1. Course title: Safety Assessment for Aircraft Systems

1.1 Course Introduction

This course has been designed by the author of Aircraft System Safety: Military and Civil Aeronautical Applications (Woodhead Publishing Ltd, Cambridge, 2005) and will also use material from his manuscript (to be published in 2013) entitled Aircraft Failure Assessments: A practical guide for System Safety.

The course material is mature and has, since 2006, been presented to Marshall Aerospace (Cambridge), Cranfield University (UK), BAE Systems (Australia), Civilian Operators in Singapore & Hong Kong, and various air forces (e.g. SAAF, RAF and RAAF) who have needed to understand the civil approach to Aircraft System Safety Assessments.

1.2 Course learning objectives

- Introduction to Safety Assessment of Complex Systems
- Functional hazard assessment
- Probability calculations
- Reliability of systems and equipment
- Common cause failures
- Particular risks and zonal safety analysis
- Fault tree analysis
- Failure mode and effect analysis (theory/practice)
- Evaluation of in service aircraft and equipment and risk management

1.3 Course duration

- 3-days

1.4 Special Requirements of Course Participants

- An understanding of CS25 and ICAO SMS Manual (Doc 9859) would be a distinct advantage although not essential.
1.5 Special Requirements of Course

NIL

1.6 Assessment Process

This will be overall and continuous, against the course objectives. We also offer a multiple choice examination paper for in-house courses, at EASA’s request.

1.7 Course Trainers

Primary Facilitator Mr. Duane Kritzinger

2. Technical specifications and training plan

Safety Assessment for Aircraft Systems

The regulatory framework/environment on which this course is based:

- CS25.1309
- SAE ARP4754
- ICAO SMS Manual (Doc 9859)

<table>
<thead>
<tr>
<th>Outline learning objectives</th>
<th>Supporting documentation, materials and training aids</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to Safety Assessment of Complex Systems</td>
<td>Modules 1.1, 1.2 and 1.3</td>
</tr>
<tr>
<td>Functional hazard assessment</td>
<td>Module 3.1</td>
</tr>
<tr>
<td>Probability calculations</td>
<td>Modules 2.1, 2.3 and 3.2</td>
</tr>
<tr>
<td>Reliability of systems and equipment</td>
<td>Module 3.2</td>
</tr>
<tr>
<td>Common cause failures</td>
<td>Module 3.4</td>
</tr>
<tr>
<td>Particular risks and zonal safety analysis</td>
<td>Modules 3.5 and 3.6</td>
</tr>
<tr>
<td>Fault tree analysis</td>
<td>Modules 2.1 and 3.3</td>
</tr>
<tr>
<td>Failure mode and effect analysis (theory/practice)</td>
<td>Module 3.7</td>
</tr>
<tr>
<td>Evaluation of in service aircraft and equipment and risk management</td>
<td>Module 1.1 and 1.3</td>
</tr>
</tbody>
</table>

Course introduction

Understand course objectives and methodology; what do we want the attendee to be able to do and understand following this training course?

- Course structure
- Methodology
- Course learning objectives/personal learning objectives

Throughout the whole training course PowerPoint presentation and projection equipment is utilised as well as flipcharts to capture thoughts and illustrate key points.

Handouts and case study materials are passed to the attendee such that they
# Course Outline Syllabus

## Safety Assessment for Aircraft Systems

### Module 1.1: Risk Management in the Safety Management System
- History & Purpose (through-life safety)
- Safety Criteria used (risk based approach)
- Safety Case Components
- SMS
- Safety Argument (in Goal Structured Notation)
- Hazard Log
- Hazards and Accidence
- Accident video and group exercise

This module addresses, (via real world case studies) the background that led to establishment of Safety Management Systems

Supports Ch 4, 6 & 9 of Aircraft System Safety: Military and Civil Aeronautical Applications

### Module 1.2: The System Safety Assessment Process
- History & Purpose (design safety)
- Safety Criteria used (goal based approach of CS25.1309)
- Regulatory Requirements and Guidance Material
- Understanding the System Hierarchy
- Safety Strategy/Argument and benefits of Goal Structured Notation
- Safety Assessment Procedure(from Concept to Certification)

This module addresses, (via real world case studies) the CS25.1309 approach to Safety Assessment of Aircraft Systems

Supports Ch 5 & 8 of Aircraft System Safety: Military and Civil Aeronautical Applications

### Module 1.3: Relating the 25.1309 Criteria to the SMS Risk Criteria
- History & Purpose (design safety)
- Safety Criteria used (goal based approach of CS25.1309)
- Regulatory Requirements and Guidance Material
- Understanding the System Hierarchy
- Safety Strategy/Argument and benefits of Goal Structured Notation
- Safety Assessment Procedure(from Concept to Certification)

Integrates the approaches in Modules 1 & 2

This module addresses the EASA requirement for "Evaluation of in service aircraft and equipment and risk management"

### Module 2.1: Failure Probability estimation in Avionic Systems
- Apply Safety Criteria to a typical avionic modification.
- From the failure severity, deduce a safety target and show what is involved in meeting that target (via FTA case study of Primary Flight Display failure scenario)

Demonstrates how the SSA improves/influences the design (in terms of functional performance and diagnostics)
Module 2.2: Misleading Avionics
- Explore the safety effects of misleading instruments.
- Show how the Safety Assessment can assist in fault diagnostics and generation of Flight Reference Cards.
- Accident video and discussion

Module 2.3: Failure Probability estimation in Mechanical Systems
- Link structural integrity to the System Safety Assessment.
- Prove safety target accomplishment for mechanical systems (qualitative vs. quantitative).
- Maintenance philosophy vs. Safety
- Introduce "Fail Safe" Concept.
- Show how the Safety Assessment influences/relies on maintenance procedures
- Accident video and discussion

Module 3.1: Functional Hazard Analysis
- Introduction and use of the FHA and its part in the product lifecycle.
- FHA objectives
- Simple process
- An FHA model (tailored from SAE ARP4761)
- Advantages and limitations

Module 3.2: Failure Probability Theory
- Background to quantitative probability assessment
- Symbols commonly used
- Probability Fundamentals
- MTBF and Failure Rates
- Combining Events
- Class Assignment
- System Architectures
- Class Assignment

Module 3.3: Fault Tree Analysis
- Purpose
- Notation

This module addresses the EASA requirement for “Reliability of systems and equipment”
<table>
<thead>
<tr>
<th>Course Outline Syllabus</th>
</tr>
</thead>
</table>

**Safety Assessment for Aircraft Systems**
- Boolean Logic
- Advantages and Limitations

**Module 3.4: Common Cause Analysis**
- Purpose
- Systemic vs Random failures
- Methodology (tailored from SAE ARP4761)
- Advantages and limitations
- Supports Ch 5 in Aircraft Failure Assessments: A practical guide for System Safety.
- This module addresses the EASA requirement for “Common Cause Analysis”

**Module 3.5: Particular Risk Analysis**
- Purpose
- Methodology (tailored from SAE ARP4761)
- Advantages and limitations
- Supports Ch 6 in Aircraft Failure Assessments: A practical guide for System Safety.
- This module addresses the EASA requirement for “Particular Risk Analysis”

**Module 3.6: Zonal Safety Analysis**
- Purpose
- Methodology (tailored from SAE ARP4761)
- Example
- Advantages and limitations
- Supports Ch 7 in Aircraft Failure Assessments: A practical guide for System Safety.
- This module addresses the EASA requirement for Zonal Safety Analysis

**Module 3.7: FMEA, FMECA & FMES**
- Purpose and distinction in FMEA, FMECA and FMES
- Safety Argument and how the FMEA relates
- Process
- Approaches at System Level 2, 3 & 4
- Example
- Advantages & Limitations
- Supports Ch 87 in Aircraft Failure Assessments: A practical guide for System Safety.
- This module addresses the EASA requirement for “Failure Mode and Effect Analysis (theory/practice)”