AIAA Modeling and Simulation Technologies Conference
Honolulu, Hawaii – August 18-21, 2008

Development of a model-based safety analysis technique from the ETF Flight Simulator

M. Battipede* P. Gili† and M. Vazzola‡
Aeronautical and Space Department, Politecnico di Torino – 10129 Torino, ITALY

The low-cost multi-purpose multi-mission platform Elettra-Twin-Flyers (ETF) is being developed by the synergy of Nautilus S.p.A and the Politecnico di Torino[1]. It is a very innovative remotely-controlled airship equipped with high precision sensors and telecommunication devices. For its peculiar features, it is particularly suitable for inland, border and maritime surveillance missions and for telecommunication coverage extensions, especially in those areas which are either inaccessible or without conventional airport facilities and where the environmental impact is an essential concern.
ETF is characterized by great maneuverability as well as low wind sensitivity[2]. Flight conditions range from forward, backward and sideward flight to hovering, both in normal and severe wind conditions. To achieve these capabilities the ETF has been conceived with a highly non conventional architecture based on a double hull with a central plane housing structure, propellers, on board energetic system and payload. The ETF command system mainly consists of two vertical rotational axis ducted propellers and four thrust-vectoring propellers mounted on rotating vertical arms. The ducted propellers provide the vertical thrust for steep rapid climb and descent and control the pitch attitude of the vehicle. In addition, their action is combined with the helium buoyancy to produce lift in hovering and forward flight, where the lift is also incremented by the aerodynamic component. The four thrust-vectoring propellers control the lateral-directional attitude of the airship through the variation of the rotational speed (RPM) together with the rotation of the supporting vertical arms.
Flight tests are in progress on a flight demonstrator[3], which is a reduced-scale reduced-complexity platform, purposely assembled to test the most critical subsystems, such as the command system and the architectural solution. The system is also undergoing the European certification process, under the supervision of the Italian authority ENAC. According to ENAC, some of the scheduled flight tests are conditioned to specific permit to fly which should be issued upon the presentation of a safety analysis which should include a thorough risk assessment at the same strength of a conventional manned aircraft prototype. The airship, in fact, can be totally considered as an aircraft which has to accomplish a task. According to the Article 8 of the Chicago Convention[4] held in 1944 to regulate the international civil aviation, an unmanned aerial vehicle may be regarded as an aircraft that can be engaged in aerial activities. Apart from the Chicago Convention, other principles of international law may apply to UAV, such as the Montreal Convention[5] of 1971 and the Cape Town Convention[6] of 2001. The criteria sanctioned in these conventions and the remarkable efforts of the newly established UAV Task Force have led to a draft document, containing the guideline principles for the development of a regulatory concept for the civil UAVs, in terms of Airworthiness & Certification, Security, Operation & Maintenance & Licensing, Air Traffic Management and Airports. Among these guideline principles, in particular, the "equivalence concept" states that '*regulatory standards should be set to be no less demanding than those currently applied to comparable manned aircraft nor should they penalize UAV systems by requiring compliance with higher standard (...)*'[7]. The assessment of the ETF reliability and safety has been hence accomplished in accordance with the aforementioned assumption. A report on the analysis is presented in [8]

There are several standards, such as MIL-STD-882[9], DO-178B[10], IEC 61508 and 61511[11], ARP4754[12], UK Def Stan 00-56[13], which provide the guidelines to achieve this purpose and establish the essential preventive and alleviating safety measures that have to be adopted in order to not exceed the tolerable risk threshold. Whatever the standard is, before any quantitative analysis can be performed, it is usually necessary to carry out an accurate analysis of all the possible failures on all the subsystems and components, in order to undertake corrective actions in case the hazard occurrence probability (*Hazard Probability*) is too high for that particular severity level. The knowledge of the cause-and-effect relationships is essential to detect the root cause of a failure and evaluate the resulting chain of events. This step is called 'Hazard Analysis' and consists in an attempt to identify the potential

*Assistant Professor, Aeronautical and Space Department, manuela.battipede@polito.it
†Associate Professor, Aeronautical and Space Department, piero.gili@polito.it
‡Ph.D. Student, Aeronautical and Space Department, matteo.vazzola@polito.it

sources of danger for any human being of for the environment. In particular, for a novel and complex system, such as the new concept Nautilus airship, many hazards might rise from its innovative control system and other critical subsystems. To perform a reliable risk analysis all these hazards must be correctly identified, since the risks associated with unidentified hazards cannot be analyzed or reduced. This process is usually very time-consuming and performed 'manually' by a work team who has a deep knowledge of the system and try to speculate on every possible failure mode, component by component. Analyses such as FMEA[14] (Failure Mode and Effects Analysis) or Hazop, however, are based on an informal model of the system, and it is unlikely that these analyses will be complete, consistent, and error-free. Using precise formal models of the system as the basis of the analysis may help reduce errors and provide a more thorough analysis. The procedure of developing a hazard analysis from a formal model is called *model-based safety analysis*[15-18] and is one of the new frontiers of the Reliability & Safety analysis.

The main aim of this paper is to develop a procedure to perform a static analysis such as the FMEA, making use of a very detailed Flight Simulator[19] implemented in Simulink mainly for design purposes. The main concept behind the idea, is that Simulink is a tool purposely design to perform dynamic analysis, but can be used as a static analysis infrastructure, provided the flow of information is correctly propagated through the blocks and blocks have been properly augmented with information about component failures. In this paper we propose an approach of model-based safety analysis, in which the system and safety engineers use the same system models, extending the system model with failure information, as well as relevant portions of the physical system, in order to provide the safety analysis with automated support.

References

[1]Inventors: Gili, P.A., Battipede, M., Icardi, U., Ruotolo, R., Vercesi, P., Owner: Nautilus S.p.A. and Politecnico di Torino, "Dual hull airship controlled by thrust vectoring," N. PCT/EP03/08950, August 2003.

[2]Battipede, M., Lando, M., Gili, P.A., Vercesi, P., "Peculiar Performance of a New Lighter-Than-Air Platform for Monitoring", *Proceedings of the AIAA Aviation Technology , Integration and Operation Forum*, AIAA, Reston, VA, 2004.

[3]Battipede, M., Gili, P.A., Lando, M., "Prototype Assembling of the Nautilus Remotely-Piloted Lighter-Than-Air Platform", *Proceedings of the AIAA Aviation Technology , Integration and Operation Forum*, AIAA, Reston, VA, 2005.

[4]International Civil Aviation Conference, 1st November – 7th December 1944, Chicago, IL, USA.

[5]Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 23th September 1971, Montreal, Canada.

[6]Convention on International Interests in Mobile Equipment and its Protocol on Matters Specific to Aircraft, 16th November 2001, Cape Town, South Africa.

[7]JAA/Eurocontrol, "UAV TASK-FORCE – Final Report – A Concept for European Regulations for Civil Unmanned Aerial Vehicles (UAVs), 11 May 2004.

[8]Battipede, M., Gili, P., Maggiore, M., Lando, P., "Risk Assessment and Failure Analysis for an Innovative Remotely-Piloted Airship", *Proceedings of the AIAA Aviation Technology , Integration and Operation Forum*, AIAA, Reston, VA, 2006.

[9]MIL-STD-882: *System Safety Program Requirements/Standard Practice for System Safety*, Department of Defence, USA, 19 January 1993.

[10]RTCA/DO-178B: *Software Considerations in Airborne Systems and Equipment Certification*, Radio Technical Commission for Aeronautics, Inc., Washington, 1992.

[11]IEC 61511, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, International Electrotechnical Commission, 2004.

[12]ARP4754, *Certification Considerations for Highly-Integrated Or Complex Aircraft Systems*, SAE International, 1996.

[13]Interim UK Defence Standard 00-56, *Safety Management Requirements for Defence Systems*, Defence Procurement Agency, 1996.

[14]IEC 60812 "Procedures for failure mode and effect analysis (FMEA), International Electrotechnical Commission, 1985.

[15]Anjali Joshi and Mats P.E. Heimdahl, "Model-Based Safety Analysis of Simulink Models Using SCADE Design Verifier", Springer Berlin / Heidelberg, Volume 3688/2005, 2005.

[16]S. Simani, "Fault diagnosis of a simulated industrial gas turbine via identification approach", International Journal of Adaptive Control and Signal Processing, Volume 21, Issue 4 , Pages 326 – 353, John Wiley & Sons, Ltd., 18th Sept 2006.

[17]P. Struss, B. Rehfus, R. Brignolo, F. Cascio, L. Console, P. Dague, P. Dubois, O. Dressler, and D. Millet, "Model-based Tools for the Integration of Design and Diagnosis into a Common Process", 13th International Workshop on Principles of Diagnosis, Semmering, Austria, 2002.

[18]Anjali Joshi, Steven P. Miller, Michael Whalen, Mats P.E. Heimdahl, "A proposal for model based safety analysis" Presented at the 24th Digital Avionics Systems Conference, Washington, D.C., October, 2005.

[19]Battipede, M., Gili, P.A., Lando, M., Massotti, L., "Flight Simulator for the Control Law Design of an Innovative Remotely-Piloted Airship", *Proceedings of the AIAA Modeling Simulation and Technologies Conference*, AIAA, Reston, VA, 2004.