UNSW AUSTRALIA

Modelling the Efficacy of Assurance Strategies for Better Integration, Interoperability and Information Assurance in Family-of-System-of-Systems Portfolios

Never Stand Still UNSW Canberra School of Engineering and Information Telecommunication

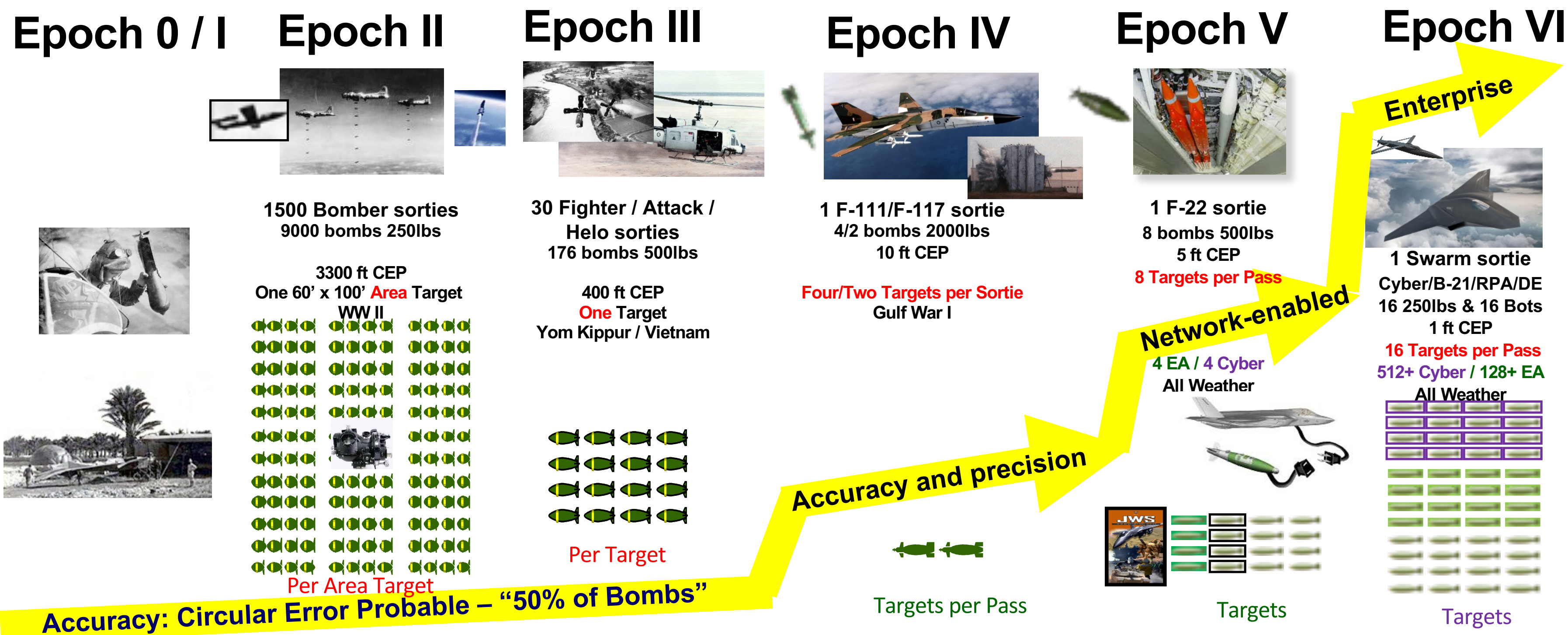
Keith Joiner, Mahmoud Efatmaneshnik, Malcom Tutty

{k.joiner,m.Efatmaneshnik,m.tutty}@adfa.edu.au

Capability Systems Centre
School of Engineering and IT
UNSW, Canberra

Capability Systems Centre
UNSW Canberra

Epochs of war and Air Armament - The Capability Transformation Story continues



Epoch 0 / I

Epoch II

1500 Bomber sorties
9000 bombs 250lbs

3300 ft CEP
One 60' x 100' Area Target
WW II

Per Area Target

Epoch III

30 Fighter / Attack / Helo sorties
176 bombs 500lbs

400 ft CEP
One Target
Yom Kippur / Vietnam

Per Target

Epoch IV

1 F-111/F-117 sortie
4/2 bombs 2000lbs
10 ft CEP

Four/Two Targets per Sortie
Gulf War I

Targets per Pass

Epoch V

1 F-22 sortie
8 bombs 500lbs
5 ft CEP
8 Targets per Pass

4 EA / 4 Cyber
All Weather

Targets

Epoch VI

1 Swarm sortie
Cyber/B-21/RPA/DE
16 250lbs & 16 Bots
1 ft CEP
16 Targets per Pass
512+ Cyber / 128+ EA
All Weather

Targets

Accuracy: Circular Error Probable – "50% of Bombs"

Accuracy and precision

Network-enabled

Enterprise

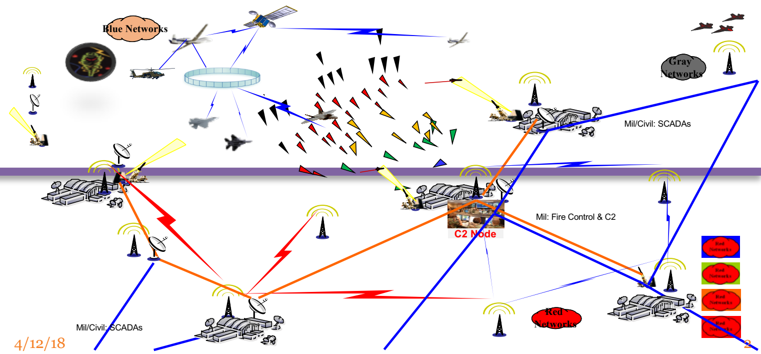
'Revolutionary' Technologies
Hand-held to Aircraft EO dispensing
Impact Fuzes / LOS to Norden Bomb Sight
First Guided Within Visual/Radar AI Seekers

'Revolutionary' Technologies
Analog IR/RF SA AI Seekers / ISR
Mechanical/Prox Fuze Options with SAFE ARM / MIL-STD-1763

'Revolutionary' Technologies
Digital Avionic Systems / Laser SA GW / MIL-STD-1760 / EW/EA+ GPS Aided / Electronic Fuzes / Low Observables

'Revolutionary' Technologies
Info Age Network enabled SoS / Cyber and Enterprise / Link 16/MADL/ ANI/AGI
Synthetical: Live Virtual Constructive

Family of Systems



- Systems of systems (SoS) or federation of system technology is believed to more effectively implement and analyse large complex, independent and heterogeneous systems, working (or made to work) cooperatively
- complex military SoS can better work effectively in coalitions, often from different countries and on multiple types of missions that have complexity and adaption beyond what was envisioned in their design and sustainment.
- Such coalitions are referred to as family-of-SoS (FoS) rather than federation

Family of Systems view

- Constituent SoSs in FoS are often intergenerational
- They can sometimes be complementary and at other times in conflict because of generational differences.
- SoS’s utility depends not only on its functionality/performance/effectiveness but also on those of other SoSs in the family.
- Thus integrality, interoperability and information (I3) are FoS level attributes rather than just SoS level attributes.
- Consider in-service SoSs as *adults* and developing SoSs as *children*, while regular assurance testing of adults will be called *team exercises* and development of children to work with the family as *schooling*.

I3 Assurance

- U.S. Department of Defense (DoD) had since 2009 undertaken six interrelated initiatives to significantly affect more Integrated, Interoperable and Information rich (I3) assurance to cope with such complexity and interconnectedness and to exploit it for information dominance which is key to fifth generation warfare

US I3 Initiatives

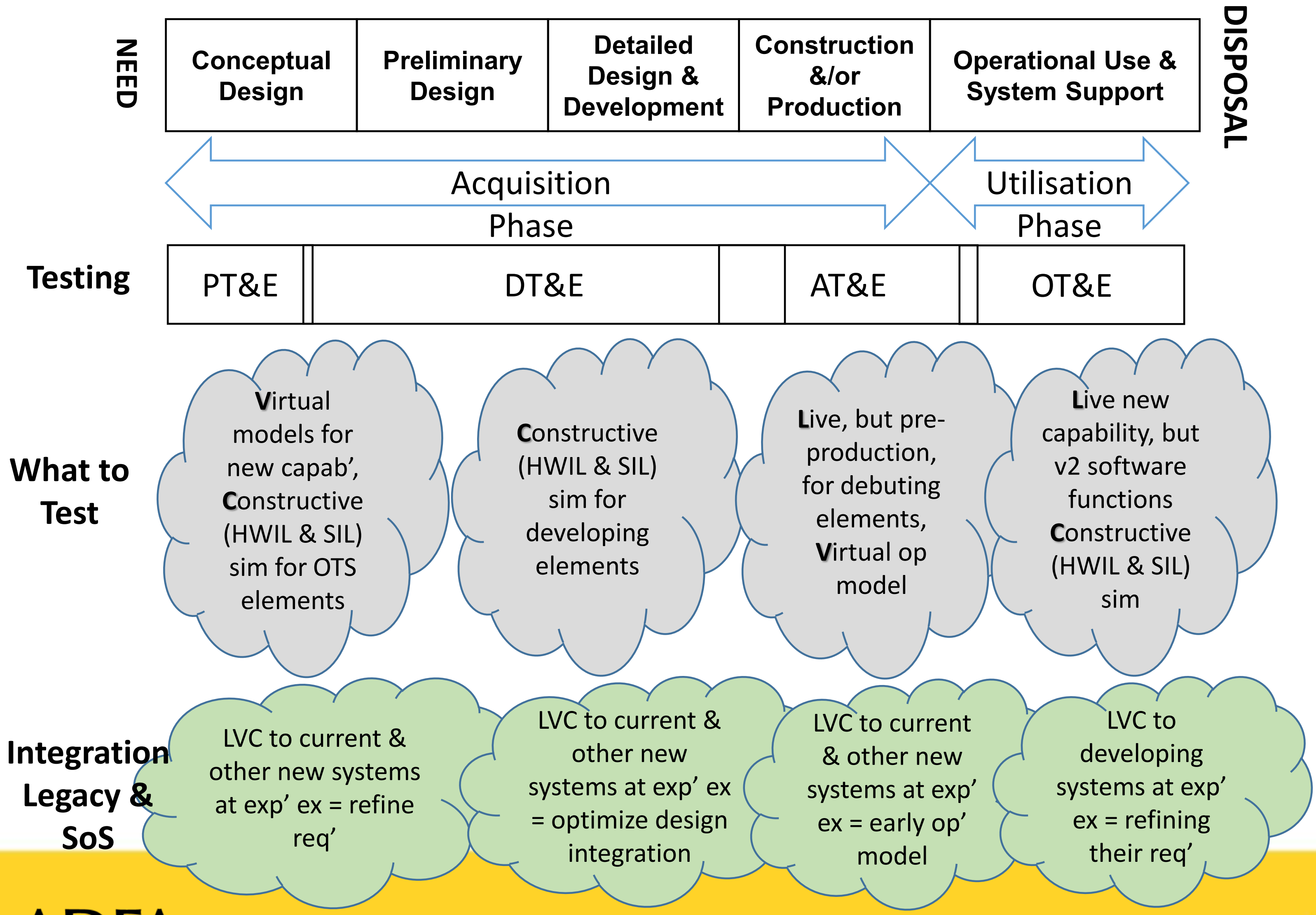
- Initiative 1 - Augmenting Operational Exercises with Formal Experimentation
- Initiative 2 - Integration System Program Offices (SPOs) and New Certifications.
- Initiative 3 - Enhanced T&E Regime – Earlier, Evidence-based Rigor.
- Initiative 4 - T&E Network Infrastructure.
- Initiative 5 - Cybersecurity Protection Plans and T&E.
- Initiative 6 - Permeating these U.S. Initiatives into Industry.

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



NEED

Conceptual Design | Preliminary Design | Detailed Design & Development | Construction &/or Production | Operational Use & System Support

DISPOSAL

Acquisition Phase

Utilisation Phase

Testing

PT&E | DT&E | AT&E | OT&E

What to Test

- **V**irtual models for new capab', **C**onstructive (HWIL & SIL) sim for OTS elements
- **C**onstructive (HWIL & SIL) sim for developing elements
- **L**ive, but pre-production, for debuting elements, **V**irtual op model
- **L**ive new capability, but v2 software functions **C**onstructive (HWIL & SIL) sim

Integration Legacy & SoS

- LVC to current & other new systems at exp' ex = refine req'
- LVC to current & other new systems at exp' ex = optimize design integration
- LVC to current & other new systems at exp' ex = early op' model
- LVC to developing systems at exp' ex = refining their req'

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

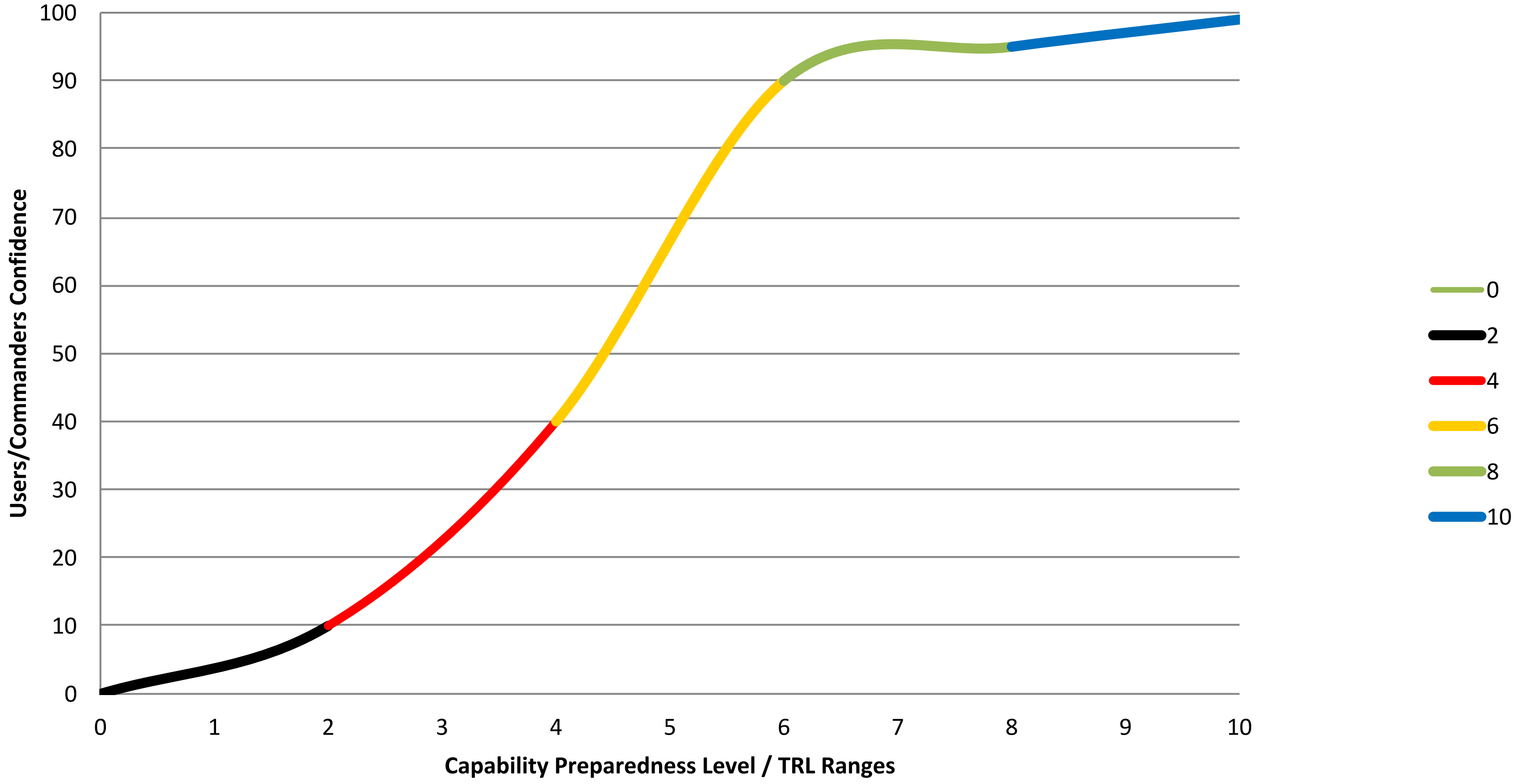
Certifications like: tactical data links, cybersecurity, joint fires (JTAC) etc

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

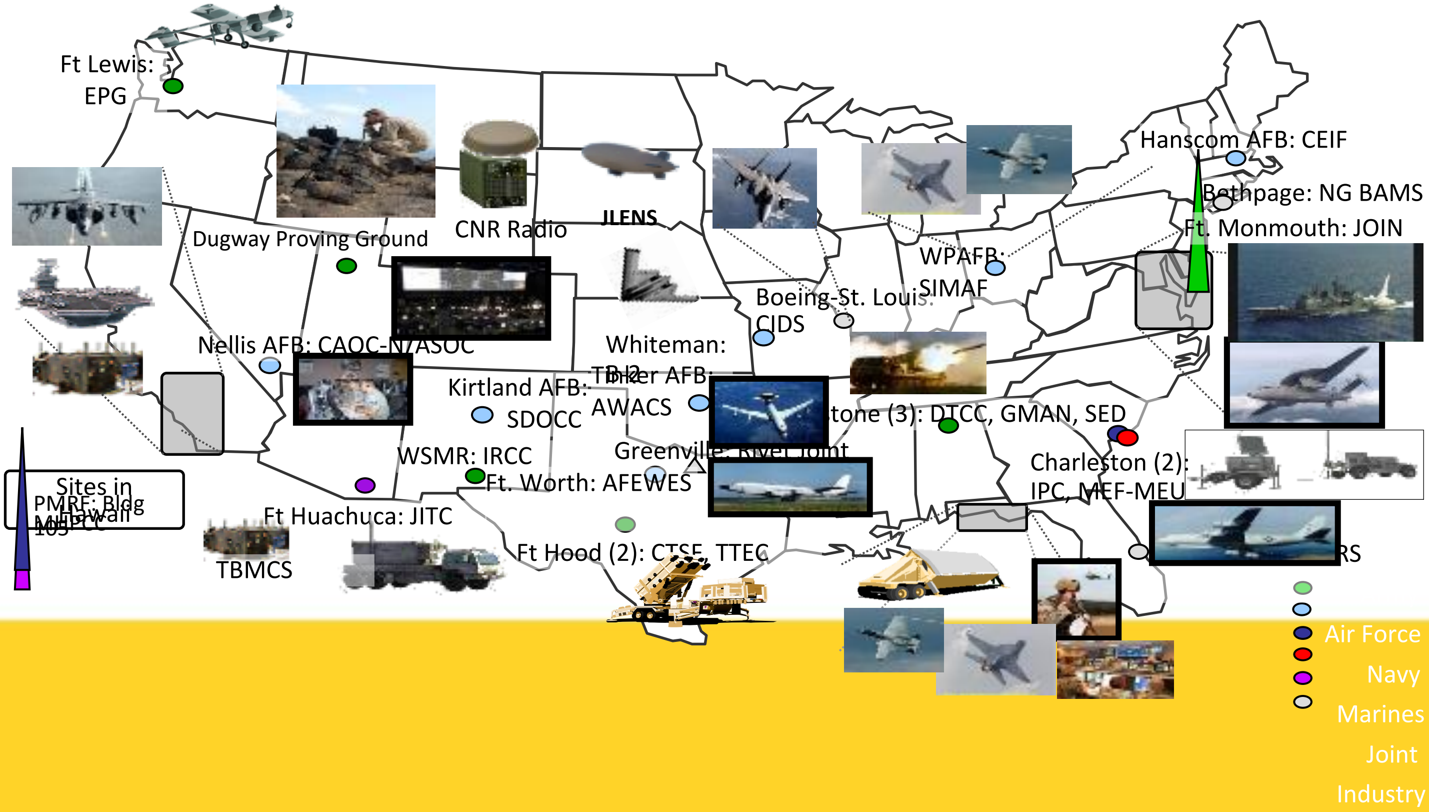


Testing early & often starting from M&S equals:

- 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)***

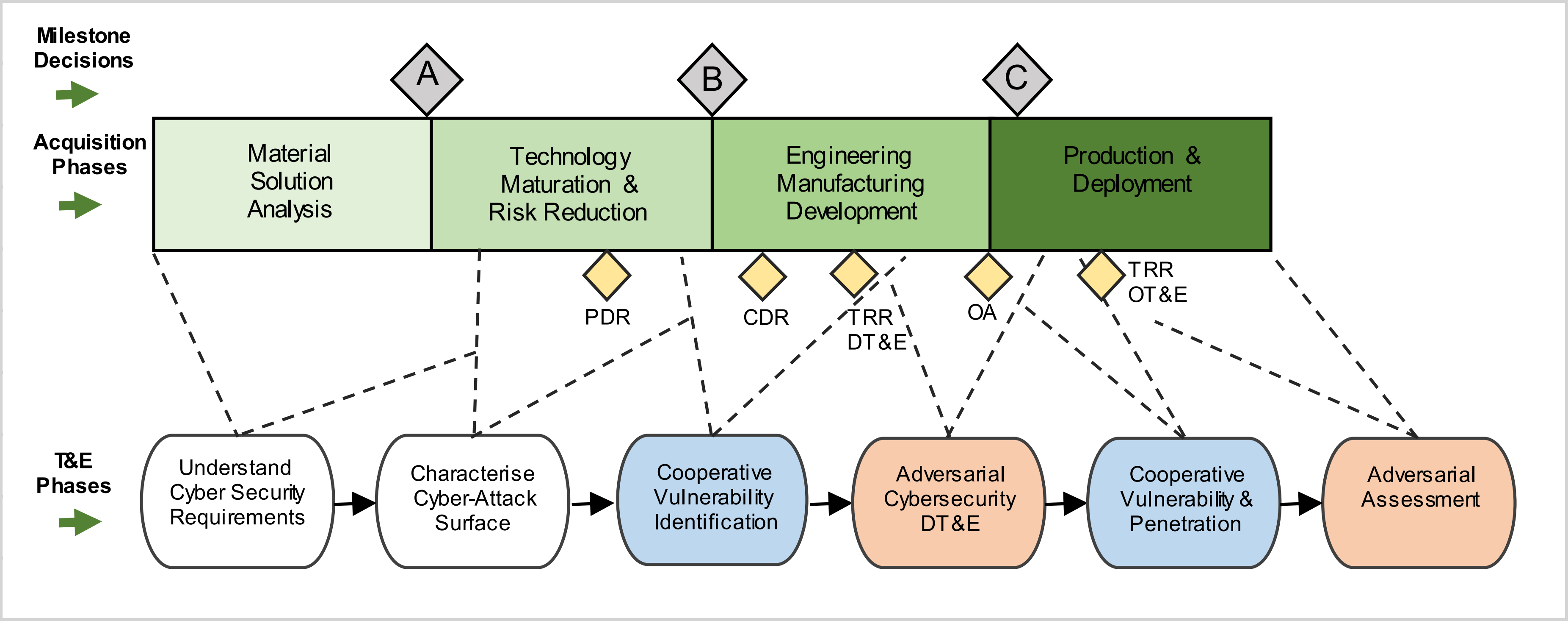


Initiative 5 - Cybersecurity Protection Plans & T&E

- 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

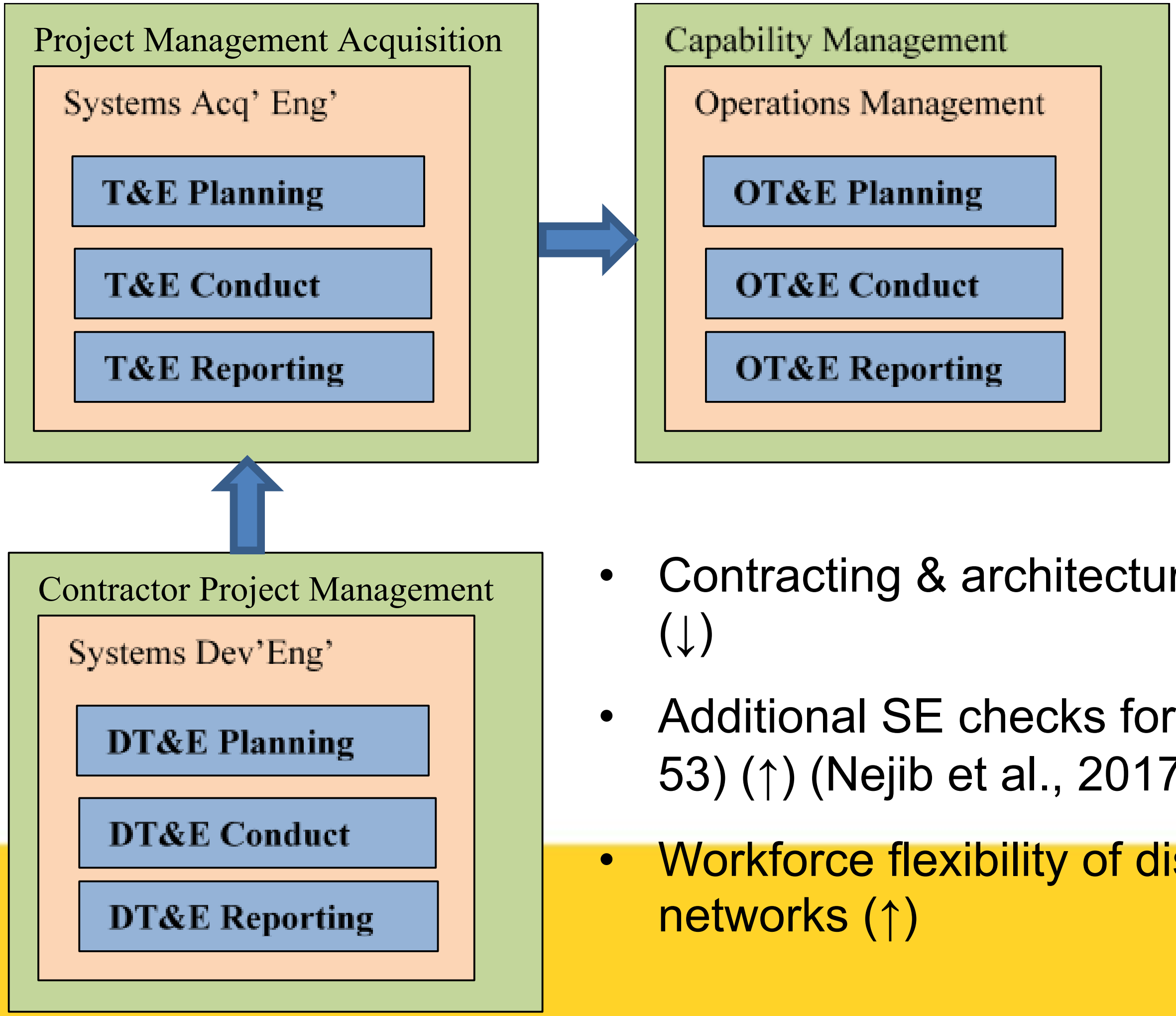

Milestone Decisions
A
B
C
Acquisition Phases
Material Solution Analysis
Technology Maturation & Risk Reduction
Engineering Manufacturing Development
Production & Deployment
PDR
CDR
TRR DT&E
OA
TRR OT&E
T&E Phases
Understand Cyber Security Requirements
Characterise Cyber-Attack Surface
Cooperative Vulnerability Identification
Adversarial Cybersecurity DT&E
Cooperative Vulnerability & Penetration
Adversarial Assessment

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 (↓)

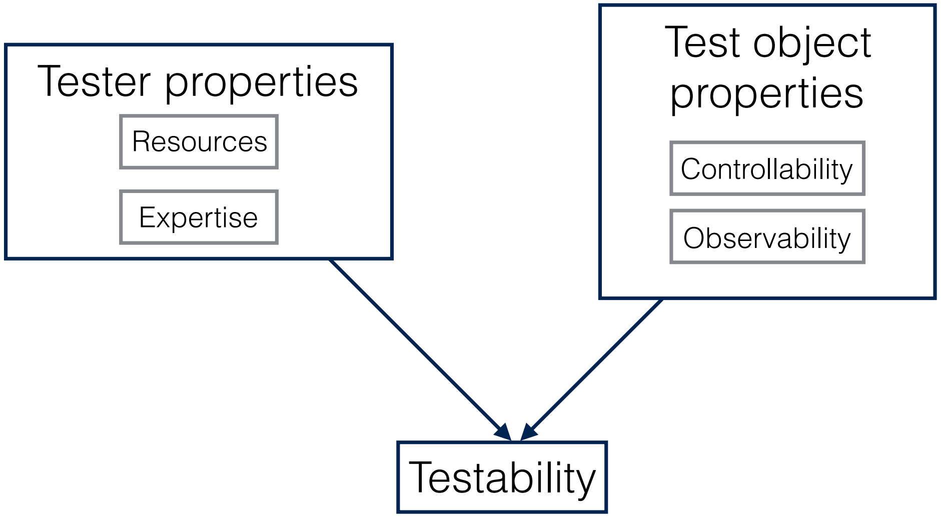
- Contracting & architectural control due Gov't I3 T&E (↓)
- Additional SE checks for cybersecurity tests (circa 53) (↑) (Nejib et al., 2017)
- Workforce flexibility of distributed T&E support via networks (↑)

Research questions

- How different Test and Evaluation (T&E) strategies work for optimum I3 assurance across the FoS level?
- What is the ideal frequency of teaming, the efficiency of schooling within teaming, and how these are affected by differing lengths of total schooling (i.e., SoS development times, and technology introduction rates).

Testability

- *Testability is commonly defined as the degree to which a component, a subsystem or a system can be tested in isolation from other components, subsystems and/or systems, and such that it de-risks the testing of the higher assemblies and whole. … Design techniques for testability improve the quality of the product in addition to reducing the costs of testing*

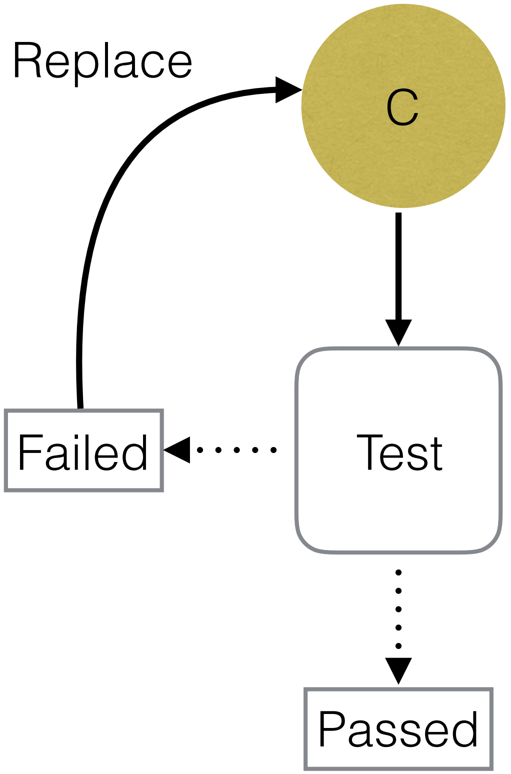


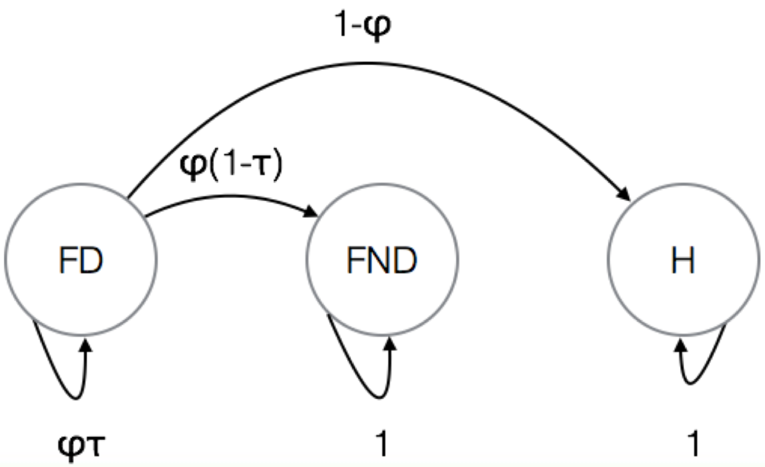
Testability of FoS

- In the context of I3 assurance of a FoS: *partitioning* is the SoSs that do or could contribute to a FoS; *observability* is the fidelity of test opportunities to disclose deficiencies within the FoS caused by any SoS; OPs are the test opportunities to assure an FoS and the key information points that disclose the I3 test metrics; and *controllability* is the ability of a FoS to control the SoS. By the definitions and outlines earlier, FoS when compared to usual systems-level should have reasonable but declining partitioning, low observability due to generational differences, and limited controllability.

Markovian Test Model

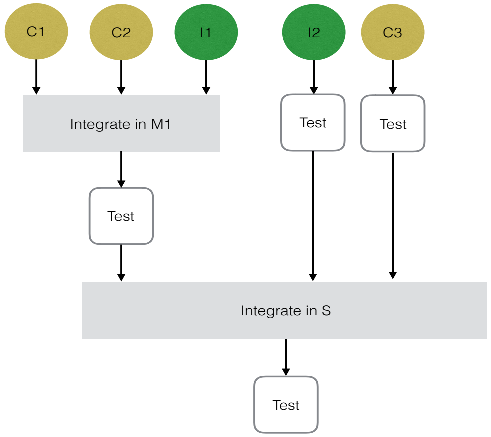
- Absorbing Markov chain state space for one unit testing
- FD = Fault Detected, FND = Fault Not Detected H = Healthy, $\varphi = Pr(Unit = Faulty), \tau = Pr(Fault = Detected \mid Unit = Faulty)$

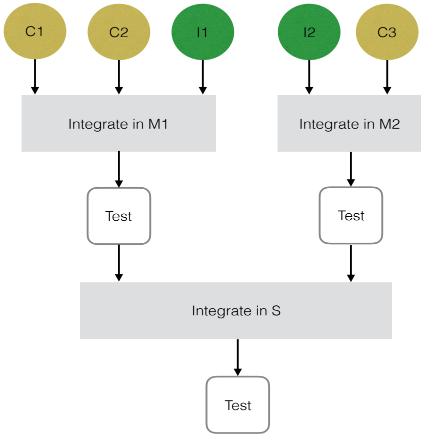


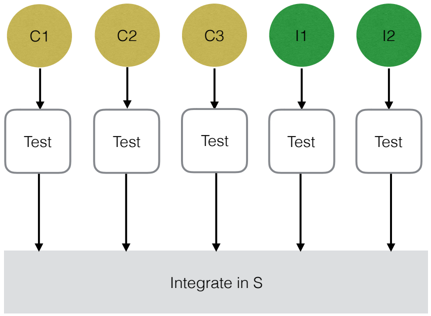


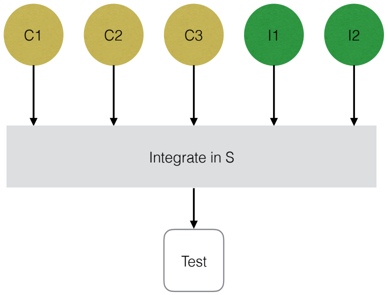
Testing Architecture (cont'd)

- Different Examples of testing a system of five components





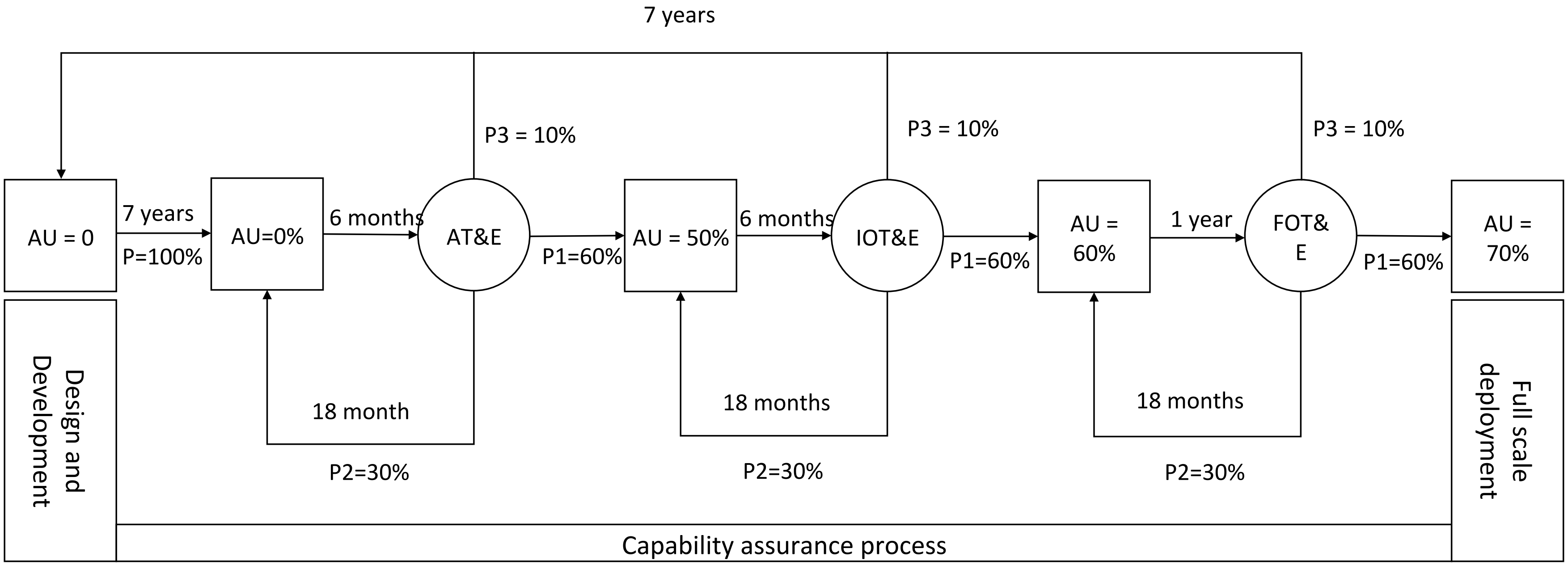




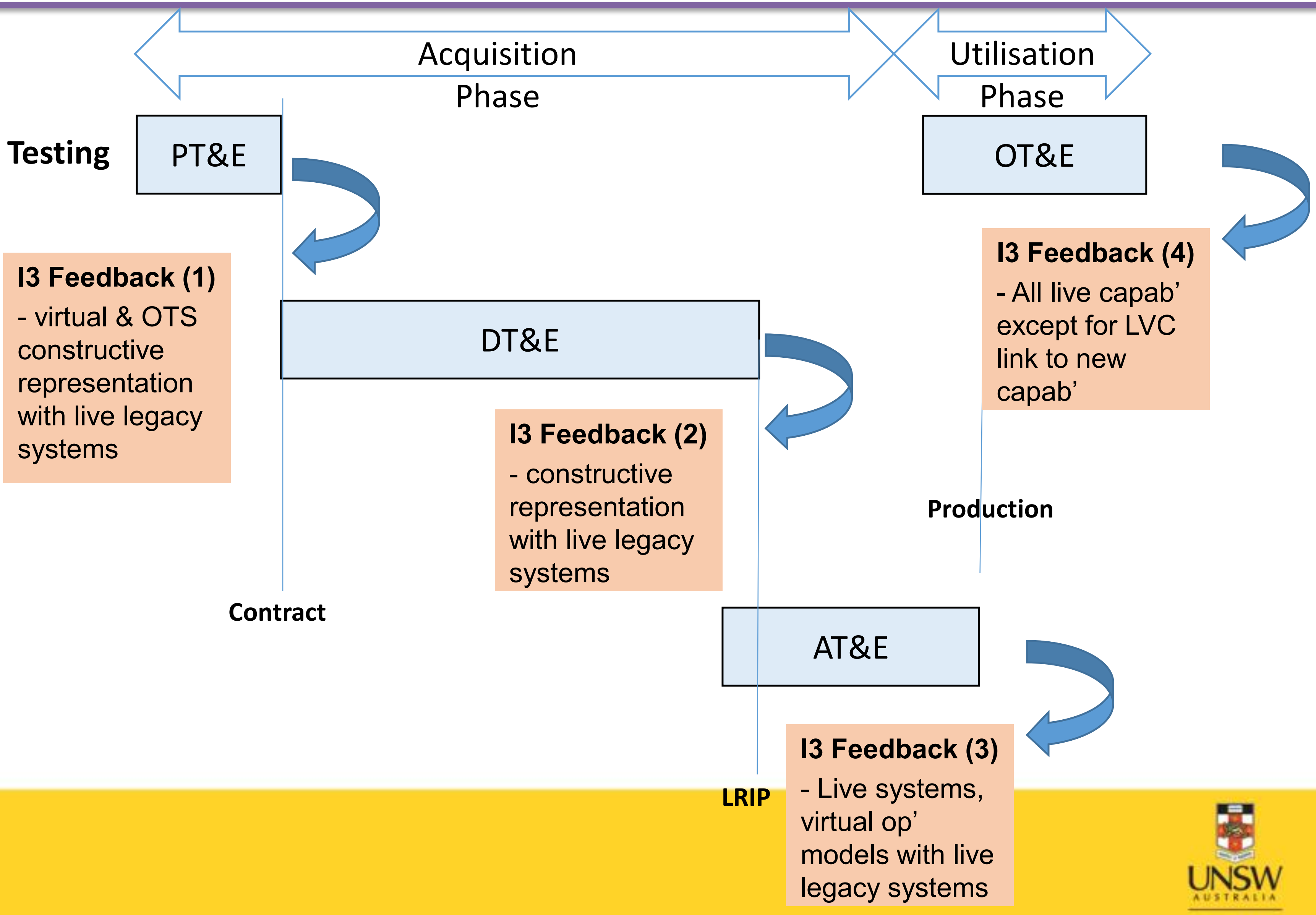
The Australian DoD approach to I2 assurance

- Focuses on operational exercises to do the team exercise for the adults of the FoS.
- Unlike the U.S. DoD, on average, no additional integration or experimental exercises exist to allow child SoSs to play with adults in a controlled environment
- The child SoSs each go through an assurance program (i.e., school) envisioned and planned during the requirements and early contract phase and implemented quite late in development during acceptance and operational testing as the systems are built, assembled and delivered.
- I2 assurance before contract is focused on reviewing the written requirements against future operating and integrating concepts.

Quantitative Modelling – Aust' Model



Explaining US Differences for Australians



Acquisition Phase

Utilisation Phase

Testing

PT&E

OT&E

I3 Feedback (1)

- virtual & OTS constructive representation with live legacy systems

DT&E

I3 Feedback (2)

- constructive representation with live legacy systems

Contract

AT&E

LRIP

I3 Feedback (3)

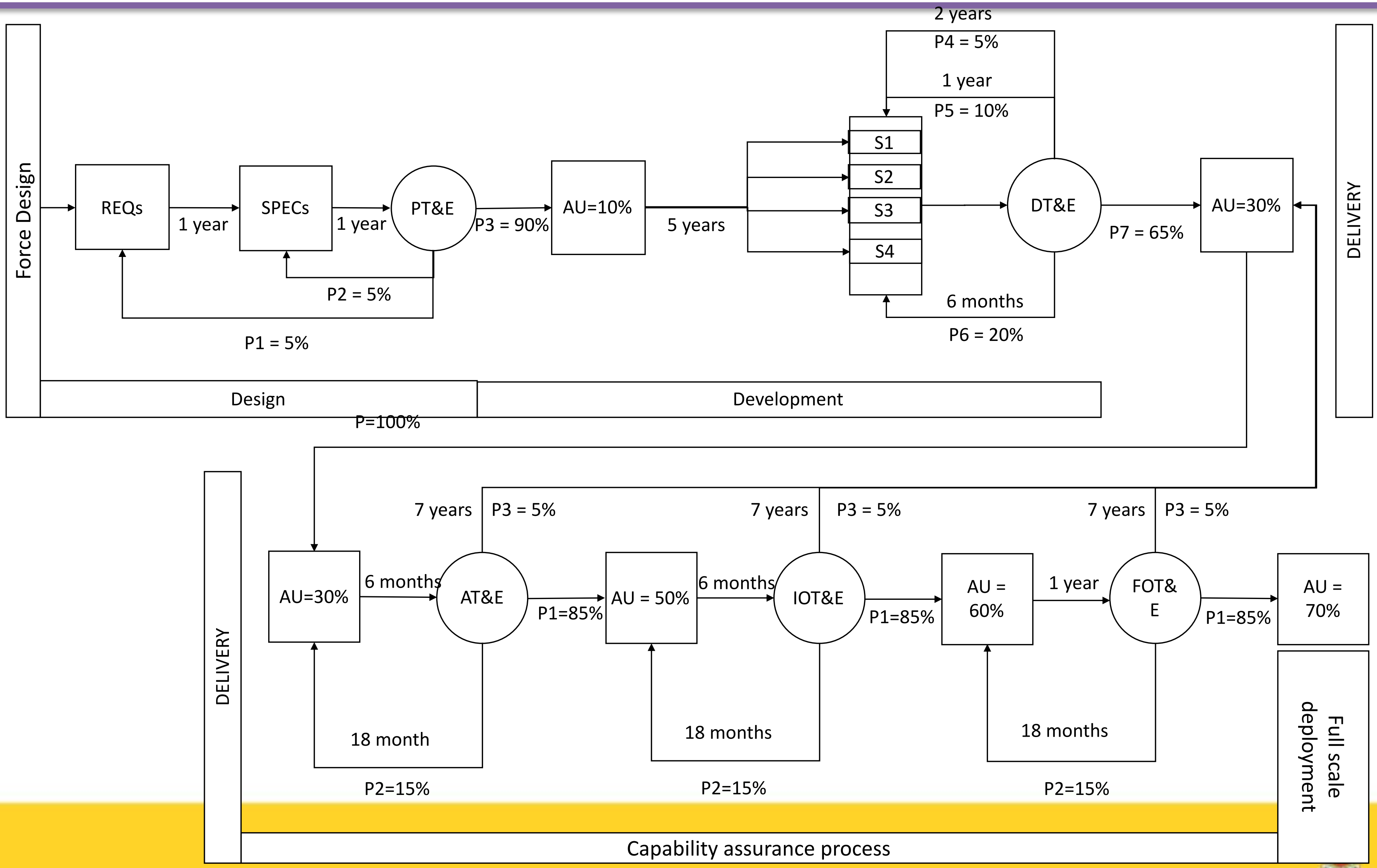
- Live systems, virtual op' models with live legacy systems

Production

I3 Feedback (4)

- All live capab' except for LVC link to new capab'

Quantitative Modelling – US Model



Quantitative modelling method

- 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**: Set 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

Efatmaneshnik, M., Shoval, S., Joiner, K. F., Ryan, M.: System Test Architecture Evaluation: A Probabilistic Modeling Approach. INCOSE International Symposium, 2018.