



# 2010 ADF Software Symposium

Achieving aviation software safety goals in a schedule driven environment.





# Welcome and Introduction

- Welcome to the 2010 ADF Software Symposium.
- Aim: To encourage constructive discussion and to share lessons regarding the development and support of software for airborne and related systems.





# Administration

- Rest Rooms
- Fire, Security, Smokers
- Morning/Afternoon Tea & Lunch
- Mobile Phones to 'Off' or 'Silent'
- Symposium Schedule
- Feedback Forms
- Copies of Symposium Presentations
  - Available on the DGTA internet and intranet web pages following the symposium.
- DRN Access – available in the Officers' Mess





# Symposium Dinner

- Customs House Hotel
  - 161 Nelson Place, Williamstown
  - Pub Meals
  - Mains \$20 - \$30
- Meet at 7pm
- Nomination List – by 12pm if you wish to attend
- Maps Available





# Discussion Forums

- New this year: feedback requested greater time for discussion and networking, this is it.
- SCI-DGTA proposed topics:
  - The suitability of aviation software and assurance benchmarks for ADF use.
  - Challenges in applying Informed Recognition of Prior Acceptance to aviation software.
  - Dealing with aviation software safety risk.
  - Certification of Mission Planning Systems.
  - Complying with the new software regulations.
- External Proposals:
  - Equivalent level of software assurance in practice.
- Nomination form circulating, please fill it in by the end of the day.
  - Just put a tick next to the presentation you wish to attend.





# Participation

- The success of the symposium rests with you.
- Though you might not think it, there are certainly people in this room who can learn from your knowledge and experience.
- If you don't share your knowledge and experience, what makes you think anyone else will? How will you take value away from the symposium?





# Participating Organisations

- Aerospace Systems Engineering SQN
- Airlift SPO
- Airborne Self Protection SPO
- Army Aviation SPO
- Australian Aerospace
- Boeing Defence Australia
- CH-47F PO
- Command & Intelligence SSO
- DGTA
- Directorate of Ordnance Safety
- Electronic Systems Division
- Guided Weapons Branch
- JEWOSU
- Land Systems Division
- Maritime Patrol SPO
- Military Geographic Information SPO
- Multi Role Helicopter LMU
- Naval Aviation SPO
- P-8A PO
- RAAF Aeronautical Information Services
- RAAF School of Technical Training
- Raytheon
- RNZAF
- Tactical Fighter SPO
- Wedgetail SPO





# What does SCI want from the symposium?

- SCI1 is the facilitator for the symposium and the centre of expertise for aviation software.
- SCI1 runs the symposium and provides presentations, but what do we want from the symposium?
- SCI1 wants:
  - You to gain something valuable from this symposium.
    - If this isn't happening, suggest changes.
  - To gain an understanding of your concerns.
    - Sometimes our view of the world is limited.
  - To obtain feedback on how we can do our business better.
    - We are always looking for ways to improve.





# Distribution List

- SCI1 have created the 'Aviation Software' distribution list on the DRN.
- We will use it for:
  - advertising DGTA sponsored courses and this symposium, and
  - distributing newly published or updated guidance.
- If you would like to be added, please add your e-mail address to the list or contact FLTLT Leon Burkamshaw.
- Can only add DRN users at this stage.
- You may use the distribution list to seek guidance.
  - Be aware of who is on the list!
  - Depending on how this goes, a public folder may be created.





# 2010 ADF Software Symposium

Presentation by DGTA  
AIRCDRE Dave Tindal





# **Background to the Theme of the Symposium: Why is DGTA concerned with schedule?**

---

**SQNLDR Patrick Redmond**

**Systems Certification and Integrity (SCI)**

---





# The Role of the TAA and TAR

- The role of the TAA and TAR is to (among others):
  - Proscribe standards that define suitable benchmarks for assuring airworthiness.
  - Establish a framework to assure that engineering assessments are robust and defensible.
  - Provide oversight of those assessments.
- Generally, the TAA will:
  - stand behind a design that is technically airworthy, or
  - inform decision makers of the risks of operating a design that is not technically airworthy.





# DGTA and Schedule

- DGTA focus is technical airworthiness.
- Strictly speaking, schedule is not a technical airworthiness issue.
  - So why are we having a symposium that considers schedule?
- We know that you are under schedule pressure.
- We want to see you achieve your schedule goals while satisfying airworthiness requirements.





# Schedule Pressures and Airworthiness

- Schedule pressures generally operate against technical airworthiness.
  - It is unlikely that schedule pressure will operate to improve technical airworthiness.
- Rightly or wrongly, airworthiness risk is sometimes traded for schedule benefits.
- Sometimes the activities necessary to assure the airworthiness of an aircraft are not completed in time.





# Why the schedule concern?

- DGTA has a vested interest in the technical airworthiness of ADF aircraft.
  - The TAA is held responsible for the technical airworthiness of ADF aircraft (whether he/she has control or not).
- Of course, DGTA is also part of the ADF community and is committed to supporting Defence capability.





# Accommodating Schedule Pressure

- Although DGTA is focussed on technical airworthiness, we will assist you to meet airworthiness requirements within your schedule goals.
- We will assist you to minimise schedule implications of certification, but be aware that:
  - an appropriate authority (not DGTA) may be required to retain risk, and
  - depending upon the extent of the shortfall, the TAA may not stand behind the design.
    - Some decision makers are particularly concerned when this occurs.





# DGTA and Risk Retention

- DGTA rarely retains risk beyond the inherent risk in specifying airworthiness standards.
  - May do so if risk is purely technical, or if there are no possible treatments to a technical problem.
- A decision to retain risk is made on the basis that tolerating the risk will provide some benefit elsewhere.
- DGTA has limited insight into cost, schedule and capability – no frame of reference to determine risk tolerability.





# Key Factors to Achieving Safety Goals

- Enough with the negative...
- What can be done to increase the likelihood that airworthiness requirements can be satisfied in a schedule driven environment?
- There's probably no silver bullet.
  - Possible that having good people will do the trick...
- There are a number of key factors that lead to achieving safety goals in a schedule driven environment.
- This is my opinion, based on my experience, not DGTA policy.





# Key Factors

## ■ Understanding

- You need to understand both the specifics and intent of the technical airworthiness regulations.
- This will help you define a strategy that satisfies the regulations and schedule constraints.
- If you don't understand the intent of the regulations, you are unlikely to adapt well to unusual situations or unexpected developments.
- Blind application of regulations without understanding why regulations exist leads to drawn out certification processes.

## ■ Foresight

- In my experience, there are leading indicators of troubled times.
- Knowing when something is going off track can help identify problems early and minimise schedule implications.





# Key Factors

- Planning
  - Often, issues arise because POs are unaware that an activity, resource or assessment is required.
  - A good plan will also clearly define completion criteria.
  - DGTA can commit to the contents of a plan.
  
- Communication
  - Projects that communicate openly with DGTA, raise IPs early, etc generally do better.
  - Hiding a problem doesn't make it go away.
  - DGTA will probably find it anyway, if we find it late, there may not be time to fix it.





# Key Factors

- Managing Stakeholder Expectations
  - Operators and PMs have expectations: these don't always align with airworthiness requirements.
  - Good Projects manage stakeholder expectations so that stakeholders don't impose unreasonable requirements.
  - Example: Directed Solutions
    - Operators or PMs may direct that particular equipment be acquired.
    - This does not necessarily mean that the equipment will satisfy relevant airworthiness requirements.
    - Need to ensure that operators and PMs are fully aware of the implications of directing a particular solution.





# Particular Concerns with Software

- Front Loading of Airworthiness Activity
  - Planning for software aspects of Design Acceptance must commence prior to contract signature.
  - Conduct of software aspects of Design Acceptance must commence shortly after contract signature.
  - It is very difficult to make this activity up if neglected early.
- Inability to Build Safety in After the Fact
  - If you don't plan for it, and you don't ask the contractor to do it, you are unlikely to stumble across acceptably safe software.
  - If you get to the end and find you haven't done enough, schedule implications of going back and doing it again could be huge.
    - Not enough time to do it right, but enough time to do it twice.





# Particular Concerns with Software

## ■ Data Requirements

- Software depends on access to data, some of it very low level.
- Requirements Specifications and Test Reports in particular are indicators of capability and may be subject to disclosure restrictions.
- Important to negotiate sufficient access. Our experience is that, if they know why you are seeking documentation, they are more likely to grant access.

## ■ Modifications and RPA

- Common argument: “Our software is the same as someone else except for...”
- Software changes are difficult to confine, small changes can have widespread effects.
- Limits use of RPA when the software is modified for the ADF.
- My experience: little difference between effort required for full assessment of assurance evidence versus RPA plus ADF oversight of changes.





# Particular Concerns with Software

- Risk Generally Comes From Uncertainty
  - Unless there is a known failure mode, risk resulting from unassured software comes from uncertainty.
  - The ADF is uncertain as to whether the behaviours of the software are appropriate.
  - How do we analyse a risk that arises from uncertainty? With great difficulty.
  - Non-Software types are unlikely to understand, difficult to explain the full context to them.





# Symposium Schedule

## ■ Tuesday, 17<sup>th</sup> August 2010

- 0930 – 0945: Symposium Administration
- 0945 – 1000: *Presentation from DGTA*
- 1000 – 1030: This Presentation
- 1030 – 1100: Morning Tea
- 1100 – 1145: *Project Wedgetail: Software Design Challenges*
- 1145 – 1245: Lunch
- 1245 – 1330: *Identifying Risk in Software Development*
- 1330 – 1400: Discussion
- 1400 – 1445: *Mission Planning System Airworthiness Consideration*
- 1445 – 1515: Afternoon Tea
- 1515 – 1600: *Planning for Software Certification in a Schedule Driven Environment*
- 1600 – 1630: Discussion



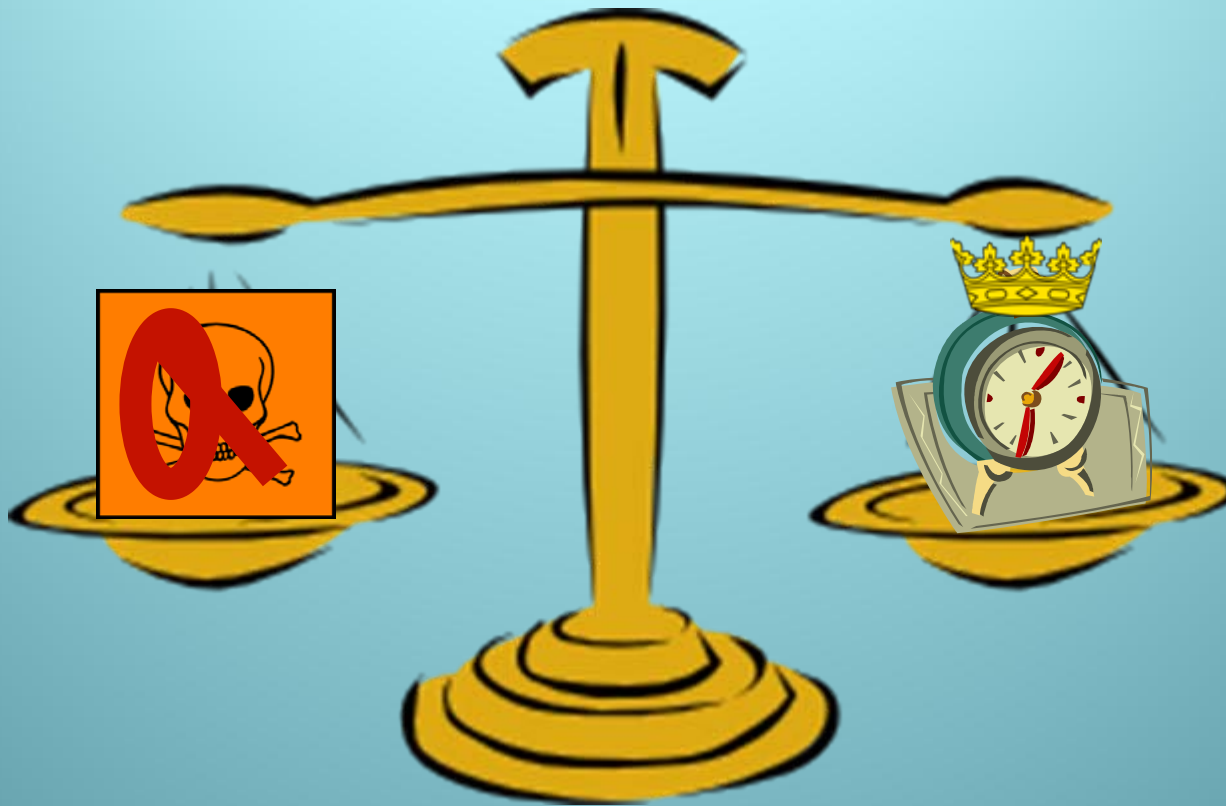


# Symposium Schedule

## ▪ Wednesday, 18<sup>th</sup> August 2010

- 0930 – 0945: Symposium Administration
- 0945 – 1030: *Software Testing: How Much is Enough? – The Balancing Act between Cost, Quality and Assurance*
- 1030 – 1100: Morning Tea
- 1100 – 1145: *Using RPA to Best Effect in Software System Acquisitions and Modifications – Can RPA Save Cost and Schedule?*
- 1145 – 1245: Lunch
- 1245 – 1330: *C-130J Block 7.0 Software Design Acceptance*
- 1330 – 1415: *Measurement and Communication of Software Risk*
- 1415 – 1445: Afternoon Tea
- 1500 – 1630: *Discussion Forums*





# Questions?

