Normal people working in normal organizations with normal equipment: System safety and cognition in a mid-air collision

Paulo Victor Rodrigues de Carvalho a,b,*, José Orlando Gomes b, Gilbert Jacob Huber b, Mario Cesar Vidal c

aComissão Nacional de Energia Nuclear, Instituto de Engenharia Nuclear, Cidade Universitária, Ilha do Fundão, CEP 21945-970 Rio de Janeiro, RJ, Brazil
bGraduate Program in Informatics-NCE&IM, Cidade Universitária, Rio de Janeiro, RJ, Brazil
cLuís Alberto Coimbra Research Institute, COPPE, Federal University of Rio de Janeiro, Rio de Janeiro, RJ, Brazil

A R T I C L E   I N F O

Article history:
Received 1 February 2008
Accepted 28 November 2008

Keywords:
Mid-air collision
System safety
Cognitive strategies
Air traffic management system

A B S T R A C T

A fundamental challenge in improving the safety of complex systems is to understand how accidents emerge in normal working situations, with equipment functioning normally in normally structured organizations. We present a field study of the en route mid-air collision between a commercial carrier and an executive jet, in the clear afternoon Amazon sky in which 154 people lost their lives, that illustrates one response to this challenge. Our focus was on how and why the several safety barriers of a well structured air traffic system melted down enabling the occurrence of this tragedy, without any catastrophic component failure, and in a situation where everything was functioning normally. We identify strong consistencies and feedbacks regarding factors of system day-to-day functioning that made monitoring and awareness difficult, and the cognitive strategies that operators have developed to deal with overall system behavior. These findings emphasize the active problem-solving behavior needed in air traffic control work, and highlight how the day-to-day functioning of the system can jeopardize such behavior. An immediate consequence is that safety managers and engineers should review their traditional safety approach and accident models based on equipment failure probability, linear combinations of failures, rules and procedures, and human errors, to deal with complex patterns of coincidence possibilities, unexpected links, resonance among system functions and activities, and system cognition.

...if there is no seed, if the bramble of cause, agency, and procedure does not issue from a fault nucleus, but is rather unstably perched between scales, between human and non-human, and between protocol and judgment, then the world is a more disordered and dangerous place

Galison (2000), p. 32

1. Introduction

Mid-air collisions of en route aircraft are extremely rare events. A review of air traffic management (ATM) related accidents worldwide, from 1980 to 2001, (Van Es, 2003) showed that ATM-related accidents account for 8% of all accidents (the ATM-related accident rate is 0.44 per million flights). This review also showed that most the fatalities are caused by mid-air collisions (63%), and the major causal factors (classified according to the ICAO taxonomy – Flight Crew, Air Traffic Controller (ATC), Environmental, and Aircraft System) that contributed to the mid-air collisions were: 1) ATC – Failure to provide separation – air, and 2) Flight Crew – Lack of positional awareness – air.

In this paper, we use a systemic framework to analyze the functioning of the ATM cognitive system during the mid-air collision between flight GLO1907 (a commercial aircraft Boeing 737-800) and flight N600XL (an EMBRAER E-145 Legacy jet) to understand how and why this tragedy happened. This ATM-related accident occurred at 16:56 Brazilian time on September 29, 2006, in the clear afternoon Amazon sky. Our aim is to understand how a mid-air collision can still happen, despite the various defense layers that exist in the ATM system to prevent just such an event. Based on our findings we develop some insights about the cognitive functioning of the Brazilian Air Traffic Controllers and its safety implications to the ATM system operation.

Accidents and incidents by themselves cannot be considered absolute and direct indicators of the safety of any system (Woods and Cook, 2006). However, the analysis of the dynamic interplay of loosely and tightly coupled subsystems during the emergence of incidents and accidents can reveal patterns of behavior in the

* Corresponding author. Comissão Nacional de Energia Nuclear, Instituto de Engenharia Nuclear, Cidade Universitária, Ilha do Fundão, CEP 21945-970 Rio de Janeiro, RJ, Brazil. Tel.: + 55 21 21733835.
E-mail address: paulov@ien.gov.br (P.V. Rodrigues de Carvalho).

0003-6870/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
functioning of the whole system that may indicate a drift to unsafe states (Snook, 2000). The basic safety goal of the ATM system during en route commercial flights is to avoid mid-air collisions. Therefore, an analysis of the system operation during a mid-air collision can provide insights about system weaknesses and safety.

1.1. A systemic framework for accident analysis

Modern organizations are complex sociotechnical systems comprised of many nested levels: government, regulators, company, management, staff, and activities/work/processes/techni- cal systems. According to Rasmussen and Svedung (2000), safety can be viewed as a control problem involving all these levels and must be managed by a control structure embedded in an adaptive sociotechnical system. From this perspective, accidents are emergent properties of complex systems that are more prone to occur when the control systems (safety barriers included) do not adequately handle the day-to-day system failures/disturbances in a broad sense (external disturbances, component failures, human failures, or dysfunctional interactions among system components). Throughout the system's life cycle (Hollnagel, 2004). The outcome of a controlled system the result of reasonably foreseen input changes is directly influenced by the system's control mecha- nisms in place. Hazardous situations occur when flaws in the control mechanisms (technical, human, organizational) enable the emergence of unexpected outcomes that generate negative consequences. Accidents in safety-critical systems, like ATM, with many layers of control (defense-in-depth concept) can happen only when there are simultaneous failures in various control mecha- nisms in different system layers (Hollnagel, 2006).

ATM systems are composed of many nested layers resulting in complex interactions. Interactions occur between human operators (controllers and pilots), between human operators and procedures (flight plans, rules to define the controlled air space, the air space sectors that must be handled by some specific controller team, general safety rules for the control of traffic, and so forth), and between operators and hardware/software technical systems (radar systems, computer processing of radar and flight data, aircraft navigation systems, traffic alert and collision avoidance system – TCAS, communication systems between controllers and pilots, flight progress strips).

Brooker (2006) simplified the ATM system description into three structural system layers acting as the system controls: Planning (pre-operational), Operation (the flight in progress), and Alert (the ground and air protection enabled by conflict alert systems, on which the controller/pilot will act). Humans in the several ATM system layers participate in control of the system, acting to operate the system in a safe manner. Failure of system control occurs when the mechanisms used to keep system stability fail and make the situation worse against reasonably foreseen threats. The fundamental issue here is how to identify reasonably foreseen threats in dynamic real-life situations. To do so, we must understand how people address the overall constraints of the control system during their daily work. The most important question regarding human control performance in safety-critical systems is to understand how and why normal work done by normal people enables the emergence of accidents (Dekker, 2006).

2. Method

The research methodology to investigate the functioning and safety of the ATM system based on the analysis of a single case study the GLO1907/N600XL collision can be justified by Yin's (1994) rationale. According to Yin case studies can be used when how and why questions are being posed, and when the focus is on a contemporary phenomenon within some real-life context. Understanding HOW two airplanes collided in the clear afternoon Amazon sky satisfies Yin's HOW criterion. The concurrence of organizational and cognitive factors that enable the emergence of this tragedy directly related to the ATM system's safety satisfies Yin's WHY criterion.

Catastrophic accidents in the domain of ultra-safe systems such as commercial fixed wing scheduled flight, with risk lower than $10^{-6}$ provide a unique opportunity to study the safety of complex systems. This condition also justifies the use of a single case study according to Yin's rationale: an extreme and unique case or a revelatory one (Yin, 1994). The mid-air collision satisfies these two criteria. It is unique and extreme in the sense that mid-air collisions are the least frequent ATM-related accidents, and it is revelatory due to the generation of a considerable amount of data that become available to the public and researchers through secondary sources. The availability of these data is especially important in the case of the Brazilian ATM system as it is operated under military administration and the data about its functioning (e.g., danger reports, near misses) are not usually available to the public and social scientists.

In our research method, we search for the mid-air collision antecedents traced through the concurrence of performances of the several actors (pilots and controllers) and their interaction with the contextual conditions of the several ATM subsystems. Our aim is to understand how and why this accident happened based on the rich data set that, because the occurrence of this tragedy is now available to the public. Data and evidences, antecedents and consequences from this mid-air collision come from a wide range of publicly available sources. These sources include official government documents, congressional hearings, including controllers', pilots', and air traffic management authorities' testimonies, video tapes, audio tapes of many media centers, press releases, newspaper clippings, flight plans, regulations, maps, directives and so forth.

3. The air traffic management system – ATM

To understand the control functions of the ATM system, we use the systems layers concepts as defined by Brooker (2006). The ATM system layers are formed by human, technological (hardware and software), and organizational components. Some of them, important to avoid mid-air collisions, are briefly described:

- Controllers and pilots, sharp-end operators at the bottom layer of the system;
- Prescribed safety rules for the control of traffic, including the minimum separation to be permitted between aircraft, flight plans;
- Communications equipment between controllers and pilots (special radio communications frequencies);
- Airways to structure aircraft traffic in the controlled air space and provide references for traffic separation;
- Air space sectors to allow the division of air traffic control among different controller teams;
- Many other software rules to discipline where and how the different types of aircraft must fly;
- Flight progress strips based on the flight plan data used by controllers to quickly recall the order (in time) and the details of the flights they have to handle; recommendations regarding the maximum number of flights that can be managed by the controller;
- Radar systems:
  - Primary Surveillance Radar (PSR), that works by passively bouncing a radio signal off the skin of the aircraft and whose advantage is that it operates totally independently of the
target aircraft – that is, no action from the aircraft is required for it to provide a radar return – but that does not positively identify the aircraft, generates imprecise altitude information, and has a range limited by distance, altitude, terrain and rain or snow:

- Secondary Surveillance Radar (SSR) that overcomes these limitations but depends on a transponder in the aircraft to respond to interrogations from the ground station to make the plane more visible and to report the aircraft’s altitude.
- Computer processing complementing the information coming from the radar and flight data;
- High quality aircraft navigation systems using Inertial Navigation Systems through to satellite-based aids such as GPS;
- Short Term Conflict Alert (STCA) and Separation Monitoring Function (SMF) that are the computer processing systems for analyzing the radar tracks to predict if aircraft might come into proximity soon and, if they might, warn the controller by flashing a message on his radar screen;
- Traffic Alert and Collision Avoidance System (TCAS), the onboard collision avoidance systems based on detection of other aircraft in the vicinity through their SSR transponders. These inform the pilot of nearby traffic – TA (Traffic Advisory) – and aircraft coming into conflict – RA (Resolution Advisory). RAs inform the pilot to climb or descend as appropriate to take the flight out of risk.

In an ATM control system functioning as described above, the safety control barriers to avoid a mid-air collision can be summarized as:

- Controlled air space with straight route, with two traffic lanes;
- Opposite traffic flows along each lane;
- Distance between the two lanes of 1000 ft (vertical separation);
- Well defined flight plans received before the flight;
- Traffic flow per lane lower than 4 aircraft/hour (longitudinal separation);
- The two aircraft are equipped with Traffic Alert and Collision Avoidance System (TCAS);
- The two aircraft are under surveillance of ground controllers, with radar tracking and radio communication.

In a system with this entire set of control safety barriers, how could an accident like this ever happen? How could a sophisticated ATM system with several safety barriers, many coordinating mechanisms, surveillance and communication equipment providing redundant layers of cross-checking possibilities allow this to happen? There was no emergency situation, no weather problems in the clear afternoon Amazon sky, and no sudden equipment failure that can be considered the cause of this tragedy.

3.1. The configuration of the Brazilian ATM system

Because the research approach attaches great significance to the work environment as the root of variation in decision-making and cognitive behavior, we present a brief description of the Brazilian ATM system using the means-end hierarchy (Rasmussen et al., 1994). In particular, we will use the Rasmussen and Svedung (2000) framework for risk management to look at management and organization structures. Fig. 1 presents the generic actor map for the Brazilian ATM system. This diagram provides a view of the whole system, including many levels ranging from governmental structures at the top, down to the local environment of sharp-end operators (controllers and pilots), the ultimate level related to the collision. The lower level represents the individual operators that are interacting with the process being controlled. The third level describes the company managers responsible for the companies’ policy and strategies, and for the supervision of the operators’ activities. The second level describes activities of regulators and associations responsible for monitoring the activities of the companies in the aviation sector. The first level details activities of the government and juridical aspects related to the same sector. The representation of all these levels is necessary because they all interact with each other, mutually directing and influencing each level behavior, to control the system and provide adaptation to environmental changes. To understand the events at any particular level, it is therefore important to understand what has gone on at all levels in the system. As pointed out by Rasmussen and Svedung (2000), any sociotechnical system is subject to severe environmental pressure in a dynamic society. The society pressure first appears at the higher levels in the definition of legislation, regulations, budget, and so forth, going down to the companies’ policies and strategies, reaching the sharp-end operators’ behaviors and actions. Adequate control strategies at all levels enable the system to operate at low risk, in which a proper co-ordination and decision-making at all levels can be achieved. These observations are particularly important considering the rapid growth of commercial fixed wing flights in Brazil, which is increasing the demands on the entire Brazilian air traffic system.

The regulation of Brazilian air traffic system complies with the international ICAO legislation. The Brazilian constitution is the source for the development of specific regulations governing the functioning of the Brazilian Air Space Control System (SISCEAB), which is also regulated by the Department of Air space Control (DECEA), responsible for the integrated air defense and air traffic control system. The SISCEAB encompasses all of the system’s operational functions: communication, air traffic control, air defense, aeronautical meteorology, cartography, aeronautical information, search and rescue, and accident investigation.

Brazilian authorities decided to have only one ATM system, the Integrated Air Defense and Air Traffic Control System (SISDACTA). The SISDACTA is responsible for the co-ordination and joint operation of the air defense and air traffic control activities. The SISDACTA acts on the entire Brazilian air space and in the international regions under Brazilian responsibility, according to ICAO agreements. The total area covered corresponds to 22 million square kilometers (8,511,965 Km² above Brazilian land). The SISDACTA comprises:

1) Tower Control Centers (TWRs) – control air traffic up to 5 km from the airports;
2) Approach Control Centers (APPS) – control air traffic between 5 and 74 km from the airports;
3) Area Control Centers (ACCs) – known as CINDACTAs (acronym for Integrated Air Defense and Air Traffic Control Centers) control air traffic in the airways.

For radar surveillance and air traffic control purposes, Brazil has been divided into 4 big regions. All radar data from each region are processed by an area control center (ACC) or CINDACTA. Each one of the four CINDACTAs has radar control of its region and is responsible for the co-ordination of the regional air traffic. Due to its centralized localization, CINDACTA I (Brasilia ACC), which operates from Brasilia and was the first center installed, is responsible for controlling most of the air traffic in Brazil. CINDACTA II operates in the south region, CINDACTA III covers the northeast air space, and CINDACTA IV (Amazon ACC) the north region, comprising the Amazon forest. The CINDACTAs control traffic of en route aircraft, when the airplane is above 19,500 feet. During the approach to airports, air traffic is controlled by the Approach Control Centers (APPs), and the final descent is controlled by the airport’s Tower Control Center (TWRs).
In each CINDACTA, there are two air traffic control systems in two different control rooms:

- Military Operations Centers (COPM) that handle flight control of military aircraft that are in military operation, operated by military controllers, under military rules.

- Area Control Centers (ACCs), responsible for the air traffic control of aircraft (civilian and military) flying under the general aviation circulation rules, operated by civilian and military controllers, under civilian rules.

Military controllers operate both centers. The integration of air space and air defense control in Brazil – an option that is not used in most countries – enables the use of the same resources for communication, detection, surveillance, control and early warning for air traffic control and for air space defense purposes.

4. The facts – what happened?

The collision was a very brief event. About 1 hour elapsed from the moment when flight N600XL, the Embraer E-145 Legacy jet, entered the air space controlled by the Brasilia ACC (CINDACTA I), until the collision with flight GLO1907, the Boeing 737-800, in the surveillance intersection zone between the Amazon and Brasilia control centers. Fig. 2 shows the collision path. Flight N600XL, even with some damage, was able to land at a military base airport.

Fig. 3 shows a time-line with the main events before and after the collision. Flight N600XL, an Embraer Legacy executive jet, took off from São José dos Campos airport (in São Paulo state) at 14:30 (Brasilia time) to Eduardo Gomes airport in Manaus (in Amazonas state) with a crew of two (pilot and co-pilot) and 4 passengers. Flight N600XL’s plan stipulated two level changes (see Fig. 3). However, the flight level stipulated for the first leg (until Brasilia) of the flight, 370 (or 37 000 ft), was reached at 15:33 and was maintained up to the moment of the collision.

Flight GLO1907, the Boeing 737-800, took off from Eduardo Gomes airport in Manaus to Brasilia International Airport at 15:35. At 15:58, it reached the 370 flight level in the UZ6 airway (a dual lane airway with 1000 ft of vertical separation between lanes), and maintained this level, as stipulated by its flight plan, up to the collision moment.

The last successful bilateral contact between the N600XL and the Brasilia ACC happened at 15:51. At 15:55, the N600XL flew over the Brasília VOR vertical line, and entered the UZ6 airway (the same as flight 1907, but in the opposite direction), without requesting or receiving any instruction from the Brasilia traffic control center and keeping the 370 flight level. At 16:02, the Brasilia ACC lost the secondary surveillance radar (SSR) information about the N600XL, which presents accurate altitude information to the traffic controller. At 16:30, there was a 2 min loss of primary radar contact with the N600XL, which transmits the aircraft’s geographic position to the controller. No contact was attempted between 15:51 and 16:26 by either the N600XL or the Brasilia traffic control center.

From 16:26 to 16:53 the Brasilia ACC made seven unsuccessful call attempts. At 16:38, the Brasilia ACC lost definitively the primary radar contact with the N600XL (it should have been transferred to the Amazon control center).

The N600XL, at 16:48, began a series of 12 call attempt to the Brasilia ACC. At 16:53:39, the N600XL was able to hear the last (unilateral) call by the Brasilia center, instructing the N600XL to call the Amazon ACC. However, the crew was not able to copy the frequencies provided. At 16:53:57, the N600XL radioed the Brasilia center requesting the repetition the decimals of the first frequency, because it had not been able to copy these values. The Brasilia center did not receive this message. After that, the N600XL made seven more unsuccessful call attempts to the Brasilia center from 16:54 to 16:57.
The mid-air collision occurred when both aircraft were in the UZ6 airway, flying in opposite directions, at the same altitude – FL370 or 37 000 ft – at 16:56:54. With the collision, flight 1907 became uncontrollable, immediately going into a dive until it crashed into the ground, causing the death of all passengers and crew members (154 people), while flight N600XL was still able to fly and succeeded in making an emergency landing at the Brigadeiro Veloso military air base.

5. The analysis – how and why it happened

The commander of the Department of Air space Control (DECEA), responding to a senator’s question in the senate public hearing after the accident said: “I am as puzzled as you Sir. A thing like this is impossible to happen.”

5.1. Preliminary investigation questions

The preliminary report elaborated by CENIPA (Ferreira, 2006) indicated the following important things that did not happen in this accident:

- There was no loss of radar surveillance between the Amazon ACC (CINDACTA IV) and flight 1907, until its transference to the Brasilia ACC;
- There is no evidence in the communication records of any N600XL request to the air traffic control centers to change its flight level, after having reached the 370 flight level.
- There is no registered evidence regarding any instruction for the N600XL to change its flight level coming from air traffic control, after the last successful bilateral contact (15:51) between this aircraft and Brasilia center.
- There is no registered evidence of any traffic alert alarm or instruction for evasive action to the respective crews to avoid collision in the TCAS systems, existing in both aircraft.
- There is no registered evidence of any manifestation in either crew related to any possible visual perception of the approaching aircraft.
- There is no attempt for action or evasive maneuver, according to the data existing in flight recorders.

Looking through the list it seems that the entire system (including man-pilots and controllers – technology and
organization) was not aware that two aircraft were flying in the same lane and in opposite directions.

5.2. Some official explanations

Charles Perrow pointed out that conventional explanations for accidents are “operator error, faulty design or equipment, lack of attention to safety features, lack of operating experience, inadequately trained personnel, failure to use the most advanced technology, and systems that are too big, under financed, or poorly run” (Perrow, 1984, pp 63). The conclusions from the Senate Public Hearing report confirm Perrow’s view and lean toward faulting the operators: “(...) it is possible to learn that several factors contributed to the accident: possible technical failures, pilot failures and air traffic controller failures. However, analyzing the event, I conclude that the human factor is the main cause. Eliminating the human errors from the causal chain, the accident would never have happened (...)” (Senado Federal, 2007, pp 61).

We want to go beyond these obvious explanations to consider the complexity of the events, understanding the details of each situation (how and why things happened). Our aim is to uncover the underlying cognitive and organizational dynamics that enabled the emergence of the tragedy, using the rich set of data that was made available by the accident investigations as a window to grasp a more fundamental understanding about the ATC system’s normal functioning. To do so, in the following sections, we will discuss HOW and WHY the safety barriers against mid-air collisions described in Section 4 eroded enough to allow the emergence of this accident.

5.3. The controlled air space

The controlled air space – the first safety barrier – is an abstract construction, which aims to create “airways” in the space by prescribing routes, altitudes, and directions to be followed by air traffic. These airways are represented on aeronautical navigation charts and should be followed by pilots and controllers. The flight plan is the artifact that enables pilots and controllers to virtually construct a flight, allocate a portion of the controlled air space to it, and then discipline the flights and air traffic control.

In this accident, the flight levels prescribed in flight N600XL’s flight plan were not followed. How could this happen? We will use the investigation findings and human decision-making theories to explain how normal pilots’ and controllers’ cognitive behaviors lead to this unwanted system outcome.

5.3.1. Pilots’ behavior

Fig. 3 includes a representation of the prescribed altitudes of flight N600XL’s approved flight plan. Starting in São José dos Campos, it passed through Poços de Caldas, in the U2W airway at flight level 370 (37 000 ft) until Brasília, where it would drop to flight level 360 (36 000 ft) and enter the UZ6 airway. The flight plan called for another altitude change at the Teres (virtual) notification point, after which the aircraft would continue in the UZ6 airway, but at FL380 (38 000 ft). The UZ6 is a dual lane airway with 1000 ft vertical separation distances, in which the odd flight levels (370, 390, 410) are used for north-south navigation (Manaus to Brasília), and the even flight levels (360, 380, 420) are used for south-north navigation (Brasília to Manaus). According to the CPI final report (Câmara dos Deputados, 2007), the submitted flight plan was approved without modification by the Brasília ACC.

Flight N600XL’s pilots had never flown in Brazil before September 29, when they came to São Paulo to fly the brand new Embraer Legacy aircraft just acquired by American Excelera. The flight plan they were using was both prepared and submitted by Embraer to the air traffic control center for approval. This flight plan preparation procedure (a normal way to prepare flight plans), did not require the pilots to look at Brazilian airways on the local aeronautical charts to configure their flight. As a consequence, some of the details of the plan, and in particular, the situation regarding the UZ6 airway, may not have come to the pilots’ attention.

The dialog in Table 1 shows the communications between flight N600XL’s pilot and the TWR controller in São Jose (SP) just before departure.

The dialog above seems to be a normal departure communication between a tower controller and a pilot. In fact, we note that, according to the basic verbal protocol rules, there are communication feedbacks and redundancies when flight N600XL’s pilot did repeat the authorizations received. However, when the air traffic controller did not communicate the complete flight plan (level changes at Brasilia to 360 and at Teres to 380), (...) ATC clearance to Eduardo Gomes, flight level three seven zero (...), the pilot did not challenge the ATC’s clearance communication asking for the clearance limits - until where he would fly at level 370 – implying that he would fly at FL370 all the way to Eduardo Gomes airport, in Manaus (against the flight plan information).

<table>
<thead>
<tr>
<th>Time</th>
<th>Operator</th>
<th>Communications</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:26:40</td>
<td>Legacy Pilot</td>
<td>São José ground november six zero x-ray lima.</td>
</tr>
<tr>
<td>14:26:47</td>
<td>TWR controller</td>
<td>November six zero x-ray lima go ahead.</td>
</tr>
<tr>
<td>14:26:51</td>
<td>Legacy pilot</td>
<td>Yes sir (...) start engines.</td>
</tr>
<tr>
<td>14:26:59</td>
<td>TWR controller</td>
<td>Er, did you request, er, about weather?</td>
</tr>
<tr>
<td>14:27:02</td>
<td>Legacy pilot</td>
<td>Yes sir, weather and runway.</td>
</tr>
<tr>
<td>14:27:05</td>
<td>TWR controller</td>
<td>Roger, Er, São José operating under visual conditions, ceiling five thousand feet, visibility one zero kilometers, runway in use one five, wind two zero two degrees, eight knots, quau eneti one zero one nine, temperature two zero, time check two five.</td>
</tr>
<tr>
<td>14:27:37</td>
<td>Legacy pilot</td>
<td>Thank you.</td>
</tr>
<tr>
<td>14:31:46</td>
<td>Legacy pilot</td>
<td>Ground, november six zero x-ray lima like to have push back for taxi.</td>
</tr>
<tr>
<td>14:32:02</td>
<td>Legacy pilot</td>
<td>Ground, november six zero lima, x-ray lima, like to give ready, clear to push for taxi.</td>
</tr>
<tr>
<td>14:32:10</td>
<td>TWR controller</td>
<td>Ah, november six zero x-ray lima, er, clear to start up, temperature two zero, Er, are you ready to taxi?</td>
</tr>
<tr>
<td>14:32:24</td>
<td>Legacy pilot</td>
<td>Ah, affirmative, yes.</td>
</tr>
<tr>
<td>14:32:31</td>
<td>TWR controller</td>
<td>Er, report ready for taxi.</td>
</tr>
<tr>
<td>14:40:31</td>
<td>Legacy pilot</td>
<td>São José ground, november six zero x-ray lima ready to taxi.</td>
</tr>
<tr>
<td>14:40:38</td>
<td>TWR controller</td>
<td>Er, roger, Er, maintain position, november six zero x-ray lima.</td>
</tr>
<tr>
<td>14:40:44</td>
<td>Legacy pilot</td>
<td>November six zero x-ray lima maintaining position.</td>
</tr>
<tr>
<td>14:41:50</td>
<td>TWR controller</td>
<td>Are you ready to copy the clearance?</td>
</tr>
<tr>
<td>14:41:53</td>
<td>Legacy pilot</td>
<td>Ah, affirmative, yes.</td>
</tr>
<tr>
<td>14:41:57</td>
<td>TWR controller</td>
<td>November six zero x-ray lima, ATC clearance to Eduardo Gomes, flight level three seven zero, direct Poços de Caldas, squawk transponder code four five seven four. After take-off perform OREN departure.</td>
</tr>
<tr>
<td>14:42:26</td>
<td>Legacy Pilot</td>
<td>Okay sir, I get the runway one five to so... ah SBEG, flight level three seven zero 1 didn’t get the first fix, I get squawk four five seven four, OREN departure.</td>
</tr>
</tbody>
</table>

Source: CPI final report (Câmara dos Deputados, 2007).
From this dialog, we conclude that the N600XL pilots had two conflicting sets of information at the moment of departure: 1) the flight plan with many level changes, and 2) the ATC’s communication clearance that mentioned only FL370. Based on the conflicting information (inputs) they had, why did the pilots not evaluate and compare the inputs and query the controller?

Traditional research in decision-making has developed normative models for human decisions that involve: first, generate a range of options, then generate a set of criteria for evaluating these options, assign weights for the evaluation criteria, rate each option on each evaluation criterion, perform calculations, and finally, compare the options determining the best choice (Doherty, 1993). If people during their normal work made decisions according to this model, we could imagine that the pilots’ actual behavior was completely unusual or abnormal (and probably very unlikely to happen again with other pilots), because their decision process did not agree with any of the normative steps described.

However, situated or naturalistic based human decision-making models, identifying deviations from the norms, e.g. Prospect Theory (Tversky and Kahneman, 1974) suggest that decision-makers generally apply a wide range of heuristics, even when these result in sub-optimal performance. Heuristic-based theories have been superseded by descriptive models emphasizing the phenomena themselves, without reference to abstract norms, such as Rasmussen’s model of Cognitive Control (Rasmussen, 1983) and Klein’s Recognition-Primed Decision-Making - RP model (Klein, 1993) and more recently the efficiency-thoroughness trade-off, the ETTO principle (Hollnagel, 2004). In such models, rather than making a concurrent evaluation of the relative advantages and disadvantages of several courses of action (the normative approach), the decision-makers in actual situations select a course of action, which is generated through heuristics and recognition. A situation similar to a previous experience, a familiar situation, is evaluated for its adequacy in the particular set of circumstances of the present situation. There are many empirical findings that even in safety-critical systems, for instance, nuclear systems (Carvalho, 2005; Carvalho et al., 2005; Carvalho et al., 2006), experienced operators use pattern recognition and simple heuristics to make decisions during their daily work in operating the system.

Flight N600XL’s pilots’ behavior – not querying the ATC controller, not searching for more information – indicates that they decided based on the recognition that the clearance they received from ATC is a familiar situation of changing a flight plan by ATC authorities. Together with their non-familiarity with Brazilian air space, the pilots did not have any doubt about the new flight plan they got after the ATC clearance communication. The pilots confirmed that they had no doubts in an interview for the Brazilian newspaper Folha de São Paulo on Feb. 19, 2007. The pilot said, “It is common for there to be differences, it happens all the time. You have to fly according to the authorization… The actual flight plan is the clearance that you receive from the control center.”, and the co-pilot, “As he said, it happens all the time, we have a flight plan to fly at one clearance that you receive from the control center.”

From other side, the air traffic controller gave a flight authorization where only the level of the first leg (FL370) was communicated in a route that included two other level changes. The ICA 100-12 publication (DECEA, 2006) regulates the air traffic services in Brazil. Chapter 8, Area Control Services, defines the rules to be applied for ATC services. According to these rules, the submitted flight plan can be different from the actual plan, and the controller must indicate the various levels of the route, or the limit for the route authorization he gave. In the ICA 100-12 there are the following definitions:

- **Flight plan** – specific Information, related to a planned flight or part of a flight of an aircraft, supplied to the air traffic services.
- **Submitted flight plan** – flight plan such as it is submitted by the pilot, or his representative, to the air traffic services.
- **Current flight plan** – actual flight plan, including the modifications (if they were necessary) made by air traffic services.

Based on these rules and controller behavior the Congressional Hearing Report concludes “(…) a message with partial authorization for the flight of an aircraft is a procedure without any normative support” (Câmara dos Deputados, 2007, p. 58).

The procedure for flight plan authorization has many steps. First, the plan is submitted in the Air Information Service Room, located in the departure airport. In this room, a Sergeant specialized in aeronautical information (not a flight controller) receives and checks the submitted plan. Next, the plan is presented to another Sergeant, specialized in communications, who inputs the flight plan data into the computerized system and sends these data to the regional ACC, where a flight controller in the Flight Plan Room checks the proposed route comparing it to the other flight plans in the region. If it is OK, he/she confirms the insertion of the flight plan data in the system and sends the “Traffic Authorization or Clearance Delivery” by an electronic message to the departure airport. Finally, the TWR controller at the departure airport, responsible for the “traffic authorization”, using a private telephone line (called “hot line”), calls the ACC controller to confirm the flight plan information for the clearance delivery. Having received the ACC’s confirmation, the TWR controller radios the “Authorized Flight Plan” to the flight’s pilot.

The last internal step of this procedure, the final communication between flight controllers (São Jose TWR controller with the Brasilia ACC) to confirm flight N600XL’s information is transcribed in Table 2.

In this dialog, which happened about 10 min before the take-off clearance communication dialog between the TWR controller and the pilot, presented in Table 1, the controllers’ verbalizations refer only to the level 370. In both dialogues, there are no explicit verbalizations regarding the complete N600XL flight plan. In all conversations involving pilots, the TWR controller in São Jose, and the ACC controller in Brasilia, the level changes in N600XL’s flight plan were not verbalized. Therefore, from this dialog, and the dialog between TWR controller and the pilot, the controllers did not follow the DECEA prescriptions.

The easiest way to address this situation is consider that we have a human error. Doing so, the problem can be confined to those specific controllers that behave in a completely different way than the other controllers working in the system.

However, from a systemic point of view, this can also be viewed as a normal behavior. On long routes, with many level changes, the ATC controller may assume that pilots are aware of the need for normal behaviors of the pilots. Normal in Perrow’s sense, not desired or expected, but a perfectly possible outcome of the system.
level changes during the flight. They also may think that there will be other communication opportunities later on, when the aircraft reaches the clearance limits (in this flight the first one was over Brasilia), at which time the pilots will receive the information regarding the other legs of the plan.

Both behaviors – pilots’ and controllers’ – can be explained by the by the efficiency-thoroughness trade-off, the ETTO principle (Hollnagel, 2004). Pilots and controllers use common and simple heuristics such as “someone one will communicate this later”,”there is no need to pay attention to that now”, “flight plans can always be changed” that characterize the ETTO principle. Initially conceived to explain coping strategies to reduce the cognitive task demands (e.g. time pressure, information overload etc.), the ETTO principle is currently viewed as a typical strategy to cope with complexity in a long-term perspective (Hollnagel and Woods, 2005). Using ETTO heuristics it is possible to reduce cognitive effort and keep spare capacity for emergency situations, making a trade-off before it is objectively required by the current situation. Thus, the choice of a coping strategy not only represents a short term or temporary adjustment but may equally well indicate a more permanent way to do things in the system functioning. The risks inherent in these strategies use are obvious, as can be seen from their part in this accident explanation.

We argue that the controlled air space as a cognitive system (a system that involves people, technology and organization) may be a weaker safety barrier than we usually expect, enabling unwanted system outcomes that may result in system accidents, depending on how the system is functioning daily. Due to the limitations inherent in analyzing only one case, we are not able do know how frequently the system is functioning daily. The risks inherent in these strategies use are obvious, as can be seen from their part in this accident explanation.

The dialouge between TWR and ACC controllers – Dialog in Portuguese, translated to English.

<table>
<thead>
<tr>
<th>Time</th>
<th>Operator</th>
<th>Communications</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:33:33</td>
<td>Brasilia ACC</td>
<td>Talk São Jose</td>
</tr>
<tr>
<td>14:33:35</td>
<td>São Jose TWR</td>
<td>Hi Brasilia. The November six zero zero x-ray lima to Eduardo Gomes São Jose Eduardo Gomes requesting level three seven zero.</td>
</tr>
<tr>
<td>14:33:50</td>
<td>Brasilia ACC</td>
<td>... Level three seven zero transponder four five seven four Poços de Caldas.</td>
</tr>
<tr>
<td>14:33:55</td>
<td>São Jose TWR</td>
<td>Three seven zero direction Poços. What is the frequency he calls you there?</td>
</tr>
<tr>
<td>14:33:59</td>
<td>Brasilia ACC</td>
<td>One two six fifteen ... one three three five</td>
</tr>
<tr>
<td>14:34:04</td>
<td>São Jose TWR</td>
<td>One three three five seven three zero direction Poços.</td>
</tr>
<tr>
<td>14:34:09</td>
<td>Brasilia ACC</td>
<td>OK</td>
</tr>
<tr>
<td>14:34:10</td>
<td>São Jose TWR</td>
<td>Bye bye</td>
</tr>
</tbody>
</table>

Source: CPI final report (Câmara dos Deputados, 2007).

5.4. The TCAS functioning

Another barrier used to avoid mid-air collisions is the Traffic Alert and Collision Avoidance System (TCAS). Both aircraft involved in this accident were equipped with TCAS equipment. According to Brazilian flight regulations, before entering air space with reduced vertical separation minimum (RVSM space, where the vertical separation distance is 1000 ft.), the pilot must check (besides other equipment) that the transponder is normally working in mode C or S. In Mode C, the transponder informs its code and the aircraft’s altitude with good accuracy. In Mode S, in addition to the Mode C information, the transponder sends other flight parameters such as speed, direction etc. The TCAS requires the transponder function to operate, and goes into standby mode (effectively off) whenever the transponder is not enabled.

One of the most puzzling notes of the accident preliminary investigation report is that “There was no attempt for action or evasive maneuver, according to the data existing in flight recorders” (Ferreira, 2006), indicating that TCAS did not give the TA (Traffic Advisory) or RA (Resolution Advisory) alarms to the pilots. According to the time-line presented in Fig. 3, Brasilia ACC failed to receive any transponder replies from flight N600XL for approximately the last 50 min of the flight before the collision.

Further investigations indicated that the transponder and TCAS of flight GLO1907 was working properly during the accident, and the transponder of flight N600XL was not functioning (it was in the OFF mode) at the moment of the collision. Evidence that flight N600XL’s transponder was in the OFF mode came from many sources:

– The lack of N600XL transponder contact with the Brasilia ACC;
– The lack of N600XL transponder contact with the Amazon ACC;
– The dialog between N600XL pilots registered in the CVR (Cockpit Voice Recorder), just after the collision.

This dialog is presented in Table 3 below.

Clearly, the Transponder/TCAS system of the N600XL aircraft failed. However, even after extensive tests, tear-downs and simulations in the aircraft manufacturer and in the transponder/TCAS manufacturer, the reason why the transponder was set in the STAND BY mode (turned off) remains “unexplained” to this day.

Three main possibilities were investigated: 1) hardware/technical failure, 2) pilots deliberately turned off the transponder, and 3) pilots accidentally turned it off with an unintentional slip. About the hardware/technical failure, all post-accident information made public up to this moment – the investigation has not finished yet – indicates that the critical transponder components were operational. The second possibility, a professional crew willingly switching off such an important piece of equipment in the RVSM space would have been an act of basic procedure violation (Reason, 1997). This behavior simply could not be admitted by any professional crew and has no support in the flight data collected (Câmara dos Deputados, 2007). The last possibility, pilots accidentally turning off the TCAS with an unintentional slip, is also not supported by the investigation findings. The only known way to put the transponder STAND BY mode is to press the button on the Radio Management Unit (RMU) control screen twice, within less than 20 s, as shown in Fig. 4, which could not be attributed to a slip.

In his testimony to the Senate Congressional Hearing, the official responsible for the Brazilian aeronautic accident investigation said, “In accordance with the description documents and its certifications, the transponder and TCAS systems did not present design or integration errors. They functioned as they had to function. (...) We now focus our investigation on the operational factor, or either, in the relation of the operation of... of the human being with that system”.

In another part of this testimony, he added some new information related to the “operational factor”: “The transponder stopped functioning. We did all the tests to try to exclude the possibility of a technical failure in the transponder. We did not find technical
malfunctions. The equipment functioned according to its specifications. Therefore, we are focusing on the operational factor. What I have to say at this moment is that I have no indication that the pilots turned off the transponder intentionally. I do not have, looking at the CVR, I have nothing that indicates an action related to this equipment.” (Câmara dos Deputados, 2007).

However, the transponder was in OFF mode and TCAS was in STAND BY mode for 50 min before the collision. The question that remains is: Why did the pilots not perceive that these important pieces of equipment were not functioning properly? The indications in the cockpit that the transponder is currently switched off, and as a consequence the TCAS is in STAND BY mode, are difficult to perceive as shown in Fig. 5, because they are not indicated in the standard failure colors, and there is no alarm signal to draw the pilots’ attention. The indication that the TCAS is in standby mode appears on the Radio Management Unit (RMU) as a small indication in green letters inside a yellow window, just underneath the transponder code selected. There are two other indications regarding the operation mode of the TCAS: on the right side of the Primary Function Display (PFD), there is a message in white and small letters indicating TCAS OFF, and on the left side of the Multi Function Display (MFD) (if this specific page is the selected one) the message is repeated in the same small white letters (see Fig. 5).

Problems with these indications had already been noted, back in 2005, by the European air traffic authorities, in a similar avionic system: “When this reversion to standby mode occurs, the ATC/TCAS standby mode is indicated on the RMU and Cockpit Displays (PFD, MFD), however these indications may not be apparent to pilots, especially during periods of high workload” (Irish Aviation Authority, 2005, pp. 2). Note that in spite of the observation dated from 2005 that the indications may not be apparent to pilots, the same indication methods are still used in avionic systems.

There were other cases of spurious failures or automation surprises in Transponder/TCAS operation in a similar avionic system. At the end of 2003, the European ATC providers noted many lost transponder tracks for several minutes. An Embraer E-145 remained invisible in the busy European air space for more than 45 min before it was identified as an “unknown target” by French military control, and the first steps for intercepting the target were initiated. The inquiry identified a software problem in a particular transponder type and the European Aircraft Safety Agency (EASA) issued an Airworthiness Directive (AD) in August 2005. According to this AD, “A design deficiency causes the transponder to revert to standby mode if a change of the 4096 ATC code (also called the Mode A code) is not completed within 5 seconds. As a consequence, the SSR radar symbol and label associated with the aircraft’s position will no longer be shown on the ATC ground radar display. In addition, aircraft collision avoidance systems (ACAS) on board own and other aircraft will be compromised. Current operational procedures, typically, do not require the crew to recheck the transponder status after changing the 4096 ATC Code. This type of failure will increase ATC workload and will result in improper functioning of ACAS.” (EASA, 2005, p. 2).

Although the specific transponder failure mentioned above has already been corrected in the new transponders’ software versions, we can conclude this section observing that, even without catastrophic technical or operational failures having been identified in flight N600XL’s transponder after more than a year of investigations in different organizations involving two countries, on September 29–2006 an aircraft remained invisible for about 50 min in the Brasilia RVSM controlled air space, without a transponder signal. Therefore, we add normal equipment to the Dekker (2006) citation. Therefore, in complex systems, accidents occur with “Normal people working in normal organizations, with normal equipment” considering that the transponder functioned (and it is still functioning) in a normal way.

To conclude this point, we argue that a search-for-failure in the transponder (mal)functioning or about human error in its
operation (as the traditional accident analysis does) would not be sufficient to explain why such an important safe-critical function (collision avoidance) remained out of operation without being noticed during this collision. As already pointed out in Section 5.3, the overall system function and the interactions agents perform in a daily basis must be addressed to explain the mechanisms that allow the function to fail.

5.5. The Brasilia ACC and their communications with flight N600XL

After the flight plan misunderstanding and the TCAS in standby mode, flight N600XL was flying in the UZ6 dual lane airway in the wrong direction near Brasilia. In this situation, the communication loop between flight N600XL’s crew and the Brasilia ACC became the last barrier to tragedy. The fundamental issues about the quality of the communication feedback loops, and how they can affect system safety have already been addressed (see Carvalho et al., 2007). In the following sections, we will describe how and why this last safety barrier did not function to avoid this accident.

5.5.1. What the Brasilia ACC controller actually saw

During the investigations, the representations of flight N600XL on the Brasilia ACC controller radar screen were reproduced. We use this information to show what the controller was actually seeing as the flight progressed. In Fig. 6, we show a radar screenshot of the Brasilia ACC. Flight N600XL, with its main flight data, is represented by the target symbol and a data block.

The meaning of the data block is explained in Fig. 7. The aircraft altitude information is located on the second line of the data block. This line is composed of three segments: a three digit number, a symbol, and another three digit number. The three digits on the left side of the second line represent the aircraft’s altitude (usually the last surveillance radar information). The symbol between the numbers is a status indicator and specifies the type of altitude information displayed by the digits to its left (actual, estimated) and its immediate future development (stable, climbing, descending). A “=” (equals) symbol indicates level flight, a “+” (plus) symbol indicates a climbing aircraft, and a “−” (minus) symbol indicates a descending aircraft. The display of the =, +, or − symbols also provides visual confirmation to the controller that the aircraft’s transponder is providing Mode C or S altitude information to air traffic control. Modes C and S of the transponder report altitude data to air traffic control that is, in turn, displayed on the radarscope in hundred foot increments. The Z (capital letter Z) symbol indicates that the aircraft altitude is not transponder reported but is estimated by the primary radar. The three digits on the right hand side of the second line of the data block represent the altitude authorized by the flight plan for that particular flight segment.

Each controller is responsible for the surveillance of specific sectors of the controlled air space that are displayed in his/her workplace. The sectors are displayed on the controller radar screen or radarscope. The screen of workplace 8 that controls sectors 7 (the sector of the collision), 8 and 9 at 15:55 (four minutes after flight N600XL entered sector 7) is presented in Fig. 8. The colors (the black background and white lines) were changed for better
The recorder confirms that flight N600XL remained level at Flight Level 370 until the collision. However, the information received from the height-finding radar estimated the aircraft at a different altitude with nearly every ten second sweep of the radarscope (at 16:29:58 the indicated level was 348). The estimated altitudes varied considerably not only from the aircraft’s actual altitude, but also from the flight’s planned altitude, depicted in the right-hand portion of the second line of the data block. When it was reaching TERES notification point, there was an intermittent detection from primary radar, and flight N600XL disappeared from the controller screen at 16:30:08 and appeared again at 16:31:28, as shown in Fig. 11.

5.5.2. The communication problems

Table 4 summarizes the major events and communication attempts that occurred in the Brasilia ACC regarding flight N600XL.

The communication frequencies used in the controlled air space are divided according to the sector the aircraft is currently flying in and are described in the aeronautical charts. Each aircraft must set its equipment to a communications frequency from which it can receive and transmit voice communications. From the other side, the ACC control center transmits in broadcast, in all frequencies activated for each sector. Therefore, its transmissions should be received by all aircraft flying in the region. Table 5 shows the frequencies used in sectors 7, 8 and 9, controlled by workstation 8 of the Brasilia ACC.

Based on the data presented in Tables 4 and 5 we note that the communications difficulties were related to the frequencies selected, not to flaws in the radio system. The first 6 attempts made by Brasilia ACC used the frequency of 125.05 and were not received in flight N600XL’s radio system. This occurred probably because flight N600XL was reaching the limit of the communication range of the sector 7 frequency, in need of a new frequency. Indeed, in his second attempt, the controller tried to communicate a new frequency to flight N600XL’s crew. Flight N600XL’s first attempts used the 123.30 and 133.05 frequencies, which were not activated in workplace 8. Finally, the last and only successful communication occurred on the 135.90 frequency. However, at the moment of this communication flight N600XL was leaving sector 7 and entering the Amazon ACC region. The Brasilia ACC registered clearly the visualization on paper. On the radar screen, in addition to the targets information (aircraft flying) the controller also has the flight plan information in the electronic flight strips, displayed in the vertical column on the right side of the screen.

The first changes in flight N600XL’s data block occurred when the aircraft entered sector 7. It appeared to the controller as presented in Fig. 9 (with inverted colors).

At 16:01 flight N600XL’s transponder failed and the ACC screen changed automatically to that presented in Fig. 10.

Even without the transponder information, the N600XL data block continues on the screen because the system “understands” that the target detected by the primary radar is the same aircraft that earlier transmitted the identification code. Therefore, the N600XL data block continues on the screen based on the correlation of the target position and the previous information received from the secondary radar.

Under the Brazilian ATC regulations (ICA 100-12), when an aircraft’s transponder ceases to present the required response signal in the RVSM air space (the case of Brasilia Vertical line), the controller must ask the pilot to verify the functioning of the transponder. Besides that, in the Reduced Vertical Separation Minimum air space, a vertical separation of 1000 ft is permitted only to appropriately equipped aircraft (i.e., those with, among other things, a functioning transponder that has Mode C and Mode S capabilities). With the loss of the transponder signal, ATC was required to suspend RVSM operations for flight N600XL and provide at least 2000 ft of vertical separation (Non-RVSM separation in the Upper Control Area is 2000 ft) between it and other traffic along its route of flight. This included flight 1907. Even considering the importance that the loss of the transponder signal has in the regulations and in the controller procedures, there is no active warning signal delivered by the system. The controller must actively seek for the information on the screen – the symbol changes in the aircraft data blocks – as described above.

On the three screens presented in Fig. 11, we see the primary radar indications with level variations, and when flight N600XL’s target disappeared completely from the radar screen, before going out of sector 7 (still without a transponder signal). The flight data recorder confirms that flight N600XL remained level at Flight Level 370 until the collision. However, the information received from the height-finding radar estimated the aircraft at a different altitude with nearly every ten second sweep of the radarscope (at 16:29:58 the indicated level was 348). The estimated altitudes varied considerably not only from the aircraft’s actual altitude, but also from the flight’s planned altitude, depicted in the right-hand portion of the second line of the data block. When it was reaching TERES notification point, there was an intermittent detection from primary radar, and flight N600XL disappeared from the controller screen at 16:30:08 and appeared again at 16:31:28, as shown in Fig. 11.

5.5.2. The communication problems

Table 4 summarizes the major events and communication attempts that occurred in the Brasilia ACC regarding flight N600XL.

The communication frequencies used in the controlled air space are divided according to the sector the aircraft is currently flying in and are described in the aeronautical charts. Each aircraft must set its equipment to a communications frequency from which it can receive and transmit voice communications. From the other side, the ACC control center transmits in broadcast, in all frequencies activated for each sector. Therefore, its transmissions should be received by all aircraft flying in the region. Table 5 shows the frequencies used in sectors 7, 8 and 9, controlled by workstation 8 of the Brasilia ACC.

Based on the data presented in Tables 4 and 5 we note that the communications difficulties were related to the frequencies selected, not to flaws in the radio system. The first 6 attempts made by Brasilia ACC used the frequency of 125.05 and were not received in flight N600XL’s radio system. This occurred probably because flight N600XL was reaching the limit of the communication range of the sector 7 frequency, in need of a new frequency. Indeed, in his second attempt, the controller tried to communicate a new frequency to flight N600XL’s crew. Flight N600XL’s first attempts used the 123.30 and 133.05 frequencies, which were not activated in workplace 8. Finally, the last and only successful communication occurred on the 135.90 frequency. However, at the moment of this communication flight N600XL was leaving sector 7 and entering the Amazon ACC region. The Brasilia ACC registered clearly the
communications of flight GLO1907 with the Amazon ACC just before the collision, during ATC service transfer from the Amazon ACC to Brasilia ACC, on the 125.20 frequency, which indicated that the ATC radio system was working properly at that moment, in a normal way.

5.5.3. The controllers’ inaction

As already noted long ago by Dailey (1984), “The central skill of the controller seems to the ability to respond to a variety of quantitative inputs about several aircraft simultaneously and to form a continuously changing mental picture to be used as basis for
planning and controlling the courses of the aircraft” (pp 134). Therefore, the aim of the air traffic controller is to construct a mental model that matches the dynamics and evolution of the air traffic situation. This mental model is constructed by a continuous comparison of the current air traffic situation with the anticipation of the situation in the near future, to plan required actions. After Endsley (1995), this special type of mental representation is called Situation Awareness (SA). To achieve an adequate SA, the controller must understand the current air traffic situation monitoring the radarscope and other information sources (flight plans, air-charts, communication frequencies), and anticipate the future aircraft trajectories using sector maps, aircraft velocities and altitudes, flight strips, communication with pilots and co-ordination with other controllers. Therefore, the controller’s work activity requires active monitoring and control strategies to cope with workload variations, maintaining the SA that is paramount to ensure that the mental picture remains consistent with the actual situation.

The dominant paradigm of the post hoc analysis of human error in accidents indicates that many operational errors can be attributed to lack of SA or to SA problems (e.g. Jones and Endsley, 1996), and in this accident the investigations reached similar conclusions. According to the final report of the Senate investigation, the accident was caused by a chain of human errors (Senado Federal, 2007), including the ATC controllers’ failures in providing adequate air traffic services to flight N600XL to ensure that it was properly separated from other traffic (flight GLO1907 included). These failures were related to monitoring the radarscope over an extended period without perceiving the potential conflict situation, procedure non-compliance (not terminating RVSM operation for flight N600XL after the loss of Mode C transponder flight level information), failures in the co-ordination with other controllers (e.g. transfer of control between sectors should include any abnormal communications status or uncertainties about flight data; incomplete relief briefings during shift changeovers), failures in taking immediate actions (e.g. to locate an aircraft which has been simultaneously or unexpectedly lost from radar and radio).

In fact, the main indications of “abnormal” behavior of flight N600XL can be summarized as:

- Actual flight level different from the planned flight level;
- Transponder ceased to reply the ATC surveillance radar (2 signals – Z letter in the data block and target symbol change);
- Erratic level variation (FL331 to FL396);
- The disappearance of the aircraft inside sector 7 (before leaving sector 7).

We note that after the first automatic change in the radarscope (15:55), when flight N600XL entered in sector 7, the radarscope indicated the loss of transponder returns (16:02), and differences between the actual and planned flight levels. The controller on duty, despite these screen changes, remained almost 22 minutes without taking any action. After the shift changeover at workstation 8 (16:17), the substitute controller took 10 min to try, without success, to contact flight N600XL’s crew.
However, how much time is needed to perceive screen changes and more importantly, consider that they are important enough to act? Can other controllers working in the same system behave in the same way? In such a cluttered display (Fig. 8 is only a small part of the radar screen where target (aircraft) data blocks are superimposed on each other, making their visualization difficult), an automatic change made by the system does not favor immediate perception by the controller. In fact, the automatic change of the “cleared altitude” in the data block, without any controller action or effective warning signal, can be easily overlooked by controllers and is potentially misleading, especially if we consider that the controller normally has his/her attention divided among several data blocks (aircraft under his/her responsibility) on the screen. Indeed, Means et al.’s (1988) cognitive task analysis indicates that controllers are more aware of flight data of aircraft that they had performed control actions on than of aircraft that they had not carried out control actions on. Barber (1988), analyzing the mid-air collision in Yugoslavia back in 1976, had already noted that in a divided-attention task when people try to pay attention to two or more simultaneous tasks, the consequences of divided-attention could be disastrous. Perception of the environment characteristics depends on the attention that allows our cognitive processes to take in selected aspects of our sensory world in an efficient and accurate manner (Palmer, 1999). Therefore, small screen changes without warning, to be quickly perceived, require a concentration of mental activity – attention – only on these inputs, which is very difficult in divided-attention tasks.

The other issue is: Is perceiving the changes enough to trigger a controller action? This depends on the strategies controllers normally use to control their workload and cognitive demands.
inaccuracy are frequent enough in a way that “abnormal” indications were being considered “normal”, then the ETTO principle and associated heuristics (these things always happen, it is not important to act now, the system is always changing symbols) function as an important factor for the construction of cognitive strategies. In this situation, we cannot attribute the cause of the accident to a chain of human errors. Doing so, we will be blind to address the real safety threats throughout the ATC system functioning.

5.5.4. The workplace in the Brasilia ACC during the event

All flight controllers who in some way acted in this event (including those who worked during the clearance of the N600XL flight in Sao Jose) are military controllers, sergeants of the Brazilian Air Force, in a military activity, control of the air space, a task that is attributed by Brazilian law to the Brazilian Air Force. The controllers work in military workplaces, the Air Space Control Centers (ACCs), all under Department of Air Space Control (DECEA) administration, part of the structure of the Air Force Command (see Fig. 2).

In the ACCs, each workplace has 2 controllers, a main controller and an assistant controller. A senior controller supervises each 2 or 3 workplaces. The investigation showed that at workplace 8 the controllers that monitored sector 7 (including flight N600XL) did not have an excessive number of aircraft under control (the maximum number of aircraft is 12) during the period before collision, and were therefore working in a low workload situation. Despite the variation of the on screen indications, the investigation concluded that there was no problem in the radar system software/hardware, and the system functioned as it was designed to function. The investigation also emphasized that there were no wrong indications or unexpected signals on the radarscope (Câmara dos Deputados, 2007). Therefore, we can conclude that the systems normally function as described above. To explain their actions the controllers said in their testimonies (Câmara dos Deputados, 2007):

– Main controller: Before flight N600XL entered sector 7, he communicated with the crew verifying that the aircraft was at level 370 (the correct level at that moment). He did not anticipate the need to change the level when the aircraft entered sector 7. In the period from 18:55 (aircraft entered sector 7) up to 19:17 (shift changeover), he perceived the loss of the surveillance radar, but it did not alarm him. He said he was satisfied with the information coming from the primary radar. He informed his relief controller that flight N600XL was at level 360, because he knew about the inaccuracy of the primary radar information and assumed that the aircraft was following the flight plan that was displayed in the electronic strips.

– Assistant controller: He perceived that the N600XL did not have complete information on the radar screen, and considered that to be a normal situation. Even though uninformed of the aircraft’s actual altitude, he coordinated with the Amazon ACC controller the level of 360, based on the electronic flight strip indication.

– Controller after shift changeover: He received flight N600XL at level 360 and did not question the outgoing controller. He said he had noticed the abnormal transponder functioning, and tried 8 times to contact flight N600XL. However, he did not take any action to avoid the conflict.

6. Conclusion

The accident described here opened a window onto the functioning of the Brazilian air traffic system. As already noted in many ergonomic field studies, in safety-critical systems operators’ cognitive strategies to maintain situation awareness are shaped by the real conditions under which [they | operators] perform their work, where resource limitations and uncertainty severely constrain the choices and action opportunities. Cognitive task analysis has been widely used (unfortunately not in Brazil) to examine how air traffic controllers develop cognitive strategies to manage their workload maintaining situation awareness. However, most of the research focus is on how extreme traffic situations influence the cognitive control strategies developed by the controllers, rather than on how normal controllers working with normal equipment in normal organizations shape their cognitive strategies. In the events described here, we saw the influence of the working constraints in shaping cognitive strategies that affect system safety.

During the antecedents of the collision, there was no special air traffic situation, no catastrophic equipment failure equipment, and no trigger event as required in traditional accident models. This accident emerges as a complex phenomenon within the normal variability of the system functioning. This tragedy and many other accidents in complex systems raise serious questions on how safety is thought about in complex safety-critical systems. This accident and accidents in other safety-critical systems have complex patterns of emergence, where coincidences, unexpected links, and resonance, substitute the old bullets such as equipment failure probability, linear combinations of failures, human errors, and so forth. Therefore, safety managers and engineers should review, among many other things, how safety barriers should be used to be effective in a defense-in-depth safety approach. The use of safety barriers to stop the propagation of some trigger event cannot avoid this type of accident simply because, as we have seen in this study, there is nothing to be stopped. Almost didactically we saw all the barriers developed to avoid mid-air collisions melt down in a situation where everything functioned normally.

References
