UNSW AUSTRALIA
Canberra

Comparing Australian and U.S. DoD strategies for testing integration, interoperability and information (I3) assurance

Never Stand Still

Capability Systems Centre, School of Engineering and Information Technology

Dr Keith Joiner, CSC

Dr Mahmoud Efatmaneshnik

Dr Malcolm Tutty

- Background for DoDs
- Background challenges (4)
- US I3 initiatives (5)
- Qualitative outcomes
- Quantitative modelling
- Quantitative Results
- Conclusions
- See you in Hawaii

ADFA
AUSTRALIAN DEFENCE FORCE ACADEMY

Background

- Operationally trying to be anywhere needed & credible
- Specialist acq' org' tightening efficiency under increasingly strident criticism
- Increasing purchase of high-tech' e.g. SATCOM, BMS, PAR, AAR, AEW&C, UAV, UUV
- Increasing US acq': 35% → 60%
- Gov't instability & Defence budget difficulties, esp. post_GFC 2010-2014
- Defence budget as low as 1.38% GDP (2012) compared to plans 2-2.5% GDP
- Funding & personnel to Middle East Ops' not CONUS
- Arguable infatuation with US allied capabilities without experiential depth on wherewithal esp. integration, interoperability & info' (I3) assurance
- Same time in the US DoD sig' synergistic agile reforms in SE & T&E for I3 assurance
- Equals growing mismatch Aust' & US DoD on I3 assurance understanding
- Two studies:
  - Qualitative – Joiner & Tutty 2018 – A tale of two defence dep'ts …
  - Quantitative – Joiner, Efatmanishnik & Tutty - Modelling the Efficacy of Assurance Strategies for Better I3 Assurance in Family-of-System-of-Systems Portfolios

2006 → Iraq → Afghanistan → Syria → 2016

Picture: RAAF KC-30A tanking USAF C-17 Globemaster III from 418th FT SQN @ Edwards AFB 2016 (USAF USAF photo/Christian Turner) original https://www.flickr.com/photos/usairforce/24867332604/in/dateposted/ & wikepedia

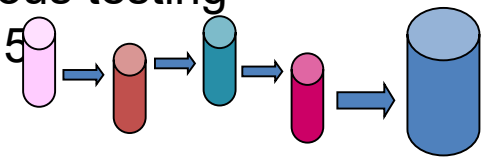
Background Challenge 1 - Growing System Synthesis

Systems – The Platform, Flight **&** Mission Simulators, Syst Eng Integ Lab, Part Task Trainers

SoS – Σ Platform **Type**(s) + Flight & Mission Sims + SE Integ Lab + Part Task Trnrs + Weapons + JWS + EW + LVC + TBMCS + Intel…

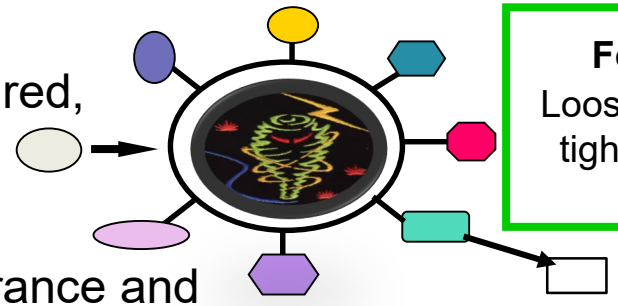
- Systems are becoming so synthesised or fused, complex and interdependent that they can, even without taking into account human agency, have *emergent properties* or exhibit *behaviours* that vary to an extent that is not easily predicted.

- The number of permutations of modern software-intensive systems make classical rigorous testing of them, all but impractical, (Cofer, 2015



SoS/FoS - Small stovepipes to large stovepipes **–** **NO**

- Reliance on some modelling required, (Hecht, 2015).
- Continuous through-life monitoring required, (Normann, 2015).



FoS - Σ SoS - Loosely coupled and tightly integrated **–** **YES**

- Situation challenges safety-critical assurance and mission system capabilities, (Tutty, 2016).

Background Challenge 2 – Higher-Order Human Functions

- Software-intensive systems are enabling higher-order human-like functions such as strategies and decision-making not simply control.
- The difficulty in specifying what the system must do becomes harder.
- More crucial to include representative human agency and decision making to adapt the systems during development.
- Usability tests for meaningful human control (Roff & Moyes, 2016) are fundamental

Level of Autonomy	Mission Decision Transitions				
	Find	Fix/Track	Target	Engage	Abort
Manual	Human	Human	Human	Human	**Human**
Human-in-the-loop	Human or System	Human	Human	System	**Human or System**
Human-on-the-loop	Human selected ??	System	System	System	**Human or System**
Human-out-of-the-loop	**System**	**System**	**System**	**System**	**Human**

Background Challenge 3 – Cyber Threat Complexity & Information Dominance

- The threat to weapon systems has adapted as a result of the [western] push for information exploitation/dominance, Jordan et al (2016).
- Cooperative engagement has systems responding in defence of other systems.
- Such inter-connected systems enables exploiting the broader cyber-attack surfaces of such systems.

- Not just about malicious attacks but as part of multi-layered hybrid/hyper warfare, Allen (2017).
- Offensive cyber
- The Threat is more complex and probably more adaptive.

Challenge 4 - Requirements Stasis

- Requirements stasis during development & build of large complex systems, largely through an emphasis on project management cost & schedule achievement on contracts, & unfortunately including their processing & software.

- Such a requirements stasis soon creates an alternative reality that is too far out of alignment with the contemporary family-of-systems & strategic/operational reality into which that complex new system must go into service.

Defence late again

Self inflicted negligence

Gross incompetence all around

Waste of taxpayers money

Project budget blowout

Initiative 1 - Augmenting Operational Exercises with Formal Experimentation

Developing capabilities are deliberately networked with legacy systems earlier in the development cycle:

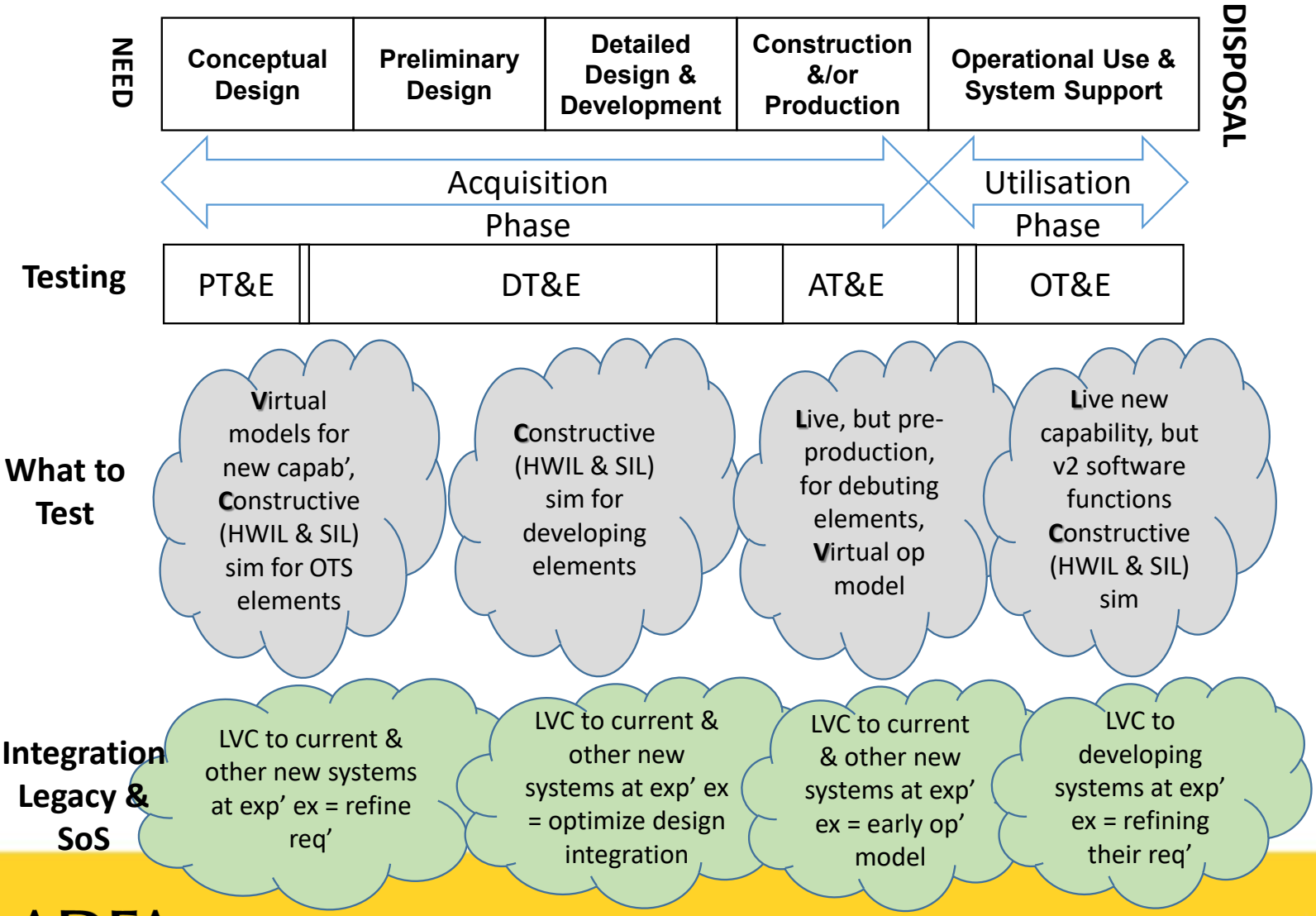
- Bold Quest in aviation
- Network Integration Exercise in conventional land forces

Involves some take-back of RDT&E from outsourced prime contractors (esp. cyber T&E)

Development of cost-effective experimentation exercises and developmental design critically involves mixing '*Live*', '*Virtual*' & '*Constructive*' (LVC) across the experimentation & T&E networks:

- *Live Simulation.* Exercises involving real people operating real systems
- *Virtual Simulation.* Simulation involving real people operating simulated systems
- *Constructive Simulation.* Simulation involving simulated people operating simulated systems

How US initiative works



Initiative 2 - Integration System Program Offices and New Certifications

Organisational alignment to System-Of-Systems view of the world

Portfolios, Programs & Projects (P3O) with I3 assurance accountabilities

Certifications like: tactical data links, cybersecurity, joint fires (JTAC) etc

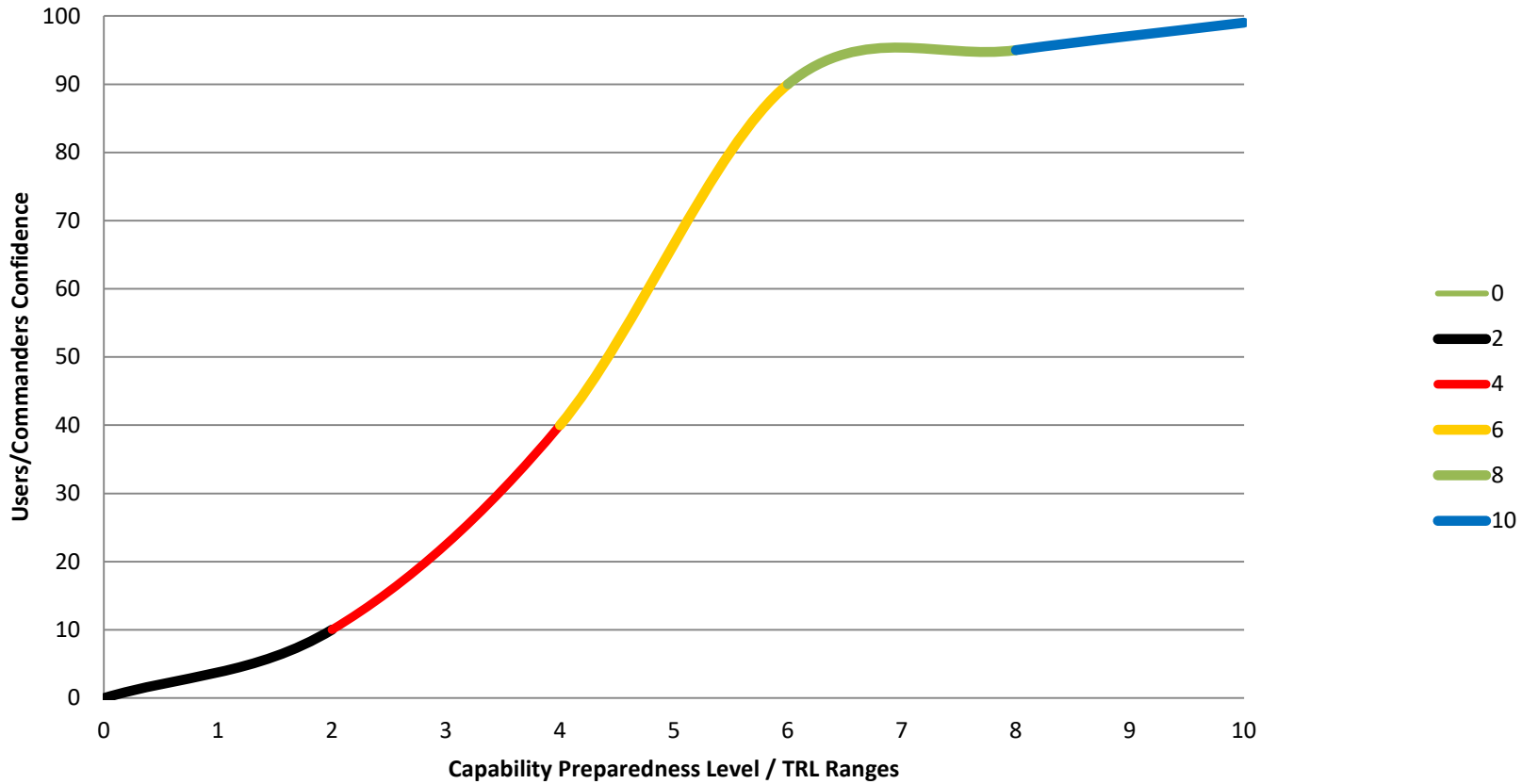
System of systems is a collection of task-oriented or dedicated **systems** that pool their resources and capabilities together to create a new, more complex **system** which offers more functionality and performance than simply the sum of the constituent **systems**.

Initiative 3 - Enhanced T&E Regime

Earlier, Evidence-based Rigour and Innovation: Test Smart not Test Often!

- Use of mandatory test measures under-pinned by rigorous & highly efficient new test design & test analysis techniques, has removed much of the scope in the U.S. DoD for '*decision by conjecture and influence*' or what is also commonly called '*paper-based analyses'*.
- Where decision-making still occurs without testing (to include modelling on VV&A models), the '*name & shame*' of independent annual reports to Congress by Director OT&E calls such practices out to Congress to help end them.
- No such legal or *name & shame* processes exist within the Australian DoD to call out acquisition practices that are not based on experimentation, test & accredited modelling, leaving it to the Parliament (Australian Senate, 2012 & 2016; Australian Parliament, 2016), ANAO (2002, 2013, 2016).

User and Commander Confidence Levels



Testing early & often starting from M&S equals:

- Resource stability
- Momentum
- Declining risk & growing confidence.

Initiative 4 - T&E Network Infrastructure

The U.S. DoD test networks connect every major design development facility & test range in the U.S. with different levels of security & purpose:

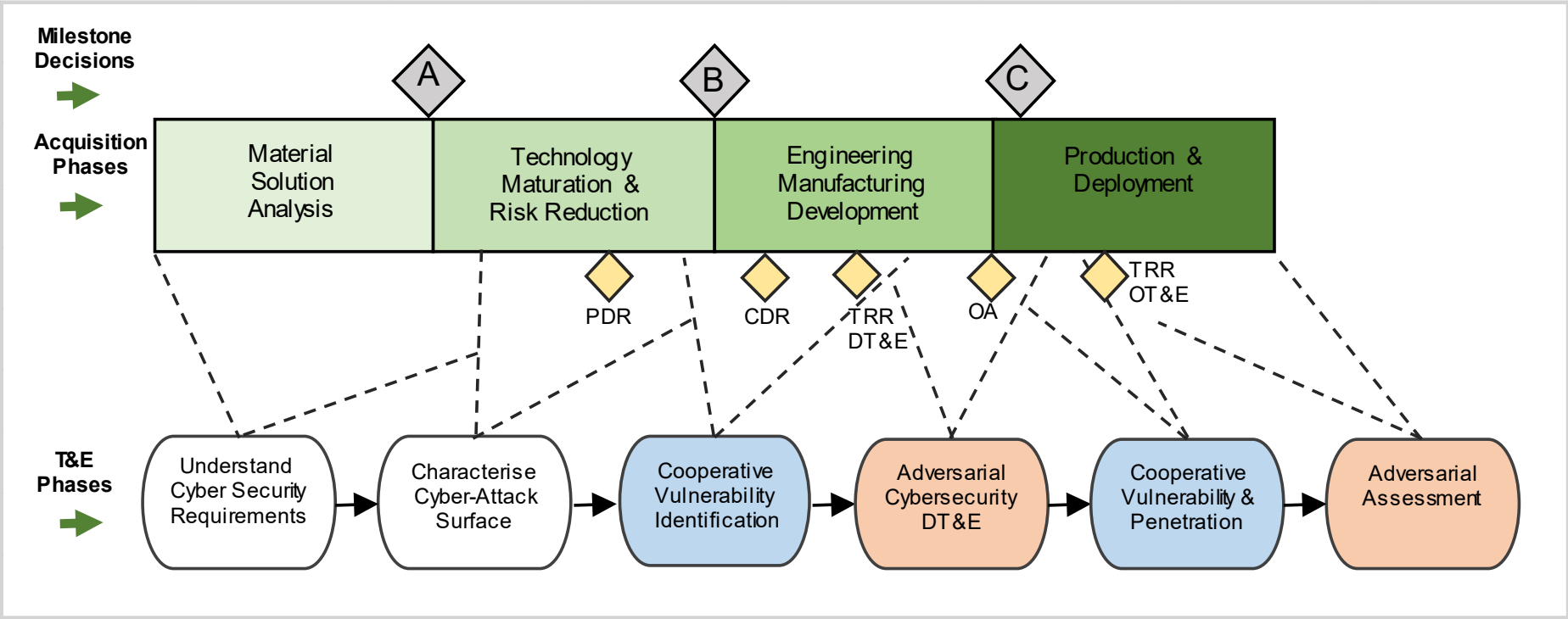
- ***Test Enabling Network Architecture (TENA)***
- ***Joint Mission Environment Test Capability (JMETC)*** &
- ***Joint Information Operations Range (JIOR)***

Initiative 5 - Cybersecurity Protection Plans & T&E

- US Presidential Directive, 2008.
- U.S. began cybersecurity reform with representative operational T&E, at the ‘right’ of the lifecycle, was fundamental to the DoD understanding the threat consequences and risks properly and then investing in the infrastructure, acquisition and T&E staff competencies, developmental design and then the subsequent two phases of ‘shift-left’ and ‘fully integrated’.
- Clear & comprehensive *Cybersecurity T&E Guide* available on-line.
- Deeper into the U.S. lifecycle there are Cyber Security Assessment & Advisory Teams.
- Cybersecurity is required in the TEMP, including: (1) architecture, (2) operational environment, (3) evaluation structure, (4) authority to operate, & (5) time & resources for the key cybersecurity T&E steps.
- Cybersecurity content required in the *Operational Test Plan*.

Picture from: http://federalnewsradio.com/wp-content/uploads/2016/02/Cybersecurity-Insights2.jpg

U.S. Cyber T&E Steps on U.S. DoD Lifecycles

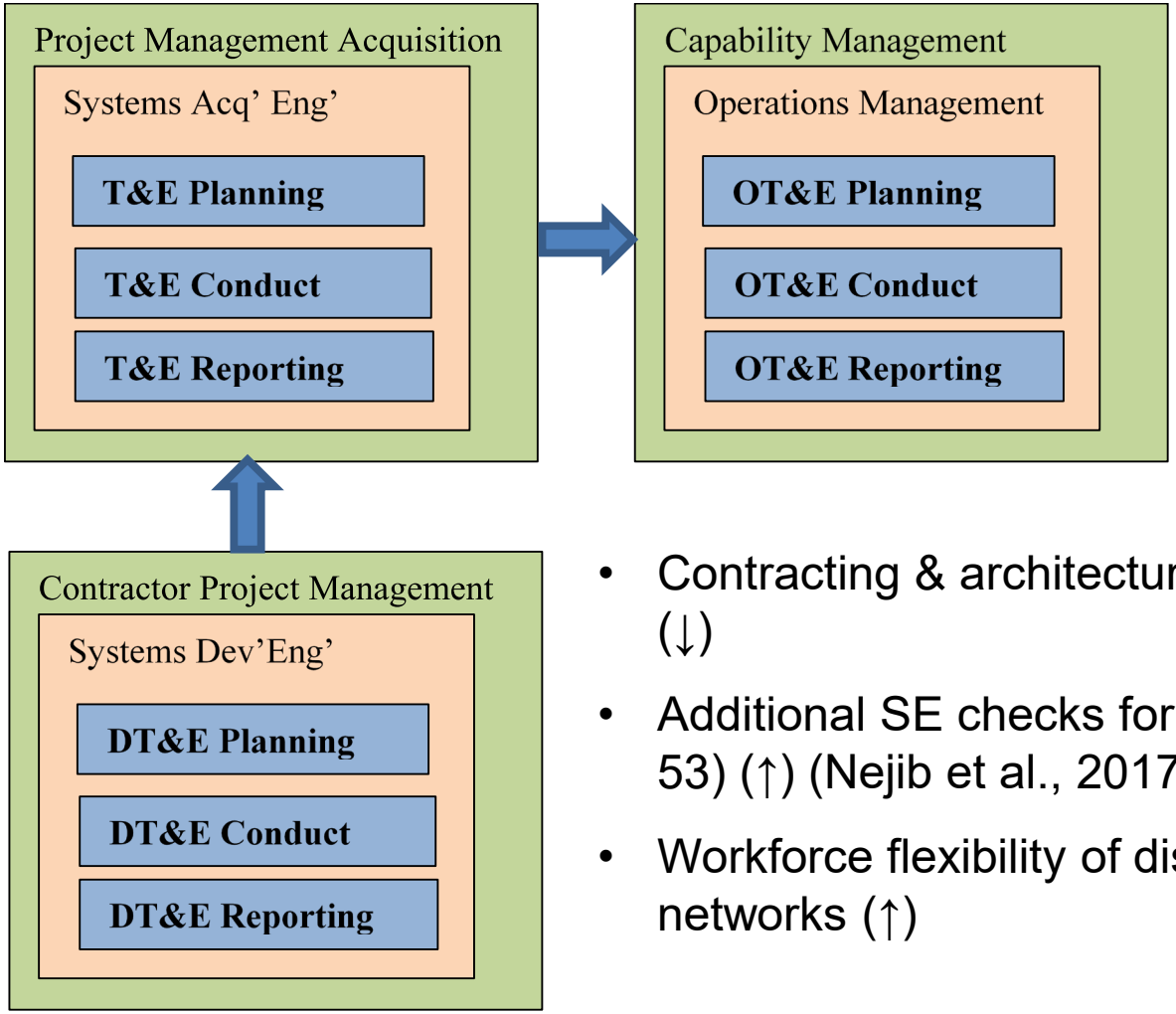


Only works by using JIOR (underpinned by JMETC etc) & the NCR

From Brown et al. (2015)

Initiative 6 - Permeating these U.S. Initiatives into Industry

The DoD is like a stage director & owner, but Defence industry (contractors) do the work. Consider the considerable impact of these U.S. initiatives on contractors:



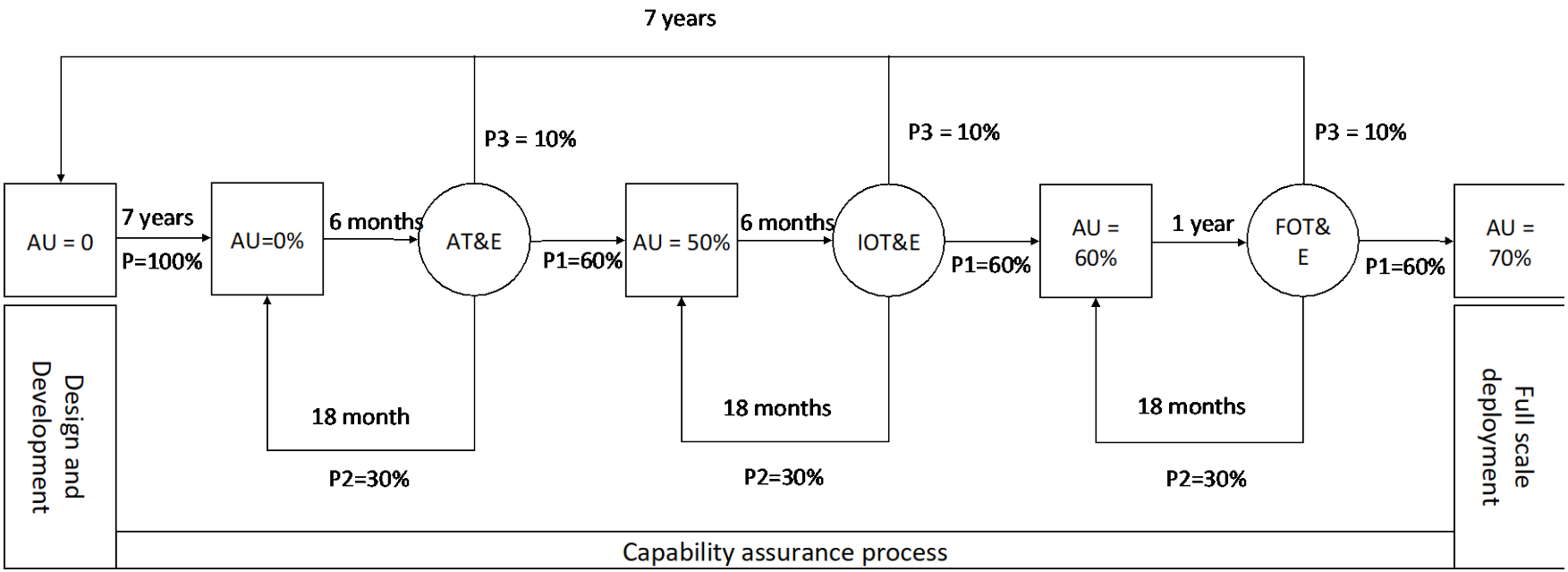
- Competency of industry testers (↑)
- Modelling & simulation skills (↑)
- Proprietary protections with pervasive LVC connectivity (↓)

- Contracting & architectural control due Gov't I3 T&E (↓)
- Additional SE checks for cybersecurity tests (circa 53) (↑) (Nejib et al., 2017)
- Workforce flexibility of distributed T&E support via networks (↑)

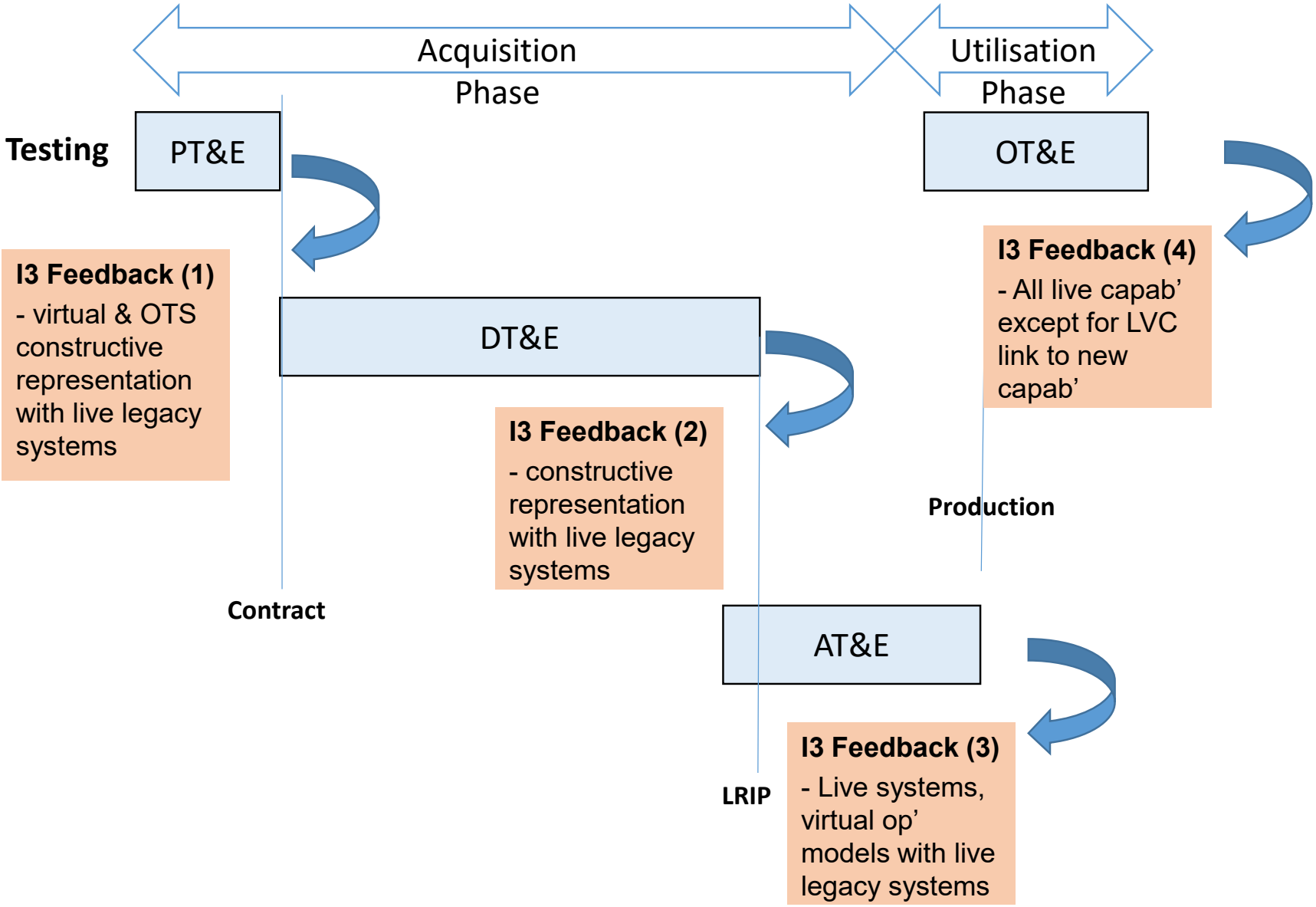
Qualitative Outcomes

- Catching up is crucial if Aust' forces are to keep operating with U.S. forces.
- Start by admitting Aust' DoD is falling badly behind in rigour necessary.
- Acquisition & T&E staffs to receive urgent education & competency in I3 assurance, so they become smart buyers. Do not be leave to individuals' initiative, but drive across all acquisition
- Aust' DoD should implement the six US DoD initiatives.
- Most expeditious way is to leverage US DoD technologies & support
- Do nothing options/outcomes:
  - Opt-out of allied Defence exercises & operations where Aust' would be weakest link (esp. near-peer warfare)
  - Accept significant work-up delays (18 months or longer) to participate in such allied exercises & operations with little flexibility to add or subtract elements once committed due to the wide assurance differences.
  - Participate in different ways, such as embedded personnel, rather than Australian force-level or platform contributions.

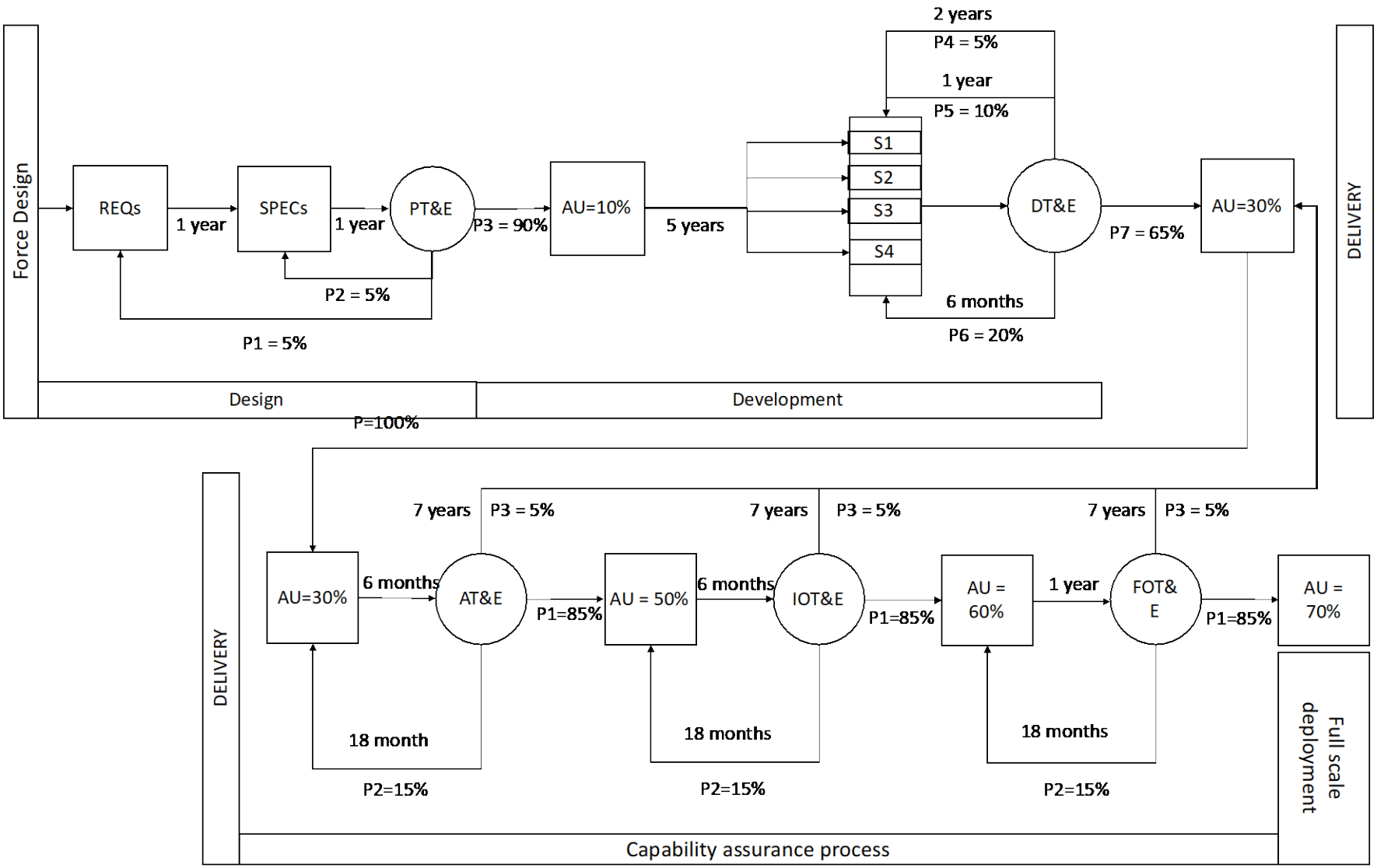
Quantitative Modelling – Aust' Model



Explaining US Differences for Australians



Quantitative Modelling – US Model



Quantitative modelling method

- Absorbing Markovian processes: can be solved using classic Markov chain formulations or for us by Monte Carlo Simulation in MATLAB
- Sample size of 100,000 random scenarios generated for each model.
- Each scenario is a possible path in the assurance models, & the number of times a particular path appears is representative of its occurrence probability
- **Limitation 1:** Testing of the unit is assumed to be simplistically as a memory-less process. In some respects in a FoS in a large organisation over so many years the bureaucracy helps give weight to this assumption. However, as projects work faster in their development and more closely work with their FoS then Markov assumptions are less likely to be realistic.
- **Limitation 2:** Sets a single project I3 assurance model of an average duration to testing for each country, when:
  - projects delivering SoS are so diverse,
  - programs managing in-service FoS are so diverse, and
  - policy only really guides such management and thus there is likely to be many worse and better exceptions.

The differences from quantitative modelling

Parameter	Australian model	US model
Mean time to deployment	15.1	12.1
Time to deployment (years) - 90% confidence interval	[9 , 26]	[9 , 18.5]
Total time with AU > 50% (years) - 90% confidence interval	[2 , 15.5]	[2 , 9.5]

In words: The 90% confidence limits for the best project SoS times are the same for both strategies, such that some projects delivering SoS will do as well in either countries' assurance regime. However, the 90% confidence limits for the worst project SoS times are 8.5 years longer for Australia (table 1), such that **some projects delivering SoS will do substantially worse in Australia or in many cases get cancelled trying (i.e., 26 years)**.

This works supports empirical and policy work in both countries as to the substantial benefits of early de-risk testing and technical maturation before contract

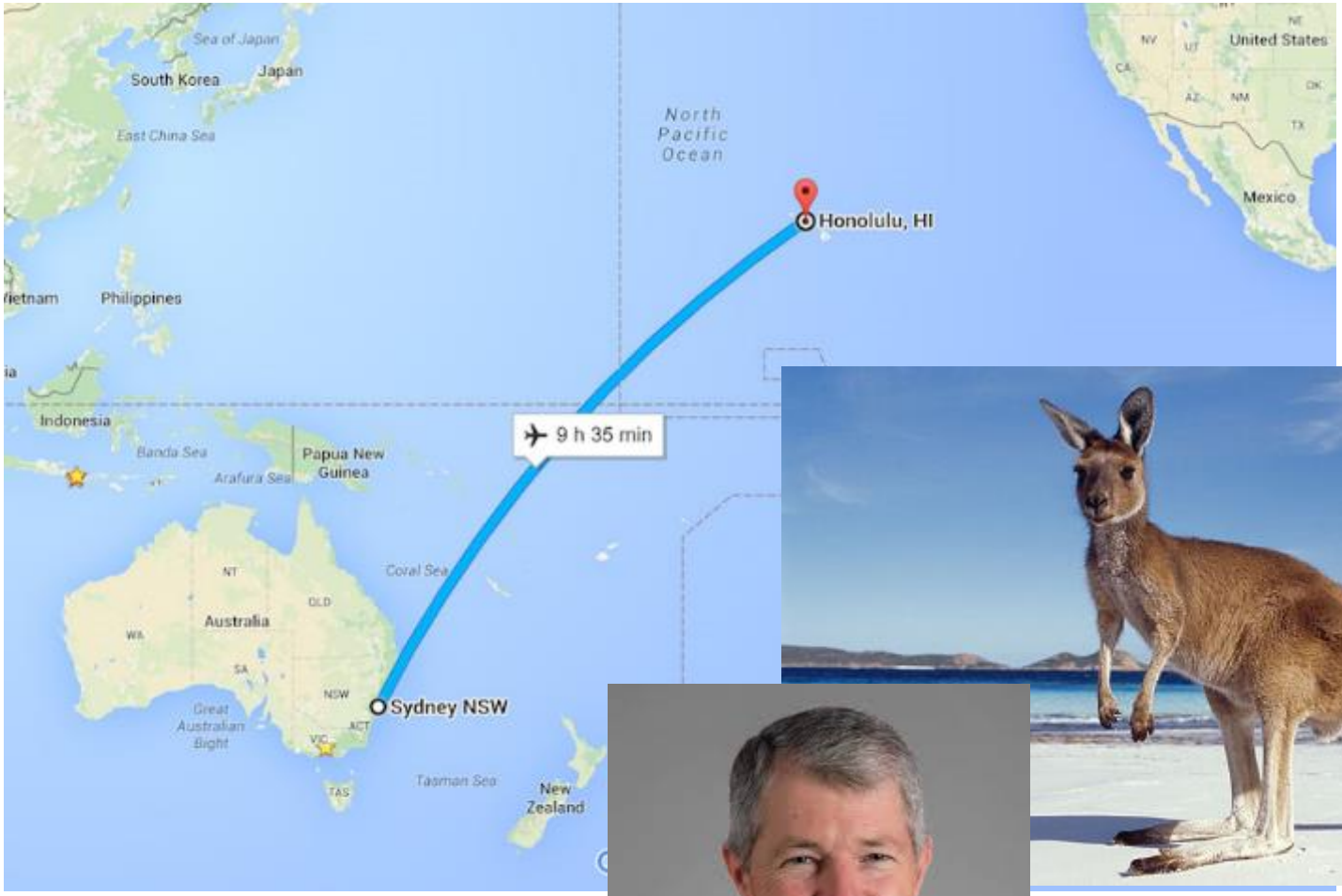
Conclusions

- U.S. I3 assurance initiatives are effective & synergistic
- Allies like Australia are rapidly falling behind due to lack of awareness of US CONUS wherewithal
- Allies must work on T&E infrastructure (federation of FoS through T&E networks), cybersecurity T&E, advanced test techniques etc if they are to remain “trusted”

References

- Joiner, K. F.; Tutty, M. G., 2018, 'A tale of two Allied Defence Departments: New assurance initiatives for managing increasing system complexity, interconnectedness, and vulnerability', *Australian Journal of Multidisciplinary Engineering*, http://dx.doi.org/10.1080/14488388.2018.1426407
- Joiner, K. F.; Efatmaneshnik, M.; Tutty, M., 2018, 'Modelling the Efficacy of Assurance Strategies for Better Integration, Interoperability and Information Assurance in Family-of-System-of-Systems Portfolios', presented at Complex Systems Design & Management (CSD&M) conference, INCOSE Singapore, 06 - 07 December 2018

Questions



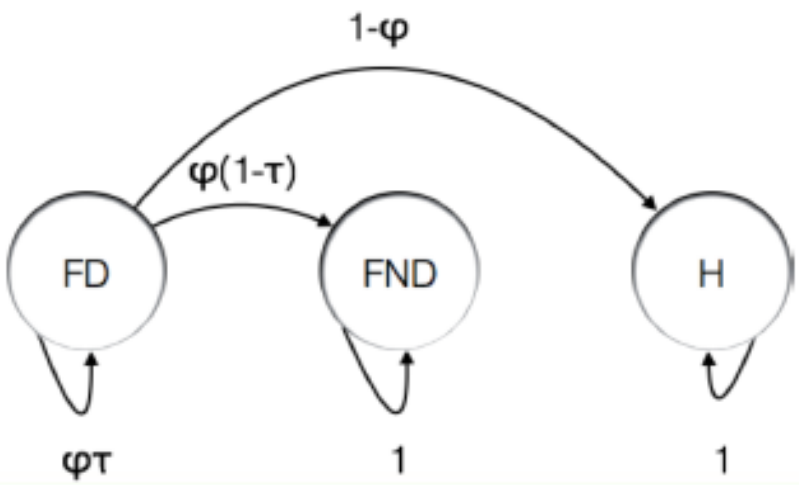
Keen Keynote:
Senator Dave Fawcett

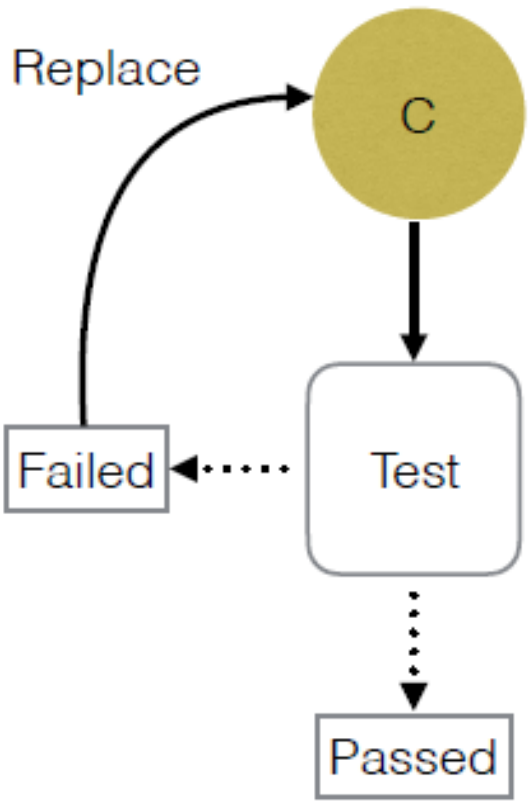
ADFA
AUSTRALIAN DEFENCE FORCE ACADEMY

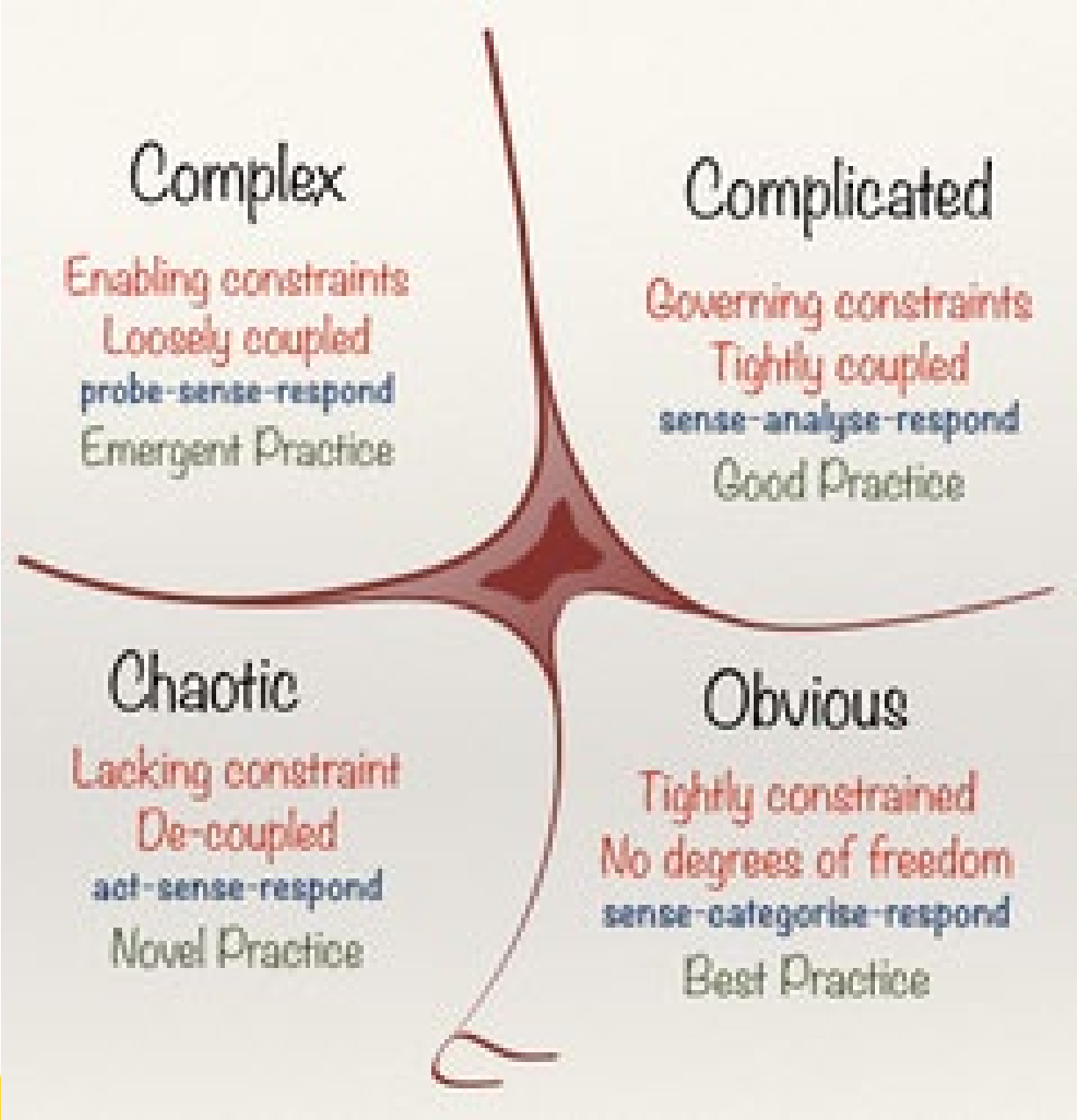
UNSW AUSTRALIA
Canberra

Backups for questions only

- Absorbing Markov chain state space for one unit testing
- FD = Fault Detected, FND = Fault Not Detected
  H = Healthy, $\varphi = Pr(Unit = Faulty), \tau = Pr(Fault = Detected \mid Unit = Faulty)$







240px-Cynefin_as_of_1st_June_2014