THESIS REVIEWER'S REPORT

I. IDENTIFICATION DATA

Thesis title:	**Evaluation of Aircraft Software Security during Aircraft Maintenance**
Author's name:	**Alexandr Sorochin**
Type of thesis :	bachelor
Faculty/Institute:	Faculty of Transportation Sciences (FTS)
Department:	Department of Air Transport
Thesis reviewer:	Julien VIDALIE
Reviewer's department:	Airbus Protect

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment	**ordinarily challenging**

How demanding was the assigned project?

The student was asked to analyze the software of an aircraft onboard software and its maintenance (The G950 NXi Integrated Flight Deck System of a Tecnam P2006T aircraft) through the scope of a STPA analysis.
This requires understanding of the system and methodology, collaboration with the development team or users of the system to understand its maintenance and assess its potential safety/security constraints, and modeling and analysis of the system.

Fulfilment of assignment	**fulfilled**

How well does the thesis fulfil the assigned task? Have the primary goals been achieved? Which assigned tasks have been incompletely covered, and which parts of the thesis are overextended? Justify your answer.

The student conducted the STPA analysis of the system. He modeled the system, analyzed its safety constraints, and defined a set of Unsecure Control Actions (UCA) that could result in loss events. These UCAs are associated to scenarios that could cause them, loss scenarios, and recommendations to avoid them (called "requirements" in the thesis). An appreciation letter written by a Compliance Manager of the F-air flight school expresses the satisfaction of the F-air Flight school towards the recommendations of the student.

Methodology	**partially applicable**

Comment on the correctness of the approach and/or the solution methods.

As stated above, the student provides satisfying results for the STPA analysis of the system.
However, the STPA methodology relies on four steps:
- Definition of the purpose of the analysis
- Modeling of the Control Structure
- Identifying Unsafe Control Actions (UCA)
- Identifying Loss Scenarios

The third and fourth steps are fulfilled, but insufficient descriptions of the first and second steps are given in the report.
The student defined a satisfying scope for the analysis. However, section 4.1 of the thesis, that describes the purpose of the analysis, is very unclear.
The student provides a control structure model as an illustration but does not provide any explanation of this control structure.
The UCA and loss scenarios are described in an exhaustive manner, although they are only superficially commented.
Overall, the STPA methodology is applied and leads to satisfying results.

Technical level	**D - satisfactory.**

Is the thesis technically sound? How well did the student employ expertise in the field of his/her field of study? Does the student explain clearly what he/she has done?

The thesis is technically sound.
The student gives sound definitions for the required concepts and uses them in a consistent manner.
The thesis sometimes lacks explanations and assumes that the reader will fully understand illustrations and tables without them, for example in section 4 with the Control Structure Model. The various tables of UCAs/scenarios are only superficially

commented. The explanation of the whole process over one UCA and one of its associated scenarios would benefit the thesis as it would give the reader deeper understanding of the process.

Formal and language level, scope of thesis	D - satisfactory.

Are formalisms and notations used properly? Is the thesis organized in a logical way? Is the thesis sufficiently extensive? Is the thesis well-presented? Is the language clear and understandable? Is the English satisfactory?

The formalisms and notations are used properly.

The thesis is structurally sound, it features an introduction to its subject, a description of the studied system, an introduction to the STPA methodology, a presentation of the STPA analysis that was carried to the student and his recommendations, and a conclusion.

Although the thesis is overall sound, the poor use of English is sometimes an obstacle to understanding.

Selection of sources, citation correctness	E - sufficient.

Does the thesis make adequate reference to earlier work on the topic? Was the selection of sources adequate? Is the student's original work clearly distinguished from earlier work in the field? Do the bibliographic citations meet the standards?

The thesis makes comprehensive introductions to the concepts that are used, which results in a relevant state of the art. Although maybe incomplete, it gives the reader an understanding of the required concepts.

However, the bibliography in this thesis is very weak. Only 8 sources are cited, 2 of which being peer reviewed articles, and one being the reference book for the STPA methodology.

It is not always clear whether the citations are related to a specific statement or to entire paragraphs, as they are almost always referred to at the end of paragraphs, and the same reference is often cited in multiple consecutive paragraphs.

The student sometimes quotes the sources without proper quotation marks, making it seem to be his own writing. As an example, the first reference is a website redacted in Russian, and parts of the introduction are direct translations of this source. Sources should be either properly quoted or reformulated.

Many affirmations in the thesis lack proper justification through citations.

Additional commentary and evaluation (optional)

Comment on the overall quality of the thesis, its novelty and its impact on the field, its strengths and weaknesses, the utility of the solution that is presented, the theoretical/formal level, the student's skillfulness, etc.

This thesis shows the interest of the STPA methodology through its application to a real-life system. This work was considered useful to the F-air flight school and some of its recommendations were implemented in their technical maintenance, with prospects of further improvements, as stated in the appreciation letter delivered by a former F-air Compliance Manager.

III. OVERALL EVALUATION, QUESTIONS FOR THE PRESENTATION AND DEFENSE OF THE THESIS, SUGGESTED GRADE

This thesis presents the use of the STPA methodology to ensure security of the onboard information infrastructure maintenance for a Tecnam P2006T aircraft. STPA being a relatively new methodology, this thesis is a good support for its diffusion.

The work that is presented is technically sound and lead to results that were useful to end-users of the system. However, the quality of this thesis is impacted by a weak bibliography, lack of comments on the figures and tables, and poor wording that sometimes makes understanding difficult.

As the student does not present the way he went from the UCAs to the loss scenarios and his recommendations I recommend asking him to detail this process on one of the UCAs.

Through the appreciation letter and the large number of UCAs and loss scenarios that were identified I assume that this work required extensive communication with the F-air flight school, which is a strength of this thesis.

However, the thesis does not describe this collaboration. I recommend asking the student which difficulties were associated to working with this partner and what was the process used to communicate and share data.

Overall, I believe that although the written report is a bit weak, the presented work is of sufficient quality and the assignment is fulfilled.

The grade that I award for the thesis is **D - satisfactory.**

Date: **27.8.2023**   Signature: Julien VIDALIE