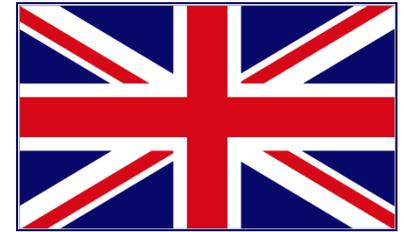




Software Security, Dependability and Resilience Initiative (S S D R I)



UK Perspective on Practice Adoption

US Software Assurance Forum – Fall 2011

12 September 2011 – Arlington VA US

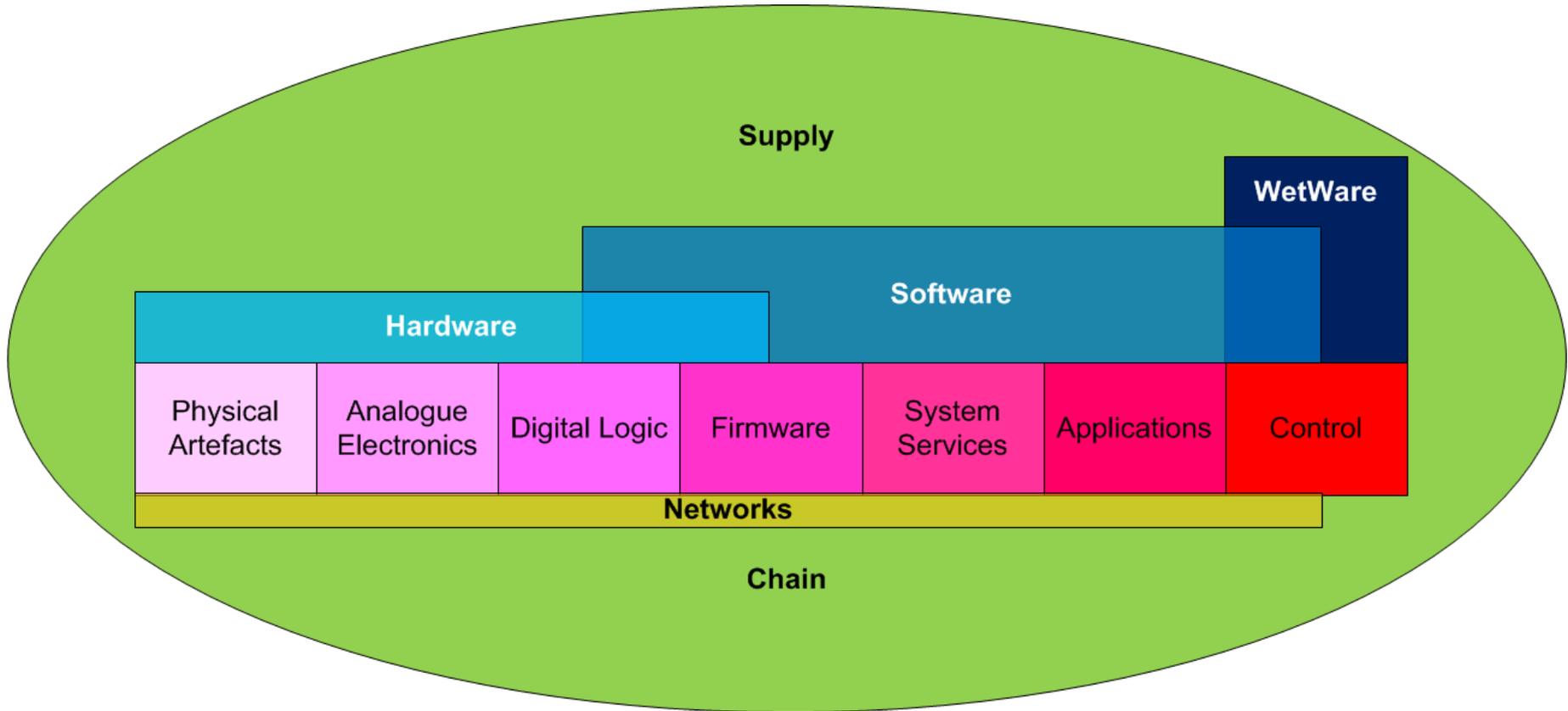
Ian Bryant

Technical Director SSDRI

[DMU/CSC/SSDR/2011/090 | v1.0 | 20110912]

UK's public-private platform for Making Software Better

Software and ICT Context

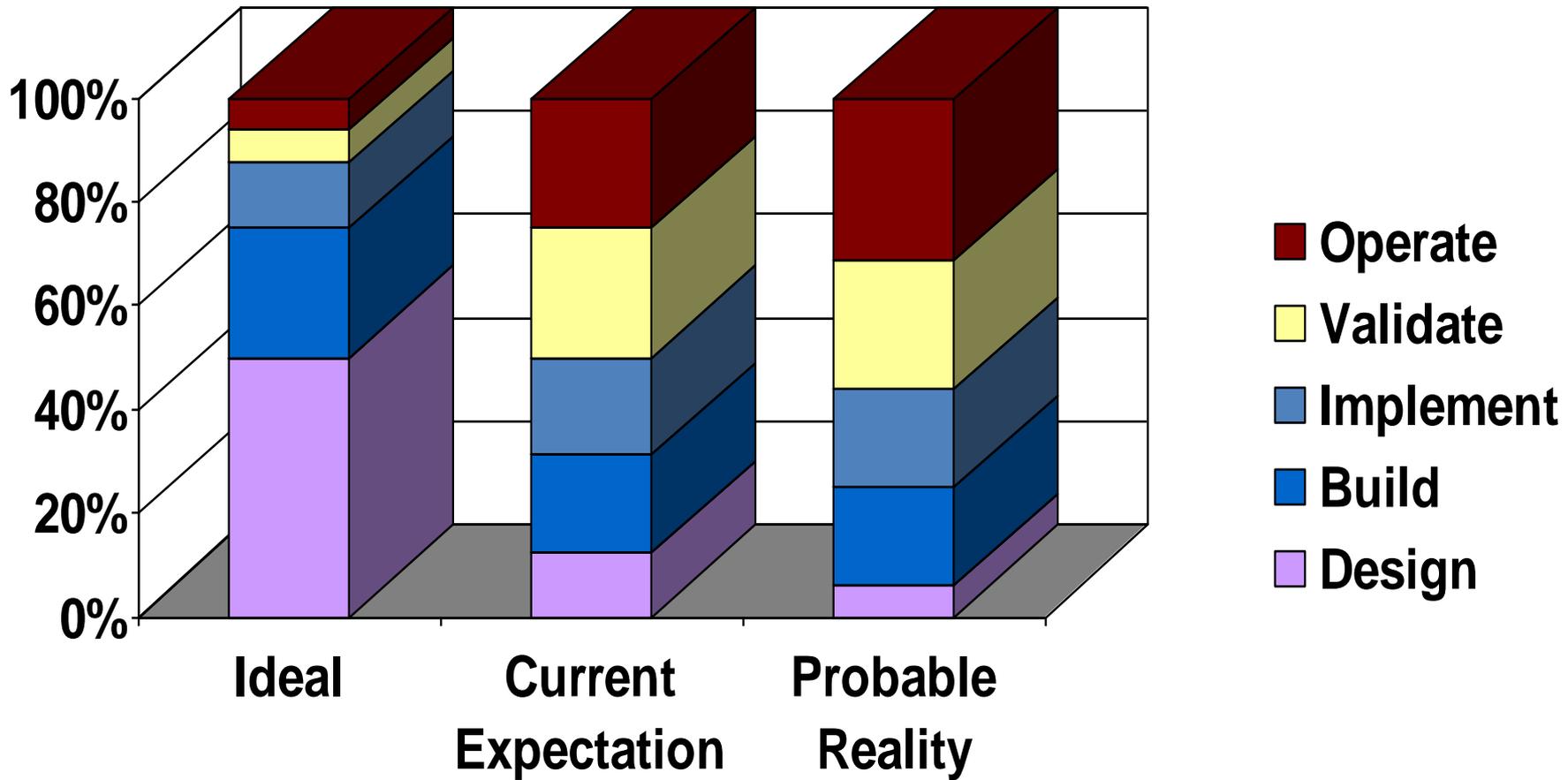


Software Development

- Underlying assumption software will be developed under engineering-style “waterfall” model, under single organisational control
- Challenges to these assumptions include:
 - Agile Development
 - Open Source
 - Multicore Processors
 - Untrusted platforms (incl. counterfeit hardware)
 - Distributed application platforms and services
 - Software / hardware boundary (e.g. VDHL)

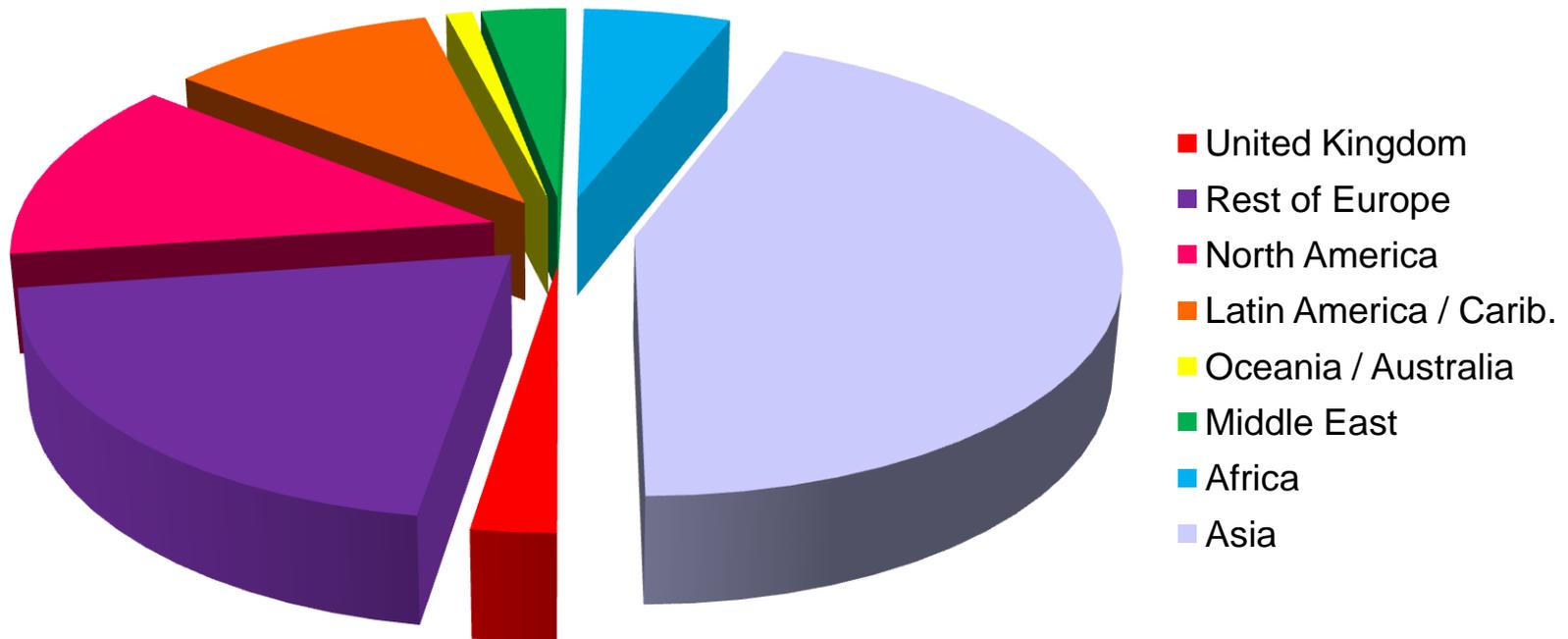


Software Effort Imbalance



Globalisation

Internet Users



Source: National IA Forum (2010)



SSDR I : UK's public-private platform for Making Software Better

Software Incident Impact

- Software problems are high cost to economy:
 - US Government National Institute of Standards & Technology (NIST) ~\$60 billion / year to US alone
 - No definitive figure for UK / worldwide
- Software a major source of IT project failure:
 - University of Oxford Saïd Business School / McKinsey 2011
 - ESSU (European Services Strategy Unit) 2007
 - Tata Consultancy 2007
 - Standish Chaos Reports 2004 onwards
 - Rand 2004



Software Adversities

- Few practitioners treat Adversity
- Information Security community address Threat
 - Deterministic model with problems handling Known, Unknown and Unknowable (KuU) factors
 - Often ignores Hazards
- System Reliability / Safety community address Hazards
 - Typically Stochastic model
 - Approach usually ignores Threat

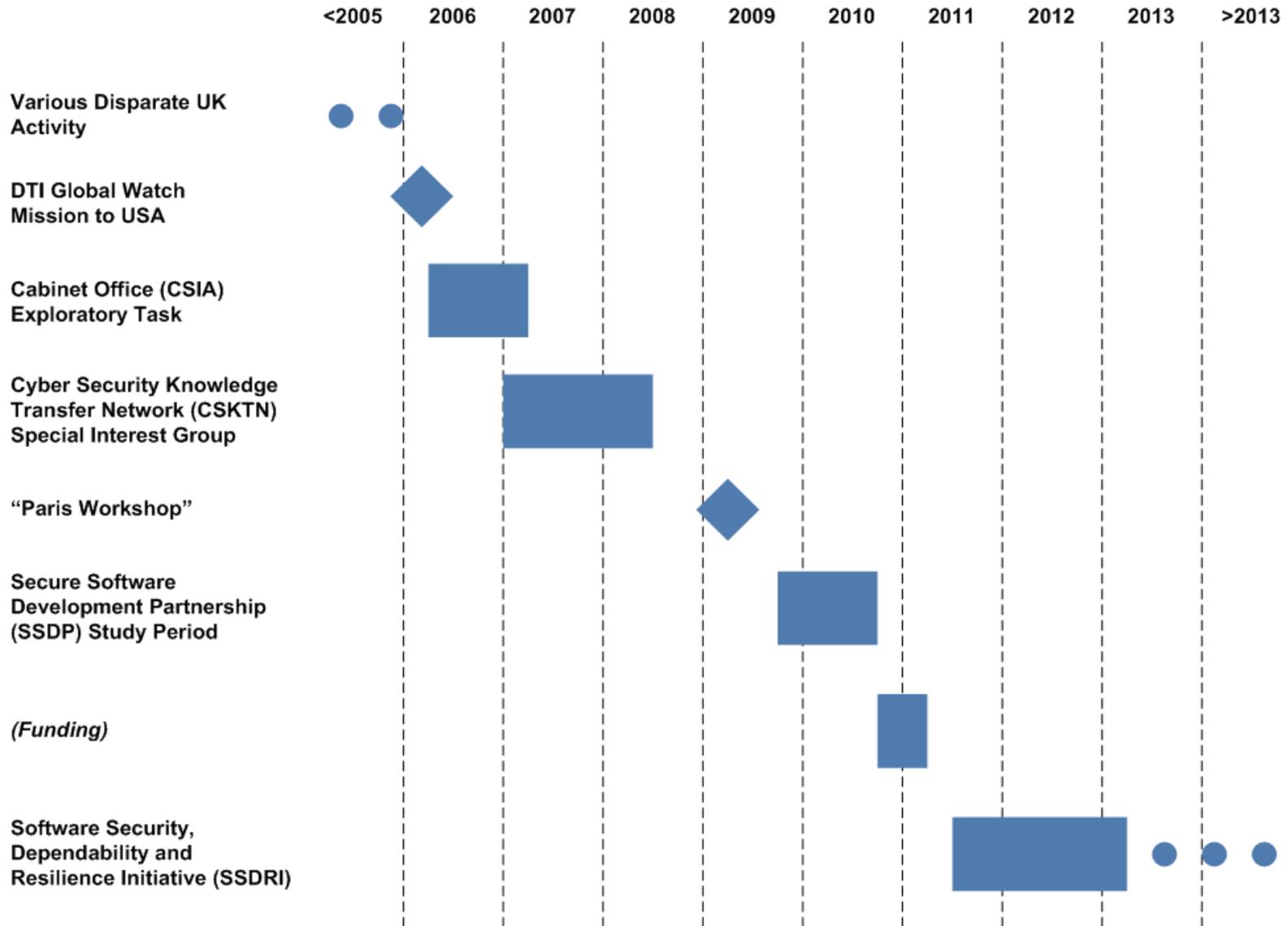


Current Drivers

- 2010 UK National Security Strategy has Cyber-attack and deficiencies as one of the 4 “Tier One” Risks
- New Technological / Societal challenges:
 - Cloud
 - Mobile Devices
 - Lightweight operating systems
 - Consumerisation / Bring-Your-Own-Device (BYOD)
 - Commoditisation in previously closed architectures
 - Consolidation for energy efficiency (Low Carbon / Green)
- These are likely to present Disruptive Challenges, **fundamentally deepening** dependence on Software



Software Security, Dependability and Resilience in UK



SSDRI: UK's public-private platform for Making Software Better

Software Security, Dependability and Resilience Initiative (S S D R I)

In response to previous work, the 2010 UK National Security Strategy, and emergent challenges, on 1st July 2011 UK formed SSDRI:

“A public-private platform for enhancing the overall software and systems culture, with the objective that all software should become designed, implemented and maintained in a secure, dependable and resilient manner”

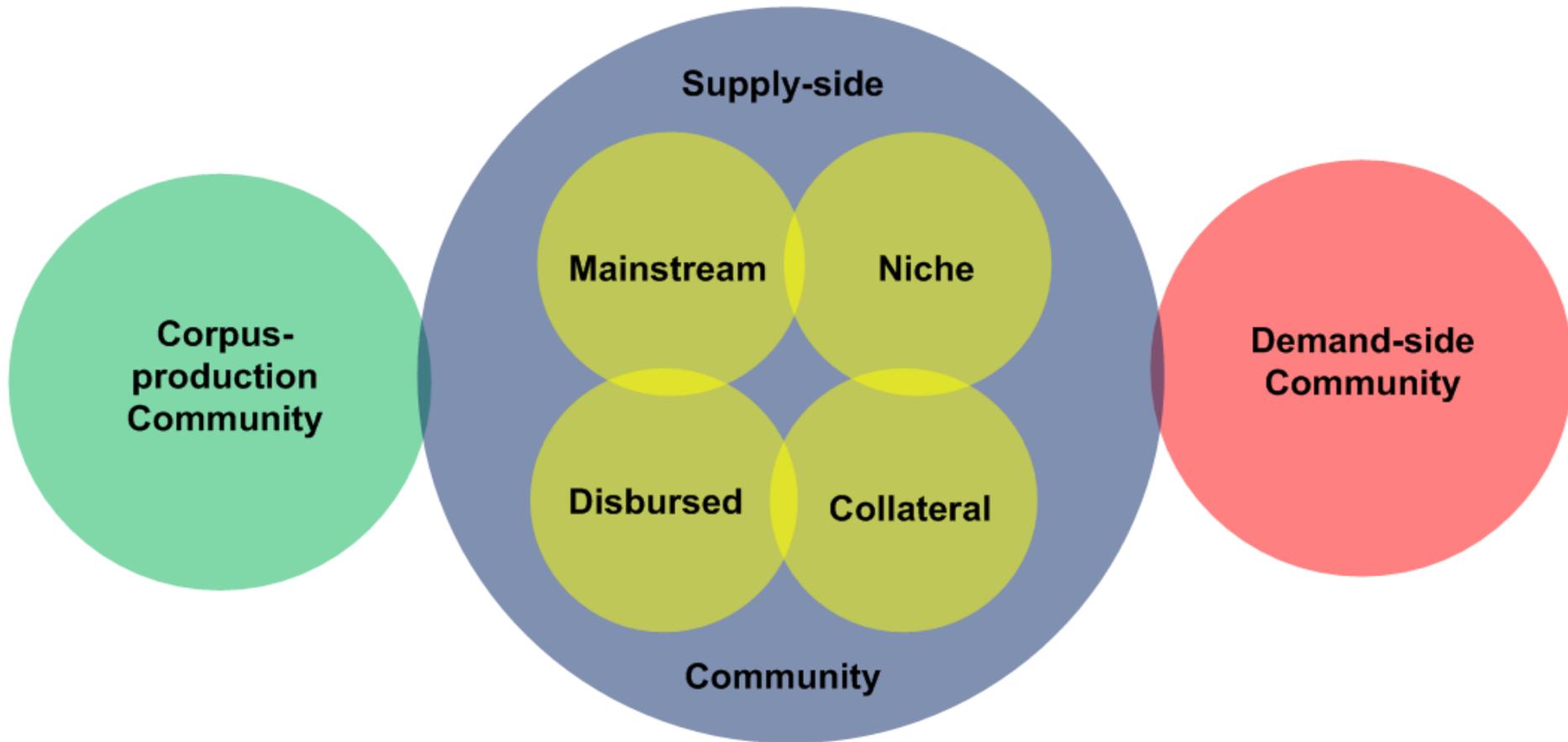


SSDRI Scope

- Goal is to improve Software
 - Security (mainly protection of Confidentiality)
 - Dependability (mainly protection of Integrity)
 - Resilience (mainly protection of Availability)
- Importantly, this applies to **both** :
 - Specific software and systems developed for specialist markets where Security, Dependability and Resilience are Functional Requirements, typically with Medium/High assurance needs
 - **And** to all other software and systems for which Security, Dependability and Resilience are Non Functional Requirements (NFR), typically with Due Diligence needs



SSDRI Audiences

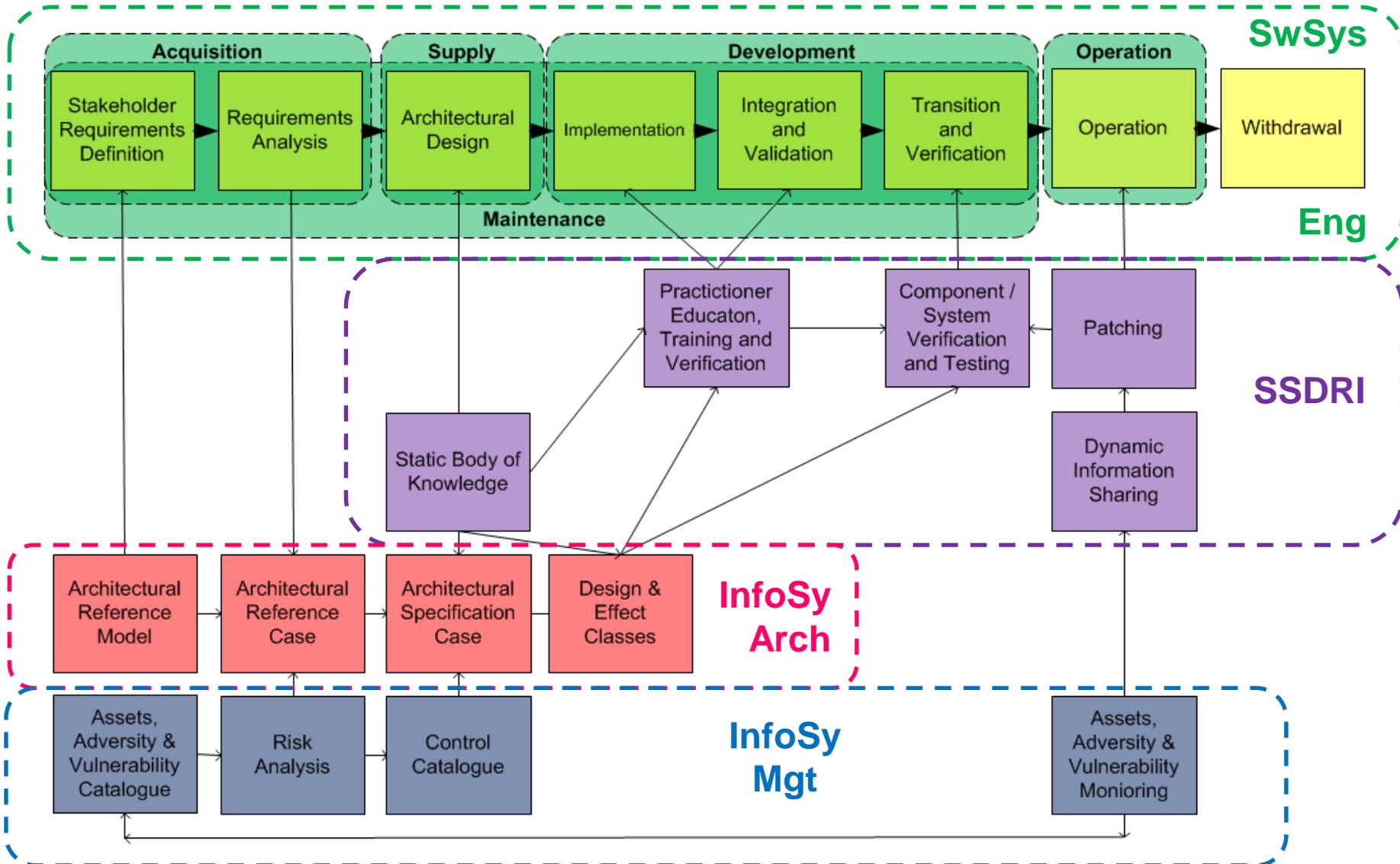


Software Supply-side Segments

- Mainstream
 - “The Industry” e.g. Microsoft, Oracle, ...
- Niche
 - Specialist Industries e.g. Aviation, “Security”
- Disbursed
 - Small scale developers e.g. SmartPhone Apps
- Collateral
 - Developers don’t consider themselves as such
 - e.g. Embedded systems, website CMS Users, spreadsheets, ...

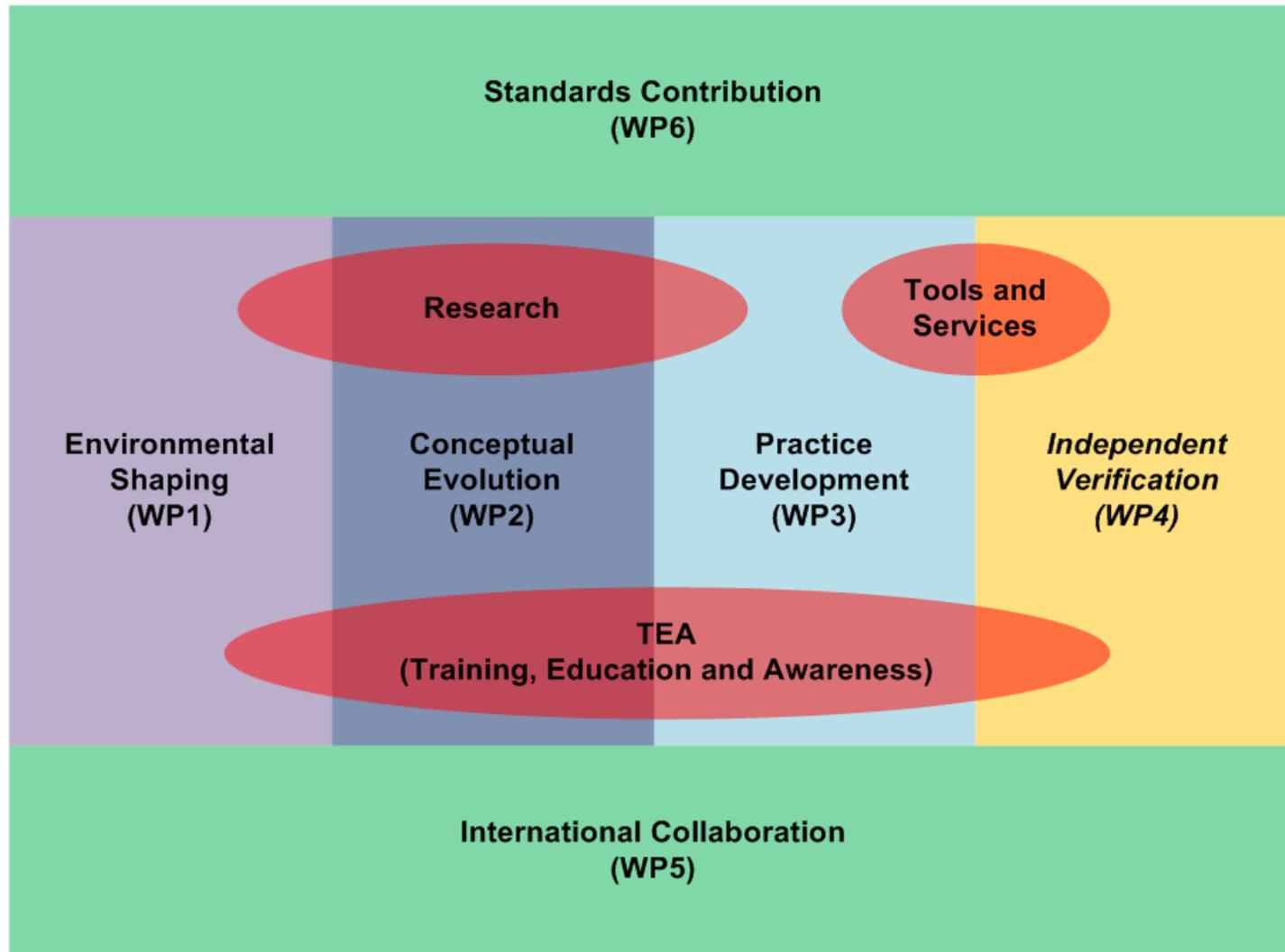


SSDRI Lifecycle and Dependencies

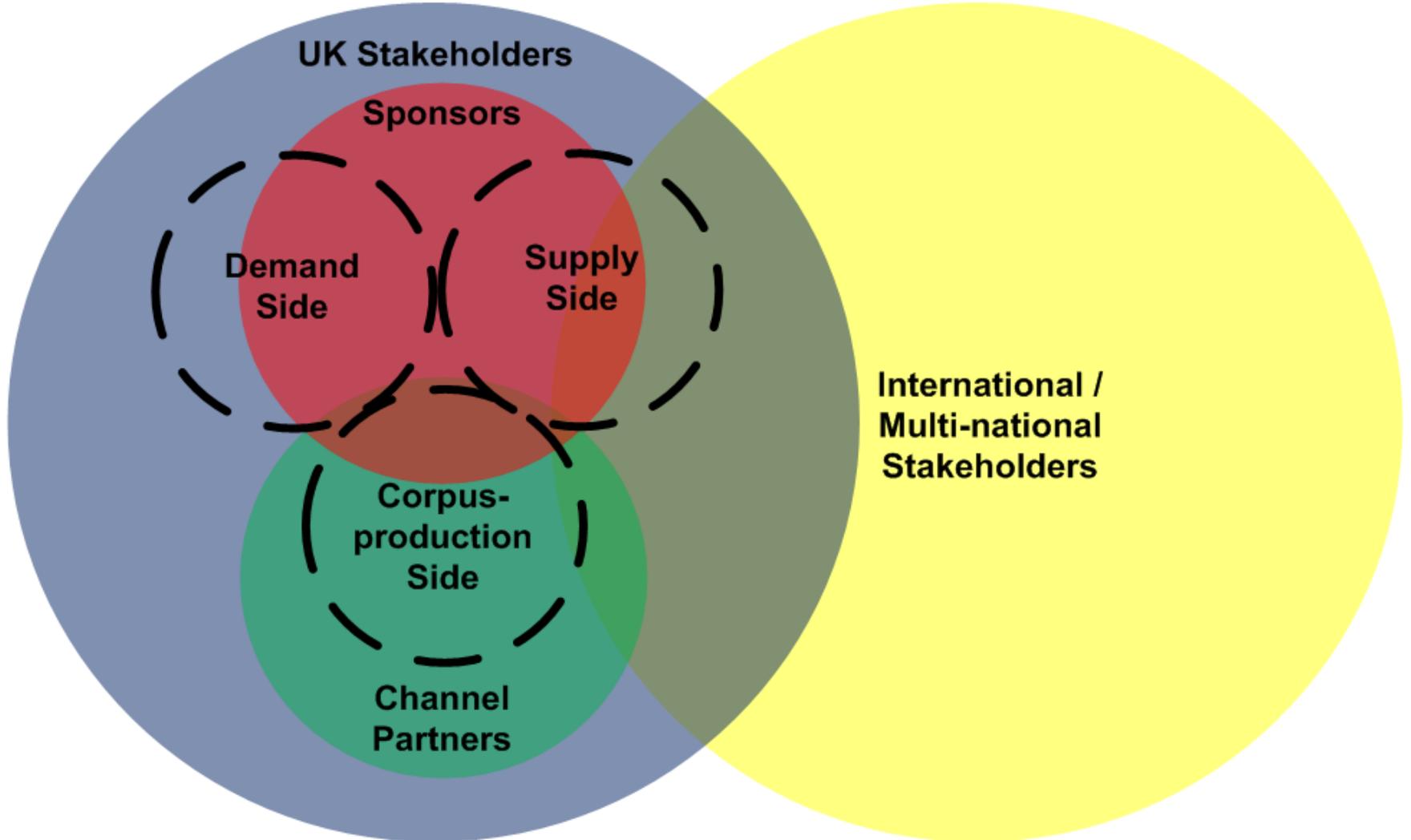


SSDRI: UK's public-private platform for Making Software Better

Software Security, Dependability and Resilience Initiative Work Packages and Effort Clusters



SSDRI Engagement



SSDRI Special Interest Groups (SIG)

- Main vehicle for SSDRI delivery of its remit for producing a harmonised, UK view of the various subject areas will be through Special Interest Groups (SIG)
- SIGs formed of *pro bono* technical contributors from across all sectors of UK economy
- List of SIGs currently **still being defined**, but **draft** set of 10 is:
 - Rationale
 - Awareness
 - Metrics
 - Guidance
 - Supply Chain Risk Management
 - Education
 - Training
 - Standards
 - Conceptual Evolution
 - Verification and Testing
(for WP4: In Abeyance)



WP5: International Collaboration

- SSSDR is not a “UK plc” problem
- International Collaboration is therefore an essential element of efforts
 - Multinational involvement was intrinsically part of the Paris Workshop
- Initial International Collaboration options
 - International Standardisation through BSI₁ (British Standards Institute)
 - Bilateral collaboration with US peer organisation, Software Assurance (SwA) / Build Security In (BSI₂)



WP5: UK/US Collaboration

UK (SSDRI) Special Interest Groups (DRAFT ^[1])	US (BSI / SwA) Working Groups
Rationale	Business Case
Awareness	-
Metrics	Measurement
Guidance	Processes and Practices
Supply Chain Risk Management	Acquisition and Outsourcing ^[2]
Education	Workforce Education and Training
Training	
Standards	-
Conceptual Evolution	Technology and Tools
Verification and Testing ^[3]	
-	Malware

^[1] This list of SIGs can be expected to be, at least partially, dynamic

^[2] Linked to DOD activity in Supply Chain Risk Management (SCRM), which includes links into hardware realm such as anti-counterfeiting

^[3] For WP4 (Independent Verification) – currently in abeyance

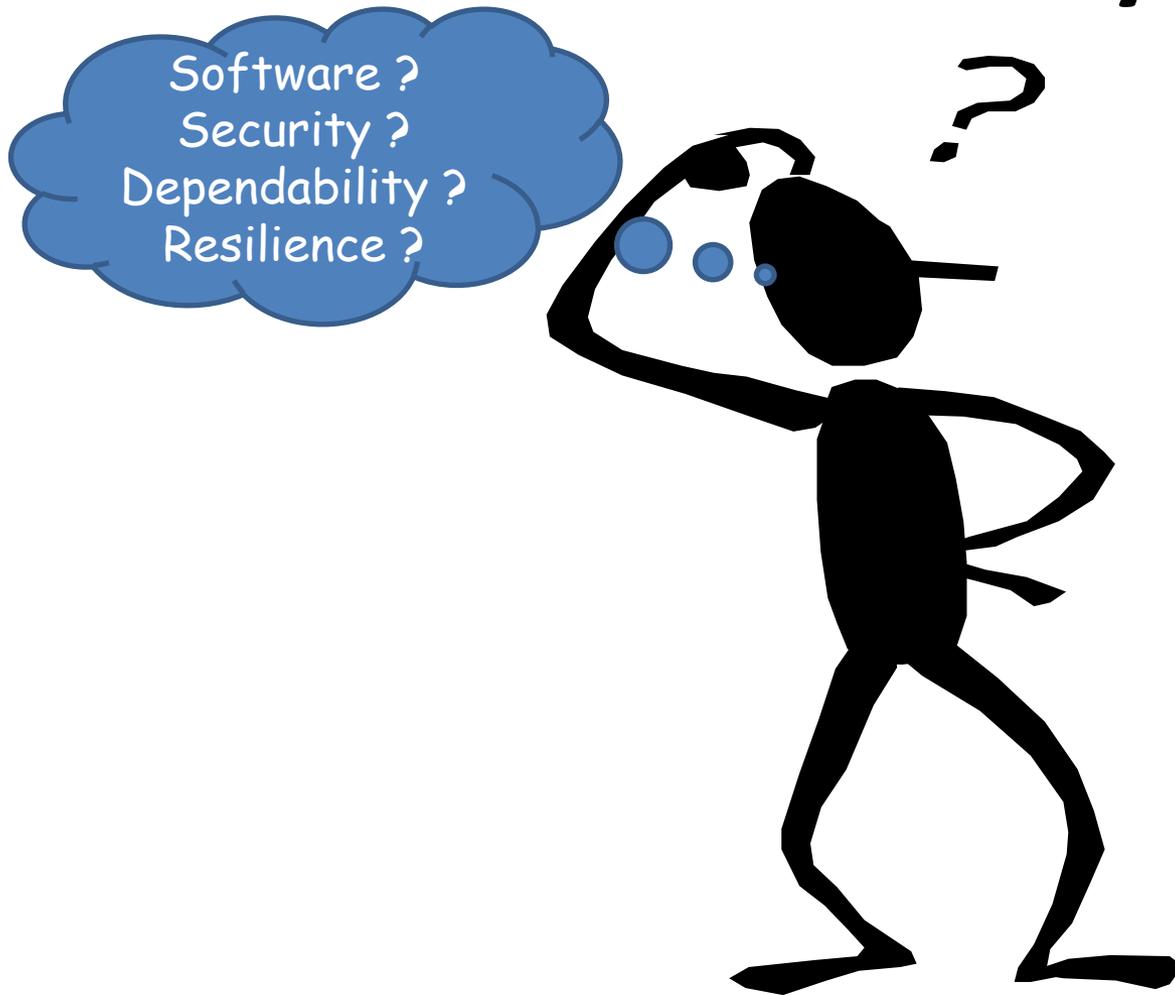


WP6: International Standardisation

- No standardisation of Standards Development Organisations (SDO) !
- Main UK recognised SDO in SSSDR area would be ISO/IEC JTC1, which has multiple active projects on this topic under SC7 and SC27
- Emergent work under ITU-T (“CYBEX”), which is linked to BSI/SwA through Mitre
- Monitoring *de facto* standardisation through other bodies, such as OWASP



Any Questions ?



Contact Details

Ian Bryant

Technical Director S S D R I

c/o Centre for Security Computing

De Montfort University

The Gateway, Leicester, LE1 9BH, England

ian.bryant@ssdri.org.uk; Internet

[+44 79 7312 1924](tel:+447973121924); Mobile

<http://www.ssdri.org.uk/>

