A Petri Net approach to the Risk Analysis of Jet Engines

Silvia Tolo

Resilience Engineering Research Group, University of Nottingham, UK.
E-mail: silvia.tolo@nottingham.co.uk

John Andrews

Resilience Engineering Research Group, University of Nottingham, UK.
E-mail: john.andrews@nottingham.co.uk

Ian Thatcher

Rolls-Royce, UK.
E-mail: john.andrews@nottingham.co.uk

David Stamp

Rolls-Royce, UK.
E-mail: john.andrews@nottingham.co.uk

Traditional risk analysis techniques such as Fault Trees and Event Trees fail to model complex aspects of systems behaviour such as components dependencies, degradation, limiting their capability of representing modern engineering systems. This is all the more true for aviation systems, whose safety and operation strongly rely on automation and control technology, often resulting in dense networks of dependencies and hence in a high degree of complexity. Moreover, due to their safety critical nature as well as intensive operation conditions, maintenance is a crucial aspect of these systems life-cycle, introducing further sources of dependency or failure. Failing to take into account these aspects may result in the misrepresentation of the systems behaviour, potentially leading to the underestimation of risk. The current study provides an alternative solution for the safety analysis of the air system of a jet engine based on the use of Petri Nets. The model implemented covers the time interval between major engine overhauls, taking into account both in-flight operation and on-wing maintenance, as well as their reciprocal influence. Components degradation as well as dependencies and common cause failures are also included in the analysis, in order to offer a realistic representation of the system behaviour.

Keywords: Fault Trees, Safety Analysis, Component Dependency, Degradation, Markov Models, Petri Nets

1. Introduction

Component dependencies and degradation processes have the potential to significantly affect systems performance. The inability of most commonly adopted risk analysis methodologies to capture these features, may translate in the unrealistic representation of the system processes. The lack of more realistic modelling tools can result in over-engineering, due to conservative approach to system design and operation, or, in worse case scenario, in the underestimation of risks, leading to safety hazards. The current study focuses on a Petri Net approach to system safety modelling Reisig (2012). The choice of this methodology was dictated by the high degree of flexibility that Petri Nets offer, allowing to accurately represent degradation processes and complex maintenance strategies as well as a wide range of component dependency types.

2. Case Study

Aviation systems are safety critical systems subject to intensive operation conditions and often diversified and complex maintenance strategies. Moreover, their designs heavily rely on automation and control technology, increasing the degree of dependency among components Rolls Royce (2015). For these reasons, the accurate representation of components degradation and dependencies is essential to reliably predict the performance of

Extended abstract collection of the 32nd European Safety and Reliability Conference.
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini and Simon Wilson

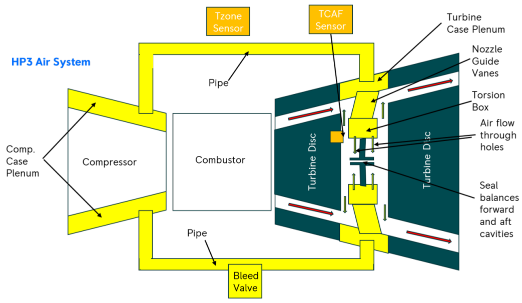

Fig. 1.: System Overview

the system and hence to estimate its safety. The current study focuses proposes the safety analysis on the air system of a jet engine (see Figure 1 using Petri Nets (PNs). The aim is to simulate the degradation of the relevant components during an operation time interval of 20000 flight hours, at the end of which a major aircraft overhaul is expected to be carried out. Inspections and light duty maintenance are assumed to performed on wing at regular intervals (i.e. every 7000 flight hours) between major overhauls. Not all the degraded states of the components are revealed at inspection, allowing for the deterioration process to progress beyond the on-wing maintenance in the case of undetected failures. The overall PN model offers two simulation modes: *on-flight* and *on-wing*. The first refers to the operation phase of the jet engine, while the second refers to the performance of inspection and on-wing repairs. The distinction between these two simulations modes allows for future development to take into account imperfect maintenance or dependencies associated with the latter. The proposed model consists of five subnetworks, representing as many sections of the system:

- Control System: operates the bleed valves and relies on the use of two control channels, each associated with a temperature sensor whose signals are cross checked during operation.
- Bleed Valves: three valves are in place to allow air into the engine bypass duct, in agreement with the temperature sensors readings. Their failure to deliver the required air flow can potentially result in engine overheat, degraded starts or engine surge. Their malfunction is detected by zone thermal readings over a number of flights. They can then be replaced on-wing.
- Pipes: 6 main conduits transport air to the turbine case plenum. The occurrence of cracks hinders the ability of the pipes to deliver the requested quantity of air, with consequences proportional to the degree of degradation (i.e. crack size). While severely affected pipes can be substituted on wing, small cracks are assumed to be not detectable by inspection.
- Nozzle Guide Vanes: allow to distribute the air flow where required in the engine. As for the pipes, different degrees of degradation are assumed, resulting in medium to large leaks, potentially leading to engine overheat. The development of holes can be accelerated by the occurrence of hot streaks. Nozzle degradation can not be detected or repaired on wing.
- Turbine Seal: stops the air escaping from the air system, balancing the flow between forward and rear cavity. Also in this case, different degrees of wear are considered for the seal. The detection of the degradation is possible only through the analysis of the zone temperature signal or during major overhauls.

All model subsections, with the only exception of the control system, have the potential to directly contribute to the occurrence of engine overheat. The significance of such contribution is estimated through the assignation of contribution factors and compared to a safety threshold defining the failure of the air system.

Acknowledgement

This work was supported by the Lloyd's Register Foundation, a charitable foundation in the U.K. helping to protect life and property by supporting engineering-related education, public engagement, and the application of research

References

Reisig, W. (2012). *Petri nets: an introduction*, Volume 4. Springer Science & Business Media.
Rolls Royce (2015). *The jet engine*. John Wiley & Sons.