ACC fielen gemäss Aussage des DOM ACC innert etwa 30 Sekunden alle Radarbildschirme nacheinander aus. Während der Dauer des Ausfalls mussten etwa 35 Flugzeuge von der ACC geleitet werden. Es waren acht Sektoren in Betrieb. Die Verkehrsmenge war eher gering und die Komplexität nicht sehr hoch. Der DOM ergriff gemäss seiner Checkliste im Notfallhandbuch (*emergency manual*, Kapitel „Radarausfall“) verschiedene Massnahmen zur Bewältigung der Situation. Unter anderem waren dies:

- Aufforderung an die CFMU Brüssel, keine Flugzeuge mehr in den Luftraum von Zürich zu bewilligen (*zero rate*)
- Sistierung aller Abflüge
- *Zero rate* bei allen benachbarten Kontrollzentren
- Information der Leitung skyguide

Weiter veranlasste er folgendes:

- Rückruf des zweiten, sich in der Pause befindlichen DOM
- Verstärkung einzelner Arbeitsplätze mit Personal, das frühzeitig aus der Pause zurückkehrte

45 Minuten nach erfolgtem Ausfall vermerkte der DOM ACC im Betriebslog, dass die Verkehrsabwicklung wieder normal durchgeführt werden konnte.

#### 1.1.2.6 Ablauf der Wiederinbetriebnahme

Der Aufstartvorgang sowohl in der ACC als auch in der APP erfolgte schrittweise. Die ersten Radarbildschirme standen den FVL nach wenigen Minuten wieder zur Verfügung. Nach etwa 15 Minuten waren sämtliche Bildschirme wieder in Betrieb. Eine eigentliche Übergabe der neu aufgestarteten Radarbildschirme vom Technischen Dienst (TD) an die FVL erfolgte jedoch nicht. Der DOM ACC erkundigte sich beim SYMA nach der betrieblichen Nutzbarkeit der Radarbildschirme. Der SYMA bejahte diese, jedoch mit der Einschränkung, dass vorläufig keine Reserve (*standby*) zur Verfügung stehe. In der Folge wurden keine weiteren Unregelmässigkeiten mehr festgestellt.

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		

Tabelle 2: Verlauf der manuellen Wiederinbetriebnahme

Die genaue Zeit "*action completed*" wird nicht protokolliert, wenn vor Abschluss des Vorgangs bereits der nächste Befehl manuell ausgelöst wird. Die Zeit "*controller position ready*" bedeutet, dass die Karten auf dem Radarbildschirm geladen sind, die Bedienung funktioniert und die Radarspuren nach der nächsten Aufdatierungszeit von 12 Sekunden für ACC, bzw. 4 Sekunden für APP wieder vollständig dargestellt werden.

## 1.2 Personenschäden

Nicht betroffen.

## 1.3 Schaden am Luftfahrzeug

Nicht betroffen.

## 1.4 Verkehrseinschränkungen

### 1.4.1 Allgemeines

Die Verkehrsmenge war während des Ausfalles der Radardaten sowohl in der An- und Abflugleitstelle (ca. 20 Flugzeuge), wie auch in der Bezirksleitstelle (ca. 35 Flugzeuge) nicht sehr hoch. Die Verkehrseinschränkungen nach dem plötzlichen Ausfall aller Radardaten im CIR mussten nur kurze Zeit aufrechterhalten werden.

Eine überwiegende Mehrheit der Flugbesatzungen, die zur Zeit des Radardatenausfalls mit der Flugverkehrsleitung Zürich in Verbindung standen, äusserte sich positiv über die Handhabung des Flugverkehrs durch die ATC während des Ausfalls. Die Informationen der bordeigenen Kollisionswarnsysteme (*traffic collision avoidance system* - TCAS) wurden in dieser Situation als hilfreich empfunden. TCAS Warnungen gab es gemäss Angaben der befragten Besatzungen keine.

Da keine Maschine länger als 10 Minuten in den Warteräumen bleiben musste, mussten keine Ausweichflughäfen angefliegen werden.

Drei in Zürich startbereite Flugzeuge erlitten Abflugverspätungen. Die maximale Verzögerung des Starts betrug 20 Minuten.

### 1.4.2 Verkehrseinschränkungen An-/Abflugleitstelle und Kontrollturm

Nachdem der *coordinator approach* (CAP) den *daily ops manager* (DOM) im Kontrollturm über den Radardatenausfall im CIR informiert hatte, stellte der DOM fest, dass die Radardaten auf den Radarkonsolen im Kontrollturm (PRN-Vigie) normal zur Verfügung standen.

In der Folge liess er als Sofortmassnahme umgehend alle Abflüge sistieren.

Nachdem im Kontrollturm die beiden Arbeitsplätze ADC2 und Bodenverkehrsleitung (*ground control* – GRO) mit den PRN-Vigie Bildschirmen als Anflugsektoren eingerichtet waren, wurden die im Anflug befindlichen Flugzeuge von der Anflugleitstelle an diese beiden Anflugsektoren übergeben. Diese waren in der Lage, mit den beiden PRN-Vigie Radarbildschirmen die Flugzeuge zum Instrumenten-Landesystem (ILS) zu führen.

Die nachfolgenden Maschinen wurden von den Sektoren West und Ost der Anflugleitstelle auf deren angestammten Frequenzen und Arbeitsplätzen in die Warteräume eingewiesen.

Von dort konnten sie anschliessend in Gruppen von den Anflugsektoren im Kontrollturm übernommen und zum Endanflug geführt werden. Neu eintreffende Flugzeuge in der Bezirksleitstelle wurden ebenfalls direkt dem Kontrollturm übergeben.

Da gemäss Betriebslog der An- und Abflugleitstelle nach ungefähr zwölf Minuten die Daten auf den Radarmonitoren wieder zur Verfügung standen, konnten die getroffenen Massnahmen schrittweise rückgängig gemacht werden und die FVL der Anflugleitstelle übernahmen die Radarführung wieder selber.

### 1.4.3 Verkehrseinschränkungen Bezirksleitstelle

Der DOM ACC hielt sich im Bereiche des Sektors U2 auf, als er vom Sektor Nord über den Ausfall der dortigen Radardaten erfuhr. Er stellte fest, dass innerhalb kurzer Zeit auch die andern Sektoren betroffen waren.

In der Folge verstärkte der DOM die Arbeitsplätze mit zusätzlichem Personal, das nach bekannt werden der Radarprobleme frühzeitig aus den Pausen in den Betriebsraum zurückgekehrt war.

Anschliessend forderte er die angrenzenden Kontrollzentren auf, keine Flugzeuge mehr in den Luftraum von Zürich einfliegen zu lassen. Zusätzlich informierte er die CFMU in Brüssel und verlangte, den Verkehrsfluss so zu steuern, dass keine Maschinen mehr in die betroffene Region gelenkt würden.

Aufgrund der getroffenen Massnahmen und Absprachen war der DOM ACC bald darauf wieder in der Lage, vereinzelte Transitflüge von den angrenzenden Kontrollzentren zu akzeptieren.

In der Bezirksleitstelle mussten die Verkehrseinschränkungen nur kurze Zeit aufrechterhalten werden.

## 1.5 Angaben zu Personen

Zur Zeit des Vorfalles waren in den verschiedenen Betrieben folgende Personen im Einsatz:

ACC	2	Daily Ops Manager (DOM)/Flugverkehrsleiter
	15	Flugverkehrsleiter
	6	Flugverkehrsleiter Trainee
	1	Daily Ops Manager (DOM)/Flugverkehrsleiter-Assistent
	5	Flugverkehrsleiter-Assistenten
APP	1	Koordinator Anflugleitstelle (CAP)
	4	Flugverkehrsleiter
TWR	1	Daily Ops Manager (DOM)/Flugverkehrsleiter
	4	Flugverkehrsleiter
FTD	1	System Manager (SYMA)
	1	ADAPT Spezialist (externe Firma)

### 1.5.1 Der Systemmanager

Der Systemmanager (SYMA) hat seinen Arbeitsplatz im CIR, er überwacht die ihm zugeteilten Anlagen und Systeme mit dem Ziel, die Flugsicherung möglichst unbeeinträchtigt von technischen Störungen ausführen zu können. Basierend auf der Stellenbeschreibung ist er unter anderem mit folgenden Hauptaufgaben betraut:

- Überwachen der im SYMA integrierten Anlagen und Systeme.
- Anpassung der Systemkonfigurationen in Abhängigkeit der operationellen Bedürfnisse.
- Problem-Analyse: Einordnen, Analysieren und Bewerten auftretender technischer Probleme unter Einbezug der Anforderungen der operationellen Flugsicherung (z.B. Verkehrsaufkommen, Flugsicherungsverfahren); Abstimmen der zu treffenden Massnahmen mit den zuständigen DOM der operationellen Dienste.

- Erstintervention / Problembehebung: Im Störfall rasche und gezielte Gegenmassnahmen einleiten (z.B. Redundanzen aktivieren, Rekonfigurationen vornehmen), um den operationellen Betrieb möglichst rasch wieder sicherzustellen.
- Dokumentation der Vorfälle: Protokollierung aller Ereignisse und Probleme im SYMA *log* und Information mittels SYMA Meldungen; Briefing beim Schichtwechsel.
- Systemdokumentation / Checklisten: Aktualisierung der Dokumentation über die betreuten Systeme und deren Vernetzung. Erarbeiten von Checklisten für „*trouble-shooting*“ von Problemen und für „*system-control*“ zur Funktionskontrolle.
- Unterstützung TD: Unterstützung bei der präventiven und korrigierenden Wartung, sowie bei Systemmodifikationen, Tests und Analysen durch Koordination mit den zuständigen DOM der operationellen Dienste hinsichtlich der operationellen Freistellung der betroffenen Anlagen.
- Periodisches Durchführen von Systemumschaltungen (Xfers) der operationell aktiven Systeme um die Systemredundanzen praxisgerecht zu testen und die Schaltprozeduren zu trainieren (OJT).
- Unterstützung des OPS-Personals in technischen Belangen.
- Information der Leitung bei grösseren Systemausfällen, welche einen Einfluss auf die Kapazität der Betriebsdienste haben.
- Ausarbeiten und Realisieren von Verbesserungen im SYMA Betrieb durch Mitwirken bei der Evaluation, Installation und Inbetriebnahme von neuen Flugsicherungs-Anlagen, soweit sie den SYMA Dienst betreffen.

Die SYMA-Stelle wird ausgeschrieben. Die Bewerber werden ausgewählt und ausgebildet. Eine Lizenz war zum Zeitpunkt des schweren Vorfalles in der Schweiz nicht erforderlich.

### 1.5.2 Der ADAPT Spezialist

Der ADAPT Spezialist hatte seine Grundausbildung mit einem Bachelor in Mathematik abgeschlossen und verfügte über eine vertiefte Zusatzausbildung in Computertechnologie. Er arbeitete bei verschiedenen Firmen als Programmierer und Softwareingenieur. Im Projekt ADAPT wurde er von der Lieferfirma als *Senior Systems Engineer* eingesetzt. Unter anderem war er zuständig für die Koordination der Integration der Teilsysteme und die Softwareänderungen, sowie für *problem tracking reports* (PTR). Aufgrund seiner Funktion hatte er vertiefte Kenntnisse über das ADAPT System. Als firmenexterner Spezialist wurde er jedoch nicht systematisch in betriebspezifischen Belangen der Flugverkehrsleitung und der Gesamtheit der eingesetzten Systeme der Flugsicherungstechnik ausgebildet.

## 1.6 Angaben zum Radarsystem der Flugsicherung Zürich

### 1.6.1 Radardatenverarbeitungssystem ADAPT

ADAPT (*air traffic management data acquisition processing and transfer*) ist der Name des von skyguide zu Beginn der Neunzigerjahre gestarteten Projekts, um die zivilen schweizerischen Flugverkehrsleitsysteme durch Arbeitsplätze zu ersetzen, die die Gesamtheit der technischen Funktionen umfassen.

### 1.6.2 Systemübersicht

Das Blockdiagramm in Abbildung 1 zeigt die Hauptkomponenten des Radarsystems von skyguide. Eingerahmt sind die Komponenten des realisierten ADAPT Systems.

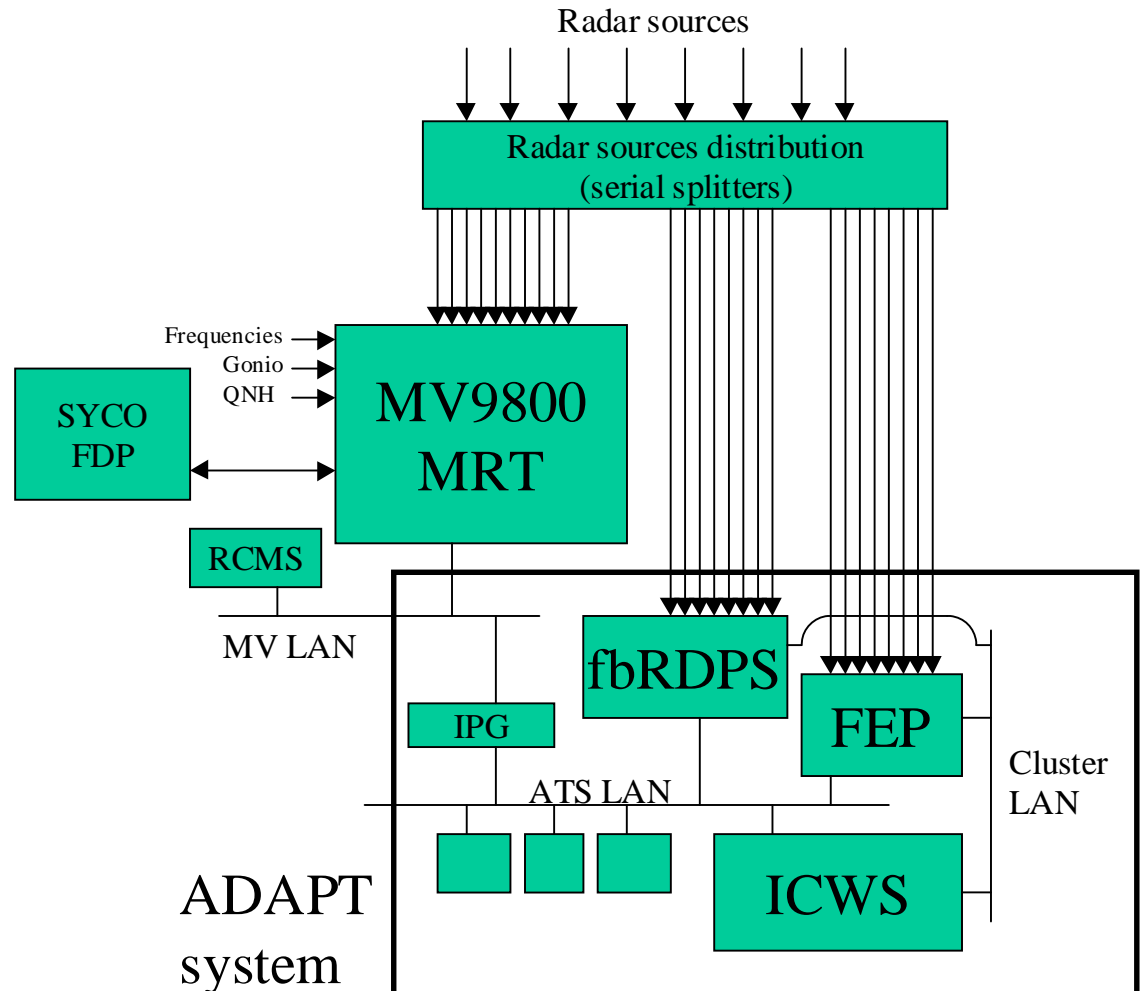


Abbildung 1: Blockdiagramm mit den Hauptkomponenten des Radarsystems von skyguide. Die Radardaten können auf drei verschiedene Arten verarbeitet und zur Darstellung gebracht werden.

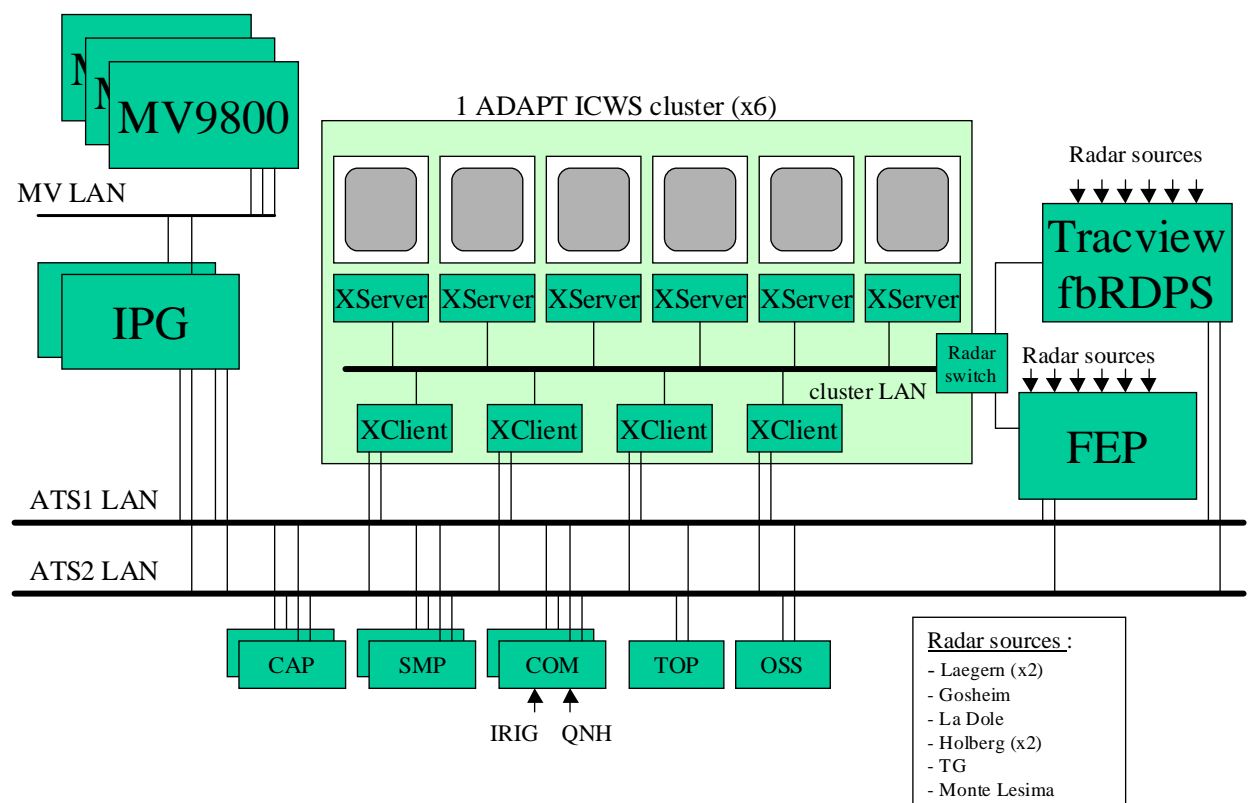
Die drei parallel arbeitenden MV9800 Computer haben direkten Zugang zu weiteren Teilen des Systems, wie z.B. der Verarbeitung der Flugplandaten durch das *système de communication* (SYCO), den Korrekturwerten für die Höhenangaben (QNH), der Information über die Frequenzteilung vom *interface* zum Funksystem SWITCH-04, den Richtungsbestimmungen durch GONIO (*direction finder*) oder der Datenaufzeichnung durch das *legal recording* (REC01, in Abbildung 1 nicht dargestellt). Das System wird durch das *remote control and monitoring system* (RCMS) gesteuert und überwacht. Die korrelierten Radardaten werden vom MV9800 System über eine IPS<sup>1</sup> *processing gateway* (IPG) ans ADAPT System weitergegeben.

<sup>1</sup> IPS – indicateur panoramique synthétique

Das *air traffic services local area network* (ATS LAN) stellt die Verbindung zwischen den Teilsystemen von ADAPT bereit. Das ATS LAN erscheint logisch als ein Netzwerk, ist aber auf dem *layer 1/2* physisch dupliziert.

Das *cluster LAN*, auch *internal LAN* genannt, verbindet die Elemente eines ADAPT ICWS *cluster*. Über einen *Ethernet switch* (*radar switch*) können Daten direkt vom fbRDPS, bzw. einem einzelnen Radar empfangen und auf den ICWS eines ADAPT *clusters* dargestellt werden.

Im Normalfall bedient ein *X-client* die ICWS von zwei verschiedenen physikalischen Sektoren. Dadurch geht beim Ausfall eines *X-client* die Information in einem physikalischen Sektor nur teilweise verloren.



### 1.6.2.1 Redundante Systeme

Das Radarsystem unterstützt drei Betriebsmodi, welche grundsätzlich die gleichen Daten der angeschlossenen Radare nutzen, sich jedoch durch unterschiedliche Verarbeitungswege unterscheiden:

1. *MV mode*: Dieser *mode* wird im Normalbetrieb verwendet. Der *MV mode* verarbeitet Daten als *multi radar tracker* (MRT) auf drei MV9800 Computern (MV1 bis MV3), die folgende Betriebszustände aufweisen:
  - ein Gerät in Betrieb (OPS)
  - ein Gerät in betriebsbereiter Warteposition (*hot standby* – STBY)
  - ein Gerät in startbereiter Warteposition (*cold standby* – TECH)
2. *fallback mode*: Dieser *mode* ist für den Fall ausgelegt, in dem der *MV mode* nicht zur Verfügung steht. Der *fallback mode* verwendet den *multi radar tracker* Tracview auf einem einzelnen HP748i Computer (fbRDPS), welcher Teil von ADAPT ist. Die im *fallback mode* zur Verfügung stehenden Funktionen sind gegenüber dem *MV mode* eingeschränkt.



3. LR/SR *mode*: Dieser *mode* ist ein Reservesystem auf einem einzelnen HP748i Computer (FEP, baugleich mit fbRDPS), welcher ohne *multi radar tracker* die Daten eines *long range* Radars bzw. eines *short range* Radars direkt zur ICWS des FVL leitet. Die Flugverkehrsleitung Zürich verwendet das *en-route* Radar Lägern als *long range* (LR) Radar oder das *approach* Radar Holberg als *short range* (SR) Radar.

Mit den drei Betriebsmodi wird eine Redundanz bei der Radardatenverarbeitung erreicht hinsichtlich:

- Überdeckung eines bestimmten Luftraumes durch mehrere Radarstationen
- Verarbeitung der Radardaten mittels unterschiedlicher Hard- und Software
- Verteilung der Daten durch physisch duplizierte Netzwerke
- Aufbereitung und Darstellung der Radardaten auf einem konfigurierbaren System von *X-client* und *X-server*

Keine Redundanz besteht hinsichtlich:

- Verwendeter Gerätetypen und der eingesetzten Betriebssysteme für die Verteilung und Darstellung der Radardaten, d.h. ICWS, ATS LAN, *X-client*, *X-server*
- Software im ADAPT System

## 1.7 Meteorologische Angaben

### 1.7.1 Allgemeine Wetterlage

Die Schweiz befand sich am westlichen Rande eines Hochdruckgebietes, dessen Zentrum über Osteuropa lag. Bei nur schwachem Boden- und Höhenwind war der Himmel in der Schweiz praktisch wolkenlos. Über den Niederungen der Alpen-nordseite lag eine Nebel/Hochnebel-Decke, deren Obergrenze im Westen um etwa 800 m/M, im Osten um etwa 900 m/M lag.

### 1.7.2 Wetterbedingungen auf dem Flughafen Zürich

Um 18:20 UTC herrschten auf dem Flughafen Zürich die folgenden Wetterbedingungen:

Wind:	110 Grad, 3 Knoten
Sicht:	2000 m
Wetter:	Feuchter Dunst
Wolken:	1-2 Achtel, Basis 200 ft 8 Achtel, Basis 500 ft
Temperatur:	+ 05 °C
Taupunkt:	+ 04 °C
QNH:	1022 hPa
TREND:	NOSIG

Um 18:50 UTC herrschten auf dem Flughafen Zürich die folgenden Wetterbedingungen:

Wind:	120 Grad, 2 Knoten
Sicht:	2000 m
Wetter:	Feuchter Dunst
Wolken:	1-2 Achtel, Basis 200 ft 8 Achtel, Basis 500 ft
Temperatur:	+ 05 °C
Taupunkt:	+ 04 °C
QNH:	1022 hPa
TREND:	NOSIG

### 1.7.3 Gefährliche Wettererscheinungen

Keine

### 1.8 Navigationshilfen

Es gibt keinen Hinweis darauf, dass die bodengestützten Navigationshilfen, wie VOR/DME, ILS zum Zeitpunkt des schweren Vorfalles beeinträchtigt gewesen sind.

### 1.9 Kommunikation

Es gibt keinen Hinweis auf Einschränkungen im Funksprechverkehr und bei den Telefonverbindungen zwischen den Sektoren sowie den angrenzenden Flugsicherungsstellen.

### 1.10 Angaben zum Flughafen

Da dieser schwere Vorfall zwar Auswirkungen auf den Betrieb der Flughäfen im Einzugsgebiet der ATC Zürich hatte, die einzelnen Flughäfen aber nicht von dieser Untersuchung betroffen waren, entfallen diesbezügliche Angaben.

### 1.11 Aufzeichnung von Ereignissen und Daten

Es gab vier Stufen der Aufzeichnung von Ereignissen und Daten. Diese Aufzeichnungen werden als *log* bezeichnet:

- Die handschriftlichen oder elektronischen *log* des DOM, des SYMA und des Personals des Technischen Dienstes.
- Das *log* des SMP, dem allgemeinen Überwachungs- und Steuerungssystem von ADAPT.

- Die *log* gewisser Netzwerkaktivitäten der ADAPT Workstations (*universal network architecture services – UNAS-log*), welche die Vorfälle oder Nachrichten auf Verlangen aufzeichneten.
- Die klassischen UNIX-*log* der ADAPT *workstations*.

Das ADAPT-System verwendete 62 UNIX-*workstations*, von denen 29 (*X-server*) lediglich die Funktion von einfachen Grafikprozessoren hatten und die Bildschirmdarstellung und Benutzeroberfläche an die ICWS lieferten.

Fünf UNIX-*workstations* waren nicht ins UNAS eingebunden: eine für technische Aufgaben (TOP), zwei für TracView (FEP und fbRDPS) und zwei für betriebliche Supportaufgaben (OSS).

Somit waren 28 UNIX-*workstations* (*X-clients*, SMP, COM, IPG, CAP) aktiv an der Aufbereitung und Darstellung der Radarluftlage beteiligt. Nur auf diesen *workstations* liefen mehrere wichtige Prozesse. All diese *workstations* waren über ein redundantes Lokalnnetzwerk miteinander verbunden, was ein Management aller aktiven Prozesse und ein Umschalten zwischen den *workstations* bei Ausfällen mittels der Software UNAS erlaubte. UNAS stellte die Basisfunktionalitäten für ein verteiltes Informatiksystem bereit, wie z.B. Kommunikation zwischen den Prozessen, das Erkennen von Fehlern und die Überwachung des Systemzustandes. Alle Prozesse gaben ihren Status mit Hilfe von SNMP-*traps* an. SNMP ist ein klassisches Protokoll, das unter UNIX und von allen TCP/IP-Netzen (wie dem Internet) verwendet wird. Die SMP *workstations* sammelten die *traps* und die *events*, um die grafischen Darstellungen des Systemstatus zu aktualisieren, und speicherten sie. Von der aktiven SMP *workstation* aus wurden zudem Befehle wie z.B. Neukonfiguration, Umschalten *standby/primary*, *shutdown*, *startup* erteilt. Im untersuchten schweren Vorfall hat die aktive SMP *workstation* die Abschaltbefehle erteilt.

Alle Ereignisse wurden mit einem Zeitstempel der Systemzeit versehen. Die Systemzeit wurde ihrerseits mit einer Präzision von ein paar Millisekunden mittels des *network time protocol* - NTP und einer absoluten externen Referenz (GPS oder Zeitzeichensender DCF77 in Mainflingen/D) synchronisiert. So wird ein Ereignis, das in einem oder in mehreren *log* in verschiedenen *workstations* gespeichert wurde, die gleiche Zeitangabe aufweisen. Das *log* zum untersuchten schweren Vorfall kann infolgedessen aufgrund seiner Redundanz und des Zeitstempels als zuverlässig betrachtet werden.

### 1.11.1 Logbücher

#### 1.11.1.1 Betriebslog ACC

Auszug aus dem handschriftlichen Betriebslog ACC vom 11.11.2003:

„19:35 UTC: Radarausfall im CIR (sowohl ACC als auch APP) ab 18:35 – 18:55 UTC

*Zero-Rate an Central Flow Management Unit (CFMU)*

*Reduced Capacity accepted von angrenzenden Sektoren / Nachbarleitstellen ab 18:55 UTC*

*DL-Checkliste ausgeführt*

*Normal OPS 19:20 UTC“*

## 1.11.1.2 Betriebslog APP

Auszug aus dem handschriftlichen Betriebslog APP vom 11.11.2003:

*„18:38 UTC: complete radar failure APP + ACC!  
alle DEP gestoppt  
INBND an Kontrollturm (ADC2)  
18:50 UTC normal OPS, ohne Backup“*

## 1.11.1.3 Betriebslog Kontrollturm

Auszug aus dem handschriftlichen Betriebslog Kontrollturm vom 11.11.2003:

*„18:37 UTC: Ausfall des ADAPT-Systems  
Keine Radardaten im ganzen CIR.  
Einige Flugzeuge im TWR mit PRN-Vigie aufliniert.  
18:52 UTC ADAPT funktioniert wieder normal.“*

## 1.11.1.4 Technisches Log SYMA

Hierbei handelt es sich um ein elektronisches *log*, das vom SYMA im Kontrollraum (CIR) erstellt wird. Es sind printouts für den 31.10.2003 und den 11.11.2003 verfügbar:

Auszug aus *log book* vom Freitag 31.10.2003 betreffend die Meldung 820015082, wobei Namen durch die Funktion ersetzt und mittels Unterstreichen markiert wurden.

Beginn / Ende Datum Zeit	Domaine Text und Meldender	System/Anlage	Status Aktion
31.10.2003 09:32:15 /	Processing-Systeme 31.10.2003 11:24:05 <u>SYMA</u>	MV2 Hardware (ANC/MV9800)	Teilausfall
31.10.2003 11:49:01	Kurzer Trackausfall am APW, Meldung von <u>FVL</u> . Fehlermeldung am MV:  "IPS APP 6 is failed" und "IPS APP 3 is failed",  16 Sek. Später, um 09:32:31, meldet ADAPT SMP1 folgenden Fehler:  "zhxcc28:ICW_SIT_20 - MRIP-SO-CAUSE - Hard- ware failure on <zhxcc27>".  Bem. zhxcc28 ist SBY und am zhxcc27 hängen DEP and FIN! Gemäss Info von <u>Pikett</u> und <u>MV Engineer</u> haben die beiden Fehlermeldungen womöglich nichts miteinander zu tun.  31.10.2003 11:48:00 <u>SYMA</u>  Seither sind keine Fehler mehr aufgetreten.  31.10.2003 11:49:01 <u>SYMA</u> Meldung abgeschlossen		

Auszug aus *log book* vom Dienstag 11.11.2003 betreffend die Meldung 820015139, wobei Namen durch die Funktion ersetzt und mittels Unterstreichen markiert wurden.

Anmerkung: Der *shutdown* und *startup* des *X-client 28* durch den ADAPT Spezialisten um 08:54 UTC wurde nicht im SYMA *log* festgehalten.

Beginn / Ende Datum Zeit	Domaine Text und Meldender	System/Anlage	Status Aktion
11.11.2003 18:30:00 / 11.11.2003 22:42:31	Processing-Systeme 11.11.2003 21:45:09 <u>SYMA</u> <u>ADAPT Spezialist</u> hat noch 2 <i>standby-X-clients</i> mit dem vom Morgen beschriebenen Fehler gefunden. <i>Shutdown</i> und <i>startup</i> von <i>X-client 04</i> . Danach wurde mit dem <i>shutdown</i> am <i>standby-X-client 10</i> begonnen.  18:37 Alle <i>X-clients</i> machen einen <i>shutdown</i> . Totaler Bildausfall in ACC und APP.  OPS Restrictions: 18:37 Zero Rate 18:50 FLAS <sup>2</sup> Transit Accept  Aufstarten der <i>X-clients</i> .  18:56 In allen <i>clustern</i> zeigen alle Bildschirme wieder ein Bild.  19:04 SMS für ASP <sup>3</sup> versendet.  19:20 keine <i>restrictions</i> mehr.  Die <i>stdby-X-clients</i> werden einer nach dem anderen durch den <u>ADAPT Spezialisten</u> hochgefahren.  <u>Chef Technik</u> hat am Pult angerufen. Bei weiteren Problemen sei direkt mit <u>Chef TD</u> Verbindung aufzunehmen.  20:15 Alle <i>stdby-X-clients</i> sind hochgefahren, alles i.O.  <u>Chef TZ</u> ruft am Pult an.  11.11.2003 22:42:31 <u>SYMA</u> – Meldung abgeschlossen -	Adapt Systeme	Totalausfall

#### 1.11.1.5 SMP-log

Die beiden SMP-*workstations primary* und *standby* am SYMA Arbeitsplatz ermöglichen es, den Status aller ADAPT-Systeme (Aktivität der Arbeitsstationen und der Prozesse) anzuzeigen, sowie die Neukonfigurationen, die Umschaltvorgänge von *standby* auf *primary* sowie die *shutdowns* und *startups* vorzunehmen. Die vom SYMA erteilten Befehle sowie die Ereignisse (Meldungen zum Prozessstatus) und die Fehler (*trap*) werden in der lokalen Datei "*trapd.log*" gespeichert.

<sup>2</sup> FLAS: flight level allocation schemes

<sup>3</sup> ASP: Bereitschaftsdienst des technischen Bereiches (*actual situation processing*)

Die Datei "*trapd.log*" der SMP-*workstations* ist die Hauptquelle zur Dokumentation und Analyse von Ereignissen im ADAPT System. Sie wird wöchentlich auf einem DAT-Datenträger (Magnetbandcartridge) gespeichert und dort zwischen einem und drei Monaten aufbewahrt. Die Daten sind redundant, denn sie werden an beiden SMP-Positionen gespeichert und erlauben eine chronologische Rekonstruktion der Ereignisse.

#### 1.11.1.6 UNAS-log (node log)

UNAS ist eine Software, die auf 28 der 62 *workstations* des ADAPT-Systems läuft, d.h. auf allen *workstations*, die aktiv am Zusammentragen der Daten beteiligt sind und die in den *primary* oder *standby mode* konfiguriert werden können. UNAS ist eine *message passing middleware*, die es den UNIX-*workstations* ermöglicht, miteinander zu kommunizieren sowie Prozesse zu starten und zu überwachen (aktivierte Programme). Die 28 UNAS-*workstations* sind also mehrfach vernetzt, d.h. es bestehen insgesamt 378 Verbindungen<sup>4</sup>. Jeder UNAS-Übermittlungsprozess (*node-server* – NSRVR) speichert lokal eine Reihe von vordefinierten Mitteilungen (Vorfälle, Konfigurationen); die Mehrzahl dieser Mitteilungen sind lokale Kopien der Mitteilungen, die an die SMP-*workstation* geschickt werden und in der Datei "*trapd.log*" gespeichert werden.

Diese *node log* werden in einem Turnus von 7 Tagen überschrieben. Die *node log* vom 31. Oktober 2003 wurden nicht gesichert und waren bis zum Zeitpunkt der Fehleranalyse am 11. November 2003 überschrieben. Die *node log* vom 11. November 2003 wurden gesichert.

Man fand dieselben Ereignisse, d. h. die Vernetzungen der *workstations* und das Starten von Prozessen, wie sie in der Datei „*trapd.log*“ gespeichert waren (siehe Anlage 5.1 und 5.2).

#### 1.11.1.7 UNIX-log

Mit der Systemfunktion `fprint()` konnte jeder UNIX-Prozess (Anwenderprogramm in Ausführung) auf der Systemkonsole Informationen anzeigen oder diese in einer lokalen Datei speichern. Grundsätzlich wurde diese Funktion nach einer Rückkehr aufgrund eines Fehlers einer Subroutine und zur Kennzeichnung eines wichtigen Ereignisses aufgerufen. Die *scripts* (Reihe von Systembefehlen) konnten Mitteilungen auch lokal speichern. Die gespeicherten Ereignisse dienten insbesondere der Fehlerbehebung (*debugging*).

Allfällige Aufzeichnungen im UNIX-*log* bezüglich des schweren Vorfalles lagen für die Untersuchung nicht vor.

### 1.11.2 Berichterstattung des ADAPT Spezialisten

Einen Tag nach dem schweren Vorfall sandte der ADAPT Spezialist dem TDZ in einem E-Mail folgenden Bericht. Die Namen wurden durch die Funktion ersetzt und mittels Unterstreichen markiert.

---

<sup>4</sup> Die Anzahl der Verbindungen errechnet sich nach der Formel:  $N \times (N-1)/2$ , wobei  $N = 28$ .

*„From: ADAPT Spezialist*

*Sent: Mittwoch, 12. November 2003 01:36*

*To: TDZ; TD; I*

*Cc: TDR; TDMX*

*Subject: RE: Analysis - Meldung 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 Spezialist“*

**1.12 Angaben über den Aufprall, das Wrack und die Unfallstelle**

Nicht betroffen.

**1.13 Medizinische und pathologische Angaben**

Nicht betroffen.

**1.14 Feuer**

Nicht betroffen.

**1.15 Überlebenschancen**

Nicht betroffen.

**1.16 Versuche und Forschungsergebnisse**

Nicht betroffen.

**1.17 Angaben zu verschiedenen Organisationen und deren Führung****1.17.1 Flugsicherungsunternehmen skyguide**

## 1.17.1.1 Geschichte

Die Radio Schweiz AG wurde 1922 zur Abdeckung der Bedürfnisse im Bereich der Telegrafie und der internationalen Telefonie gegründet. Diese Unternehmung führte auf den Flughäfen Zürich und Genf die ersten Kommunikations- und Ortungssysteme (Kurzwellen- und telegrafische Verbindungen, Funkpeiler) ein. Die Weiterentwicklung der Systeme und Verfahren führte jedoch erst 1931 zur Einführung der eigentlichen Flugsicherung. 1988 änderte die Radio Schweiz AG ihren Namen zuerst in swisscontrol und schliesslich nach dem Zusammenschluss der militärischen und zivilen Flugsicherungsdienste am 1. Januar 2001 in skyguide.

Ende 2003 beschäftigte skyguide 1326 Personaleinheiten; die Hälfte davon war als Flugverkehrsleiter angestellt, ein Viertel arbeitete als technische Angestellte (Bereich Technik) und ein Viertel bestand aus der Direktion, der Administration, Praktikanten und temporär Angestellten. Skyguide ist an diversen Betriebsstandorten, wie beispielsweise auf den Flughäfen Genf, Zürich, Bern und Lugano sowie auf verschiedenen Regionalflugplätzen tätig. Zusätzlich betreibt sie zwanzig ausschliesslich technische Standorte (Radarstationen, Stationen zur Navigationshilfe oder zum Senden/Empfangen von VHF/UHF).

## 1.17.1.2 Technischer Dienst

Der technische Dienst von skyguide war zum Zeitpunkt des schweren Vorfalles hauptsächlich für Beschaffung, Installation, Unterhalt und Entwicklung von Flugsicherungs- und Navigationsanlagen verantwortlich. Im November 2003 waren mit dieser Aufgabe 303 Personaleinheiten beauftragt. In der technischen Leitung sowie für die technische Betreuung der Region West waren 166 Personaleinheiten in Genf beschäftigt, 137 Personaleinheiten waren in Zürich für die Region Ost zuständig. Der technische Dienst war in fünf Bereiche mit je einem technischen Zuständigkeitsbereich (TN, TC, TD, TZ, TG) und in vier Support- oder Entwicklungsbereiche (TA, TS, TB, TI) unterteilt:



- TT (13) Führung und Stab des Bereichs Technik
- TN (46) Navigation und Aufsicht: ILS, VOR, DME, Radarstationen, Anlagen zur Darstellung und Beurteilung der Wetterlage
- TC (59) Kommunikation: Kommunikationssysteme Boden/Luft, Telefon, Funk, Datennetze
- TD (74) Datenverarbeitung: Verarbeitung der Radar- und Flugplandaten, Anzeige und Austausch von Flugdaten
- TZ (31) SYMA & Logistics Zürich: Aufsicht über die Systeme und deren Überwachung, allgemeine Dienste: Elektrizität, Klimatisierung, Stromerzeuger, Sicherheit, Zeichnungsbüro und Konstruktionswerkstatt
- TG (33) SYMA & Logistics Genf: Aufsicht über die Systeme und deren Überwachung, allgemeine Dienste: Elektrizität, Klimatisierung, Stromerzeuger, Sicherheit, Planungsbüro und Konstruktionswerkstatt
- TA (16) ATMAS Project
- TS (7) Systemplanung
- TB (4) Facility Management: Verwaltung der Bauten und Gebäude
- TI (20) Management Information System

Die technischen Bereiche TN, TC, TD, TZ und TG stellten das Projektmanagement in ihrem Bereich sowie den Unterhalt der Anlagen, für die sie verantwortlich waren, sicher. Der Unterhalt wurde durch zwei Spezialistengruppen sichergestellt:

Die erste Spezialistengruppe war für die präventiven und korrigierenden Unterhaltmassnahmen sowie die Installation neuer Systeme zuständig. Ein Mitglied dieser Gruppe leistete tagsüber von 07:30 LT bis 16:30 LT Bereitschaftsdienst vor Ort. Nachts und an Feiertagen wurde der Bereitschaftsdienst von zu Hause aus geleistet.

Die zweite Spezialistengruppe löste schwierige Fälle, führte Änderungen und Weiterentwicklungen aus. Für diese Arbeiten konnten auch Techniker der ersten Gruppe herangezogen werden, die für einen bestimmten Anlagentyp spezialisiert (Kurse in Instituten, beim Hersteller oder langjährige Praxiserfahrung) oder Entwicklungsingenieure waren.

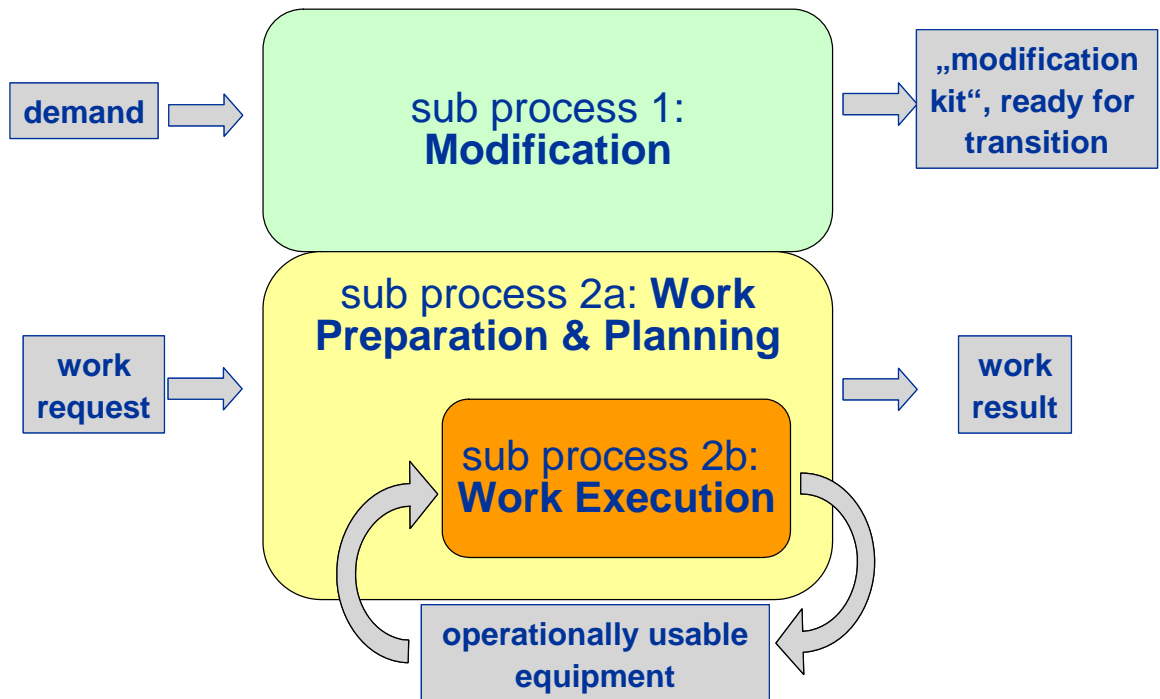
Der Bereich TG war der Flugsicherung in Genf, der Bereich TZ der Flugsicherung in Zürich zugeteilt. Jeder der Bereiche war unter anderem für die Aufsicht über die Luftfahrtsysteme in der jeweiligen Bezirksleitstelle zuständig (SYMA-Arbeitsplatz: Systemmanagement).

Der SYMA-Arbeitsplatz war täglich von 05:00 LT bis 23:30 LT besetzt. Ausserhalb dieser Stunden bestand ein Bereitschaftsdienst von zu Hause aus.

Der SYMA verfügte über zahlreiche Terminals und Bildschirme, um alle wichtigen technischen Anlagen der Flugsicherung überwachen und verwalten zu können. Er koordinierte seine Aktivitäten mit den Betriebsdiensten und konnte die Anlagen bei Abweichungen von der Norm neu konfigurieren oder umschalten. Gegebenenfalls liess er den Techniker des betroffenen technischen Dienstes (erste Spezialistengruppe) den Eingriff vornehmen.

### 1.17.1.3 Koordination und Prozesse zwischen den technischen Diensten und den Betriebsdiensten

- OPS-TEC-*meeting* in Zürich: Es fanden monatliche Treffen statt, die eine Plattform für die Koordination der jeweiligen Bedürfnisse der technischen Dienste und der Betriebsdienste oder für einen ersten Meinungsaustausch zu allen Interventionen und Änderungen boten.
- *planned work on ATM equipment* (PWAE): Dieser von einem Computerhilfsmittel unterstützte Prozess diente der Verwaltung der Änderungen (Anpassungen, Verbesserungen und neue Softwareversionen) sowie auch der Installation neuer Anlagen. Er wurde in Zürich Ende 2002 eingeführt.



Es wurden zwei Formulare verwendet:

- *process tracking form* – PTF: Damit konnten Schritt für Schritt die Entwicklung einer Intervention oder eines Projekts mit verfolgt werden; gleichzeitig war deren Rückverfolgbarkeit gewährleistet.
- *degradation announcement* – DA: Dieses Formular enthielt alle Verwaltungsdaten, d. h. die Beschreibung, die Dauer und den Beginn der geplanten Arbeiten sowie die Informationen betreffend das *risk management* und die Minderung der Risiken.

Zum Zeitpunkt des schweren Vorfalls waren im PWAE-Prozess noch keine Abläufe für die präventiven und korrigierenden Unterhaltmassnahmen sowie für die technische und betriebliche Ausbildung vorhanden und eingeführt.

## 1.17.1.4 Angaben zum Bereich Technik TD (Datenverarbeitung)

Der Bereich Technik TD umfasste 74 Personaleinheiten, davon 39 am Standort Zürich und 35 in Genf. Er war verantwortlich für den Unterhalt und die Entwicklung aller Anlagen, welche Radardaten und Flugplandaten an den Arbeitsplätzen der Flugverkehrsleiter anzeigen. Der Bereich TD bestand aus den Gruppen TDR, TDE, TDA und TDP:

TD (G: 4) *data processing division head*

TDR (Z: 12) AIM & ADAPT

TDE (Z: 14) APP, DEP und Flughäfen

TDZ (Z: 13) Plattform Support ZRH

TDG (G: 10) Plattform Support GVA

TDA (G: 12) *surveillance processing and ATM support*

TDP (G: 9) Transitverkehr (*en-route*)

Liste der PWAE, die vom Bereich TD (Datenverarbeitung) seit deren Einführung in Zürich herausgegeben wurde:

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 bis 17:00 LT  
Umplatzierung der InfoNet PC's in den App. Raum im AIS Zürich
- 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 TracView, fbRDPS and rFEP systems)
- MV 9800  
Issued 02.07.2003  
Scheduled 09.07.2003 21:00-23:00 LT  
Modification Sectorisation APP für TWR

- TACO/CALM Neuer 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  
Neue Tabellen laden
- 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 adress Range
- AFPS  
Issued 24.10.2003  
Scheduled 06.11.2003 23:00 – ca. 24:00 LT  
Monthly "Kettenwechsel" (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  
Nachtrag zum DVO  
"PWAE in progress"
- SYCO  
Issued 17.11.2003  
Scheduled 26.11.2003 nach Absprache mit dem Betrieb  
Neue Tabellen laden
- AFPS Bern  
Issued 17.11.2003  
Scheduled 19.11.2003 19:30 - 20.11.2003 21:00 LT  
Ghost der Software installation erstellen

- InfoNet Bern  
 Issued 17.11.2003  
 Scheduled 19.11.2003 23:00 - 20.11.2003 05:00 LT  
 Ghost der Software installation erstellen
- ADAPT  
 Issued 19.11.2003  
 Scheduled 20.11.2003 23:30 - 21.11.2003 02:00 LT  
 Software Tool für CPU Last Überwachung

### 1.17.2 Technischer Dienst TDZ

Der aus 13 Technikern bestehende Dienst TDZ (Technik - Data Processing - Plattform Support Zürich) war unter anderem verantwortlich für die ADAPT-Anlagen und insbesondere für die Bildschirme der ICWS. Die Angestellten waren in zwei Untergruppen aufgeteilt, die in den Bereichen ASP und PSP (erste Spezialistengruppe) spezialisiert waren.

*actual situation processing* – ASP (8 Techniker):

MV9800	<i>mainframe</i> für die Verarbeitung der Radar-/Flugplandaten
RCMS	Überwachungssystem für die MV9800
ADAPT	<i>Air traffic management Data Acquisition Processing and Transfer</i> - UNIX-workstations (X-client/X-server) - Kontrollschirme (Displays 19" und 29") - Zentralserver (SMP, CAP, IPG und COM) - ADAPT-eigenes LAN - redundante Verarbeitungsketten für Radardaten (Trackview FEP und fbRDPS)
PRN-Vigie	<i>Position Radar de Nuit à la Vigie</i> (Radarbildschirme im Kontrollturm)
TASD	<i>Tower Air Situation Displays</i> für ZRH, Bern, Lugano, Altenrhein, Friedrichshafen usw.
SAMAX	<i>Swiss Airport Movement Area Control System</i> (X: phonetischer Zusammenschluss von C und S)
ADR	<i>All-purpose Data Stream Replicator</i> zur Darstellung der Meteorologischen Daten für die Flugverkehrsleiter
IDM	<i>Integrated Data Management</i> , Verwaltung der statischen Luftfahrt Daten

*planned situation processing* - PSP (5 Techniker):

SYCO ZRH	System für die Verteilung und Darstellung der Flugpläne
SYCO MIL	System für die Verteilung der Flugpläne ans Militär
COM-Server	Kommunikationsserver für den Austausch der OLDI Meldungen ( <i>On-Line Data Interchange</i> Protokoll von Eurocontrol) mit den benachbarten Zentren

TACO	<i>Tower Approach Communication</i>
CALM	<i>Computer-assisted Approach and Landing Management</i>
AFPS	<i>AIS/ARO Flight Plan Server</i>
STARS	<i>Statistical Traffic Analysis Route Charge and Flight Plan Data Processing System</i>
COPAIN	<i>Computerized Preflight Aeronautical Information and NOTAM:</i> System zur Verarbeitung, Verifikation und Verteilung der NOTAM's
ETFMS	<i>Enhanced Tactical Flow Management System:</i> System zur Optimierung des Verkehrsflusses
CFMU	<i>Central Flow Management Unit:</i> Zentrales System zur Planung des Flugverkehrs
AFTN	<i>Aeronautical Fixed Telecom Network:</i> Luftfahrt Fernmeldenetz
EAD	<b>E</b> uropean <b>A</b> eronautical Information Services <b>D</b> atabase
T-Boxes	Schnittstelle zwischen FLORAKO und ADAPT

Die meisten Techniker der TDZ waren zudem Spezialisten für eine oder mehrere Anlagen. Sie stellten mit der Unterstützung verschiedener Ingenieure der lokalen Entwicklungsgruppen (TDR und TDE) den Unterhalt sicher.

Zum Zeitpunkt des schweren Vorfalles stand dem TDR in Zürich ein externer ADAPT Spezialist zur Verfügung. Ein zweiter war seit Juni 2003 abwesend. Diese ADAPT Spezialisten gehörten ursprünglich zum ausländischen Entwicklungsteam des Systemlieferanten und wurden später vertraglich über eine externe Firma verpflichtet.

Da in Genf im Juni 2003 ADAPT ausser Betrieb gesetzt worden war, standen von dort für dieses System keine Spezialisten mehr zur Verfügung.

### 1.17.3 Technische Aus- und Weiterbildung

Die Voraussetzungen für eine Anstellung im technischen Bereich von skyguide basierten auf den Grundausbildungsstufen des schweizerischen Ausbildungssystems mit Abschlüssen auf Stufe Lehre, Fachhochschule oder Universität. Je nach Aufgabenbereich waren unterschiedliche Ausbildungsgrade erforderlich.

In der Schweiz gab es zum Zeitpunkt des schweren Vorfalles keine Fachschule im Bereich der Luftfahrt. Aus diesem Grund fand skyguide kein technisches Personal, das auf dem lokalen Arbeitsmarkt bereits entsprechend ausgebildet war. Infolgedessen hatte skyguide ein eigenes Ausbildungskonzept erarbeitet, dessen Ziel es war, das technische Personal im Hinblick auf die Erfüllung seiner Aufgabe auszubilden.

Diese fachspezifische Ausbildung bestand aus drei aufeinander folgenden Phasen:

#### 1.17.3.1 Common Basic Training (CBT)

Für diese Ausbildungsphase im Unternehmen standen 30 Kurstage zur Verfügung. Sie sollte für alle neu Angestellten durchgeführt werden, um deren berufliche Kenntnisse im Bereich der Luftfahrt im Allgemeinen und der Firma im Speziellen zu vervollständigen. Sie umfasste folgende Themenbereiche:

- Luftfahrt (Luftfahrzeuge, Flugregeln, Wetterlage)
- Flugverkehrsorganisation (ICAO, BAZL, Eurocontrol)
- Organisation des Luftraums (FIR, CTA, CTR, TMA)
- Organisation der Flugverkehrsleitung (ACC, APP, TWR)
- Technische Methoden für die Luftfahrt (Telefon, Ortsnetze, RDP/FDP, Nav-aids, Radareinführung)
- skyguide (Auftrag, Organisation, Infrastruktur)

#### 1.17.3.2 Qualification Training

Hierbei handelte es sich um eine Ausbildungsphase, die speziell auf den künftigen Tätigkeitsbereich des Angestellten ausgerichtet war (Kommunikation, Datenverarbeitung, Navigation und Überwachung). Die unten aufgeführten Module dauerten zwischen einer und mehreren Wochen und wurden teilweise an eine ausländische Institution delegiert (ENAC in Toulouse, IANS in Luxemburg, DFS-Akademie):

- HF-Techniken und Funk
- Primärradar
- Sekundärradar, MSSR und Mode S
- Navigationshilfen: Grundlagen ILS/VOR, System ILS, System VOR, System DME
- Trends in der Flugsicherungstechnik

#### 1.17.3.3 System Training

In der letzten Phase lernten die einzelnen Angestellten Anlagen zu bedienen, für die sie zuständig sein würden (Betrieb, Unterhalt, Entwicklung usw.). Es handelte sich dabei oft um Kurse oder Praktika bei einem Lieferanten oder in einer verwandten Luftfahrtorganisation (ENAC, Eurocontrol, NAV Canada):

- Radare ASR10 (primär) / MSSR9600 (sekundär)
- Reformatierungs- und Verteilungssystem für Radardaten RMCDE
- Modellierung von Objekten UML
- Systemadministration HP-UX-11.0
- Multiradardaten-Verarbeitung ARTAS
- Radarbildschirme mit hoher Auflösung
- Wetterradar

#### 1.17.3.4 Training Organisation for Technical Equipment Management (TOTEM)

Um den Anforderungen der Empfehlung ESARR5 (Eurocontrol Safety Regulatory Requirement – ATM Services' Personnel) bis 2005 zu genügen, entwickelte skyguide eine Datenbankapplikation.

In einer ersten Phase im Jahr 2003 ging es um die Verwaltung des Ausbildungs-kursangebots (Liste und Termine der Kurse).

In den weiteren Phasen wurden die folgenden Ziele angestrebt:

- Analyse der Bedürfnisse auf Stufe Anlage
- Festlegen der Ausbildungslehrgänge nach Bereichen
- Bestandesaufnahme der vorhandenen Kenntnisse und des bestehenden technischen *know-how* der Firma

In der Praxis wurde das CBT gemäss Aussagen von skyguide-Mitarbeitern nur in etwa 50 % der Fälle durchgeführt. Der Terminplan der einzelnen Mitarbeiter war so gedrängt, dass diese für den Besuch der Kurse nicht freigestellt werden konnten. Zudem waren die Ausbildungsinhalte nicht genau definiert und die Wahl der Kurse war dem freien Ermessen der einzelnen Mitarbeiter überlassen.

Der Abschluss der Kurse oder Praktika erfolgte nicht in Form von Prüfungen. Damit fehlte eine wesentliche Voraussetzung, die Ausbildung zertifizieren zu können.

Wie erwähnt, waren die ADAPT-Spezialisten nicht bei skyguide angestellt, sondern vertraglich beauftragt und hatten das CBT daher nicht absolviert.

#### **1.17.4 Internationale Richtlinien bezüglich Ausbildung und Lizenzen im Bereich der Luftfahrt**

##### 1.17.4.1 International Civil Aviation Organization (ICAO)

Anhang 1 des Übereinkommens über die internationale Zivilluftfahrt der ICAO "*Personnel Licensing*" umfasst das Ausstellen der Lizenzen sowie die allgemeinen Anforderungen an das gesamte Personal, welches im Bereich der Luftfahrt tätig ist (Piloten, Luftfahrzeug-Unterhaltungspersonal, Flugverkehrsleiter, Unterhaltungstechniker und Flugdienstberater).

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

Die Empfehlung ESARR5 ist in der Version vom 11.04.2002 eine Ergänzung zu Anhang 1 des Abkommens der ICAO im Bereich der Sicherheit. Sie wurde erlassen, um die Anforderungen auf das gesamte Personal der ATM-Dienste inklusive jenem technischen Personal auszudehnen, dessen Funktion mit der Flugsicherheit zu tun hat. In diesem Dokument wird spezifiziert, dass einerseits die Flugverkehrsleiter zur Ausübung ihres Berufs qualifiziert sein und eine gültige Lizenz besitzen müssen und dass andererseits das Flugsicherungsunternehmen sicherstellen muss, dass das technische Personal über eine Ausbildung und entsprechende Fähigkeiten verfügt, um die ihnen übertragenen Aufgaben zu erfüllen. Zum Zeitpunkt des schweren Vorfalles war diese Empfehlung in der Schweiz noch nicht in Kraft.



### 1.17.5 Internationale Fachverbände

Die Vereinigungen des technischen Personals in der Flugsicherung (*Air Traffic Safety Electronics Personnel* – ATSEP) verschiedener Länder haben sich 1972 zusammengeschlossen und die *International Federation of Air Traffic Safety Electronics Associations* (IFATSEA) gegründet. Diese Organisation hat sich zum Ziel gesetzt, die Sicherheit, die Leistungsfähigkeit und die Vorschriftsmässigkeit der Luftfahrt zu fördern sowie die beruflichen Interessen des technischen Personals (ATSEP) zu schützen.

In der IFATSEA sind 54 Länder vertreten, darunter auch die Schweiz. In der Schweiz hat sich das technische Berufspersonal der Flugsicherung in der *Swiss Air Traffic Control Technical Association* – SATTa zusammengeschlossen.

Die IFATSEA hat erreicht, dass die Internationale Arbeitsorganisation (*International Labour Organisation* – ILO) der UNO den Beruf des technischen Personals (*Air Traffic Safety Technicians*) in gleicher Weise wie die Flugverkehrsleiter (*Air Traffic Controllers*) anerkannt hat.

### 1.17.6 Umsetzung von ICAO-Anhang 1 und ESARR5

Die Qualifikation und die Erteilung von Lizenzen<sup>5</sup> sind in den oben erwähnten Unterlagen der ICAO und von Eurocontrol näher umschrieben. Für das technische Personal wird hier keine Lizenz verlangt.

Es obliegt dem Flugsicherungsunternehmen sicherzustellen, dass das technische Personal über eine entsprechende Ausbildung und ausreichende Qualifikationen verfügt, um die ihm übertragenen Aufgaben zu erfüllen.

Das Bedürfnis, auch dem technischen Personal Lizenzen auszustellen, entstand erst in den letzten Jahren, weil die elektronischen Anlagen und die Informatiksysteme in der Abwicklung und der Überwachung des Flugverkehrs immer mehr an Bedeutung gewannen.

Zu Beginn der gewerbsmässigen Luftfahrt beschränkten sich die Ausrüstungen der Flugsicherung auf eigenständige elektronische Anlagen, wie z.B. HF- und VHF-Sender/-Empfänger, ungerichtete Funkfeuer, die Funkpeiler und das Landesystem ILS. Heute sind die Systeme der Flugsicherungstechnik vernetzt und umfassen neben elektronischen Anlagen auch Informations- und Kommunikationssysteme. Die Multidisziplinarität der Flugsicherungssysteme hat die IFATSEA dazu geführt, am 5. April 2000 vorzuschlagen, den Anhang 1 des Abkommens der ICAO im Bereich der Qualifikationen und der Lizenzen der ATSEP zu ändern.

Weiter hat die IFATSEA in Zusammenarbeit mit der ICAO im Jahr 2000 die Ausarbeitung eines Ausbildungshandbuchs für das technische Personal initiiert. Dieses Dokument wurde von der ICAO im Jahr 2004 veröffentlicht (Doc 7192-AN/857 Part E-2); darin werden die Ziele, die Phasen und die Kenntnisse beschrieben, die für die Grundausbildung und die Qualifikation in den Hauptbereichen der Flugsicherung verlangt werden.

---

<sup>5</sup> Eine Lizenz ist eine von der übergeordneten Behörde zur Ausübung einer reglementierten Tätigkeit ausgestellte Bewilligung.

- Kommunikationssysteme
- Navigationsanlagen
- Überwachungssysteme
- Datenverarbeitungsanlagen
- Sicherheits- und Risikomanagement

In der dritten Ausbildungsphase soll das technische Personal befähigt werden, die ihm anvertrauten Anlagen zu beherrschen. Für diese Ausbildungsphase (Rating) sind nur die Ziele beschrieben. Sie muss jedoch immer absolviert werden, bevor das technische Personal die Arbeit an operationellen Systemen aufnimmt. Dabei soll auf die folgenden Aufgaben besonderes Gewicht gelegt werden:

- Kontrolle und Überwachung der Systeme
- Präventive Unterhaltmassnahmen
- Korrigierende Unterhaltmassnahmen zur Fehlerbehebung
- Änderung und Aufrüstung der operationellen Systeme
- Kalibrierung und Validierung der Systeme bezüglich Einhaltung der Spezifikationen
- Zertifizierung und Rezertifizierung

Dieses Ausbildungshandbuch orientiert sich zum grossen Teil an den Arbeiten der IFATSEA und der ICAO sowie auch an den Beiträgen verschiedener Staaten oder internationaler Organisationen.

Ende 2002 änderte Eurocontrol die Empfehlung ESARR5 ab und fügte als Ergänzung den Abschnitt 5.3 ein. Dieser beinhaltet die Anforderungen an das technische Personal, das sicherheitsrelevante Aufgaben der Flugsicherung wahrnimmt.

Gemeinsam mit der ICAO veröffentlichte Eurocontrol am 06.10.2003 einen Leitfaden zum *Qualification Training* der ATSEP und am 02.04.2004 einen solchen zum *Common Base Training*.

## 2 Analyse

### 2.1 Technische Aspekte

#### 2.1.1 Konzept des Systems

Das ADAPT System wird durch einen zentralen Überwachungs- und Steuerungsrechner SMP kontrolliert. Für diesen SMP gibt es einen baugleichen Rechner im *hot standby*. Alle *X-client* und *workstations* (IPG, CAP, COM) im CIR werden vom aktiven SMP gesteuert. Für die Darstellung der Radardaten durch das ADAPT System besteht somit nur bezüglich der *workstations* eine Redundanz, nicht aber hinsichtlich der zentralen Steuerungsfunktion. Ein Fehler in der Steuerungsfunktion kann damit, wie im schweren Vorfall, zum Totalausfall der Darstellung der Radarluftlage führen. Die unabhängige Aufteilung der Steuerungsfunktion oder die Bereitstellung eines unabhängigen Darstellungssystems wurde bei der Konzeption des ADAPT Systems unterlassen.

#### 2.1.2 Vorfall vom 31. Oktober 2003

Der Vorfall wurde ordnungsgemäss im SYMA Protokoll festgehalten und der zuständige Bereitschaftsdienst telefonisch informiert. Das Protokoll des SYMA enthält Fehlermeldungen vom MV und vom ADAPT SMP. Der Bereitschaftsdienst zog zur Fehleranalyse das MV *engineering* bei. Nachdem das Vorgehen, welches im Protokoll als „*some MV investigations*“ bezeichnet wurde, keine Resultate zeigte und der Fehler nicht mehr auftrat, wurde beschlossen, keine unmittelbaren Massnahmen einzuleiten. Der SYMA schloss die Meldung ab.

Obschon im SYMA Protokoll festgehalten wurde, dass die ADAPT SMP Fehlermeldung womöglich nichts mit der MV Fehlermeldung zu tun habe, wurde das ADAPT *engineering* nicht in die Ursachenanalyse miteinbezogen. Primär aufgrund der Symptombehebung, d.h. es war kein weiterer Trackausfall zu beobachten, wurde von weitergehenden Abklärungen und Massnahmen abgesehen. Es kann nicht nachvollzogen werden, weshalb mit Ausnahme des SYMA Protokolls keine Daten für die Analyse des Vorfalls gesichert wurden. Dadurch gingen die *log files* des ADAPT Überwachungs- und Steuerungsrechners SMP sowie der betroffenen *X-client* 27, 28 und der *X-server* 27, 30 verloren.

Am darauf folgenden Montag, 3. November 2003, beschloss der TDZ aufgrund der telefonischen Nachfrage des SYMA und einer Diskussion mit dem Bereitschaftsdienst und MV *engineering*, den Vorfall zur Untersuchung ans ADAPT *engineering* weiterzugeben. Unmittelbar nach dem Vorfall vom 31. Oktober 2003 war nicht genügend qualifiziertes technisches Personal für eine fundierte Analyse vorhanden. Aus diesem Grund beschloss der TDZ, die Rückkehr des ADAPT Spezialisten aus den Ferien am kommenden Montag, 10. November 2003, abzuwarten. Zu diesem Zeitpunkt wäre es noch möglich gewesen, die Daten des Vorfalls zu sichern, was aber unterblieb. Ebenso wurde keine Risikoanalyse durchgeführt und keine betrieblichen Vorkehrungen getroffen.

Die Analyse des Vorfalls vom 31.10.2003, die Einschätzung der Lage und der Entscheidung, mit Massnahmen zuzuwarten, waren unzweckmässig. Ein totaler Ausfall der Radarspuren auf zwei ICWS hätte eine sorgfältige und vertiefte Ursachenanalyse erfordert.

Ein Prozess mit Arbeitsanweisungen und Checklisten zur Handhabung von Systemfehlverhalten fehlte. Einzig für geplante Arbeiten am System bestand ein *planned work on ATM equipment* (PWAE) Prozess. Damit wurden Neuinstallationen und Systemupgrades, bzw. Modifikationen erfasst, nicht aber präventive oder korrigierende Unterhaltseingriffe ins System.

### 2.1.3 Schwerer Vorfall vom 11. November 2003

Der ADAPT Spezialist, welcher am 10. November 2003 mit der Untersuchung des Ausfalls vom 31. Oktober 2003 beauftragt wurde, stellte als Anomalie eine ungewöhnlich hohe CPU Last des *standby X-client* 28 aus dem betroffenen *cluster* fest. Nach dem Prinzip „*trial and error*“ wurde um 08:54 UTC ein *shutdown/startup* des *X-client* 28 vorgenommen.

Die Bearbeitung des Vorfalls durch das Flugsicherungsunternehmen beinhaltete folgende Mängel:

- Ein ursächlicher Zusammenhang mit dem Vorfall vom 31. Oktober 2003 wurde nicht gesucht und ist auch nicht belegt.
- Nachdem mit der Analyse des genannten Vorfalls 10 Tage zugewartet wurde, entschied man sich aufgrund der als vermindert eingeschätzten Funktionalität des *standby X-client* 28 für einen unverzüglichen korrigierenden Eingriff ins operationelle System, dies ohne weitere Vorbereitungen zu treffen.
- Der Vorgang am operationellen System wurde zwar mit dem SYMA besprochen, aber weder hinsichtlich operationeller Risiken bewertet noch im SYMA-*log* festgehalten.
- Der korrigierende Eingriff wurde zu einem Zeitpunkt mit Verkehrsaufkommen vorgenommen, welches zwingend betriebliche Vorkehrungen für den Fall eines Misslingens des Eingriffes erfordert hätte.
- Der korrigierende Eingriff umfasste eine nicht geprüfte Operation an einem betrieblich genutzten System. Diese Operation war im Systemmanual nicht dokumentiert und die Auswirkungen nicht beschrieben. Aus diesem Grund wird im vorliegenden Bericht von einem ungeprüften Eingriff gesprochen.
- Für solche korrigierenden Eingriffe existierte kein Prozess, welcher die Abläufe, die Zuständigkeiten oder die Koordination mit der Flugverkehrsleitung geregelt hätte.

#### 2.1.3.1 Zusätzliche korrigierende Eingriffe vom 11. November 2003

Nach dem *shutdown/startup* des *X-client* 28 wurde das System auf weitere *X-client* mit erhöhter CPU-Last geprüft. Dabei wurde bei den *X-client* 4 und 10, welche im *standby mode* arbeiteten, eine erhöhte CPU-Last festgestellt. Nachdem der korrigierende Eingriff am *X-client* 28 vom Morgen als erfolgreich hinsichtlich des Problems der CPU Last erschien, wurden auch für diese Rechner gemäss SMP *log* um 18:31:17 UTC und 18:34:28 UTC dieselben korrigierenden Eingriffe vorgenommen. Zusätzlich zu den bereits erwähnten wies dieses Vorgehen folgende Mängel auf:

- Eine Abklärung der Ursache und der Auswirkungen der erhöhten CPU Last bei den *X-client* wurde nicht vorgenommen.
- Der zweite korrigierende Eingriff am *X-client* 10 wurde gestartet, bevor der erste Eingriff am *X-client* 4 vollständig abgeschlossen war.

Der Ablauf des korrigierenden Eingriffs vom Vormittag am *X-client* 28 begann um 08:54:18 UTC mit dem *shutdown*-Befehl:

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

Nach knapp 2 Minuten war der Prozess wieder aktiv, d.h. grün auf dem Bildschirm:

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

Das SMP *log* zeigt aber, dass der Prozess „*standby sit 5*“ erst gut neun Minuten später vollständig betriebsbereit war:

```
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
```

Der korrigierende Eingriff am *X-client* 10 erfolgte gut drei Minuten nach dem *shutdown*-Befehl für *X-client* 4 und etwa zwei Minuten, nachdem der Prozess auf *X-client* 4 wieder aktiv, aber noch nicht betriebsbereit war.

```
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 SHUT-  
DOWN - Node zhxcc10 shut down.
```

Die Meldungen über „...*process ready for operation*...“ sind nicht mehr protokolliert, da der Totalausfall vorher eintrat. Drei Sekunden nach dem *shutdown*-Befehl für *X-client* 10 und eine Sekunde, nachdem die Netzwerkverbindungen zu den übrigen Rechnern gelöst wurden, ging die Kontrolle über den Zustand des Netzwerks verloren:

```
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.
```

Sind die Rechner für den zentralen Überwachungs- und Steuerungsrechner SMC nicht mehr kontrollierbar, so erteilt das Programm des SMC ohne Vorwarnung Abschaltbefehle. In der gleichen Sekunde wurden so automatisch Abschaltbefehle an alle *X-client* gegeben. Dies führte in der Folge zum raschen Totalausfall der Radardarstellung auf den ICWS.

In der folgenden Nacht wurde vergeblich versucht, den Vorfall mittels der am Abend durchgeführten Operationen gemäss der neuen Systemkonfiguration an den *standby X-client* 3 und 10 zu reproduzieren.

Die zeitliche Koinzidenz zwischen dem korrigierenden Eingriff und der Instabilität der Netzwerkkonfiguration, welche zum Abschalten aller *X-client* durch den SMC führte, lässt den Schluss zu, dass besagter Eingriff ins operationelle System den Totalausfall ausgelöst hat.

## **2.1.4 Ausbildung, Zertifizierung und Unterhalt**

### **2.1.4.1 Ausbildung und Zertifizierung**

Die Ausbildung und insbesondere die Zertifizierung des technischen Personals sowie die Zertifizierung der Anlagen der Flugsicherung stellen eine komplexe Aufgabe dar. Die eingesetzten Systeme, wie z.B. SYCO, MRT oder ADAPT, verwenden verschiedene Technologien und werden zudem in sehr kleinen Serien oder sogar als Einzelanfertigungen hergestellt. Lange Zeit diente dieser Sachverhalt als Argument, um solche Systeme und das mit deren Unterhalt betraute Personal als nicht zertifizierbar zu bezeichnen.

### **2.1.4.2 Sicherheitsanforderungen von Eurocontrol**

Sowohl beim Unterhalt von Anlagen als auch bei der Ausbildung des technischen Personals bezieht sich skyguide gemäss eigenen Aussagen auf die Empfehlungen ESARR4 und ESARR5 und beabsichtigte, diese anzuwenden.

Diese Empfehlungen waren zum Zeitpunkt des schweren Vorfalls noch nicht in Kraft; das beteiligte technische Personal verfügte nicht über die Ausbildung und Qualifikationen gemäss Empfehlung in ESARR5.

## **2.2 Betriebliche Aspekte**

Dieser Totalausfall der Darstellung der Radarluftlage bedeutete für den Flugverkehr ein erhebliches Gefahrenpotential.

Die nach dem Ausfall durch die beteiligten Flugverkehrsleiter getroffenen Massnahmen waren durchwegs zweckmässig. Die gegenseitigen Absprachen erwiesen sich als richtig.

Günstig wirkte sich zudem aus, dass zur Zeit des Vorfalles ein eher geringes Verkehrsaufkommen herrschte und die Arbeitspositionen DOM Kontrollturm, DOM Bezirksleitstelle und Koordinator An- und Abflugleitstelle mit erfahrenem Personal besetzt waren.

### 3 Schlussfolgerungen

#### 3.1 Befunde

##### 3.1.1 Vorgeschichte und Verlauf des schweren Vorfalles

- Am 31. Oktober 2003, um ca. 09:30 UTC, ereignete sich auf zwei ICWS in der Anflughöhe im CIR ein plötzlicher Ausfall aller Radarspuren von einigen Sekunden Dauer.
- Zur Analyse und Behebung des Problems beschloss der TDZ, die Rückkehr des abwesenden Spezialisten abzuwarten.
- Die *log files* dieses Vorfalles wurden nicht gesichert und waren zum Zeitpunkt der Analyse am 11. November 2003 überschrieben.
- Am 11. November 2003 wurde eine stark erhöhte Prozessorlast des *standby X-client 28* festgestellt.
- Um 08:54 UTC des gleichen Tages erfolgte ein *shutdown/startup* des *X-client 28*. Dieser korrigierende Eingriff ins operationelle System wurde nicht im SYMA *log* eingetragen.
- Im Verlaufe des Tages wurden zwei weitere *standby X-client* (4 und 10) mit erhöhter Prozessorlast festgestellt.
- Um 18:31:17 UTC wurde dem *X-client 4* ein *shutdown/startup*-Befehl übermittelt.
- Um 18:34:28 UTC wurde dem *X-client 10* ein *shutdown*-Befehl übermittelt.
- Während des *shutdown* von *X-client 10* erteilte der zentrale Überwachungs- und Steuerungsrechner SMP Abschaltbefehle an die aktiven ADAPT Prozesse.

##### 3.1.2 Technische Aspekte

- Für die Verarbeitung der Radardaten waren drei redundante Systeme vorhanden.
- Im System zur Darstellung der Radarluftlage bestand keine wirksame Redundanz, da gleiche Gerätetypen, Betriebssysteme und Software eingesetzt wurden.
- Ein ursächlicher Zusammenhang zwischen der erhöhten CPU-Last und dem Vorfall vom 31. Oktober 2003 wurde nicht gesucht und ist auch nicht belegt.
- Der korrigierende Eingriff umfasste eine nicht geprüfte Operation an einem betrieblich genutzten System.
- Der korrigierende Eingriff wurde ohne vertiefte und dokumentierte Risikoabschätzung vorgenommen.
- Für korrigierende Eingriffe in betrieblich genutzte Systeme waren keine Prozesse, Verfahrens- oder Arbeitsanweisungen definiert und eingeführt.

### 3.1.3 Betriebliche Aspekte

- Die Flugverkehrsleitung wurde über die korrigierenden Eingriffe ins System nicht informiert.
- Auf den Radarbildschirmen der Flugverkehrsleiter waren keine Anzeichen für einen bevorstehenden Ausfall der Darstellung der Radarluftlage zu erkennen.
- Vom Ausfall ab 18:34:48 UTC waren sämtliche Radarbildschirme der Bezirksleitstelle sowie der An- und Abflugleitstelle betroffen.
- Der Ausfall breitete sich innert einer Minute über alle 29 Radarbildschirme aus und dauerte etwa 15 Minuten.
- Nach dem Ausfall wurden in Zürich alle Abflüge während einer Dauer von ungefähr 20 Minuten sistiert.
- Die Radarbildschirme im *tower* waren vom Ausfall nicht betroffen. Diese wurden für die Führung der Flugzeuge, die sich bereits im Nahbereich befanden, benutzt. Die nachfolgenden Maschinen wurden in die Warteräume eingewiesen und von dort von den Anflugsektoren im Kontrollturm übernommen.
- Die durch die beteiligten Flugverkehrsleiter getroffenen Massnahmen waren durchwegs zweckmässig.

### 3.1.4 Rahmenbedingungen

- Das an diesem schweren Vorfall beteiligte technische Personal von skyguide verfügte nicht über die Ausbildung und die Qualifikationen gemäss Empfehlung in ESARR5. Zum Zeitpunkt des schweren Vorfalls war diese Empfehlung noch nicht in Kraft.



### 3.2 Ursachen

Der schwere Vorfall ist darauf zurückzuführen, dass der zentrale Überwachungs- und Steuerungsrechner aus unbekanntem Grund alle aktiven Prozesse zur Darstellung der Radarluftlage beendete, ausgelöst durch korrigierende Eingriffe ins ADAPT System.

Folgende Faktoren haben zur Entstehung des schweren Vorfalls beigetragen:

- Im Flugsicherungsunternehmen fehlten Prozesse für korrigierende Eingriffe.
- Inwieweit der übergreifende Kenntnisstand des beteiligten Personals, welches an den technischen Anlagen des Flugsicherungsunternehmens korrigierende Eingriffe vorgenommen hat, genügend war, muss offen bleiben.
- Der bevorstehende korrigierende Eingriff wurde mit der Flugverkehrsleitung nicht koordiniert.
- Das Programm des zentralen Überwachungs- und Steuerungsrechners verfügte über keine Sicherheitsvorkehrungen und Warnsysteme.
- Ein redundantes System zur Darstellung der Radarluftlage war nicht vorhanden.

## 4 Sicherheitsempfehlungen und seit dem schweren Vorfall getroffene Massnahmen

### 4.1 Vorgehen nach technischen Ausfällen

#### 4.1.1 Sicherheitsdefizit

Der Vorfall vom 31. Oktober 2003 wurde unvollständig dokumentiert:

- die Daten wurden nicht gesichert
- die Ursache wurde nicht systematisch abgeklärt
- vor der Einleitung von Korrekturmassnahmen wurde keine breit abgestützte Risikoanalyse vorgenommen

Mit der Symptombhebung durch den *restart* des *X-client* 28 wurde das Problem als gelöst erachtet.

#### 4.1.2 Sicherheitsempfehlung Nr. 320 (vormals Nr. 90)

Das Bundesamt für Zivilluftfahrt sollte veranlassen, dass sämtliche technischen Vorfälle und Ausfälle nach einem einheitlichen und definierten Prozess behandelt und in einem technischen Logbuch systematisch dokumentiert werden. Insbesondere müssen die Beschreibung des Vorfalls, die gesicherten Daten, die Ursachenanalyse und die getroffenen Massnahmen Bestandteil einer solchen Dokumentation sein.

### 4.2 Eingriffe in im Einsatz stehende Systeme

#### 4.2.1 Sicherheitsdefizit

Im Zusammenhang mit der Untersuchung der Kollision von zwei Linienflugzeugen bei Überlingen hat die Bundesstelle für Flugunfalluntersuchung Deutschland folgende Sicherheitsempfehlung herausgegeben:

#### **Safety Recommendation Nr. 01/2003 der deutschen Bundesstelle für Flugunfalluntersuchung (SE Entwurf 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.*

Aufgrund der langen Wartezeit zwischen dem Vorfall vom 31. Oktober 2003 und dem damit verbundenen Eingriff am 11. November 2003 hätte die Intervention nach dem Prozess für geplante Eingriffe (PWAE) durchgeführt werden sollen. Stattdessen entschied sich der Fachexperte für einen spontanen Eingriff (*corrective action*). Für diese Art von Eingriff in ein operationelles System bestand kein definierter und eingeführter Prozessablauf. So war insbesondere der Informationsfluss zu den operationellen Diensten nicht gewährleistet.

Schon bei der Kollision von Überlingen war der Flugverkehrsleiter nur teilweise über die geplanten technischen Arbeiten informiert und konnte daher die betrieblichen Auswirkungen nur unvollständig abschätzen.

#### 4.2.2 Sicherheitsempfehlung Nr. 321 (vormals Nr. 91)

Das Bundesamt für Zivilluftfahrt sollte veranlassen, dass die Sicherheitsempfehlung der BFU Deutschland wie folgt ergänzt wird:

Sämtliche Eingriffe in operationelle Systeme sind nach einem definierten und eingeführten Prozessablauf abzuwickeln. Dieser Prozess muss zusätzlich folgende Massnahmen beinhalten:

- Information der operationellen Betriebe für sämtliche Eingriffe
- Abschätzung möglicher betrieblicher Auswirkungen
- Planung allfälliger operationeller und technischer Präventivmassnahmen

Das Bundesamt für Zivilluftfahrt sollte ferner überprüfen, welche Eingriffe in die im Einsatz stehenden technischen Systeme der Flugsicherung strikt auf die Zeiten zwischen 24:00 und 05:00 LT zu beschränken sind.

### 4.3 Zertifizierung von Anlagen der Flugsicherung

#### 4.3.1 Sicherheitsdefizit

Die Untersuchung hat ergeben, dass wichtige technische Anlagen der Flugsicherung keine wirksamen Redundanzen aufwiesen und dass keine ausreichenden Sicherheitsvorkehrungen und Warnsysteme vorhanden waren.

Anlässlich einer *Air Navigation Conference* hat die ICAO folgendes Dokument erstellt:

„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 investigate the need for the development of provisions for safety certification of ATM systems and service providers."*

#### **4.3.2 Sicherheitsempfehlung Nr. 322**

Das Bundesamt für Zivilluftfahrt sollte veranlassen, dass das technische Flugsicherungspersonal und die Anlagen der Flugsicherung zertifiziert werden.

#### **4.4 Seit dem schweren Vorfall getroffene Massnahmen**

Gemäss Schreiben von skyguide vom 22. März 2006 wurden folgende Massnahmen zur Verbesserungen der Flugsicherheit getroffen:

- 1. Unmittelbar nach dem Vorfall hat skyguide sofort alle manuellen Switch-over, Shutdown/Startup-Eingriffe über die SMP bis auf Widerruf untersagt; in den Tagen nach dem Vorfall wurde die Bereitschaft der Wartungsmannschaft erhöht, um auf eventuelle weitere Störungen sofort reagieren zu können.*
- 2. Im Dezember 2003 wurde im Sinne einer Sofortmassnahme die SW der SMC-Applikation so angepasst, dass nie mehr als 3 Knoten miteinander automatisch abgeschaltet werden können.*
- 3. Der Grund für die erhöhte CPU-Auslastung wurde gesucht und konnte eindeutig ermittelt werden. Eine entsprechend angepasste SW, die das am 10. November erstmals erkannte Problem behebt, wurde am 19. Februar 2004 in Betrieb genommen.*
- 4. skyguide hat sich dafür eingesetzt, den Vorfall auf der ADAPT-Testplattform zu reproduzieren, um damit weitere Hinweise zu dessen Ursache zu erhalten. Erst nach einem dreimonatigen Test und nach über 120'000 automatisch durchgeführten Shutdown/Startups (entsprechend etwa 500 Betriebsjahren) trat ein vergleichbarer Fehler auf.*
- 5. Die Wartungsverfahren wurden von Grund auf überarbeitet. Im Besonderen wurde ein Vorgehen für so genannte „nicht erwartete Situationen“ definiert. Das gesamte Paket aller neuen Wartungsverfahren wurde im September 2005 im Rahmen eines ISO-Audits durch eine unabhängige Stelle geprüft.*

6. *Im April 2004 wurde in Zürich ein zweites, vom Hauptsystem unabhängiges Luftlagedarstellungssystem in Betrieb genommen. An jedem Flugverkehrsleiter-Arbeitsplatz besteht seither die Möglichkeit, bei einem Ausfall des Hauptsystems, die aktuelle Luftlage auf einem Hilfsbildschirm darzustellen.*
7. *Im Rahmen einer am 10. Juni 2003 beschlossenen Phase der Systemerneuerung wurde im Mai 2004 das gesamte ADAPT-Darstellungssystem durch ein neu entwickeltes System ersetzt.*

#### **Bemerkungen des BFU**

Zu Punkt 3: Das BFU verlangte während der Untersuchung schriftlich Auskunft über den Grund der erhöhten CPU-Last. Diese Frage wurde bis zum Abschluss der Untersuchung nicht beantwortet.

Zu Punkt 4: skyguide präzisiert nicht, mit welcher Softwareversion der dreimonatige Test durchgeführt wurde.

Bern, 26. August 2008

#### **Eidgenössische Flugunfallkommission**

André Piller, Präsident

Tiziano Ponti, Vizepräsident

Ines Villalaz-Frick, Mitglied

## Anlagen

### Anlage 1: Auszug aus der Datei "trapd.log"

Der Befehl "*Node Startup*" wird gegeben und die Bestätigung "*Node Confirm*" akzeptiert, um alle Prozesse der Station *X-client* 13 neu zu starten:

```
....
....
....
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 zhcs02 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 zhcs01;1
.1.3.6.1.4.1.19.0.64 0
Tue Nov 11 18:39:11 2003 zhsuc02 - Network State: CONNECT_NODE zhcs01 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 CRE-
ATE_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 CRE-
ATE_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 CRE-
ATE_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
```

**Anlage 2: Auszug aus der Datei 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*

*....*

*....*

*....*

Anlage 3: Radarluftlage bei Beginn des schweren Vorfalles

