Tracking Failures in the Air Traffic System: A model Based on Physical and Functional Decompositions

Maxime Gariel, Erwan Salaün, and Eric Feron
School of Aerospace Engineering
Georgia Institute of Technology
Atlanta, Georgia 30332–0250, USA
maxime.gariel@gatech.edu, erwan.salaun@gatech.edu, feron@gatech.edu

***Abstract*—This paper presents a model for the air traffic system that aims at tracking failures and at measuring their impact on air traffic operations. This model is based on physical and functional decompositions of the air traffic system, which splits into facilities, aircraft, technologies, human operators, communication media, functions, tasks and operations. Possible failures are introduced at different levels of the decomposition and their consequences can be easily analyzed thanks to links between the blocks of the model. Two case studies illustrate how this model allows to anticipate the failures propagation and to find alternative solutions.**

I. Introduction

The Air Traffic System (ATS) is a complex system that involves thousands of pieces of equipments, vehicles, facilities and people working together. The current system is aging and its modernization requires new technologies, automation and operations that should be compatible with the existing system. Weaknesses in the current centralized, voice-communication-based system include travel delays due to weather, safety and security breakdowns, the inability to adapt to new technologies such as uninhabited aerial vehicles, and a lack of dynamic adaptability in the face of disturbances and failures. The goals for the Next Generation Air Transportation System (NextGen) [1] in the United States and SESAR [2] in Europe focus on significantly increasing the safety, security, and capacity of air transportation operations, via new procedures and technological advances for all modes of air transport. In NextGen and SESAR, aircraft are expected to have a wider range of capabilities than today and support varying levels of total system performance via onboard capabilities and associated crew training. Many aircraft will have the ability to perform airborne self-separation, spacing, and merging tasks independently. Increased use of automation, reduced separation standards, Super-Density arrival/departure operations, and additional runways allow busy airports to move a large number of aircraft through the terminal airspace during peak traffic periods. However, in order to enable future capacity, NextGen will encompass novel technologies, vehicle types and operational concepts, and will ultimately bring forth new types (or modes) of failures and disruptions. If unattended, these disruptions could result in severe setbacks for the NextGen and SESAR agendas and the health of the air transportation system as a whole. Tracking the propagation and the impact of failure gets always more difficult with the increasing complexity of the system.

The introduction of new technologies and new aircraft is not possible unless they have been certified with a very low failure tolerance, resulting in very few critical onboard failures. Nevertheless, some faults still occur but are often due to exogenous factors such as the bird strike that downed flight 1549 [3] in the Hudson river. Ground infrastructure are also regularly affected by unexpected exogenous factors. On April 23, 2009, the Atlanta Hartsfield Jackson International Airport control tower was hit by a lightning and severe storms knocked out power to the area and the airport lights [4]. The tower had to be evacuated, leaving the airport inoperative, no aircraft being able to take off nor land. Probably more critical was the evacuation of the Southern California TRACON (SCT) in 2003 because of wildfires [5] threatening the facility. Technologies, or pieces of equipment are also subject to failures such as radar outages: in May 2007, the SCT was affected by an outage that let the controllers mapless for an hour [6]. Similarly, in 2004, a computer glitch in the radar system disabled the surveillance of flights above 24,000ft [7] in the United Kingdom. Flight data had to be entered manually, resulting in a decrease in capacity and increase in spacing distances. Air Traffic Controllers (ATCs) are the eyes of the pilots and require a good sight to maintain the safety of the airspace. Surveillance is critical but cannot be achieve without reliable communications, which are used to transmit surveillance data from the radar to the control facilities, to transmit information between ground facilities and aircraft, and among ground facilities. If a control center loses its communication capacities, tens or hundreds of aircraft are left deaf and blind. On September 25, 2007, Memphis ARTCC experienced a total communication failures. Controllers had to coordinate with other ARTCC using their cellphones [8], [9], [10], [11]. The breakdown lasted for about 4 hours. Communication are also critical for navigation purposes. If the frequencies carrying the GPS signals are jammed [12] or spoofed, GPS navigation is not possible anymore. The irresponsiveness of flight 188 [13] is an interesting example of

communication and navigation failures due to a human error, when the pilots did not contact ATCs for over an hour and a half and overshot their destination point by 90 NM.

In all of the examples above, disastrous consequences were avoided thanks to the extraordinary ability of humans to accommodate to unexpected situations. With the increase of automation in the Air Traffic Management (ATM) system, it becomes more difficult to track the impact of a partial or total failure. Sheridan analyzed the issues [14] associated with the human-automation interactions in the next generation air transportation systems: *"Because of the greater interconnectedness of aircraft and subsystems, equipment failures and misapplied procedures can cause perturbations that cascade throughout the whole system."* In the event of a failure of the automation, degradation mode should be available for the human controller to safely handle the system. A thorough knowledge and modeling of the degradation modes of the ATS is necessary to ensure its safety.

This paper presents a model of the ATS based on a multi-dimensional decomposition, aiming at analyzing the impact of failures. A large share of the work in ATM is devoted to improving the performances of the current system and assessing new concepts of operations. Being at the center of air traffic operations, ATCs have been often modeled ([15], [16]). Human in the loop simulations are used to validate new concepts [17] and tools to identify human errors in air traffic control have been developed [18]. At a higher level, Pinon et al. modeled the air transportation system as a supply chain [19] to measure its performances and constraints. Using a modeled network of airports they studied the benefits of 4-D trajectory-based operations. Pinon et al. also presented a morphological decomposition of the air traffic operations, to evaluate and select airport technologies [20]. The system was decomposed from traffic phase, to possible improvements, to operational concepts, to functions, to technologies and finally, to sub technologies. A matrix of alternatives is created from this morphological analysis [21]. This decomposition is oriented towards finding appropriate technologies to optimize operations. However, this decomposition is unidirectional and does not allow to keep track of failures and to measure the loss of performances.

The objective of this paper is to present a model that captures how failures or perturbation cascade throughout the system and that measures their impact in terms of loss of capabilities. If the impact of a failure is known, it becomes easier to ensure the graceful degradation of operations when the failure will occur. A "graceful degradation" of air traffic operations is defined as the smooth transition from nominal to degraded modes of operations [22]. Algorithms and maps have been developed to spread out the traffic in the event of a degradation [23], [24].

The remainder of this paper is organized as follows: section II introduces the model, its objectives, how the ATS is decomposed, the links between the blocks, and how failures are introduced and tracked. Section III consists of case studies to illustrate some implementation of the model, before the concluding remarks.

II. A Model for failure tracking in air traffic systems

A. Presentation of the model

1) Objective of the model: The objective of the model is to provide a better understanding of the propagation of failures in the ATM system, and to measure their impact in terms of loss of capabilities. The model shows the propagation of failures, from a facility, a controller or a technology, all the way to operational capabilities. The model allows the identification of alternate or backup technologies, to analyze how a loss of automation can be handled by a human controller to ensure the safe transition from a nominal and automated, mode of operation to a degraded and manual mode of operation.

2) System: The modeled system is the air traffic system, consisting of all the infrastructures, technologies, communication media, people, etc, that are necessary for the air traffic system to be fully operative. The system also includes aircraft and pilots. The introduction of new technologies and automation systems can be tested and added to the model as they are being developed.

3) Model description: The model combines a physical decomposition of the major components of the ATS, and a functional decomposition of the air traffic operations into tasks and then functions. This model combines elements from the decompositions presented by Pinon et al. on the one hand ([20]), and Kim et al. on the other hand ([25]). Pinon et al. decomposed air traffic operations to identify enabling technologies. Kim et al. proposed a task decomposition for function allocation.

This model starts from a physical decomposition of the system in facilities and aircraft, then decomposes them into technologies and human operators. Human operators and technologies execute functions that are enabled by other functions and communication media. Then, those functions are used to execute tasks. Finally, tasks are combined together to enable operations.

Figure 1 presents a diagram of the decomposition of the elements of the model. The terms used in this model are defined as follow:

- **Facilities/Aircraft:** This category groups physical pieces of equipment and/or people located at the same place. A *Facility* refers to a building or place that provides a particular service or is used for a particular purpose. For instance, the TRACON facility refers to the physical building in which air traffic controllers work to direct aircraft in the corresponding TRACON airspace. A facility can also refer to a simple building, e.g. the building and mount for a radar or an Automatic Dependent Surveillance - Broadcast (ADS-B) ground station.
  An *Aircraft* refers to a vehicle that can fly and enter the controlled airspace, such as an airplane, a helicopter or an unmanned aerial vehicle.
- **Technologies:** A *Technology* refers to a physical piece of equipment such as a transponder, a radar, etc. A

TABLE I
INFLUENCE STRUCTURE AND DIMENSIONNALITY

Origin		Destination	Dimension	Meaning
Facility	→	Technology	Hosts	The technology is physically located inside the facility.
Facility	→	Human operator	Hosts	The human operator is physically located inside the facility.
Technology	→	Function	Executes	The technology executes this function. The information available to the technology is used to perform the function that will generate new information.
Function	→	Technology	Provides information	The output of this function is used by the function. The information generated by the function is used by the technology.
Human operator	→	Function	Executes	The human operator executes this function, generating new information.
Function	→	Human operator	Provides information	The human operator uses the output of this function. The information is received by the operator.
Function	→	Communication media	Emits on	The output of the function is transmitted over the communication medium. The communication medium must be available for the information to be successfully transmitted.
Communication media	→	Functions	Transmits	The communication medium transmits information that can be captured by the receiving function.
Function	···	Function	Is equivalent	The two functions are equivalent, in terms of role. They might have a different level of performance.
Function	→	Tasks	Enables	The function enables the task. A task might require several functions to be achieved.
Tasks	→	Operation	Enables	The accomplishment of the task is required for the operation to be conducted.

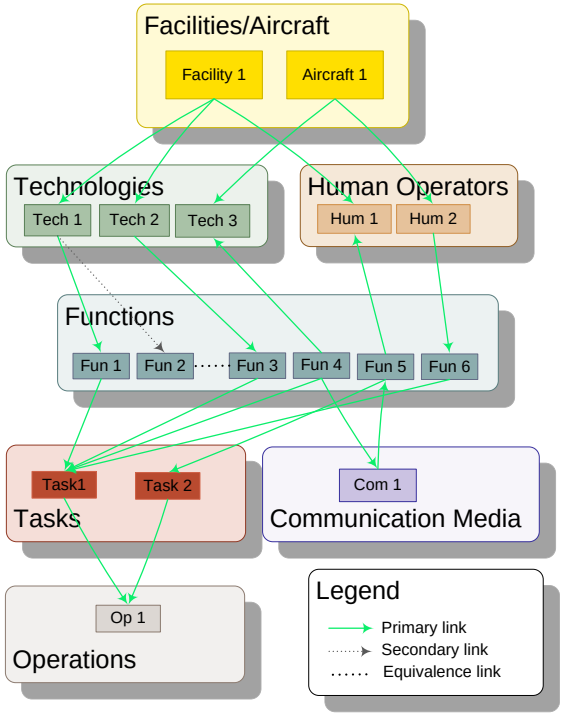

Fig. 1. Model's decomposition

technology is located in a facility or an aircraft and executes one or several functions.

- **Human Operators:** A *Human Operator* refers to a human being qualified to execute the tasks required by his position/job. Human operators include pilots and air traffic controllers. Human operators are located in facilities or an aircraft and execute one or several functions.
- **Communication Media:** A *Communication Medium* refers to the transmission channel or tool used to deliver information, such as radio waves in a given range of frequencies, phone lines, etc.
- **Functions:** A *Function* refers to "a capability without a goal", of a technology or a human being. Transmitting information or displaying information on a screen are examples of functions.
- **Tasks:** A *Task* refers to a tangible activity with a goal. A task is made possible through the combination of functions. Monitoring aircraft position is an example of task.
- **Operations:** An *Operation* refers to a tangible activity with a goal resulting from the combination of several tasks. For instance, sequencing and merging is an operation that requires air traffic controllers to direct aircraft, pilots to follow ATC instructions and fly the aircraft.

This decomposition allows the introduction of failures at different levels (Section II-B). The propagation of a failure can be tracked in the model using its influence structure.

4) Influence structure and dimension: The influence structure of the model is the set of relationships and links existing between the different components of the model. The signification of the links between the elements is presented in Table I. The dimension corresponds to the type of relationship existing between the linked blocks. The term *origin* refers to the block at the tail of the arrow, and *destination* refers to the block located at the head of the arrow. The relationship "Hosts" means that the destination block is located inside the origin block. The relationship "Executes" means that the origin block executes the destination block. The relationship "Emits" means

TABLE II
EXAMPLE 1: PROPAGATION OF A FAILURE DUE TO INOPERATIVE BAROMETRIC ALTIMETER

Origin (Type)		Destination (Type)	Explanation	Level of Failure
Barometric altimeter (Tec)	→	Measure Altitude (Fun)	The altimeter cannot measure the altitude.	Total
Measure Altitude (Fun)	→	Onboard Mode-S Transponder (Tec)	The Mode-S transponder cannot get the altitude information.	Total
Onboard Mode-S Transponder (Tec)	→	Transmit Information (1090MHz) (Fun)	The Mode-S transponder cannot transmit the altitude information.	Partial
Transmit Information (1090MHz) (Fun)	→	Radio Waves (1000Mhz) (Com)	There is no altitude information to transmit.	Partial
Radio Waves (1000Mhz) (Com)	→	Receive Information (1090MHz) (Fun)	There is no altitude information to receive.	Partial
Receive Information (1090MHz) (Fun)	→	Ground Mode-S Transponder (Tec)	The transponder cannot receive the altitude information.	Partial
Ground Mode-S Transponder (Tec)	→	Display of aircraft position (Fun)	The position of the aircraft cannot be accurately displayed since the Mode-S transponder did not receive altitude information.	Partial
Display of aircraft position (Fun)	→	Surveillance (Task)	The surveillance task cannot be executed properly as the altitude of an aircraft is missing.	Partial
Measure Altitude (Fun)	→	Fly holding Pattern (Task)	It is not possible to fly a holding pattern since it requires to maintain the altitude, which is not available.	Total
Fly holding Pattern (Task)	→	Sequencing and Merging	Sequencing and merging might require an aircraft to fly a holding pattern. Since this task cannot be achieved by all aircraft, this operation runs in a degraded mode.	Partial
Surveillance (Task)	→	Sequencing and Merging	Sequencing and merging requires that the surveillance task is achieved properly.	Partial

that the origin block emits information using the destination block. The relationship "Transmits" means that the origin block transfers the information to the destination block. The relationship "Enables" means that the origin block makes the achievement of the destination block feasible. The relationship "Equivalence" does not carry any dependence information. It is used to determine redundancy in the technologies.

The model has three types of links: primary, secondary and equivalence.

- **Primary links:** Primary links correspond to nominal interactions between the different components. They are represented by colored arrows: a green and plain arrow indicates a link working nominally. A dashed orange link indicates that some of the information nominally carried by the link is missing. A dotted red arrow indicates the the link is no functional.
- **Secondary links:** Secondary links correspond to redundancies, not used in nominal modes. They are also represented by colored arrow: when the link is inactive, it is represented by a dashed gray line and when active, it takes the colors of a primary link. For instance, the primary radar can be used as a backup for the secondary radar, but does not provide the same level of performance. The functions enabled by the primary radar are contained in the model, but the links are listed as secondary, since they are not used during nominal operations.
- **Equivalence links:** Equivalence links join blocks with similar characteristics. They are represented by black dotted lines. Two technologies are equivalent if and only if they are identical. If they are not, they can perform identical functions which will have the equivalence relationship. Two equivalent functions can have different level of performance. Equivalence links allow the model to find redundant systems to perform failed functions.

B. Failures and degradations modes

The model enables the introduction of failures at all the levels of the decomposition. Failures can affect single or multiple blocks but cannot be introduced on links. The color of the links presented in the previous section refers to the type and the availability of the information they carry. Failures can affect:

- **Facilities/Aircraft:** Failures affecting facilities and aircraft are potentially the most difficult to handle, since they host many people and technologies. Such failures can be total or partial. When a facility failure is total, it is propagated to technologies and human operators located in this facility. When the failure is partial, only some technologies or human operators will be set as "failed". A total failure can be visualized as a master switch for all the technologies and people in the facility. A partial failure can be seen as a switch for a particular room.
- **Technologies:** A technology can fail because the facility in which it is located fails, or because the technology itself fails. The same way facilities fail, technology failures can be partial or total. If the failure is total, all the functions enabled by the technology will be set to inoperative. If the failure is partial, only a set of functions will be set to inoperative.

- **Human Operators:** Failures affecting human operators are modeled the same way than failures affecting technologies.
- **Communication Media:** When a communication medium fails, the information it carries cannot reach its destination. Therefore, the link exiting the medium will be disabled, meaning that the information cannot be transmitted.
- **Functions:** A failure cannot be introduced at the function level. If a technology or an operator cannot execute a function, it is modeled as a partial failure of the technology or operator. A function can fail if its input link(s) carry failures.
- **Tasks:** Tasks can fail by the propagation of functions failures. Failures at a task level can also be introduced to model human errors. Task failures propagate to the operation level. Backtracking of task error is possible but likely to provide too many possible origins.
- **Operations:** Operations can fail by the propagation of tasks failures.

When a failure is introduced in the model, the failure is propagated along and its impact can be measured by an incapacity of executing tasks and operations. Since links also carry partial failures, the model also allows to measure decrease in performances.

III. Case Study

This section presents two case studies for the model. The first case illustrates the propagation of a failure of the barometric altimetry in one aircraft. The second case shows how the model can be used to find alternative technologies in the event of a GPS jamming.

A. Failure of the barometric altimetry in one aircraft

In this example, a failure is introduced in the barometric altimetry of an aircraft. It is assumed that the technologies providing this function are inoperative. Figure 2 presents a simplified version of the model. The blocs are depicted in red if they are the origin of the failure, or if this element has failed totally. A block in orange is partially affected by the failure. It is visually easy to follow all the elements that completely failed and those which suffer of a loss in capabilities. Table II explains how the failure propagate along the model. The diagram in Figure 2 is a simplified version of the model, as it does not present all the elements of the system. Only some blocks were selected to illustrate the example.

B. Jamming of the GPS signal

Future operations highly rely on accurate positioning using GPS. Super Density Operation will require aircraft to precisely follow predetermined trajectories consisting of a sequence of way-points coordinates. GPS is necessary to ensure Required Navigation Performance (RNP) operations. ADS-B literally depends on the aircraft being able to determine its position, in order to broadcast it to ground stations and to other aircraft. Figure 3 depicts the impact of a GPS jam on ADS-B operations. This representation is slightly simplified and is organized by entity for a more compact view. This example presents only one direction of communication, that is only aircraft 2 trying to determine the position of aircraft 1 using ADS-B. This example shows how Traffic Information Services (TIS) could be used as a backup to ADS-B in operations in terminal areas. The link between ADS-B out of aircraft 1 and ADS-B in of aircraft 2 is the primary link for aircraft 2 to obtain surrounding traffic's information. If this link fails, the secondary link is activated and TIS is used as a backup system.

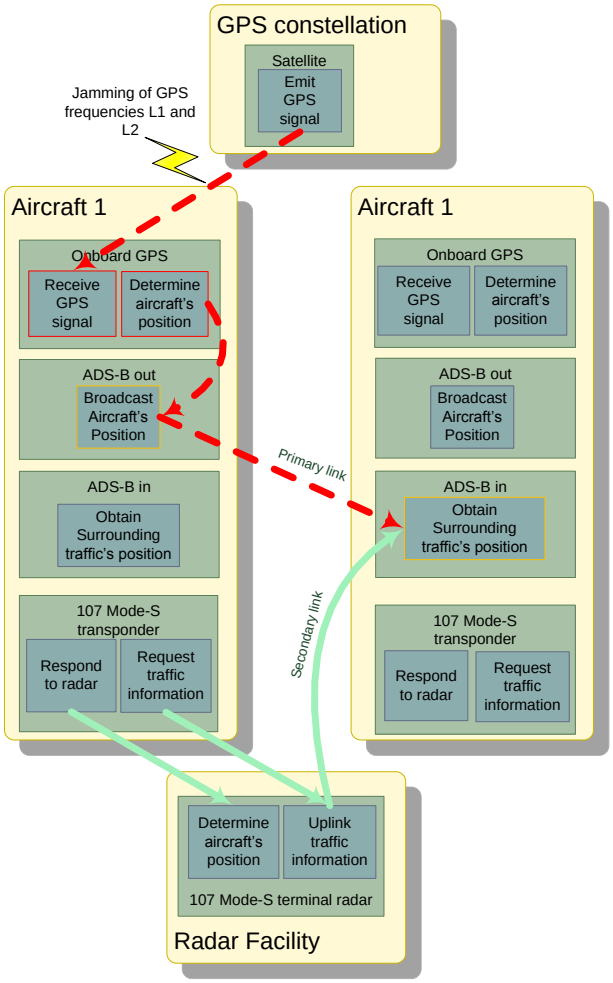

Fig. 3. Impact of GPS jamming on ADS-B operations

IV. Conclusion

This paper presented a model for the air traffic system based on a physical and a functional decomposition of the system. The physical decomposition includes facilities, aircraft and communication media and is linked to the functional decomposition of the operations into tasks and functions. Failures of systems or subsystems can be introduced at different level and their impact can be tracked all the way to the decrease of performances in the operations. As new technologies are

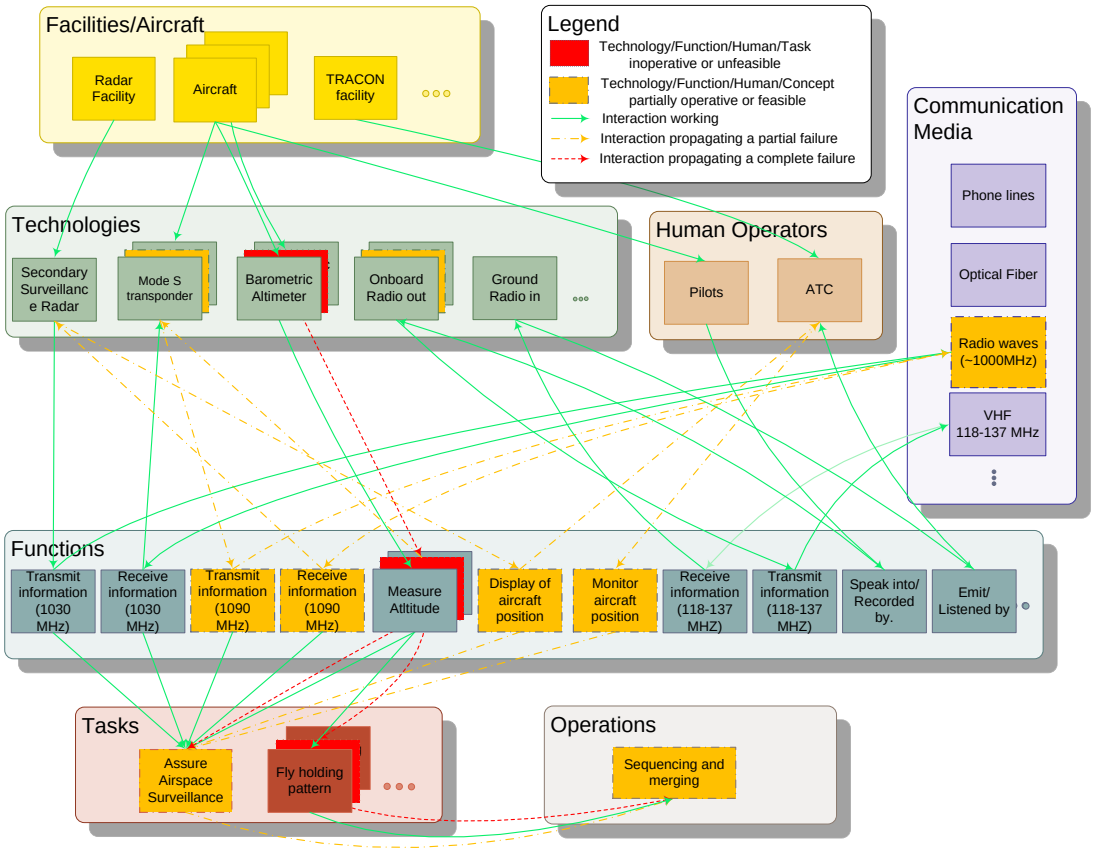

Fig. 2. Air Traffic System Model with a failure of the barometric altimeter in one aircraft

introduced to leverage new concepts of operation, this model allows to study their modes of failure and find alternative solutions to ensure the graceful degradation of the ATS.

Acknowledgments

This work was supported by Thales ATM inc, and under NASA Grant NNX08AY52A.

References

[1] Joint Planning and Development Office. NextGen. http://www.jpdo.gov/.

[2] Eurocontrol, The European Organisation for the safety of Air Navigation. SESAR, The Single European Sky ATM Research Programme. http://www.eurocontrol.int/sesar/.

[3] Wikipedia. US Airways Flight 1549, January 15 2009. http://en.wikipedia.org/wiki/US_Airways_Flight_1549.

[4] CNN. Atlanta airport reopens after lightning strike, April 2009. http://edition.cnn.com/2009/US/04/23/ga.airport.storms/index.html.

[5] pprune.org. Southern california tracon (sct) evac, October 2003. http://www.pprune.org/atc-issues/106897-southern-california-tracon-sct-evac.html.

[6] The Sweep / North County Times. Southern california tracon goes mapless, May 2007. http://atcmuseum.wordpress.com/2007/05/25/southern-california-tracon-spends-a-mapless-hour/.

[7] Guardian.co.uk. Flight delays continue after air traffic control failure, September 2008. http://www.guardian.co.uk/uk/2008/sep/26/transport.theairlineindustry.

[8] Encyclopedia.com. Air traffic control failure is examined, October 2007. http://www.encyclopedia.com/doc/1Y1-111174919.html.

[9] highbeam.com. Atc zero: even with backup systems and master plans, a catastrophic failure may still have critical air traffic control being done by cell phone.(system notes), December 2007. http://www.highbeam.com/doc/1G1-203027937.html.

[10] Memphis Business Journal. Telecom glitch stops departures at memphis international, September 2007. http://memphis.bizjournals.com/memphis/stories/2007/09/24/daily12.html.

[11] Yahoo News. Air traffic control failure is examined, October 2007. http://www.newsmgr.com/nm2/uploads/101107_ap_air_traffic_control_failure_is_examined.pdf.

[12] A. Pinker and C. Smith. Vulnerability of the GPS Signal to Jamming. *GPS Solutions*, 3(2):19–27, 1999.

[13] Airline Biz Blog. How the faa scolded the pilots, October 2009. http://aviationblog.dallasnews.com/archives/2009/10/how-the-faa-scolded-the-pilots.html.

[14] T.B. Sheridan. Next Generation Air Transportation System: Human-Automation Interaction and Organizational Risks. In *Proceedings of the 2nd Symposium on Resilience Engineering*, November 8-10, 2006, Juan-les-Pins, France.

[15] C. Niessen, K. Eyferth, and T. Bierwagen. Modelling cognitive processes of experienced air traffic controllers. *Ergonomics*, 42(11):1507–1520, 1999.

[16] S. M. Lee, S.Y. Kim, K. Feigh, and V. Volovoi. Structural framework for performance-based assessment of atm systems. In *9th AIAA Aviation Technology, Integration, and Operations Conference (ATIO)*, September 21 - 23, 2009, Hilton Head, South Carolina.

[17] T. Prevot, E. Palmer, N. Smith, and T. Callantine. A multi-fidelity simulation environment for human-in-the-loop studies of distributed air ground traffic management. In *American Institute of Aeronautics and Astronautics Modeling and Simulation Conference and Exhibit*, August 5 - 8, 2002, Monterey, CA.

[18] S.T. Shorrock and B. Kirwan. Development and application of a human error identification tool for air traffic control. *Applied Ergonomics*, 33(4):319–336, 2002.

[19] O. J. Pinon, K. Fry, and J.-P. Clarke. The air transportation system as a supply chain. In *AIAA Guidance, Navigation, and Control Conference and Exhibits, Chicago, Illinois*, August 10 - 13, 2009.

[20] O. J. Pinon, E. Garcia, and D. Mavris. A methodological approach for

airport technology evaluation and selection. In *26th International Congres of the Aeronautical Sciences*, September 14 - 19, 2008, Anchorage, Alaska.

[21] T. Ritchey. General Morphological Analysis. *A general method for non-quantified modeling, 16th EURO*, 1998.

[22] M. Gariel and E. Feron. Graceful Degradation of Air Traffic Operations: Airspace Sensitivity to Degraded Surveillance Systems. *Proceedings of the IEEE*, 96(12):2028–2039, 2008.

[23] M. Gariel, E. Feron, and J.P. Clarke. Air Traffic Management complexity maps induced by degradation of Communication, Navigation and Surveillance. In *AIAA Guidance, Navigation and Control Conference and Exhibit*, August 18 - 21, 2008, Honolulu, Hawaii.

[24] M. Gariel and E. Feron. 3D Conflict Avoidance under Uncertainties. In *Digital Avionics Systems Conference, DASC '09. IEEE/AIAA 28th*, pages 4.E.3–1 – 4.E.3–8, October 23-28, 2009, Orlando, Florida.

[25] S.Y. Kim, K. Feigh, S.M. Lee, and E. N. Johnson. a task decomposition method for function allocation. In *AIAA Infotech@Aerospace Conference*, April 6 - 9, 2009, Seattle, Washington.