Summary of the FAST Analysis of the Top Priority Area of Change “Increasing Reliance on Flight Deck Automation”

Prepared for the FAST-ConOps workshops
Organized by EUROCONTROL in June and July 2006

Introduction

The FAST Phase 3 report summarizing the FAST analysis of this highest priority Area of Change AC [Aircraft] 13 “Increasing Reliance on Flight Deck Automation” was presented to the JSSI StG in January 2004.
Hazards, hazards themes, Technology Watch Items and Recommendations were identified. The JSS StG has not officially approved these.
The analysis uses an integrated Air Ground Space system approach and identifies priorities at different time horizons.
This summary prepared for the FAST-ConOps workshops organized by EUROCONTROL in June and July 2006, addresses the following material:

1. FAST Four Hazard Themes and Related Technology Watch Items

This first Section also defines the vision of the future adopted by FAST as a basis for its analysis.

Theme I: GLOBAL AIR–GROUND–SPACE SYSTEM ISSUES

Introduction:

By the year 2020, we expect aircraft, Air Traffic Control Centers, Airline Operation Centers, and satellites to be the nodes of an integrated Air Ground Space System (AGS) that will operate during the all phases of flight (gate-to-gate) and communicate through data-link.
The airspace system will undergo significant changes (e.g. free routing/free flight; new airspace classification; development of 4 Dimensions trajectories) that will change the way the different actors or “stakeholders” will operate, individually and globally, co-ordinate their activities, and co-operate.
The progressive development of such a “distributed multi-agent system” in which artificial agents, automation, computers, data-bases and even Artificial Intelligence will play an important role is a response to the challenges posed to the future civil aviation. That is: increased airspace capacity, better respect to the environment (in a “sustainable growth” approach), and improved safety.

The various changes that will affect the aviation system are therefore oriented towards improved performance and safety. But this future global Air-Ground-Space system will also give rise to a series of Hazards, which require attention today. FAST has tried to identify those hazards and to formulate recommendations, or proposals for future work, in order to prevent, control, or manage them in a proactive way.

Seven hazards grouped in one theme:

With the above perspective in mind, seven Hazards out of the 21 prioritized ones form the "Global Air-Ground-Space System Issues" theme. These seven Hazards are:

1) Hazards inherent to new airspace paradigm and from a large, distributed and inter-related Air / Ground / Space (AGS) system: Failure to integrate onboard and ground systems, e.g. control functions, data link, personnel, responsibilities
   - ATM/ATC and aircraft control functions (distributed multi-agent control system)
   - Data link with many outside partners: ATM / ATC and SCC (under the Fully Automated Flight hypothesis)
   ATM / ATC / OPS / SCC (under the FAF hypothesis) / Flight Crew / Cabin Crew, including security and medical personnel (in particular for FAF) / Maintenance (in particular for FAF): **Env 2.1** (future-medium)
2) Flight Crews - Conflict between air/ground information sources: Inadequate escape maneuver decision due to conflict between different information sources (e.g. TCAS, ATC verbal messages, data link) and lack of explicit prioritization: **Live 4.1** (current)
3) CNS/ATM/ATC and SCC – Adverse conditions / failure / emergency / crisis mgt issues**: Live 15.4** (future-near)
4) CNS/ATM/ATC and SCC – Crew / automation interactions issues **--**–Local or wide-area loss of control may result due to data link failures, unintentional or intended interference or other factors: **Live 13.2** (future-medium)
5) Hazards inherent to new airspace paradigm and from a large, distributed and inter-related Air / Ground / Space (AGS) system -- Loss of situation awareness (global, local): **Env 2.3** (future-near)
6) Hazards inherent to new airspace paradigm and from a large, distributed and inter-related Air / Ground / Space (AGS) system -- Inability of individual & total system to deal with aircraft not behaving as expected, with sudden weather problem, airport closure, air or ground accident, etc. (more serious hazard regarding Fully Automated Flight): **Env 2.5** (future-medium)
7) Inadequate processes for certification of computer software (including interactions with other software systems and artificial intelligence) onboard the aircraft and in the larger airspace system (C1, ANS20): **Soft 2.8** (future-near)

One of these hazards, **Live 4.1** is already present today, while the others should start to appear from future-near (1 to 5 years) to future-medium (5 to 10 years). In addition, all of them of them are expected to *evolve* as time is passing by and changes are introduced in the global AGS system.

Perspective:

A new AGS system

In the next twenty years, we expect aircraft, Air Traffic Control Centers, Airline Operation Centers, and satellites are the nodes of an integrated Air Ground Space System (AGS) that will operate during the all phases of flight (gate-to-gate) and communicate through data-link. This AGS system recognizes the interdependence of stakeholder operational decisions, e.g., Collaborative Decision Making, Flexible Use of Airspace.

The airspace system will undergo significant changes (e.g. free routing/free flight; new airspace classification; development of 4 Dimensions trajectories).
This is likely to occur step by step, such system will be performance oriented, but *compatibility and safety* will come first.

Technological moves

Older technologies and modern technologies will co-exist both for aircraft and ground systems, at least in a transitory period.
Human operators remain in the loop but are assisted by automation tools and use elaborate displays. Automation tools will be supported by sophisticated databases. Data and warning/alert information will be generated at an ever-increasing pace within the aviation system and these data will play an increasingly important role in flight critical situations. These data are stored in air and ground repositories and the information generated from the data will be presented to both airborne and ground-based operators.

More generally, there will be an increasing use of computer software, including complex software systems and artificial intelligence. Specialized techniques and tools may in particular be used to support co-operation and Collaborative Decision Making, such as Groupware, Computer Support to Cooperative Work (CSCW) and Computer-based Operating Aids and Management Systems.

On the way to Fully Automated Flight

New vehicles such as Vertical Take-Off and Landing aircraft (VTOL) (Other than helicopters) and Un-inhabited Aerial Vehicle (UAV) may use the airspace. Furthermore, single pilot or supervisory pilot freighter operations might appear in the decade 2010-2020 and might pave the way in the longer term for Commercial Fully Automated Flight.

Discussion:

Globalization, failure propagation and required system responses

In the future airspace paradigm and AGS system, failures, unintended or intended interferences (including security infringements), human errors and other adverse conditions (i.e., weather) may have global effects such as loss of situation awareness or loss of control. Such failures could be local or global, e.g., GPS failures.

Interactions, interferences and failure propagation should be assessed from the design stage and assumptions and requirements made at the design stage should be monitored all through the life cycle.

The system should ideally be designed, operated and maintained to ensure that failures (intended and unintended) will be prevented or won't propagate through the system (containment). Because this might not be always possible, global multi-actors responses e.g., crisis management, need to be provided to global, or "globalized" failures. All interested actors should be adequately trained to prevent and/or manage such failures and manage crises, individually and jointly.

Computer, software, and Artificial Intelligence issues

All six automation topics identify computer software safety and security issues, either as inherent hazards or as hazards generated by interactions. Artificial Intelligence and rapid pace of software and technology development were identified as two of these interactions.

In particular the following issues were raised:

1) What the system learns is not predictable and may not be shared with subsequent operators;
2) Certification issues with Artificial Intelligence (e.g. neural nets, fuzzy logic), etc.;

3) Formal V&V techniques lacking, increasing demand for complex V&V;
4) Inconsistent versions of software within the same fleet;
5) CRM adaptation to artificial intelligence automation;
6) Malicious code and/or data (e.g. virus, Trojan horse, intentional uplink corruption).

In addition current issues were also identified, such as configuration management, programming errors, data corruption, incorrect or partial requirements definition, update and upgrade issues. As such issues are dealt with by current certification standards, no proposals have been made hereunder to address them.

Air-ground inconsistencies: the need for conflict resolution

Unsafe situations may also develop when there are inconsistencies between air/ground databases as well as conflicts between alerts and warnings generated from separate systems. In absence of clear prioritization or conflict resolution rule, the way in which flight crew and ground controllers prioritize and respond to these inconsistencies and conflicts are subject to their own interpretation, in particular of the related information from automated systems as TCAS, EGPWS and systems to prevent runway incursion.

The inadequate escape maneuver decisions due to conflict between different information sources (e.g. TCAS, ATC verbal messages, data link) and lack of explicit prioritisation that were already experienced nowadays prefigure what the situation could look like in the future multi-agent system. In the future, the wide variety of information sources available to the flight crew will therefore require strict prioritization of cockpit warnings and alerts.

Related Human Factor issues

There are significant Human Factors issues in how to integrate and differentiate presentation of these alerts. Issues such as sensory modality to use for warning/alert presentation (visual, auditory, etc.), color, clutter, etc. must be addressed.

Furthermore, in accordance with HF principles, systems should also be designed so that human errors (or, in the SHEL model terms, "Human-Software-Hardware-Environment interaction breakdowns") which may reasonably be expected to occur in service:

a) Are not contributed to by design characteristics.
b) Can be detected by the operators (directly or indirectly), or if not readily detectable, the system must be tolerant of such error
c) Have means to be reversed or recovered from, or in not possible, the effect on the system must be evident or not result in catastrophic outcome.

Technology Watch Items:

Monitoring the following advances in technology should help determining the possible realization and evolution of these Global Air-Ground-Space System related Hazards. 12 topics of concern have been identified. They are presented below without prioritisation:

1) It is advisable to maintain a close monitoring of the strategies developed by bodies responsible for Air Navigation Services such as the EUROCONTROL ATM 2000+ strategy. In a similar fashion it is advisable to also monitor the development of Strategic Research Agenda such as ACARE in Europe that give good indications of the technologies being developed.
2) Emergence of FMS Systems designed and certified for sole means of navigation.
3) Decommission plans of ground navigation aids.
4) Systemic use of satellite for communication, navigation and surveillance and development of associated technologies and services (e.g. Ground or Space

Based Augmentation Systems (GBAS, SBAS); Automatic Dependant Surveillance- Broadcast (ADS-B); Data-link Technologies (ACARS; VDL 4; High Band-with)

5) Free-flight / free-routing plans such as Free Routing Airspace Plans (FRAP) or Mediterranean Free Flight (MFF).
6) Introduction of new warning systems and alerting techniques, and consolidation/integration of warnings and alerts involving problems with internal vehicle systems (such as HUMS) with those from external traffic, terrain, and weather avoidance/alerting systems.
7) Emergence of 4D trajectories.
8) Development of system using Artificial Intelligence (e.g. neural nets, fuzzy logic). Monitoring of general and applied research in these areas should be made to identify scientific breakthroughs.
9) Development of “intelligent” aircraft (e.g. active flow control using a combination of propulsive forces; micro surface actuators and fluidic device operated by an intelligent flight control system; Intelligent system of smart sensors, microprocessors and adaptive control will monitor performance and environment and help operators to avoid danger).
10) Development of “intelligent” vehicles (e.g. smart cars) as cross-fertilization can be very beneficial.
11) Nanotechnologies, new computing techniques such as molecular computing and intelligent materials. Monitoring of general and applied research should be made in these areas to identify scientific breakthroughs.
12) In addition, significant developments should be tracked in the following technological domains: Collaborative decision making (CDM); Computer Support to Cooperative Work (CSCW), Computer-based operating aids and management systems, Groupware, Monitoring and Supervisory Control, Industrial, Human, and Cognitive Engineering (Main application: ATM-ATC and SCC control rooms and operations; crisis management).
13) In addition, significant developments should be tracked in the following technological domains (supported in particular by the EC in the 6^{th} FWP): eSafety of road and air transport and eHealth, Information and Communications Networks based upon all-optical technologies and new Internet protocols, advanced Middleware, global networking and distributed architectures, Multimodal Interfaces, Semantic-based knowledge systems, Networked audio-visual systems, technology-enhanced learning, advanced displays, optical, opto-electronic, photonic functional components, open development platforms for software and services, cognitive systems, GRID-based Systems for solving complex problems, risk management.

Risk Monitoring:

Risk monitoring should be performed at the AGS system level by developing integrated operational feed-back and feed-forward from / to the manufacturers, regulators, education and training organizations, and other relevant actors.

All actors of the AGS system should work with the rest of the aviation community to develop processes that will establish and maintain historical documentation containing the requirements, design details and assumptions that were made during initial design and any subsequent changes to the system. This process should include the establishment of reporting requirements and preservation of in-service feedback.

Because the future AGS is bound to evolve, new Hazards can emerge over time. All actors should therefore monitor the frequency and trends of events (e.g. system/ component failures) arising from unknown or unexpected reasons.

In addition, it is recommended to monitor the realization of the AGS related Hazards over time in order to continually and timely update the list of hazards identified by FAST and the corresponding recommendations or proposals for future work.

Theme II: FLIGHT CREW-AUTOMATION INTERACTIONS ISSUES

Introduction:

Automation, as a concept, is the allocation of functions to machines that would otherwise be allocated to humans. The term is also used to refer to the machines, which perform those functions. Flight deck automation, therefore, consists of machines on the commercial transport aircraft flight deck, which perform functions otherwise performed by pilots. Current flight deck automation includes autopilots, flight path management systems, electronic flight instrument systems, and warning and alerting systems.

At the larger level of the Total AGS System, automation should also contribute to enhancing the awareness of the global AGS distributed multi-agents control, command and management system to all personnel concerned: flight crew, cabin crew, ATM/ATC staff and maintenance personnel, and Strategic Command and Control (SCC) personnel under the Fully Automated Flight (FAF) hypothesis.

With the advent of advanced technology, so called "glass cockpit", commercial transport aircraft and the transfer of safety-critical functions away from human control, pilots, scientists, and aviation safety experts have expressed concerns about the safety of flight deck automation. For example, Wiener (1989) surveyed a group of pilots of advanced technology commercial transport aircraft and found significant concerns. Based on incident and accident data, Billings (1991a, 1994) cited problems with flight deck automation and proposed a more human-centered approach to design and use.

New automated control, command and assistance systems may modify the ways the different personnel will interact with the technology and between themselves, not only in the cockpit but also in the other nodes of the global AGS system. Some problems are likely to be resolved and other to be reinforced, while new problems due to the unique characteristics of the future global AGS system will probably arise. Among them are for instance the difficulty for each agent to be and remain aware of the state and dynamic behavior of the other agents, human and artificial, within the global system, and the difficulty to operate in case of failure, breakdown or inoperability of the automated systems.

In order to get the best possible results in terms of efficiency and safety from the future automation, “accompanying measures” such as adapted regulations, procedures, education and training, in particular Crew Resource Management (CRM) are therefore recommended.

Four hazards grouped in one theme:

Four Hazards out of the 21 prioritized ones form the “Flight Crew-Automation Interactions Issues” theme. These four Hazards are:

1. Flight Crews - Crew Automation Interactions Issues: Abnormal/emergency situations combined with automation breakdown or failure (subtle or sudden) may create situations exceeding crew experience or training level: **Live 6.11** (current)
2. Flight Crews - Crew Automation Interactions Issues: A poor automation logic/interface may lead to decision-making based on false or misleading assumptions: **Live 6.1.4** (future-near)
3. Operations - Flight operations / interactions with automation: Loss of automation behavior awareness due to complexity of automation modes. Pilot needs to know what the airplane “thinks” is going on (matching expectations) (C3): **Soft 6.3** (current)
4. Flight crews - Crew-automation interactions issues: Predominant use of automation may cause aircrew to have trouble performing traditionally simple

operations such as manually switching to other runways, or overriding the autopilot in tight situations. Lack of aircrew training and/or experience coupled with manual flight in highly automated airplanes may lead to loss of aircraft control in unusual situations such as upsets, traffic avoidance or maneuvering. Loss of basic piloting skills through further automation may increase this problem further: **Live 6.2** (current)

Three of these Hazards are already present today and one is foreseen in the near future. But all of them are expected to *evolve* in the future AGS system.

Perspective:

The introduction of Glass Cockpit technology into modern airline aircraft has shown that there are a lot of issues associated with flight mode confusion as well as the complexity or perceived complexity of straightforward tasks by flight crew.

Fatal accidents and significant incidents and "near misses" have occurred due to mode confusion leading to loss of situation awareness and loss of control. Information regarding observed instances of flight crew mode confusion is well documented (e.g. CAST Safety Enhancement-36).

Some loss of control accidents/incidents involved cockpit displays of engine parameters, flight information and auto flight system mode status as contributory factors. The problems centered on not having sufficient, obvious and unambiguous information to the pilot to adequately assess the aircraft status and then to accomplish the appropriate action to resolve problems (CAST SE-34). In some cases, the problem could also be that the pilot has to interpret too much information's.

Changed training and operational requirements have also become important issues as well as the development and maintenance of manual flying skills. During times of high demand and low supply of experienced pilots (which is today the case for instance in South-East Asia), basic training of manual flight may be minimal and as low as a few hundred flight hours on light aircraft before beginning training on highly automated aircraft in a very different weight class than the aircraft and simulators used during the training towards the license.

Predominant use of automation may cause aircrew to have trouble performing traditionally simple operations such as manually switching to other runways, or overriding the autopilot in tight situations. Lack of aircrew training and/or experience coupled with manual flight in highly automated airplanes may more easily lead to loss of aircraft control in unusual situations such as upsets, traffic avoidance or maneuvering. Loss of basic piloting skills through further dependency on automation may increase this problem further.

Nevertheless, to partially address this problem, the two main commercial airplane manufacturers have introduced a flight envelope protection to reduce the risk of loss of control on their new generation of aircrafts. In addition, Fokker 70 & Fokker 100 aircraft also have envelope protection, while the new Embraer 170-195 family has speed protection.

Finally, design changes, by nature, take a long time and cost a lot of money. Incorporating new safety features into new aircraft designs is technically feasible and desirable. However, it may take many years for these changes to have a significant impact on overall fleet safety, given the time it takes to develop a new aircraft and for these aircraft to become a significant part of the fleet (CAST SE-36).

Discussion:

<u>Various sorts of changes</u>

The hazards associated with advances in cockpit technology have to be explored in order to make appropriate recommendations. These hazards are possibly related to both physical and psychological changes that flight crew have been, and will be, subjected to.
These changes have in some cases had the effect of inducing a misunderstanding by the flight crew of the automation behavior and consequently have led to incorrect decision making in both critical and non-critical situations.

Changes to certification rules normally only affect new aircraft designs; therefore any near-term benefits to be realized through retrofit of the existing fleet require voluntary implementation by manufacturers and operators (CAST SE-36).
The trend is for pilots to have fewer flight hours in armed forces or lighter commercial aviation than before when upgrading /downgrading to medium/large commercial transports with highly automated cockpits, as well as less actual prior stick time. Better automation and flight planning may have decreased previous exposure to conditions such as adverse weather, saturated airspace, etc.

Difficulties in interacting with automation

Problems have arisen with the development and implementation of logical and user-friendly man-machine interfaces such as systems used in previous versions of same type certificated aircraft when they are updated and automation developed in newer generation of same aircraft. In the past this issue has not been completely addressed by the manufacturers and the regulators.

There is plenty of evidence (coming for instance from LOSA, flight checks, simulator training, accident and incident analysis and surveys) that flight crews (particularly those new on type) do not always fully understand what the automation is doing and want to override it even if functioning properly.
It has also been shown that flight crews do not always understand the information being presented to them in highly automated cockpits and make errors in diagnostic analysis and decision-making. The reason for this may be inadequate training, flight department operational policies or poorly designed man-machine interfaces.

In addition, actual range of pilot behavior (cultural/CRM/responses to automation failures) and skill levels have not always been understood by designers.
Poor understanding of what operation the flight deck automation is commanding the aircraft to perform has the potential to increase the stress and fatigue levels of the flight crew. This can have an adverse effect on the decision making process.

On the other hand, pilots fully familiar with flight deck automation have brought themselves and the aircraft in extremely dangerous situations, not being able to program themselves out of it, nor disconnecting the automation to hand fly themselves to safety. Reasons for this may include pilot fatigue, sudden or subtle developments of automation failures resulting on "automation surprises" and the like.

Technology Watch Items:

Monitoring the following signs and advances in technology should help determining if these Flight Crew – Automation Interactions associated hazards are coming about:

1. Implementation of new technology in future cockpits modifying crew interface (e.g. Emergence of 4D trajectories) and modifying crew-automation interaction (e.g. systems using Artificial Intelligence).
2. Introduction of "Free flight" concept introducing new automation modes (e.g. Free-flight / free-routing plans such as Free Routing Airspace Plans (FRAP) or Mediterranean Free Flight (MFF)).

3. Emergence of FMS Systems designed and certified for sole means of navigation.
4. Decommission plans of ground navigation aids.
5. Systemic use of satellite for communication, navigation and surveillance and development of associated technologies and services (e.g. Ground or Space Based Augmentation Systems (GBAS, SBAS); Automatic Dependant Surveillance- Broadcast (ADS-B); Data-link Technologies (ACARS; VDL 4; High Band-with).
6. Introduction of new warning systems and alerting techniques, and consolidation/integration of warnings and alerts involving problems with internal vehicle systems (such as HUMS) with those from external traffic, terrain, and weather.
7. In addition, this list should be revisited on a regular basis or after significant events (e.g. accidents, critical incidents, near-misses). The use of technology watch items is therefore linked to Risk Management.

Risk Monitoring:

The level of operational risk should be assessed with respect to the crew behavior whist operating with a highly automated cockpit.

It should be determined whether risk of accident / incident is increased or decreased through greater reliance on technology.

Information reporting and sharing, in particular between operators and manufacturers, should be used as a tool in order to identify problems.

Theme III: GENERAL THREATS

Introduction:

Five Hazards, considered as affecting several area's, in particular "Crew Automation issues", "Air to Ground Systems Interactions", and "Fully Automated Flights" have been classified as General Threats.

Three of the threats are in Hardware - one already present today and two in the future-near category, the two others are in Liveware - one present today, one in the future-near category. This highlights the fact that hardware including its software and Liveware also present interacting new hazards especially on the interfaces.

Five hazards grouped in one theme:

Five main hazards are listed in this theme General Threats, two of which were already grouped for producing recommendations.

- **LIVE14.1** addresses the use of automation or of automated systems outside of intended function that may cause safety problems.
- **Hard 4.4b** addresses compatibility, integration, configuration management issues (including for Human-Machine Interfaces and Software applications): Failure or malfunction caused by incorrect functional interfaces.
- **LIVE 15.5** addresses sabotage or intentional damage or degradation of systems, either through physical means or through cyber or electronic interference attacks.
- **Hard 7.4.1 and Hard 7.1b** address database integrity failure and software issues such as lack of software capability to recover from some hardware failures. Both may concur to aggravate a situation.

Perspective:

The aviation system is faced with increasing technical and business complexity. Systems now cost more than in the past, and this investment is causing extreme longevity of use of systems. The experience base for system design is eroding, with system longevity far outliving the careers of the designers, builders and the regulators that developed it. All these factors contribute to increased likelihood of unforeseen or forgotten system failures and system interface failures having major safety impact. In the far future these issues may cause increasing hazards unless systematic structures are put in place to avoid those hazards**.**

Use of systems outside intended use

Operators today sometimes use systems for tasks for which they were not intended. Four examples:

- Use of FMS as sole means to determine V speeds.
- Use of FMS as sole means of navigation.
- Use of TCAS to maintain separation.
- Use of TAWS as primary means of navigation.

There are many reasons why that occur. Some of the main reasons why systems are improperly used are as follows:

- The designers of the system make it possible to do so.
- Operators are under pressure to meet efficiency requirements and so are tempted to misuse systems.
- *Pilots perceive the technology as so compelling that they may use ad-hoc procedures.*
- *In some cases regulators allow its use under temporary conditions, e.g. FMS for PRNAV in the TMA under TGL 10.*

The human tendency is to minimize complexity and workload.

Databases

Use of databases has evolved into many aerospace applications, both on board as well as on the ground. Typical examples are databases in FMS, but also in EGPWS, TCAS, AFCAS, EICAS/ECAM/MFDS, ATC systems, etc. Use of databases is currently only in its infancy, with an exponential increase just around the corner, if only for CNS/ATM use. The same is even true for interactions where the integrated AGS will also call for an exponential increase.

Sabotage and cyber attack

Use of computer software has evolved into many aerospace applications, both on board as well as on the ground. The connections of S/W with the "outside world" are through a) Loading in the shop: Initial Program Load on the chip/EPROM, b) physical on board S/W loading by means of floppy or cable and c) logical, through a data link or wireless network. Today, the threat of cyber terrorism against aircraft is minimal. But when looking into the future airspace paradigm, with many aircraft and ground systems in a multi-agent distributed air ground [AGS] system, *ever more critical information* will be transmitted via data link, this is considered a serious threat.

Discussion:

Items for consideration:

- Increasing complexity
- Attrition of experience
- Increasing business pressure for diverse organizations building components
- Making design of very complex systems safe – recommendation for R&D
- Concise, simple, not dependant on legacy relationships
- Isolation of simple safety practices in system design

Database errors/malfunctions

Data base errors/malfunctions may lead in part to loss of situational awareness, or misleading and/or incorrect information or just a plain overload of the human being. This being the case where the right information is given at the right time, but is simply either not processed or incorrectly processed due to this situation.

Items for consideration:

- Increasing complexity that gives room for failure propagation with increased difficulty to predict.
- Interaction between component failures and S/W design
- Use of processors with ever increasing complexity. The concern is transfer of risk from current technology to future technology. All processors have the potential for errors, while RISC [Reduced Instruction Set Computer] chips minimize the chance for unknown failure modes like the Pentium 4 floating point calculation, and other, not tested processor specific risks.
- Inadequate data link protocols.
- What if a node in the system, in flight or on the ground, does not respond at all, are "light flares" (as used for sea rescue) to be used to get the non-responder to wake up?
- Use of flight critical Software to be promoted.
- Increasing number of components
- Increasing probability of multiple IEEE parts failure.
- Obsolescence of IEEE parts creates maintenance and/or configuration management issues
- Design specifications to be made compatible with very ambitious Safety requirements and systems complexity.
- Design trace ability and resources to take care of systems aging
- More involvement of automated systems in flight safety.
- Discussion placed in the frame of 1.10-7 TLS.
- Increasing importance of precursors to detect incidents that in worst cases may propagate throughout the system and end up in serious situations.

Sabotage/cyber attack

Sabotage/Cyber attack maybe the presence of unwanted and/or malicious code fed into the box, the absence of a code or the removal of a code, either directly or attached to a timing device that would allow the removal and/or destruction of a code during flight.

Hazard amplification for Data bases:

Since the use of databases will increase exponentially, ever more information will be uploaded and downloaded increasing the risk for errors. Database integrity, i.e. *"end-to-end aeronautical data integrity"* starts at the beginning, e.g., two DME's (4 nm apart) were given the same identifier and then processed through the system into the FMS. Other issues: how is certification maintained after incremental uploads?

Examples: 1. Where an Authority upon checking an EGPWS in a simulator could not find the highest obstacle (>100M) next to the airfield because it was not in the database. 2. Lookup table upon A/C go-around looks at wrong engine thrust table 3. One operator regularly comparing a 28-day FMS revision cycles with the previous edition using software tools finding numerous errors.

IEEE parts and S/W failures and propagation of these errors throughout the system

This statement considers that:

- SW never fails, has only design and coding errors, and may be inadequately designed to face all envisaged power and electronic hardware failures. SW design / functional breakdown errors can be understood as procedural errors satisfying SHEL definition.

- Increasing technical complexity goes with an increased number of components making hardware more sensitive to accumulation of component failures, and especially the [unknown] failure modes of ever more complex processors are a source of concern.
- When the same type or IEEE parts exist in a given system, a common failure mode affecting a batch becomes more likely.
- Long life of electronic systems will (while facing components obsolescence) create maintenance burdens and possible configuration management errors.
- Configuration management issues / changes due to maintenance during systems life can create new types of failures.
- Since an increasing number of systems will communicate via data links, the protocol that will be used between (layers of) systems, needs to be sufficiently protected [ref today’s discussion for implementation of new IP address protocol for the internet and static or dynamic addressing]
- If the industry is to succeed in preventing these errors, true modularity of all component building blocks need to be assured.

All these factors contribute to increased likelihood of unforeseen or forgotten system failures and system interface failures having possible safety impact. In the far future, these issues may cause increasing hazards *unless systematic structures, and a building block approach*, are put in place to avoid those hazards.

Sabotage/cyber attack

Sabotage in the military world used to be cutting wires, i.e. cutting physical connections. In a highly automated aircraft, breaking the logical connection between stick and controls maybe the next option for sabotage and/or terrorism. This could take the form of a high power RF source in the wing close to the aileron controls, with the intent to break or interrupt the roll control logic. Another option could be to change the code logic via a cyber attack.

Sabotage used to be predominantly done and found by maintenance. Future sabotage/cyber attack may be more difficult to find and may be accomplished by individuals without physical access to the aircraft.

Technology Watch Items:

Monitoring the following signs and advances in technology should help determining if these security hazards are coming about:

R&D and Industry work to ensure that the lessons learned from specific experience is permanently captured and made readily available to the aviation industry.*

Appearance, development & implementation of more robust approach to design and a process that challenges the assumptions made in the safety analysis of flight critical functions.*

Manufacturers, trainers and regulators increasingly sharing applicable experience and lessons learned.*
Note: all of these *) watch items are related to Certification Process Study (CPS) conducted in the USA.

Use of systems outside intended use - watch items

- Airlines & training institutions insisting that crews are made aware of manufacturers’ design assumptions and regulators’ requirements in execution of company operating procedures.

- Active awareness programs.

Database Technology watch items

- Tools to speed uploads including proper certification,
- Changes to Software Certification rules that would speed up the process.
- Regulators allowing red label S/W use during revenue flights.
- Pressure from manufacturers to self certify or reduce certification time /effort, in order to reduce cost and or reduce time to market of upgrades!
- Appearance of more RISC processors in system applications.
- Increased use of flight critical S/W (especially for FMS) and increased use of ARINC specs for data link applications.

Security Technology watch items

- Increases in jamming technology capability.
- Identification of change/modify/delete existing code attack plans on the internet.
- Increase in cyber threat level directed at aviation.
- Availability of devices on the internet, pre-built or as a kit to accomplish them.
- Appearance of movies and or books on the subject that would give people ideas [we are not talking about the average person, state sponsored vs. the individual attack].
- Social- [organized crime] and Political issues [tension between states].

Risk monitoring:

- Set up of a data base incident tracking system including error resolution.
- Pursue accident precursors
- Track S/W revisions by number and complexity
- Reporting and tracking of cyber attack/sabotage anomalies

Theme IV: ABSENCE OF HUMAN AGENT (On Board)

Introduction:

Detection technologies for unexpected problems will be developed if un-crewed passenger carrying airplanes are to be built. If these technologies are not developed, then those airplanes will not be built. Therefore, the hazards associated with future detection systems for unexpected problems lie in failure to accurately detect, or solve, an unexpected safety-related hazard on a so-equipped airplane.

Despite the low probability of operational fully automatic flights within the next 20 years, FAST decided to investigate this possibility as an extreme case of automation permitting:

- to highlight tendencies valid for automated manned flights (e.g. situation awareness)
- To highlight that in a silent cockpit of a plane, crew awareness of phenomena maybe poor and new detection technologies may be necessary in the near future.

There are several required technologies that could contribute to the technical solutions of these detectors. Improved aural (hearing), olfactory (smell), tactile (feel), and visual sensors could be part of the technology. Nano-sensors and “smart” sensors that do not broadcast information unless the information is deemed significant could provide a network of basic sensors, which if properly interpreted, could sense a problem. Networking technologies will also play a part; wireless detection and transmission to the decision-making computer will be a key for manufacturing purposes. The “decision-making computer” must also “ping” remote sensors if problems are expected and no information is flowing to it from the sensors.

Main hazards in one theme:

There are 4 main hazards that need to be addressed for Commercial Fully Automatic Flight, these are:

1. Mechanisms to replace human sensing and processing of abnormal conditions: smoke, odors, vibration, noise, etc. (in particular for Fully Automated Flight) may be *insufficient* to cope with critical situations, hazard: **Hard 2.1a**
2. Lack of mechanisms to replace human cross-check of *misleading* or *inaccurate* data transmitted to & from the aircraft (in particular for Fully Automated Flight) may result in inappropriate actions being taken to ensure safety of flight. Lack of human redundancy (in particular for Fully Automated Flight), hazard: **Hard 2.2,** area's of change (MRO5) (AC1)(AC19) interact with this hazard.
3. Even when functioning properly, onboard sensors may give to airline operation centers and ground controllers' *insufficient information* to correctly analyze and resolve situations. Lack of mechanisms to replace human cross-check of misleading or inaccurate data transmitted to & from the aircraft (in particular for Fully Automated Flight) may result in inappropriate actions being taken to ensure safety of flight. Lack of human redundancy (in particular for Fully Automated Flight), hazard: **Live 5.3**, area's of change (MRO5) (AC1)(AC19) interact with this hazard.
4. Crew automation interactions issues: Loss of strategic and tactical situation awareness, including automation & mode awareness and airspace system functions may occur if flight management, system management and control of flight is transferred completely or partly from on-board crew to ground based crew, hazard **Live 6.1.4.**

Perspective:

In the next 10 years, we will see a continually increasing percentage of airplanes operating in civil airspace having a continually increasing level of “autonomy”. Autonomy in this case is defined as operation without human control. This transition will not occur all at once. It will have a phased introduction. Increasingly autonomous military airplanes will be introduced along with long endurance communication and civil surveillance platforms for detecting fires, security threats and the like.

<u>A gradual introduction of ever more "autonomous" aircraft</u>

In the future operational scenario, it may become desirable if not outright necessary to develop autonomous aircraft that do not require the presence of a human flight crew on board. Such airplanes operating in civil airspace will have a continually increasing level of “autonomy.” Autonomy in this case is defined as gate-to-gate operation without the presence of human pilots on board.

This transition will not occur all at once. It will have a phased introduction. Increasingly autonomous military airplanes will be introduced along with long endurance communication and civil surveillance platforms for detecting fires, security threats and the like. Twenty years from now, it is possible that there will be fairly autonomous cargo carrying airplanes flying, and passenger airplanes may be being designed at that time.

<u>Processing of inconsistent or misleading information</u>

Today (2003), the human operator of a vehicle can often identify and process inconsistent or misleading information sooner and sometimes more accurately than onboard systems. Current flight crews operate in a data-rich environment. This enables them to respond appropriately to unforeseen circumstances and maintain safety of flight

Present-day airplane systems are able to detect and process data that are outside pre-established standard values. For instance, today’s transport airplanes detect low hydraulic pressure and inform the flight crew in order to facilitate corrective action. However if the state data being provided by the onboard systems is inconsistent with other related information, misleading conclusions maybe drawn by automated systems or even human pilots. Human pilots are trained in methods for recognition, confirmation, and subsequent recovery from abnormal situations.

Similar capabilities must be provided in any kind of future automatic flight capability.

In the future, there will be public demand that passenger airplanes must automatically sense and identify anomalous and/or inconsistent data in order to prevent unwanted and perhaps hazardous responses to situations that are not real.

In order to replace the capability of the human to perform data/information cross check functions, some kind of automated decision-making functionality must be provided. This may take the form of artificial **“**intelligent **agent(s)”** (e.g. a computer or network of computers) that must compare sensor readings to identify unusual patterns and “outlier” information.

The development of such a robust capability is in itself a significant technology challenge. It should take care of and analyze the whole set of flight data from incident effect and criticality analysis to flight contingency management strategy (e.g. alternate fields are in FMS, but including check with ATC, airfield runway conditions, etc available).

Therefore it should trade-offs all information available with quasi human intelligence with equivalent confidence level. If artificial intelligent agents cannot at least functionally replicate human cross checks unsafe situations may be created. Automated systems can generally be programmed to detect and respond to expected system failures or to recognize expected anomalous indications.

However, in future scenarios in which no flight crew is present in the aircraft to make sense of the available information, the safety risk may increase due to the inability of automated systems to adequately sense and diagnose unexpected events and situations.

Sensor processing, Artificial Intelligence

Sensor information from many good sources is useless unless it can be interpreted regarding what the unexpected problem is. For instance, a flight crewmember could walk to the aft cabin while in flight, see a mist trailing the right wing, and determine that a fuel leak probably exists. Having a similar sensing and deduction capability will be necessary for decision-making and subsequent problem-solving.

This may require substantial application of diagnostic, decision-making, planning and action capabilities, most of them being currently addressed by Artificial Intelligence (AI). It must be noticed however that such capabilities of functionalities can be dispatched on both the aircraft and the ground, and can be performed by either artificial (computers) or natural agents (human crew). It is then likely that final decision, planning, and strategic and tactical choice of actions will be left to ground personnel (e.g. ATM/ATC crew, SCC crew under the FAF hypothesis).

But onboard sensors may not give airline operation centers and ground controller’s *sufficient* information to correctly analyze and resolve unexpected situations. Two issues must be addressed:

- Signal quality (lost communications, communication congestion, signal interference)

- Adequacy of information during dramatic in-flight events (such as in-flight fires, required ditching, emergency diversion to alternate fields or unforeseen interactions with other traffic due to weather or airport capacity problems.)

Current data streams, integrity as well as the quantity of raw data available, are not sufficient for ground control teams to select the optimal course of action. In the future, provision must be made for "electronic mayday" calls that create high-priority communication channels. In addition, for fully automated flight, consideration must be given for increased communications bandwidth for the aircraft in distress.

Without a human operator, replication or substitution of human information processing and interpreting capability will become a technical challenge for designers. Passenger-carrying un-crewed airplanes will present an additional challenge because the public will demand a higher level of "safety" for passenger airplanes and because passengers are sensitive to additional non-safety-related irritations.

Even if these very challenging technologies are developed, the burden of proof for its acceptability will be "that a FAF airplane will need to be at least as good as a piloted aircraft".

One serious concern will be that this may lead to a regulatory overkill due to the many uncertainties around FAF, a typical example from the past being automatic landing. Under autoland conditions, unrealistically harsh conditions need to be simulated, for instance under crosswind limits, leading to manual landings when crosswind exceeds the simulated limit of e.g. 25 knots. Flight-testing has shown that the automatics under these conditions would have made a perfect landing, while the manual landings in excess of 25 kts crosswind have shown in several cases to end up in significant mishaps.

The issue of transition from an intermediate level of automation (no pilots on aircraft but monitor or stand-by crew on ground) to fully automated flight (no flight crew in air or on ground) must be addressed. For instance, aircraft and support systems required for intermediate level of automation may be inadequate or require major revision if fully automated flight is to be realized.

All these questions could potentially be addressed by technology. Unless they are solved economically, the un-crewed airplanes will never be a reality, and hence, no hazards will exist. All of these issues could be avoided if there was public acceptance of an un-crewed airplane that could not deal with unexpected safety-related problems. From today's view, the main barrier to implementation of an un-crewed passenger airplane is lack of public acceptance of an airplane. If public acceptance of additional risks changes, then the un-crewed airplane could proceed with minimal technology changes.

Towards fully automatic flight: mixing of piloted and non-piloted aircraft

Under the fully automated flight (FAF) hypothesis, flight management, system management and control of flight will be transferred completely or partly from on-board crew to ground-based crew.

Such transfer of functions might be done step by step, so that there might be a transition before management and control will be mainly or totally exerted by the ground.

In addition, the management and control of FAF need to be co-ordinated to classical ATM/ATC. This co-existence of various management and control functions or systems (under the hypothesis of secure control and command (SCC) facilities) further determines what the future AGS system may look like at the 20+ year horizon.

Transfer of functions to a SCC [Secure Command & Control]

The transfer of certain functions to ground-based SCC crew introduces particular safety requirements:

a) Ground-based SCC crew should receive and be capable of processing all necessary information in order to carry out his missions and maintain a proper situation awareness and control (local and global) control
b) ATM/ATC personnel should be provided with all necessary information in order to maintain a proper situational awareness (SA) (local and global) and perform his management and control missions in relation to SCC ground-personnel (under the SCC hypothesis)
c) Flight crew in piloted aircraft should receive and be capable of processing all information necessary to share the airspace with FAF vehicles
d) Co-operation and communication issues, which will become more and more crucial in this new, distributed air ground space system (AGS) system, must be supported by appropriate technologies, design, organization, procedures and training. Co-operation and communication issues mainly concern 4 categories of personnel: 1) Ground-based SCC, 2) ATM/ATC personnel, 3) Flight crew on-board piloted aircraft and 4) Personnel (e.g. Cabin crew) on-board the un-piloted aircraft

From ATC's to SCC's: the integrated Air Ground System

Before 2020, we expect aircraft Air Traffic Control Centers, Airline Operation Centers, airports and satellites to be the nodes of an integrated Air Ground Space System (AGS) that will operate during the all phases of flight (gate-to-gate) and communicate through data-link. This AGS system recognizes the interdependence of stakeholder operational decision, e.g., Collaborative Decision Making, Flexible Use of Airspace

Human operators remain in the loop but are assisted by automation tools and use elaborate displays. Automation tools are supported by sophisticated databases. However single pilot or supervisory pilot freighter operations might appear in the decade 2010-2020.

Under the FAF hypothesis, i.e. Commercial Fully Automated Flight, which won’t be implemented before 2020+, flight management, system management and control of flight will be transferred completely or partly from on-board crew to ground-based crew. This transfer of functions might, especially in abnormal or emergency conditions, introduce a risk of loss of strategic and tactical situation awareness, including automation & mode awareness and airspace system functions.

Maintaining a proper situation awareness and situation control is made even more complex as the management and control of FAF must be performed in co-ordination with the management and control of piloted flights.

In order to prevent loss of situation awareness and loss of control, it is therefore essential to perform research of the implications of FAF in all personnel directly or indirectly concerned, to derive from research appropriate safety requirements and to satisfy these requirements through adapted technological, design, procedures, organization and training solutions.

Discussion:

Biggest hurdle

The biggest technology hurdles however are data merging, diagnostic, interpretation, decision-making and problem solving. Sensor information from many good sources is useless unless it can be interpreted regarding what the unexpected problem is. For instance, a flight crewmember could walk to the aft cabin while in flight, see a mist trailing the right wing, and determine that a fuel leak probably exists. Having a similar (at least functionally) sensing and deduction capability will be necessary for decision-making and subsequent problem-solving (When a problem is rightly detected and interpreted, appropriate recovery measures still need to planned and executed). This may require substantial application of diagnostic, decision-making, planning and action and capabilities, most of them being addressed by Artificial Intelligence (AI).

Even if these very challenging technologies are developed, the burden of proof for its acceptability will be “that a FAF airplane will need to be at least as good as a piloted aircraft”.

One serious concern will be that this may lead to a regulatory overkill due to the many uncertainties around FAF, a typical example from the past being automatic landing. Under autoland conditions, unrealistically harsh conditions need to be simulated, for instance under crosswind limits, leading to manual landings when crosswind exceeds the simulated limit of e.g. 25 knots. Flight testing has shown that the automatics under these conditions would have made a perfect landing, while the manual landings in excess of 25 kts crosswind have shown in several cases to end up in significant mishaps.

<u>Can "cross checking" technology be as good as a pilot?</u>

All these questions could potentially be addressed by technology. Unless they are solved economically, the un-crewed airplanes will never be a reality, and hence, no hazards will exist.

Crew cross checks consist of mental comparisons of various sources of data to confirm whether a situation is the same or different than the current perception and mental model of the aircraft state and flight progress. Cross-checks provide a means to confirm situational diagnosis and a means to identify unusual events and or conditions within or external to the aircraft.

Normal cockpit procedures call for cross checks of flight parameters (airspeed, altitude, heading, track, vertical speed, etc.), navigation and planning displays, charts and maps (4-D position awareness and planning), traffic checks (visual, TCAS, and radio), etc.. Cross checks in abnormal situations may additionally include other cues from caution and warning panels, aural indicators, abnormal sounds and noises, and smoke, vibration, information from other humans on board, in the vicinity of the aircraft or on the ground.

<u>Cross checking of misleading or inaccurate data</u>

Human operators have the ability to quickly identify misleading or inaccurate data. Cockpit instrumentation in transport category aircraft provides such a rich suite of information that unusual indications can be quickly cross-checked against other related information by the flight crew. In many cases, the human in the cockpit is the last line of defense against failures in other domains.

Examples of these failures may include inappropriate design, weather conditions not as forecasted, traffic separation failures on the ground an in the air, procedural weaknesses, and failures in management and operational procedures. In a future scenario in which onboard pilots may be replaced by automated flight systems, such cross checks may not happen.

<u>Insufficient information</u>

Even when functioning properly, onboard sensors may give airline operation centre and ground controller’s insufficient information to correctly analyze and resolve situations. Situations to consider include lost communications, communication congestion, and signal interference.

In unexpected or unforeseen circumstances such as in-flight fires, required ditching or emergency diversion to alternate fields current data streams available are not sufficient for ground control teams to select the optimal course of action. In the future, provision must be made for "electronic mayday" calls that create high-priority communication channels. In addition, for fully automated flight, consideration must be given for increased communications bandwidth for the aircraft in distress.

Technology Watch Items:

Look for these signs to determine if this technology and associated hazards are coming about:

- Artificial Intelligence technology advancements enabling inexpensive replication or substitution of human sensing and reasoning to an extent that a machine can successfully interpret a situation that it has never encountered, diagnose the problem with at least human reliability, and instigate system changes to address the problem.
- Networking technologies that support efficient, high-bandwidth communication; wireless network, smart sensors, etc.
- Track technology progress and public acceptance of safety-sensitive domains such as other transportation modes Track advances in the medical field such as remote surgery and automated, implanted medical devices
- Systemic use of satellite for communication, navigation and surveillance and development of associated technologies and services (e.g. Ground or Space Based Augmentation Systems (GBAS, SBAS);
- Automatic Dependant Surveillance- Broadcast (ADS-B); Data-link Technologies (ACARS; VDL 4; High Band-with))
- Free-flight / free-routing plans such as Free Routing Airspace Plans (FRAP) or Mediterranean Free Flight (MFF)
- Collaborative decision making (CDM)
- Assuming that " decision making computers" will have a learning capability, track appearance of solutions to share/exchange the individual learning between decision making computers [via " learning ground nodes/hubs"?]

Risk monitoring:

This will also be an essential ingredient for continued safe operation:

- Develop tools and methods for monitoring frequency and trends of system/component failures arising from unknown or unexpected reasons
- Identify, track, and process occurrences of incomplete, misleading, conflicting or insufficient data where flight crew performed this function

SUMMARY

- **Theme I: GLOBAL AIR–GROUND–SPACE SYSTEM ISSUES:**

A new AGS system

In the next twenty years, we expect aircraft, Air Traffic Control Centers, Airline Operation Centers, and satellites are the nodes of an integrated Air Ground Space System (AGS) that will operate during the all phases of flight (gate-to-gate) and communicate through data-link. This AGS system recognizes the interdependence of stakeholder operational decisions, e.g., Collaborative Decision-Making, Flexible Use of Airspace.

The airspace system will undergo significant changes (e.g. free routing/free flight; new airspace classification; development of 4 Dimensions trajectories).

This is likely to occur step by step, such system will be performance oriented, but *compatibility and safety* will come first.

Technological moves
Older technologies and modern technologies will co-exist both for aircraft and ground systems, at least in a transitory period.
Human operators remain in the loop but are assisted by automation tools and use elaborate displays. Automation tools will be supported by sophisticated databases. Data and warning/alert information will be generated at an ever-increasing pace within the aviation system and these data will play an increasingly important role in flight critical situations. These data are stored in air and ground repositories and the information generated from the data will be presented to both airborne and ground-based operators.
On the way to Fully Automated Flight
New vehicles such as Vertical Take-Off and Landing aircraft (VTOL) (Other than helicopters) and Un-inhabited Aerial Vehicle (UAV) may use the airspace. Furthermore, single pilot or supervisory pilot freighter operations might appear in the decade 2010-2020 and might pave the way in the longer term for Commercial Fully Automated Flight.

- **Theme II: FLIGHT CREW-AUTOMATION INTERACTIONS ISSUES:**

Automation, as a concept, is the allocation of functions to machines that would otherwise be allocated to humans. The term is also used to refer to the machines which perform those functions. Flight deck automation, therefore, consists of machines on the commercial transport aircraft flight deck which perform functions otherwise performed by pilots. Current flight deck automation includes autopilots, flight path management systems, electronic flight instrument systems, and warning and alerting systems.

At the larger level of the Total AGS System, automation should also contribute to enhancing the awareness of the global AGS distributed multi-agents control, command and management system to all personnel concerned: flight crew, cabin crew, ATM/ATC staff and maintenance personnel, and Strategic Command and Control (SCC) personnel under the Fully Automated Flight (FAF) hypothesis.

With the advent of advanced technology, so called "glass cockpit", commercial transport aircraft and the transfer of safety-critical functions away from human control, pilots, scientists, and aviation safety experts have expressed concerns about the safety of flightdeck automation. For example, Wiener (1989) surveyed a group of pilots of advanced technology commercial transport aircraft and found significant concerns. Based on incident and accident data, Billings (1991a, 1994) cited problems with flightdeck automation and proposed a more human-centered approach to design and use.

New automated control, command and assistance systems may modify the ways the different personnel will interact with the technology and between themselves, not only in the cockpit but also in the other nodes of the global AGS system. Some problems are likely to be resolved and other to be reinforced, while new problems due to the unique characteristics of the future global AGS system will probably arise. Among them are for instance the difficulties for each agent to be and remain aware of the state and dynamic behavior of the other agents, human and artificial, within the global system, and the difficulty to operate in case of failure, breakdown or inoperability of the automated systems.

- **Theme III: GENERAL THREATS:**

The aviation system is faced with increasing technical and business complexity. Systems now cost more than in the past, and this investment is causing extreme longevity of use of systems. The experience base for system design is eroding, with system longevity far outliving the careers of the designers, builders and the regulators that developed it. All these factors contribute to increased likelihood of unforeseen or forgotten system failures and system interface failures having major safety impact. In the far future these issues may cause increasing hazards unless systematic structures are put in place to avoid those hazards**.**

Use of systems outside intended use
Operators today sometimes use systems for tasks for which they were not intended. (E.g. Use of FMS as sole means to determine V speeds; Use of TCAS to maintain separation; Use of TAWS as primary means of navigation)

Databases
Use of databases has evolved into many aerospace applications, both on board as well as on the ground. Typical examples are databases in FMS, but also in EGPWS, TCAS, AFCAS, EICAS/ECAM/MFDS, ATC systems, etc. Use of databases is currently only in its infancy, with an exponential increase just around the corner

Sabotage and cyber attack
Use of computer software has evolved into many aerospace applications, both on board as well as on the ground. The connections of S/W with the "outside world" are through a) Loading in the shop: Initial Program Load on the chip/EPROM, b) physical on board S/W loading by means of floppy or cable and c) logical, through a data link or wireless network. Today, the threat of cyber terrorism against aircraft is minimal. But when looking into the future airspace paradigm, with many aircraft and ground systems in a multi-agent distributed air ground [AGS] system, *ever more critical information* will be transmitted via data link, this is considered a serious threat.

- **Theme IV: ABSENCE OF HUMAN AGENT (On Board):**

  In the next 10 years, we will see a continually increasing percentage of airplanes operating in civil airspace having a continually increasing level of "autonomy". Autonomy in this case is defined as operation without human control. This transition will not occur all at once. It will have a phased introduction. Increasingly autonomous military airplanes will be introduced along with long endurance communication and civil surveillance platforms for detecting fires, security threats and the like.

  A gradual introduction of ever more "autonomous" aircraft should occur. One main issue will be processing of inconsistent or misleading information: Similar capabilities as in piloted aircraft must be provided in any kind of future automatic flight capability. This could be achieved by improving Sensor processing and introducing Artificial Intelligence. When moving towards fully automatic flight a mix of piloted and non piloted aircraft will have to be envisaged and successfully addressed. Functions will be transferred to a SCC [Secure Command & Control]. Moving from *ATC's to SCC's* will achieve the integrated Air Ground System.

Technology Watch Items Related to the Four Hazards Themes

Monitoring the following advances in technology should help determining the possible realization and evolution of the hazards related to these 4 trends. The following "Technology Watch Items" (TWI) have been identified and they are presented below without prioritization. They may evolve in time and it is advisable to maintain a close monitoring of the strategies developed by bodies responsible for Air Navigation Services such as the EUROCONTROL ATM 2000+ strategy. In a similar fashion it is advisable to also monitor the development of Strategic Research Agenda such as ACARE in Europe that give good indications of the technologies being developed.

1. **<u>Aircraft and CNS/ATM technologies:</u>**
   i. Systemic use of satellite for communication, navigation and surveillance and development of associated technologies and services
   ii. Introduction of Free flight / free-routing plans. These concepts will introduce new automations modes.
   iii. Emergence of 4D trajectories and their consequences of crew interface.
   iv. Decommission plans of ground navigation aids.
   v. Emergence of FMS Systems designed and certified for sole means of navigation.
   vi. Introduction of new warning systems and alerting techniques, and consolidation/integration of warnings and alerts involving problems with internal vehicle systems with those from external traffic, terrain, and weather avoidance/alerting systems.
   vii. Development of “intelligent” aircraft

2. **<u>Aviation processes:</u>**
   i. <u>Aircraft design and certification and circulation of safety information:</u>

      1. R&D and Industry work to ensure that the lessons learned from specific experience is permanently captured and made readily available to the aviation industry.
      2. Appearance, development & implementation of more robust approach to design and a process that challenges the assumptions made in the safety analysis of flight critical functions.
      3. Manufacturers, trainers and regulators increasingly sharing applicable experience and lessons learned.
      4. Airlines & training institutions insisting that crews be made aware of manufacturers’ design assumptions and regulators’ requirements in execution of company operating procedures.
      5. Active awareness programs.

   ii. <u>Software and data bases certification processes</u>
      1. Tools to speed uploads including proper certification,
      2. Changes to Software Certification rules that would speed up the process.
      3. Regulators allowing red label S/W use during revenue flights.
      4. Pressure from manufacturers to self certify or reduce certification time /effort, in order to reduce cost and or reduce time to market of upgrades!
      5. Appearance of more RISC processors in system applications.
      6. Increased use of flight critical S/W and increased use of ARINC specs for data link applications.

3. **<u>Security technologies:</u>**
   i. Increases in jamming technology capability.
   ii. Identification of change/modify/delete existing code attack plans on the Internet.
   iii. Increase in cyber threat level directed at aviation.
   iv. Availability of devices on the Internet.
   v. Appearance of movies and or books on the subject that would inspire terrorists.
   vi. Social- [organized crime] and political issues [tension between states].

4. **<u>Scientific and Technological advances:</u>**
   i. <u>Artificial Intelligence:</u>

1. Development of system using Artificial Intelligence (e.g. neural nets, fuzzy logic) and their consequences on crew automation interaction.
2. Assuming that " decision making computers" will have a learning capability, track appearance of solutions to share/exchange the individual learning between decision making computers [via " learning ground nodes/hubs"?].
3. Artificial Intelligence technology advancements enabling inexpensive replication or substitution of human sensing and reasoning to an extent that a machine can successfully interpret a situation that it has never encountered, diagnose the problem with at least human reliability, and instigate system changes to address the problem
4. Monitoring of general and applied research in these areas should be made to identify scientific breakthroughs.

ii. Micro and Nanotechnologies
   1. Nanotechnologies, new computing techniques such as molecular computing and intelligent materials.
   2. Monitoring of general and applied research should be made in these areas to identify scientific breakthroughs

iii. Computer-aided decision-making and cognitive engineering:
   1. Collaborative decision-making (CDM); Computer Support to Cooperative Work (CSCW), Computer-based operating aids and management systems, Groupware, Monitoring and Supervisory Control, Industrial, Human, and Cognitive Engineering.

iv. Network Technologies:
   1. Information and Communications Networks based upon all-optical technologies and new Internet protocols, advanced Middleware, global networking and distributed architectures, Multimodal Interfaces, Semantic-based knowledge systems, Networked audio-visual systems, technology-enhanced learning, advanced displays, optical, opto-electronic, photonic functional components, open development platforms for software and services, cognitive systems, GRID-based Systems for solving complex problems, risk management (Supported in particular by the EC in the 6^{th} & 7^{th} Framework Programs)

v. Other fields technologies:
   1. Track advances in the medical field such as remote surgery and automated implanted medical devices. eHealth
   2. eSafety of road and air transport.
   3. Track technology progress and public-acceptance of other safety sensitive domains.

2. FAST Complete List of Hazards Related to the Area of Change "Increase Reliance on Cockpit Automation" (AC13)

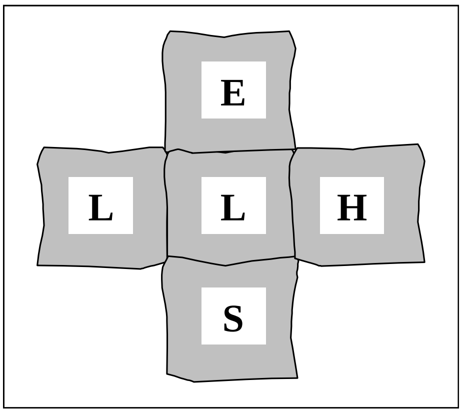
This Section presents the un-prioritized and therefore *complete* list of hazards FAST identified regarding to the highest priority Area of Change "Increase Reliance on Cockpit Automation" (AC13).

Hazard is defined here as any condition, event or circumstance within or outside the airspace system leading to an unanticipated or undesired event such as loss of life, injury or property damage.

Hazards have been derived, and are categorized, using the SHEL (Software, Hardware, Environment, and Liveware) model as a reference, in which the different letters mean:

- Liveware = "Human"
- Hardware = "Machine"
- Software = "Procedure, symbology, etc."
- Environment = the socio-technical and physical "situation in which in which the L-H-S systems must function".

Edwards (1972) originally developed the SHEL concept. In 1987, Hawkins proposed a modified version of the model in order to explicitly represents the man-man interaction, and make the Liveware element central in the model. This resulted in the introduction of another Liveware block, to symbolically represent the fact that the human beings (Liveware) not only interact with H-S-E, but also with the other human beings, i.e. the second L of SHELL. This also allowed the correct spelling of the English word 'shell', which made this acronym easier to remember.



The SHELL model (after Hawkins, 1987)

References

Edwards, E. (1972). Man and machine: Systems for safety, in Proceedings of British Airline Pilots Association Technical Symposium. British Airline Pilots Association, London. pp. 21-36.

Hawkins, F. H., (1987) *Human Factors in Flight,* Gower Technical Press, 1987.

Part 1 – "Increase Reliance on Cockpit Automation" – "Software" (by reference to the SHELL Model) related Hazards

Note: The term "software" is used herewith the meaning of information only. Software products & applications are part of the "Hardware" section.

SOFT1	**Operating Procedures**
SOFT1.1	• Inability of procedures (and systems) to adapt to changing operating conditions, new aircraft, and new systems and to cope with new or previously encountered situations may create hazardous conditions (i.e., reduced safety margins) or the inability to recover from abnormal events (ANS1)
SOFT1.2	• Failure to harmonize ATM/ATC/SCC procedures with flight crew operations
SOFT1.3	• Failure to develop or implement appropriate SOP's within supervisory command & control organizations
SOFT1.4	• Inadequate methods for updating procedures, implementing/monitoring changes, and prioritizing the timing of received information
SOFT1.5	• Proliferation of warnings and alerts requires CRM procedures adapted to phase of flight; crew needs to be mutually aware that logic driving order of priority may be affected (AC22)
SOFT1.6	• CRM/task-sharing not acceptable in certain cultures. Implicit command and control stereotypes in certain cultures may lead to misuse (C11)
SOFT1.7	• Failure to properly account for novel operating procedures (normal, abnormal, and emergency) - e.g. automation breakdown or failure, communication breakdown, weather, unanticipated sudden closure of airport, crisis management) for all categories of operators, in particular for aircraft command & control as well as supervisory command & control of multiple aircraft (i.e., Fully Automated Flight paradigm)
SOFT1.8	• "Gaming the System"
SOFT1.9	• Inadequately defined procedures (e.g. handoffs) for resolving traffic conflicts for instance when Conflict Detection Traffic Information (CDTI) is linked to FMS in future (ANS1)
SOFT1.10	• Malfunction of automated minimum equipment list for take-off and for continued flight (i.e., Fully Automated Flight) due to failure of sensors and built-in, functionality self-tests prior to dispatch
SOFT1.11	• Failure to achieve continued airworthiness due to unsuitable or inadequate maintenance procedures
SOFT1.12	• Procedures may be more of an issue for GA operating in a CNS/ATM/Free flight environment using future FMS systems. GA sensitive to wide range of issues
SOFT1.13	• Inadequate incident and service problems reporting and tracking requirements
SOFT1.14	• Inability to maintain updated GPS databases (AC14)

SOFT2	Certification
SOFT2.1	• Lag between pace of certification rules development and technology development and implementation (E9)
SOFT2.2	• Inflexibility of certification rules in adapting to changing operating conditions, new aircraft, and new technology
SOFT2.3	• Inconsistency between designs of FMS; aircraft-ATM system; FAF and certification (TC/STC) standards (C1, E8)
SOFT2.4	• Inadequate certification of the interactions among ATC, crew, SCC (FAF only) and operations (ANS19)
SOFT2.5	• Cross-border implications (Chicago Convention) for UAV flight operations (ANS19)
SOFT2.6	• Inoperability issues, standardization of communication protocols, (ANS19, AC12)
SOFT2.7	• Difficulty in certification of large distributed systems (accounting for interactions among systems)
SOFT2.8	• Inadequate processes for certification of computer software (including interactions with other software systems and artificial intelligence) onboard the aircraft and in the larger airspace system (C1, ANS20)
SOFT2.9	• Airspace transition issues
SOFT2.10	• Aircraft transition issues
SOFT2.11	• Difficulty in assuring continued airworthiness
SOFT2.12	• Inadequate certification processes for aging hardware, computer software, and procedures
SOFT2.13	• Development of certification standards for operation of fully automated aircraft must account for continued existence of legacy aircraft and ATM systems (ANS21)
SOFT2.14	• Lack of guidelines or reference materials for certification authorities
SOFT2.15	• Standardization, etc. may be more of an issue for GA operating in a CNS/ATM/Free flight environment. GA sensitive to wide range of issues
SOFT2.16	• Inadequate incident and service problems reporting and tracking requirements
SOFT2.17	• Inability to maintain updated GPS databases (AC14)

SOFT3	Design
SOFT3.1	• Inappropriate or unintentional application of design specifications
	• Incorrect or partial system requirements definition, for all technological and organizational applications (e.g. advanced FMS, terrain recognition, navigation aids, situation awareness displays and other media, ATM/ATC/SCC command and control rooms, Air / Ground / Space communication and integration systems)
SOFT3.2	• Lack of practical guidelines, standards, and/or methods for component and system design (i.e., establishing specifications and performance validation/verification/usability standards) (C1)
SOFT3.3	• Failure or inability to involve original aircraft system designers in retrofit of older aircraft or lack of guidelines detailing respective authorities requirements
SOFT3.4	• Need for better methods to define requirements and evaluate HF in system • Design process. Conformity between design presentations including cognitive display standards and norms. Integration and conformity

	verifications among hardware design functionality and presentation (i.e., SCC for FAF). Representation may appear quite compelling; background data may not be as good as display appearance. Proper amount and type of information to be presented (C1, C3, AC20)

SOFT4	**Training**
SOFT4.1	• Inadequate training requirements (both technical and organizational) for all categories of personnel, particularly for supervisory command and control personnel (under the hypothesis of Fully Automated Flight)
SOFT4.2	• Inappropriate training and revised CRM practices (in particular Inconsistent CRM performance evaluation standards and conformity among CRM practice and CRM adaptation to AI automation (C1)
SOFT4.3	• Adaptation of CRM to account for possible shift in responsibility for separation from ground to air. Requirement for change in CRM approach at transition points from Free-Flight/Free-Routing to controlled-flight - traffic vigilance techniques (ANS1)
SOFT4.4	• Variation of automation capabilities may require alternate CRM approaches. Inconsistent configuration management and cross-check of aircraft may not be detected by CRM (AC10, MRO5, AC4)
SOFT4.5	• Incorrect or misleading data provided to crew from ground-based systems may not be detected by CRM. CRM required to ensure proper data entry by flight crew (ANS19)
SOFT4.6	• Failure of CRM philosophies to accommodate "old-school" designers/users and "new school" designers/users. Need users skilled in use of automation and corresponding CRM (C5)
SOFT4.7	• Proliferation of warnings and alerts requires CRM procedures adapted to phase of flight; crew needs to be mutually aware that logic driving order of priority may be affected (C3)
SOFT4.8	• Failure to achieve checks of message coherence (do commands make sense?) (C1)
SOFT4.9	• Need input from designers and pilots to the CRM procedures Information distribution between PF & PNF. CRM provides a decision framework for interpretation, prioritization, and use of this additional data (C3)
SOFT4.10	• Unresolved cultural and regional aspects of CRM (C11)
SOFT4.11	• Automation simplifies CRM but may add unanticipated complexity in extreme cases. • Danger of lack of standardization within a fleet. Subtle differences among aircraft controls, displays, and automated systems may lead to either confusion as well as improved awareness of system functions and may or may not influence CRM. CRM must address subtle and overt differences among aircraft. Carriers want to avoid costs associated with different displays and different CRM (reduced training cost – trading retrofit cost for training cost) (AC12)
SOFT4.12	• CRM must take into account system state and role of flight crew in managing active flight controls. CRM should enable coordinated actions by flight crew in response to failures of active flight controls (AC12)
SOFT4.13	• Introduction of new training curricula for pilots of conventional aircraft and ATM/SCC to address unique characteristics of fully automated aircraft including role of human operators as translators/interpreters of information originating from multiple devices of varying vintages (C5, C7)
SOFT4.14	• Flight-deck training issues change to issues for training of remote SCC personnel that address remote monitoring and control of an aircraft (AC20)

SOFT4.15	• New generation of training simulators for SCC personnel (C7)
SOFT4.16	• Failure to target CRM to new aircraft types, control systems, and fleet capabilities (AC11, MRO9, AC1, AC8)
SOFT4.17	• Failure of CRM to take into account various ATM configurations and system behaviors (ANS21)
SOFT4.18	• Failure of CRM to assist in resolving loss of pilot airmanship. If SAD or FMS fails or provides misleading information of data is intentionally corrupted, pilots must revert to basic airmanship (C8, E20)
SOFT4.19	• What artificial intelligence systems learn is not predictable and may not be shared with subsequent operators or aircraft, making tactical decisions and validation more difficult - Specific to FAF: valid only for non-symbolic systems • Failure of AI systems to mimic human problem-solving processes. (ANS20, C1)
SOFT4.20	• Failure of CRM to prepare the flight crew to cope with decreased separation standards (ANS5)
SOFT4.21	• Failure of training to address unique issues raised by use of Commercial-Off-The-Shelf (COTS) products (E8)
SOFT4.22	• Failure of training to prepare flight crew to deal with information and displays from supplementary weather information systems (AC21)
SOFT4.23	• Training issues for general aviation aircraft may be similar to those listed above for commercial transports (AC4)
SOFT4.24	• Lack of mechanisms to keep CRM up to date with software and technology development (E8)
SOFT4.25	• Lack of understanding of automation behavior due to lack of training
SOFT4.26	• Inadequate training for abnormal and emergency conditions (e.g. automation breakdown or failure, communication breakdown, weather, sudden closure of airport, crisis management)
SOFT4.27	• Inadequate training for designers particularly in the human factors domain
SOFT4.28	• Inadequate transition across the spectrum of training methods and devices (i.e., absence of suitable automation training devices)
SOFT4.29	• Inadequate linkage between system requirements/design and training requirements

SOFT5	**Licensing**
SOFT5.1	• Failure to consider licensing requirements (including medical certificates) for all categories of personnel within the airspace system
SOFT5.2	• Inadequate licensing of safety management system (organizational & decision making processes, departure from traditional analytical approaches, etc) due to change of airspace paradigm (e.g. free flight, distributed multi-agent control system, new air space paradigm)
SOFT5.3	• Inadequate or non-existent licensing procedures for ground based supervisory command and control personnel (under the hypothesis of Fully Automated Flight)

SOFT6	**Operations - Flight operations / interactions with automation**
SOFT6.1	• Loss of situation awareness due to increased dependence on automation
SOFT6.2	• Inadequate traffic awareness – from controlled-flight to Free-Flight transition points (trajectory vs. way point negotiation) (ANS1)
SOFT6.3	• Loss of automation behavior awareness due to complexity of automation modes. Pilot needs to know what the airplane "thinks" is going on (matching expectations) (C3)
SOFT6.4	• Loss of control due to inadequacies of automation combined with inadequate recurrent training for flight crew/operators
SOFT6.5	• Procedures for operation of regional jets may differ from those of larger transport category (OP3)
SOFT6.6	• Failure of operational procedures to ensure adequate understanding and management of failures due to increasing complexity of automated systems
SOFT6.7	• Failure to provide adequate data selectability and homogeneity based on context (phase of flight, aircraft configuration) above some minimum set of required information to operate the aircraft (C3)
SOFT6.8	• Failure of procedures to facilitate correct parameter detection
SOFT6.9	• Delayed or inappropriate responses during transition from automated functions to partial or full manual control
SOFT6.10	• Failure of operational procedures to cope with breakdown or failure of automation, system or communication (inconsistent lat/lon position information between air and ground) (ANS1)
SOFT6.11	• Failure to adapt autonomous control to various types of controlled airspace (ANS1)
SOFT6.12	• Failure to detect anomalous conditions when trajectory is compromised by an outside source (ANS1)
SOFT6.13	• Inadequate or inappropriate formal software verification and validation processes and methods due to increasing demand for V&V
SOFT6.14	• Lack of appropriate procedures for setting of personal preferences for automated systems

SOFT7	**Operations - Global air space system**
SOFT7.1	• Failure of operating procedures to support awareness or understanding by the different categories of personnel of the global air space system

SOFT8	**Operations - ATC / ATM and SCC under the FAF hypothesis**
SOFT8.1	• Failures due to unfriendly operational procedures
SOFT8.2	• Un-cleared departure of aircraft from established conflict-free operating corridors (in particular for FAF)
SOFT8.3	• Incompatible automated sequencing of aircraft in terminal areas, in particular in case of mixed fleet of automated & piloted aircraft
SOFT8.4	• Problems arising from transfer of responsibility from crew to SCC (C3)
SOFT8.5	• Increasing amount of information available to SCC and other traffic. (C3)

Part 2 – “Increase Reliance on Cockpit Automation” – “Hardware” (by reference to the SHELL Model) related Hazards

HARD1	**General issues**
HARD1.1	Significant changes posed by highly complex array of command & control software increases the potential for unknown or unanticipated failures
HARD1.2	Failure due to inflexibility of systems to adapt to changing operating conditions (ANS1)
HARD1.3	Failure as a result of inadequate redundancy/fail-safe features of air & ground systems
HARD1.4	Pilot and/or crew confusion resulting from a wide range of aircraft/spacecraft performance capability (impact on CNS/ATM and SCC under the Free Flight Hypothesis) (ANS1)(C6)(MRO5)(AC1)(C11)

HARD2	**Absence of human agent (onboard)**
HARD2.1	Mechanisms to replace human sensing and processing of abnormal conditions: smoke, odors, vibration, noise, etc. (in particular for Fully Automated Flight) may be insufficient to cope with critical situations. Control of equipment failure (fires, fluid loss, off-airport landings etc) (AC19)(AC17)(AC1)(C4)
HARD2.2	Lack of mechanisms to replace human cross-check of misleading or inaccurate data transmitted to & from the aircraft (in particular for Fully Automated Flight) may result in inappropriate actions being taken to ensure safety of flight. Lack of human redundancy (in particular for Fully Automated Flight) (MRO5)(AC1)(AC19)
HARD2.3	Mechanisms for replacing human cross-check and error detection and correction mechanisms will depend on availability and accuracy of Air – Ground communications (MRO5)(ANS22)(AC17)
HARD2.4	Malfunction or failure of mechanisms which compensate for the loss of third party communication in Ground – Air communications (ANS22)

HARD3	**Communication issues**
HARD3.1	Available bandwidths (in particular for FAF) may become congested creating dependency on new communication technologies not necessarily optimized for aviation and the redundancy level required for FAF. (AC1)(AC19)(ANS19)
HARD3.2	Excessive time lag in control communication links for tactical manoeuvring (in particular for FAF) (AC1)(AC19)(ANS19)
HARD3.3	Possible interference from passenger communication using personal electronic devices: phones, Internet, computers (in particular for FAF) (AC1)(AC19)
HARD3.4	Lack of fail-safe autonomous operation following degraded or lost communication links (in particular for Fully Automated Flight) (AC1)(AC19)

HARD4	**Compatibility, integration, configuration management issues** (Including for HM Interfaces and Software applications)
HARD4.1	Failure or malfunction caused by inadequate design specification or inappropriate application (C1)(AC20) Example: concept definition weaknesses: lack of compatibility between some systems (e.g. terrain awareness systems) with the rest of the cockpit systems
HARD4.2	Failure to maintain compatibility between different data sources e.g. between airborne and ground based ATC systems (AC20) (ANS1) (ANS19)
HARD4.3	Failure to maintain compatibility between hardware and software (AC20)
HARD4.4	Functional compatibility between different information and alert systems Failure or malfunction caused by incorrect functional interfaces
HARD4.5	Failure or malfunction caused by incorrect integration of various interdependent information and alert systems
HARD4.6	Failure or malfunction caused by incorrect information / data sources: lack integrity, not in the same format (e.g. map standards, approach plates, etc. for terrain recognition systems), derived from multiple, inconsistent sources (ANS1)
HARD4.7	Failure or malfunction caused by improper sensor / data base integration (AC20) (ANS1)
HARD4.8	Failure or malfunction caused by wrong or incompatible versions of software or database, type of aircraft, type of aircraft system, engine configuration, etc. (AC20) (ANS1) (AC10)
HARD4.9	Failure or malfunction influenced by operator specific configuration (AC20)

HARD5	**Upgrades, updates and retrofit issues** (Including for HM Interfaces and Software applications)
HARD5.1	Failures caused by retrofit issues and issues for dealing with mixed equipment
HARD5.2	Failures caused by lack of continuity: update and upgrades issues
HARD5.3	Unknown or unanticipated impact of new equipage on legacy equipment Failures due to compatibility problems between older hardware & newer software (ANS7)
HARD5.4	Failures caused by insufficient ongoing hardware, HMI or software support (supplier viability)

HARD6	**HM Interfaces**
HARD6.2	Inadequate design specification or inappropriate application (C1)
HARD6.3	Inappropriate command & control user interfaces. Inadequate physical ergonomics
HARD6.4	Failure to maintain SAD readability in all foreseeable operational and environmental conditions including incompatibility with future ATC environment Breakdown during IAL (Instrument approach and landing) operations (C6) (AC20)
HARD6.5	Information is correct but presentation is incorrect or misleading. (ANS1)
HARD6.6	Confusion of crew as a result of reset (automatic, intended or unintended), power loss (possibly widespread), power transients, EMI effects, partial or total loss of information and resulting behavior, quick restart (Inappropriate and un-commanded operation of equipment)? (C4) (ANS7)
HARD6.7	Failure of the HMI design to show or display all necessary current & future behavior information available, e.g. Mode and mode function awareness (are the users aware of / do they understand current mode version and behavior, and mode logics?) (AC22)
HARD6.8	Failure of design of HMI to allow for coherence checking (between multiple sources, systems or instruments) (C4)(C6) (AC22)
HARD6.9	Failure to design flight deck to accommodate CRM procedures (control effectors, mode annunciation, displays, etc.) and more generally HF principles (C6) (AC22)
HARD6.7	Failure to follow airborne automated systems warnings and commands in future ATC and non-ATC controlled environments
HARD6.8	Potential loss of control due to lack of critical flight information and alerts to the SCC and/or cabin crews (C4)
HARD6.9	Inadequate alert due to new separation (spacing) criteria (ANS5)

HARD7	**Databases, software products & applications**
HARD7.1	Significant changes posed by highly complex array of command & control software increases the potential for unknown or unanticipated failures. Widespread power failures and software failure / error propagation increases the potential for unknown failure conditions. More interactions between more software systems causes potential for problems.
HARD7.2	Hazard resulting from more accurate data (lose randomness)
HARD7.3	Inadequate design specification or inappropriate application
HARD7.4	Insufficient database integrity Note detail below: Failures in databases caused by wrong data or errors in updating the databases can affect the integrity and result in inaccurate, misleading (content errors), obsolete or inadequate information (AC10) (C7) (AC20)
HARD7.4.1	Malfunction caused or influenced by database integrity failure: lack of software integrity. (AC10) (C7) (AC20)
HARD7.6	Malfunction or failure caused or influenced by anomalies: programming errors, bit flips, data corruption, update consistency.
HARD7.7	Failures caused by incorrect or incomplete verification & validation of database, software, etc. (AC10) (C7)
HARD7.8	Failures caused by or influenced by malicious code and/or data: virus, Trojan horse, intentional uplink corruption Failure cause by unintended use of database, software, etc. (C7)
HARD7.9	Inconsistent versions of software within the same aircraft fleet/ATM centres (AC10) (C11)
HARD7.10	Malfunctions and/or failures caused by impact of new software / architecture on legacy software / architecture
HARD7.11	Malfunction of fail-safe operation following software failures (in particular for Fully Automated Flight) (AC19)
HARD7.12	Lack of extended self-check capabilities (in particular, but not only, for Fully Automated Flight) Un-commanded or uncontrolled automated fault detection & systems reconfiguration (in particular, but not only, for Fully Automated Flight) Failure of fault detection system (C4) (AC19)
HARD7.13	Lack of sound mode logics and easy mode awareness
HARD7.14	Artificial Intelligence (neural nets systems, adaptive systems, etc.)
HARD7.14.1	Failure caused by lack of predictability and lack of transparency (C4)
HARD7.14.2	Failure caused by database, software integrity problems (currently designed for supplementary use only, not for primary use) (C4)

Part 3 – "Increase Reliance on Cockpit Automation" – "Environment" (by reference to the SHELL Model) related Hazards

ENV1	**Hazards arising from a change or air space paradigm**
ENV1.1	• Failure to manage the transition from present airspace to future airspace paradigm

ENV2	**Hazards inherent to new airspace paradigm and from a large, distributed and inter-related Air / Ground / Space (AGS) system**
ENV2.1	• Failure to integrate onboard and ground systems, e.g. control functions, data link, personnel, responsibilities - ATM/ATC and aircraft control functions (distributed multi-agent control system) - Data link with many outside partners: ATM / ATC and SCC (under the Fully Automated Flight hypothesis) - ATM / ATC / OPS / SCC (under the FAF hypothesis) / Flight Crew / Cabin Crew, including security and medical personnel (in particular for FAF) / Maintenance (in particular for FAF)
ENV2.2	• Failure to establish compatible strategic and tactical global vs. local goals
ENV2.3	• Loss of situation awareness (global, local)
ENV2.4	• Loss of strategic and tactical command and control within distributed AGS system
ENV2.5	• Inability of individual & total system to deal with aircraft not behaving as expected, with sudden weather problem, airport closure, air or ground accident, etc. (more serious hazard regarding Fully Automated Flight)
ENV2.6	• Loss of signal, loss of power, damage / breakdown / failure effects propagation issues
ENV2.7	• Unsafe functioning in emergency / downgraded conditions (power loss, failure, breakdown and damages of systems, equipment and communication and data links) or back-up modes

ENV3	**Certification & regulation issues**
ENV3.1	• Failure to resolve certification issues related to large, distributed systems, new airspace paradigms and fully automated flight
ENV3.2	• Failure to resolve institutional issues for a global CNS / ATM / ATC (e.g. free flight) / SCC (for FAF) system
ENV3.3	• Failure of worldwide ATM regulators to timely adopt standardized automation philosophies or phraseologies
ENV3.4	• Failure of regulations to timely adopt standards for the evaluation of software behavior, e.g. Artificial Intelligence, Commercial Off-The-Shelf (COTS) (E8)
ENV3.5	• Failure to revise or failure to adopt new international conventions for harmonization of regulations for fully automated aircraft, e.g., modification of Chicago Convention to cover cross-border flight of fully automated aircraft
ENV3.6	• Failure of regulators to timely establish standards for the mixing of flights from countries/regions with different technological and cultural background, in particular that are not practicing state of the art CRM
ENV3.7	• Failure of regulatory & certification authorities to timely adapt to implementation of Fully Automated Flight

ENV4	**Legal issues (accident-related)**
ENV4.1	• Adverse safety consequences that result from the failure of the judicial system to adapt to new airspace paradigm

ENV5	**Public opinion and political issues**
ENV5.1	• Unintended consequences of changes to aviation system due to public and political reactions to accidents or incidents

ENV6	**Work market issues**
ENV6.1	• Failure to adequately prepare for the expected shortage (e.g. maintenance) of qualified personnel (or excess, e.g. pilots in case of FAF)

ENV7	**Education and training issues**
ENV7.1	• Failure to integrate in the education and training programs (including CRM / TRM / MRM) of each personnel, (including operational, ground, cabin crew, security, medical personnel, etc.) the constraints arising from the change of airspace paradigm and of global aviation system
ENV7.2	• Failure to integrate organizational and cultural perspectives in education and training (including CRM)

ENV8	**Cultural and social aspects**
ENV8.1	• Failure to adequately prepare for the potential disparity of technological levels, of perceptions, attitudes and behaviors across the world
ENV8.2	• Failure to adequately prepare for the variation in organizational cultural perspectives on automation
ENV8.3	• Failure to adequately prepare for the possible loss of motivation and resistance of certain personnel which could result in social conflicts (e.g. pilots in case of FAF)
ENV8.4	• Failure to maintain corporate knowledge (airline or ATM/ATC)

ENV9	**Company / alliance management / market issues**
ENV9.1	• Inadequate human/financial resource/reputation management when undergoing changes, e.g., during transition to new airspace paradigms or after an accident, etc.
ENV9.2	• Failure to adequately manage organizational shortcomings (integration during operations)

ENV10	**Operational environments**
ENV10.1	• Failure to properly co-ordinate and synchronize worldwide system (central flow management units, hub structure, etc.)
ENV10.2	• Failure to adequately manage operational demands and constraints, e.g., time pressure, reduced margins (ANS10)
ENV10.3	• Failure to adequately manage changes in navigation requirements: e.g., free flight, fully automated flight

ENV10.4	• Failure of aeronautical information agencies to adapt charts or database to new air space paradigm
ENV10.5	• Failure to adequately prepare for adverse/emergency/crisis conditions, e.g., wide area weather impacts; closed/inoperative runways, closed airports, inoperative navigational aids, aircraft not responding as expected, etc. in particular for FAF
ENV10.6	• Failure to coordinate between ATM / ATC and military authorities and/or other organizations, in particular for FAF

ENV11	**Design issues**
ENV11.1	• Failure to manage integration problems (Air/Ground, companies and systems) during design & development

ENV12	**Security issues**
ENV12.1	• Failure of protection systems against malicious code or cyber attacks
ENV12.2	• Failure to protect from intentional damage or degradation of systems, equipment, materials
ENV12.3	• Failure to response to terrorist threats and subsequent actions (in particular for FAF)

ENV13	**Physical environment aspects**
ENV13.1	• Failure to address or manage adverse atmospheric conditions (in particular for FAF): icing, lightning, turbulence, wind shear, volcanic dust, etc.
ENV13.2	• Failure to address or manage vibrations
ENV13.3	• Failure to address or manage physical location, radiation, cosmic flares, bad or noisy sensors (input devices)
ENV13.4	• Failure to address or manage electronic noise, saturation, electromagnetic emissions, etc
ENV13.5	• Failure to address or manage temperature, humidity and dust sensitivity: cooling (risk of overheating), humidity and atmosphere requirements
ENV13.6	• Failure to address or manage contaminants in equipment, drinks, food, dust (dirty mouse, contaminated track pad (using gloves), printer, noisy, unclear, etc.)
ENV13.7	• Failure to address or manage diurnal fluctuations (in particular for FAF)
ENV13.8	• Failure to address or manage bird strikes
ENV13.9	• Failure to address or manage loss of integrity of satellite weather, communication & navigation aids
ENV13.10	• Failure to address or manage cockpit smoke, cabin depressurization (oxygen mask) causing loss of readability / usability of advanced systems and equipment (e.g. advanced FMS, terrain recognition and navigation systems)
ENV13.11	• Failure to address or manage noise, e.g. unusual warnings & alerts from automation or equipment failure and/or noise from rain/hail

Part 4 – "Increase Reliance on Cockpit Automation" – "Lifeware" (by reference to the SHELL Model) related Hazards

LIVE1	**Organizational Agents**
LIVE1.1	• Unclear areas of responsibility and liability among various contributors to the development and use of automated systems may result in weaknesses and/or unforeseen circumstances when components of future systems or components are developed, designed, built, tested and put into service

LIVE2	**Designers**
LIVE2.1	• Lack of proper coordination between designers of airborne systems and their counterparts for ground-based systems could result in latent incompatibilities in systems that would not show up until in service
LIVE2.2	• Fewer aircraft types and technologies in development may result in a loss of cross-industry development skills; loss of experience transfer
LIVE2.3	• Role of traffic situational awareness – from controlled-flight to Free-Flight transition points (trajectory vs. way point negotiation) is not yet understood (ANS1)
LIVE2.4	• Pilot needs to know what the airplane "thinks" is going on (matching expectations) (C3)
LIVE2.5	• Complex displays may make it more difficult to clearly report problems and symptoms – multiple systems may feed the SAD & FMS making it difficult to identify and rectify the fault (MR05)

LIVE3	**Flight crews - New air space management / Multi-agent issues**
LIVE3.1	• New forms of airspace management need to be integrated with manned and unmanned aircraft and their operators. Coordination problems may arise between ATC controllers, aircrew and Un-crewed Aeronautical Vehicles (UAV) operators operating the same airspace. There also may be unforeseen interaction issues between these agents caused by system failures
LIVE3.2	• Airspace management philosophies may create cultural compatibility problems when designing future airspace system • New issues between regions with various infrastructure, culture and implementation requirements
LIVE3.3	• There is a lack of consistency between designs of FMS; aircraft-ATM system; FAF and certification standards for both existing and new designs (C1) In particular: - There is currently no world standard for ATM system design - Better methods are needed to define requirements and evaluate human factors in the system design process. - Conformity between design of displays, controls and ergonomics and other display interface characteristics is lacking - Cognitive display standards and norms have not been set. - Integration and Conformity Verifications among hardware design functionality and presentation is lacking
LIVE3.4	• Flight Crew are increasingly serving as interpreters/translators of information originating from multiple sets of equipment, of widely varying vintage and origins (C5) • CNS/ATM/Free-flight environment may cause a paradigm shift in flying as aircraft are seen as part of the system instead of individual entities (C5)

LIVE4	Flight crews **-** Conflict between air / ground information sources
LIVE4.1	• Poor escape maneuver decision due to conflict between different information sources (e.g. TCAS, ATC verbal messages, data link) and lack of explicit prioritization
LIVE4.2	• New air traffic management philosophies may leave present traffic planning and – avoidance procedures obsolete. Introduction of new separation and avoidance procedures based on automation requires a high level of standardizing and cooperation among certification authorities, operators and airspace management agencies. Different procedures in various regions may create procedural errors

LIVE5	**Flight crews** - **Absence of human agent (onboard)**
LIVE5.1	• Transfer of authority and problem solving responsibility from crew onboard to ground based crew will remove humans from the site of the problem and may result in errant problem solving in complex or time critical situations
LIVE5.2	• Communication faults will leave aircraft autonomous and reliant on completely automated systems, requiring an "all bases covered" approach to autonomous situation analysis and problem solving
LIVE5.3	• When functioning, onboard sensors may not give ground crew sufficient information to correctly analyze and resolve situations

LIVE6	**Flight crews - Crew-automation interactions issues**
LIVE6.1	• **Situation and Automation Awareness** - Increased automation and reduced training may lead to failure in correct monitoring, understanding, anticipation and control of automated systems and their functions - Loss of strategic and tactical situation awareness, including automation & mode awareness and airspace system functions may occur if flight management, system management and control of flight is transferred completely or partly from on-board crew to ground based crew - Increased automation may cause a loss of mutual strategic or tactical situational awareness. For example, data-linking ATC clearances will remove pilot awareness of the intentions of other aircraft in the vicinity - A poor automation logic/interface may lead to decision-making based on false or misleading assumptions
LIVE6.2	• Predominant use of automation may cause aircrew to have trouble performing traditionally simple operations such as manually switching to other runways, or overriding the autopilot in tight situations. Lack of aircrew training and/or experience coupled with manual flight in highly automated airplanes may lead to loss of aircraft control in unusual situations such as upsets, traffic avoidance or maneuvering. Loss of basic piloting skills through further automation may increase this problem further
LIVE6.3	• Advanced digital audio and alerting systems in aircraft cockpit may change crew workload and situational awareness. Highly automated alerting systems and checklist systems may make it difficult to discriminate between actual and nuisance warnings, resulting in inappropriate action. Checklist systems may be "too smart", bringing up the wrong checklist in a non-normal situation (AC 22)
LIVE6.4	• Complicated automatic or semi-automatic FMS modes make it difficult for crew to execute short term plan changes such as a change of runways on

	final approach or unexpected clearances
LIVE6.5	• There may be difficulty in reverting to less automated aircraft
LIVE6.6	• Automation may increase the possibility of monitoring errors, and degradation in situation awareness (flight crews, ATC, etc. are less in-the-loop)
LIVE6.7	• Lack of standardization, multiple hardware and software version issues, and compatibility issues between types, versions and models may cause operational and transitional difficulties
LIVE6.8	• High reliance on automation may cause reluctance to override automation or other flight crewmembers when required
LIVE6.9	• Prolonged dependency of high automation levels may lead to involuntary complacency in delegating, crosschecking, or challenging actions of other crewmembers when using automated flight guidance systems. It may also lead to the assumption that that automated flight trajectory is always free of obstacles. This is of particular concern at low altitudes en route and in terminal area navigation • Failure to fully understand all aspects of automation behavior may lead to non-intervention in cases where automation level or automation response is not appropriate for the situation
LIVE6.10	• Authorities and operators' trust in automation may lead to cost-driven reductions in training requirements, further increasing crew reliance and dependency on automation and lack of qualified intervention when required
LIVE6.11	• Abnormal/emergency situations combined with automation breakdown or failure (subtle or sudden) may create situations exceeding crew experience or training level
LIVE6.12	• Information can be transmitted to the pilot/crew, accepted by pilot/crew & then deleted before actual use (could be a data recovery issue) (advanced FMS)
LIVE6.13	• Sensor inadequacies may lead to incorrect parameter detection, for flight monitoring and failure detection, resulting in inappropriate automatic action being taken by system
LIVE6.14	• Hidden assumptions by designers may be inappropriate for all types of operator/crew cultures and operation environments, leading to unforeseen situations
LIVE6.15	• Difficulties to diagnose and manage of failures where system response is automatic or semi-automatic, in particular multiple system failures and automation failures, may lead to inappropriate responses
LIVE6.16	• Inability of pilots, ATM personnel, other airplanes or the SCC system to deal with aircraft not behaving as expected or as commanded
LIVE6.17	• Personal preference settings could possibly override basic safety features in Situational awareness displays, alerting systems or other safety-related flight deck functions
LIVE6.18	• Mode awareness: displays could be designed to not clearly display system modes by observation; the crew might be surprised
LIVE6.19	• Multiple alarms regarding related problems annunciating simultaneously and distracting from normal operational issues, causing confusion
LIVE6.20	• There potentially is different interpretation of information based on experience, culture, perception, training, and fatigue

Note. Many crew-automation interaction problems listed above, when considered at a sufficient level of generality, also apply to ATM / ATC / SCC personnel.

LIVE7	**Flight crews - Physical and physiological problems**
LIVE7.1	• Fatigue may lead to improper hand-off briefing on state of automation / traffic situation upon rest crew rotation

LIVE8	**Flight crews - Operational issues**
LIVE8.1	• Pilot experience: Reduced previous experience levels in pilot community may not be aligned with changing operational environment. More experienced pilots on older generation (pre-glass-cockpit) airplanes may have difficulty in adapting to a highly automated airplane
LIVE8.2	• Failure to develop and manage processes and procedures between flight crewmembers as well as between flight and ground crew members may lead to breakdown in compatibility of CRM processes and level of automation.
LIVE8.3	• Inappropriate reliance on automation: e.g. Failure to delegate, cross-check, and/or challenge actions of other crew members when using automated flight guidance systems (Example: crew assumption that automated flight trajectory is free of obstacles)
LIVE8.4	• Misuse (over-confidence and/or over-reliance) of CRM leading to loss of SA or hidden differences in assumed information and variance between crew mental models
LIVE8.5	• Real world conditions generate operational situations or requirements that were unanticipated by designers, so the flight crew is hampered in handling the situation by the technology itself. Examples: a. Failure of crew to coordinate actions and use of automation during close-in approach changes or when using non-customary runways, b. Excessive inherent flight deck noise or unusual warnings and alerts from automation
LIVE8.6	• Inappropriate application of CRM based on experience, culture, perception, training, fatigue causes CRM safety issues
LIVE8.7	• If flight crews are made responsible for traffic separation flight deck workload may increase beyond safe levels
LIVE8.8	• Human-Machine interface technology is improving, but complete requirements are currently not mandated
LIVE8.9	• Lack of all-weather capability at airports and on aircraft puts constraints on facilities available depending on weather. IFR reserves are affected and hence safety is affected
LIVE8.10	• ATC clearances: Procedures for updating clearances in the new ATM environment are uncertain. Applies to Fully Automatic Flight (FAF) too
LIVE8.11	• Requirements proscribing compliance to ATC Clearances may differ regarding mandating where to fly the aircraft, causing confusion and hazards
LIVE8.12	• Changing roles and responsibilities between flight crews and ATC (SCC) are likely to cause confusion during transition to the new airspace systems (C3) • Increasing amount of information available to ATC personnel and pilots are likely to cause confusion unless excellent human factors technology is used in development of the new airspace system (C3) • Determining appropriate amount and correct type of information to be displayed for adequate command and control by SCC and flight crews will be a significant challenge (C3)

LIVE9	**Flight crews - Training issues**
LIVE9.1	• Pilots may be incorrectly and/or partially trained
LIVE9.2	• CRM specific problems: failure by designers to understand crew processes and procedures, failure by training authorities and operators to fully understand relationship between automation and CRM. There is psychological resistance to use of automation at the proper level for normal and abnormal situations due to incorrect or partial training
LIVE9.3	• Inappropriate application of CRM based on experience, culture, perception, training, fatigue may lead to differences in assumptions and limitations
LIVE9.4	• Failure of CRM principles and/or retention of wrong principles due to repeated exposure to different CRM practices in training result in incompatible flight crews
LIVE9.5	• During transition to the new ATM environment, there may be training issues associated with differing levels of navigational technology installed on each airplane. Variation of automation capabilities may require alternate CRM approaches

LIVE10	**Flight crews - Qualification and cultural issues**
LIVE10.1	• Differences between pilots according to age, experience, national or cultural origin, education and training, may lead to different levels of trust of automation

LIVE11	**CNS/ATM/ATC and Supervisory Command and Control (SCC) system (regarding the Fully Automatic Flight (FAF) hypothesis) – New air space paradigm / Multi-agent issues**
LIVE11.1	• A sharing of responsibility and authority between air and ground agents may lead to differing perceptions during time-critical situations leading to inappropriate actions being taken
LIVE11.2	• Miscommunication between operators (CNS/ATM/ATC/SCC/Flight and/or Cabin crew under the FAF hypothesis, Airline, Ground and Airport personnel). Fully automatic flight removes operational decision makers from aircraft and may lead to communication problems between any other staff on board, and personnel on the ground. In the spirit of FAF, considerations should also be made for further functions becoming replaced by automated; i.e. ground-based traffic control and in-flight safety/service
LIVE11.3	• Available Bandwidth for SCC-Airplane communication is saturated so that proper coordination and control is not exercised for aircraft and other vehicles in the airspace system
LIVE11.4	• Because of information distribution problems, ATM/SCC/Operations of controlled vehicles may have different information (update type, amount, accuracy)

LIVE12	**CNS/ATM/ATC and SCC –** **Operations with mixed aircraft performance capabilities**
LIVE12.1	• Incompatible manned/automated sequencing of aircraft in terminal areas, with a mixture of automated & piloted aircraft could be a safety issue
LIVE12.2	• Operational errors by CNS / ATM / ATC personnel could occur while

	attempting to integrate traffic flows of automated & piloted aircraft
LIVE12.3	• Human intervention is needed by ATM personnel, but the ATM person may make a poor decision that propagates errors into the ATM system that the machines cannot solve
LIVE12.4	• There is a danger of aircraft departing from established operating corridors or aircraft taking action other than intended due to failure of ground operators to fully understand capabilities and limitations of aircraft in various energy states

LIVE13	**CNS/ATM/ATC and SCC – Crew / automation interactions issues**
LIVE13.1	• Local or minor problems may lead to a loss of situational awareness, distracting from dealing with a major problem elsewhere
LIVE13.2	• Local or wide-area loss of control may result due to data link failures, unintentional or intended interference or other factors

LIVE14	**CNS/ATM/ATC and SCC – Operational issues**
LIVE14.1	• Use of automation or of automated systems outside of intended function cause safety problems. Example: "climb in trail" with TCAS/ACAS
LIVE14.2	• Operational errors, e.g. danger of jumping checklist items & failure to cross check programming / control / supervision / command actions may be a hazard
LIVE14.3	• Improper Standard Operating Procedures within the SCC could be developed, causing inconsistent and hazardous ops
LIVE14.4	• Standard Operating Procedure updates and changes within the SCC could be improperly built
LIVE14.5	• Standard Operating Procedures within the SCC may be not properly linked through the information distribution network
LIVE14.6	• Receipts for distributed information from the vehicles or SCC may be incorrectly returned to the sender
LIVE14.7	• Lack of awareness and failure to acknowledge limitations of aircraft performance or automation programming limitations when issuing clearance may result in failure of aircraft to follow intended clearance
LIVE14.8	• Improper hand-off briefing on state of automation / traffic situation during shift handover may cause a hazard
LIVE14.9	• Transmitted data or clearances may be lost in transmission or by the receiver, resulting in "loss of control"
LIVE14.10	• Compliance with updated instructions from the SCC may be impossible because of performance limitations of vehicles, communication or humans
LIVE14.11	• Lack of following CRM may cause a failure of flight crew/ATM team to stay ahead of the airplane or the traffic situation, hence degrade the crew's ability to conduct the flight safely
LIVE14.12	• Poor Human Design or manufacture may cause misinterpretation of collision avoidance information (whether the source is on the aircraft or on the ground)
LIVE14.13	• Onboard pilot or ATM intervention may be needed but not available

LIVE15	**CNS/ATM/ATC and SCC –** **Adverse conditions / failure / emergency / crisis mgt issues**
LIVE15.1	• Failure to cope with adverse conditions: wide area weather impacts; closed/inoperative runways, closed airports, inoperative navigational aids, local situation not conforming to expectations (low braking action, wind gusts) etc. compromises safety
LIVE15.2	• Use of automation could allow controller/manager to exceed human recovery capabilities in the event of failure or automation breakdown. For example, CNS/ATM system failures could have more severe consequences when airplanes are more closely spaced, increasing the likelihood of collision when compared to current system
LIVE15.3	• In a non-normal situation, may be dependent on automation to keep the workload low enough
LIVE15.4	• Sole reliance on an off board navigational information source such as GPS, combined with the unavailability of that system, causes CNS-ATM system failure and severe accident hazards simultaneously throughout the ATM System
LIVE15.5	• Sabotage; Intentional damage or degradation of systems, either through physical means or through cyber attacks is a possibility
LIVE15.6	• Crew interpretation and reporting of aircraft system faults may not be adequately duplicated by automated remote sensing systems. For instance, the smoke detectors may not be able to sense a faint odor that would have alerted a human flight crew of onboard smoke (MR05)
LIVE15.7	• Interactions with cabin crews: automatic or ground-based alerts may not have development issues for FAF. Examples of cabin crew alerts include turbulence encounters, coordination of use of Portable Electronic Devices, medical emergencies, security issues, etc.

LIVE16	**CNS/ATM/ATC and SCC – Training issues**
LIVE16.1	• Controllers not appropriately trained may cause safety problems
LIVE16.2	• ATC Managers not appropriately trained cause safety problems
LIVE16.3	• Failure to provide awareness of flight crew CRM principles (crew workload, etc.) and related automation issues, in particular in stressful situations, to CNS / ATM / ATC and SCC (in case of FAF) personnel (Management / Authorities issue)
LIVE16.4	• Inappropriate application of Team Resource Management based on experience, culture, perception, training, fatigue could be hazardous
LIVE16.5	• Failure of Team Resource Management principles and/or application of wrong principles due to repeated exposure could lead to complacency, causing a reduction in safety

LIVE17	**CNS/ATM/ATC and SCC – Qualification and cultural issues**
LIVE17.1	• Experience, education, training and qualification, currency, knowledge and skills problems may result the in aircraft not being operated as designed, or a design not being appropriate for intended types of operation
LIVE17.2	• Different interpretation among the SCC personnel of operational conditions/events based on experience, culture, perception, training, fatigue, lack of Situational Awareness, language difficulties, may cause inappropriate commands being given to airplanes and other vehicles

LIVE18	**Maintenance**
LIVE18.1	• Difficulties in passing to and discussing information between flight and maintenance crews (in particular for FAF) and lack of intelligent problem analysis may create difficulties in responding to situations in a timely and appropriate manner

LIVE19	**Cabin crews**
LIVE19.1	• Cf. LIVE15.7

LIVE20	**Passengers**
LIVE20.1	• Fully automated flight may create unforeseen passenger behavior and reactions in abnormal or emergency conditions
LIVE20.2	• Portable Electronic Devices (PED’s) onboard airplanes may produce Electromagnetic Interference, endangering the communication or control functions of the airplane and other components of the airspace system. This is also a security issue; intentional interference with airplane though Electromagnetic Means

LIVE21	**General**
LIVE21.1	• Humans may "game" the system in unanticipated ways, causing unanticipated hazards
LIVE22.2	• Without agreements regarding transitions and handoffs in Free Flight environment, confusion, navigational uncertainty and risk of collision will be increased

3. FAST Top Priority Hazards related to AC13 "Increase Reliance on Cockpit Automation"

Using a **prioritization** process FAST came with a list of principal automation hazards shown hereunder.

The SHEL statements were prioritized using a technique called the data grid method. Each of the SHEL statements was assessed by **severity** (if it occurs, how bad will it be) and **temporal horizon** (when will it occur). The categories of severity were modeled after JAR/AC 25.1309, i.e., no effect to Catastrophic. The temporal horizon ranged from current to future-long (>20 years). This process resulted in a listing that could be grouped by SHEL Category and severity within a pre-determined temporal horizon. Unfortunately, the resultant listings within each temporal horizon were grouped quite closely, so the "ten-vote" method (first used in the prioritization of the ATA listings) was used to identify the top candidates in each temporal zone across SHEL categories. The results were used to create consolidated lists of hazards for future use by the FAST team. The list of principal hazards is presented below.

This list is organized using **4 time frames**: 6 principal hazards are considered current (Up to 1 year); 7 are considered future-near (1-5 years); 6 are considered future-medium (5 to 10 years); 2 are considered future-long (more than 10 years).

This list represents the **top-21 hazards out of a total of 286.**

Note: One may be surprised to find hazards in relation to fully automated Flight in the time-frame future-medium:
Fully Automated Flight (FAF) has been used as automation extreme with the objective to avoid overlooking essential details. FAST does not foresee FAF for Commercial Air Transport before 20 years from now. However, in FAST opinion, the operation of UAV's (Uninhabited aerial vehicles) mixed with normal traffic in civil airspace will be the first step towards FAF and this poses already major safety issues.

Hazards List			
	Current (Up to 1 year) [Reference time = 2003]		Related Hazards
1	LIVE 4.1	**Flight crews - Conflict between air / ground information sources**: Poor escape maneuver decision due to conflict between different information sources (e.g. TCAS, ATC verbal messages, data link) and lack of explicit prioritization	
2	LIVE 6.11	**Flight crews - Crew-automation interactions issues**: Abnormal/emergency situations combined with automation breakdown or failure (subtle or sudden) may create situations exceeding crew experience or training level	Live 6.1.1 Soft 4.26 Soft 6.4
3	LIVE 6.2	**Flight crews - Crew-automation interactions issues**: Predominant use of automation may cause aircrew to have trouble performing traditionally simple operations such as manually switching to other runways, or overriding the autopilot in tight situations. Lack of aircrew training and/or experience coupled with manual flight in highly automated airplanes may lead to loss of aircraft	

		control in unusual situations such as upsets, traffic avoidance or maneuvering. Loss of basic piloting skills through further automation may increase this problem further	
4	Soft 6.3	**Operations - Flight operations / interactions with automation**: Loss of automation behavior awareness due to complexity of automation modes. Pilot needs to know what the airplane “thinks” is going on (matching expectations) (C3)	Live 6.9b Soft 4.25 Soft 6.1
5	Hard 7.4.1	**Databases, software products & applications**: Failures in databases caused by wrong data or errors in updating the databases can affect the integrity and result in inaccurate, misleading (content errors), obsolete or inadequate information. (AC10) (C7) (AC20)	
6	LIVE 15.5	**CNS/ATM/ATC and SCC – Adverse conditions / failure / emergency / crisis mgt issues**: Sabotage; Intentional damage or degradation of systems, either through physical means or through cyber attacks is a possibility	
	Future – near (1 – 5 years)		
7	LIVE 6.1.4	**Flight crews - Crew-automation interactions issues**: A poor automation logic/interface may lead to decision-making based on false or misleading assumptions	
8	Soft 2.8	**Operating Procedures**: Inadequate processes for certification of computer software (including interactions with other software systems and artificial intelligence) onboard the aircraft and in the larger airspace system (C1, ANS20)	
9	LIVE 15.4	**CNS/ATM/ATC and SCC – Adverse conditions / failure / emergency / crisis mgt issues**: Sole reliance on an off board navigational information source such as GPS, combined with the unavailability of that system, causes CNS-ATM system failure and severe accident hazards simultaneously throughout the ATM System	
10	Env 2.3	**Hazards inherent to new airspace paradigm and from a large, distributed and inter-related Air / Ground / Space (AGS) system**: Loss of situation awareness (global, local)	
11	Hard 4.4b	**Compatibility, integration, configuration management issues** *(Including for HM Interfaces and Software applications):* Failure or malfunction caused by incorrect functional interfaces	
12	Hard 7.1b	**Databases, software products & applications**: Widespread power failures and software failure / error propagation increases the potential for unknown failure conditions	

13	LIVE14.1	**CNS/ATM/ATC and SCC – Operational issues**: Use of automation or of automated systems outside of intended function cause safety problems. Example: "climb in trail" with TCAS/ACAS	
	Future-Medium (5 to 10 years)		
14	Env 2.1	**Hazards inherent to new airspace paradigm and from a large, distributed and inter-related Air / Ground / Space (AGS) system**: Failure to integrate onboard and ground systems, e.g. control functions, data link, personnel, responsibilities - ATM/ATC and aircraft control functions (distributed multi-agent control system) - Data link with many outside partners: ATM / ATC and SCC (under the Fully Automated Flight hypothesis) - ATM / ATC / OPS / SCC (under the FAF hypothesis) / Flight Crew / Cabin Crew, including security and medical personnel (in particular for FAF) / Maintenance (in particular for FAF)	
15	Env 2.5	**Hazards inherent to new airspace paradigm and from a large, distributed and inter-related Air / Ground / Space (AGS) system**: Inability of individual & total system to deal with aircraft not behaving as expected, with sudden weather problem, airport closure, air or ground accident, etc. (more serious hazard regarding Fully Automated Flight)	
16	LIVE5.3	**Flight crews - Absence of human agent (onboard):** When functioning, onboard sensors may not give ground crew sufficient information to correctly analyze and resolve situations	
17	LIVE6.1.2	**Flight crews - Crew-automation interactions issues**: Loss of strategic and tactical situation awareness, including automation & mode awareness and airspace system functions may occur if flight management, system management and control of flight is transferred completely or partly from on-board crew to ground based crew.	
18	LIVE15.2	**CNS/ATM/ATC and SCC – Adverse conditions / failure / emergency / crisis mgt issues**: Use of automation could allow controller/manager to exceed human recovery capabilities in the event of failure or automation breakdown. For example, CNS/ATM system failures could have more severe consequences when airplanes are more closely spaced, increasing the likelihood of collision when compared to current system+C54	
19	LIVE13.2	**CNS/ATM/ATC and SCC – Crew / automation interactions issues**: Local or wide-area loss of control may result due to data-link failures, unintentional or intended	

		interference or other factors	
	Future-Long (more than 10 years)		
20	Hard 2.2	**Absence of human agent (onboard):** Lack of mechanisms to replace human cross-check of misleading or inaccurate data transmitted to & from the aircraft (in particular for Fully Automated Flight) may result in inappropriate actions being taken to ensure safety of flight. Lack of human redundancy (in particular for Fully Automated Flight) (MRO5)(AC1)(AC19)	
21	Hard 2.1a	**Absence of human agent (onboard):** Mechanisms to replace human sensing and processing of abnormal conditions: smoke, odors, vibration, noise, etc. (in particular for Fully Automated Flight) may be insufficient to cope with critical situations.	

List of Acronyms

Acronym	Meaning
AC	Aircraft
ACAS	Also TCAS, the Traffic Awareness and Collision Avoidance System
AGS	Air / Ground / Space system
ANS	Air Navigation System Area of Change
AoC	FAST Areas of Change, classified into the following 11 categories: Aircraft (AC) Maintenance, Repair & Overhaul (MRO) Operations (OP) Crew (C) Passenger (P) Organization (O) Authority (AUTH) Air Navigation System (ANS) Airport (AP) Environment (E) Space (S)
AI	Artificial Intelligence
ATA	Air Transport Association
ATC	Air Traffic Control
ATM	Air Traffic Management
COTS	Commercial Off-The-Shelf (products)
CNS	Control, Navigation and Surveillance
CRM	Crew Resource Management, also refers to the Crew Resource Management focus topic for AoC AC13.
CTDI	Conflict Detection Traffic Information
EMI	Electro-Magnetic Interference
FAF	Fully Automatic Flight
FAST	Future Aviation Safety Team
FMS	Flight Management System
GA	Go Around
GPS	Global Positioning System
HF	Human Factor(s)
HMI	Human Machine Interface
IAL	Instrument Approach and Landing
MRM	Maintenance Resource Management, or CRM for Maintenance

	personnel
MRO	Maintenance, Repair & Overhaul Area of Change.
OPS	Operations, Operations personnel
PED	Personal Electronic Device. Examples: Cell Phones, Laptop Computers, and Pagers
PF	Pilot Flying
PNF	Pilot Non Flying
SAD	Situational Awareness Display
SCC	Supervisory Command and Control system. For these documents, it is an envisioned future airspace-system-wide function that coordinates air traffic
SHEL	Software, Hardware, Environment, Liveware taxonomy.
SOP	Standard Operating Procedure
STC	Supplemental type certificate
TC	Type Certificate
TCAS	Also ACAS, the Traffic Awareness and Collision Avoidance System
TRM	Team Resource Management, or CRM for larger crew, for instance ATC crew
UAV	Un-piloted Aeronautical Vehicle
V&V	Validation and Verification