Software

Security, Dependability and Resilience

Initiative (S S D R I)

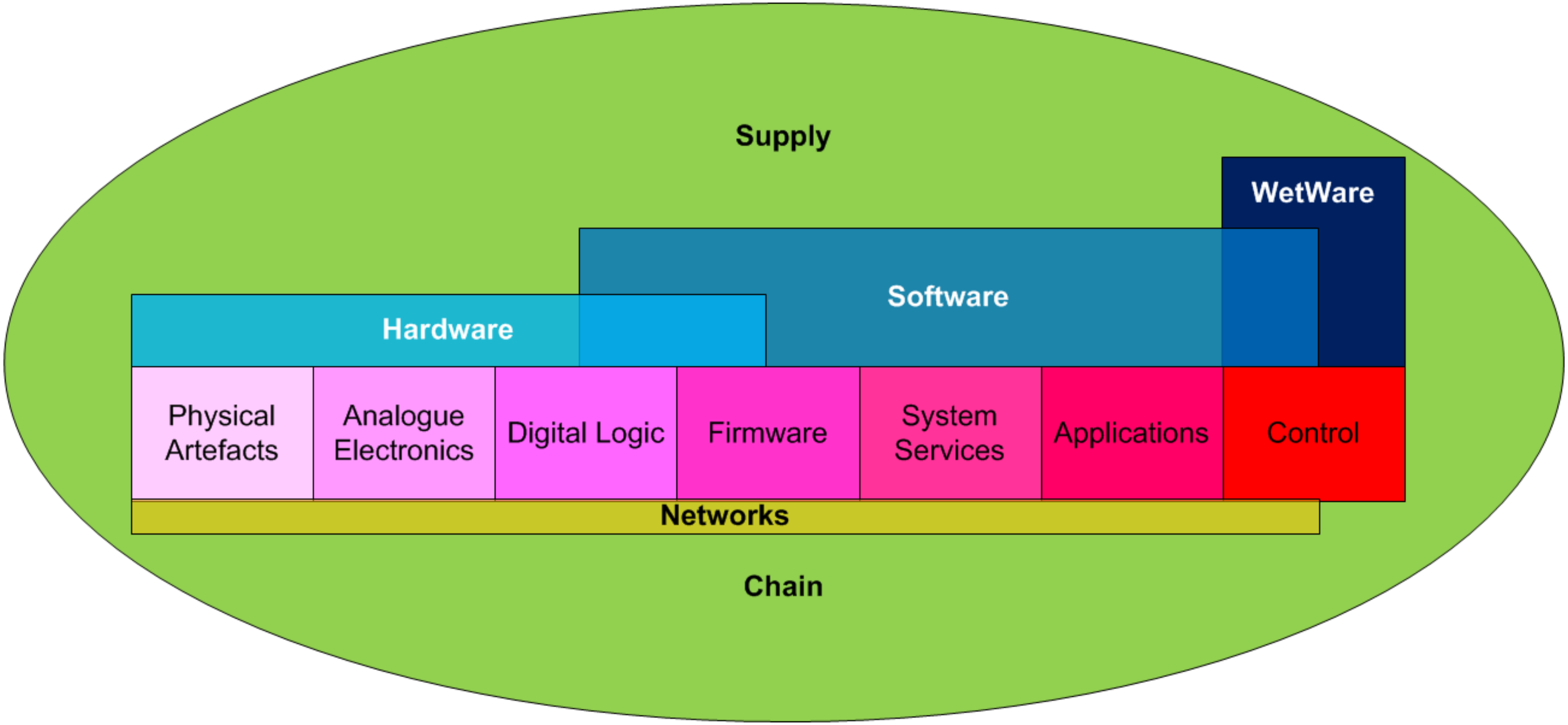
Case Study:
Treating Challenges
in Software Trustability

Ian Bryant
Technical Director SSDRI

[DMU/CSC/SSDR/2011/142 | v1.1 | 20111207]

ACSA Conference 2012 (ACSAC)
Orlando FL US
7 December 2011

Software and Wider ICT Context



Software Defects

- 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

Malicious Software

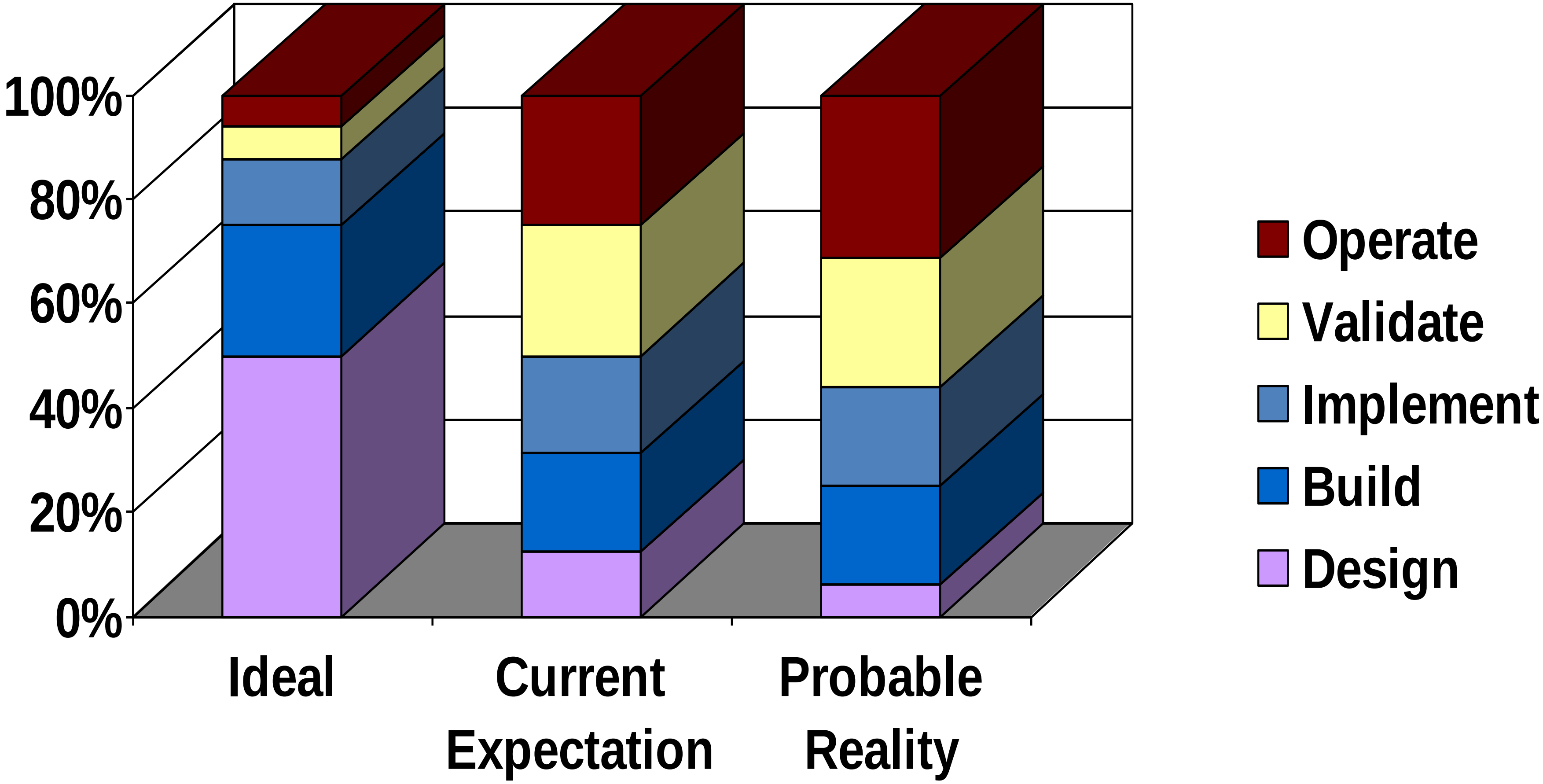
- Malicious Software (MalWare) ecosystem
- Ever increasing number of MalWare strains has challenges for reactive mitigation approaches (analysis workload and host performance)
- ICT marketplace is evolving in ways that will seem a proliferation of new types of platforms and software, increasing potential attack surface
- Software supply base broadening to those with little knowledge of good development practices

Software Composition

Segment	Embedded Systems	SCADA Systems	Communications Systems	IT Infrastructure	IT Applications
Reuse	Limited	Libraries	Libraries; Mobile Code	Libraries; Mobile Code; Cloud Services	Libraries; Mobile Code; Cloud Services; Mashups

◄── Trusted Supply Chain Required ──►

Context: Effort Imbalance



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
  - Untrusted platforms (incl. counterfeit hardware)
  - Software / hardware boundary (e.g. VHDL)
  - Multicore Processors
  - Use of structured data (e.g. XML) to control behaviour

Emerging Challenges

Top 10 Strategic Technology Trends for 2012

- Media Tablets and Beyond
- Mobile-Centric Applications and Interfaces
- Contextual and Social User Experience
- Internet of Things
- App Stores and Marketplaces
- Next-Generation Analytics
- Big Data
- In-Memory Computing
- Extreme Low-Energy Servers
- Cloud Computing

Source*:* *Gartner, Inc.* (18 October 2011)

Current SDR Drivers

- 2010 UK National Security Strategy has Cyber-attack and deficiencies as one of the 4 “Tier One” Risks
- New Technological / Societal challenges:
  - Distributed application platforms and services (“Cloud”)
  - Mobile Devices and 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 Faults

- Mitre’s Common Weakness Enumeration (CWE) is a community developed, formal list of software weakness types created to:
  - Serve as a common language for describing software weaknesses in architecture, design, or code
  - Serve as a standard measuring stick for software tools targeting these weaknesses
  - Provide a common baseline standard for weakness identification, mitigation, and prevention efforts
- Currently 810 distinct CWE entries identified

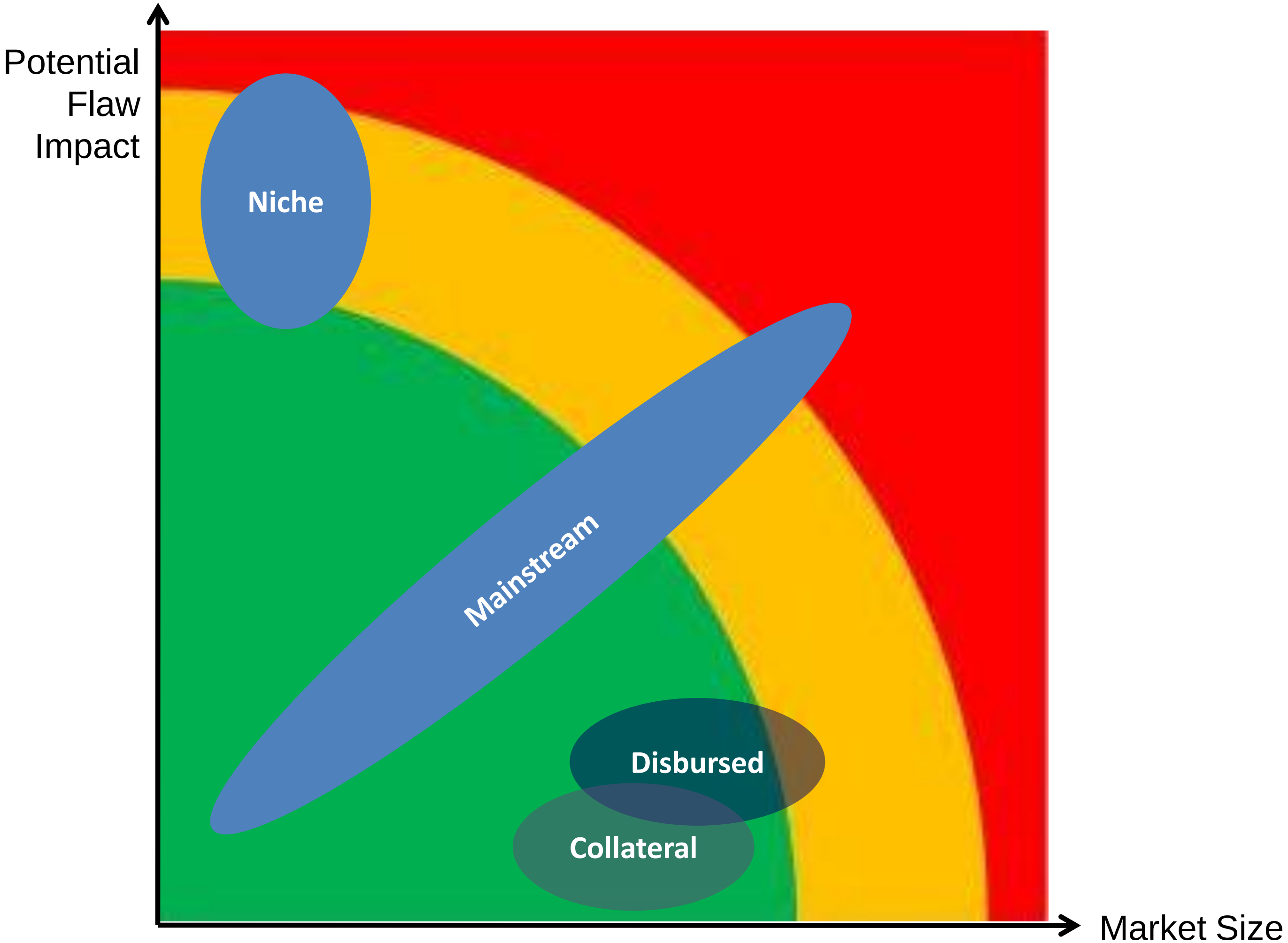
Mitre/SANS CWE Top 25 (1)

Rank	ID	Name
1	CWE-79	Failure to Preserve Web Page Structure ('Cross-site Scripting')
2	CWE-89	Improper Sanitization of Special Elements used in an SQL Command ('SQL Injection')
3	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
4	CWE-352	Cross-Site Request Forgery (CSRF)
5	CWE-285	Improper Access Control (Authorization)
6	CWE-807	Reliance on Untrusted Inputs in a Security Decision
7	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
8	CWE-434	Unrestricted Upload of File with Dangerous Type
9	CWE-78	Improper Sanitization of Special Elements used in an OS Command ('OS Command Injection')
10	CWE-311	Missing Encryption of Sensitive Data
11	CWE-798	Use of Hard-coded Credentials
12	CWE-805	Buffer Access with Incorrect Length Value
13	CWE-98	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP File Inclusion')

Mitre/SANS CWE Top 25 (2)

Rank	ID	Name
14	CWE-129	Improper Validation of Array Index
15	CWE-754	Improper Check for Unusual or Exceptional Conditions
16	CWE-209	Information Exposure Through an Error Message
17	CWE-190	Integer Overflow or Wraparound
18	CWE-131	Incorrect Calculation of Buffer Size
19	CWE-306	Missing Authentication for Critical Function
20	CWE-494	Download of Code Without Integrity Check
21	CWE-732	Incorrect Permission Assignment for Critical Resource
22	CWE-770	Allocation of Resources Without Limits or Throttling
23	CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
24	CWE-327	Use of a Broken or Risky Cryptographic Algorithm
25	CWE-362	Race Condition

Risk Segmentation



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

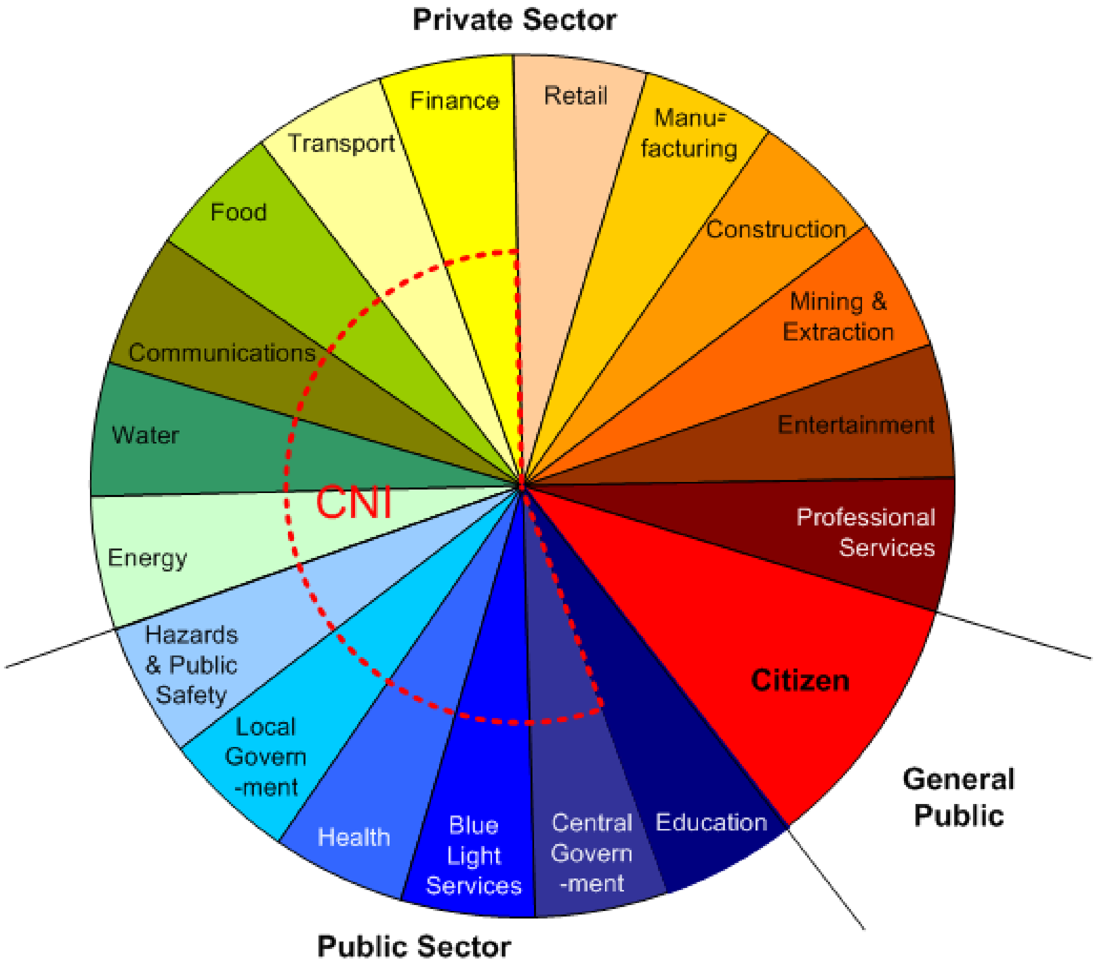
In response to previous work, the 2010 UK National Security Strategy, and emergent challenges, on 1st July 2011 UK formed SSDRI:

> “***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
  - **S**ecurity (mainly protection of **C**onfidentiality)
  - **D**ependability (mainly protection of **I**ntegrity)
  - **R**esilience (mainly protection of **A**vailability)
- Importantly, this applies to **both** :
  - Specific software and systems developed for specialist markets where Security, Dependability and Resilience (SDR) are Functional Requirements, typically with Medium/High assurance needs
  - **And** to all other software and systems for which Security, Dependability and Resilience (SDR) are Non Functional Requirements (NFR), typically with Due Diligence needs

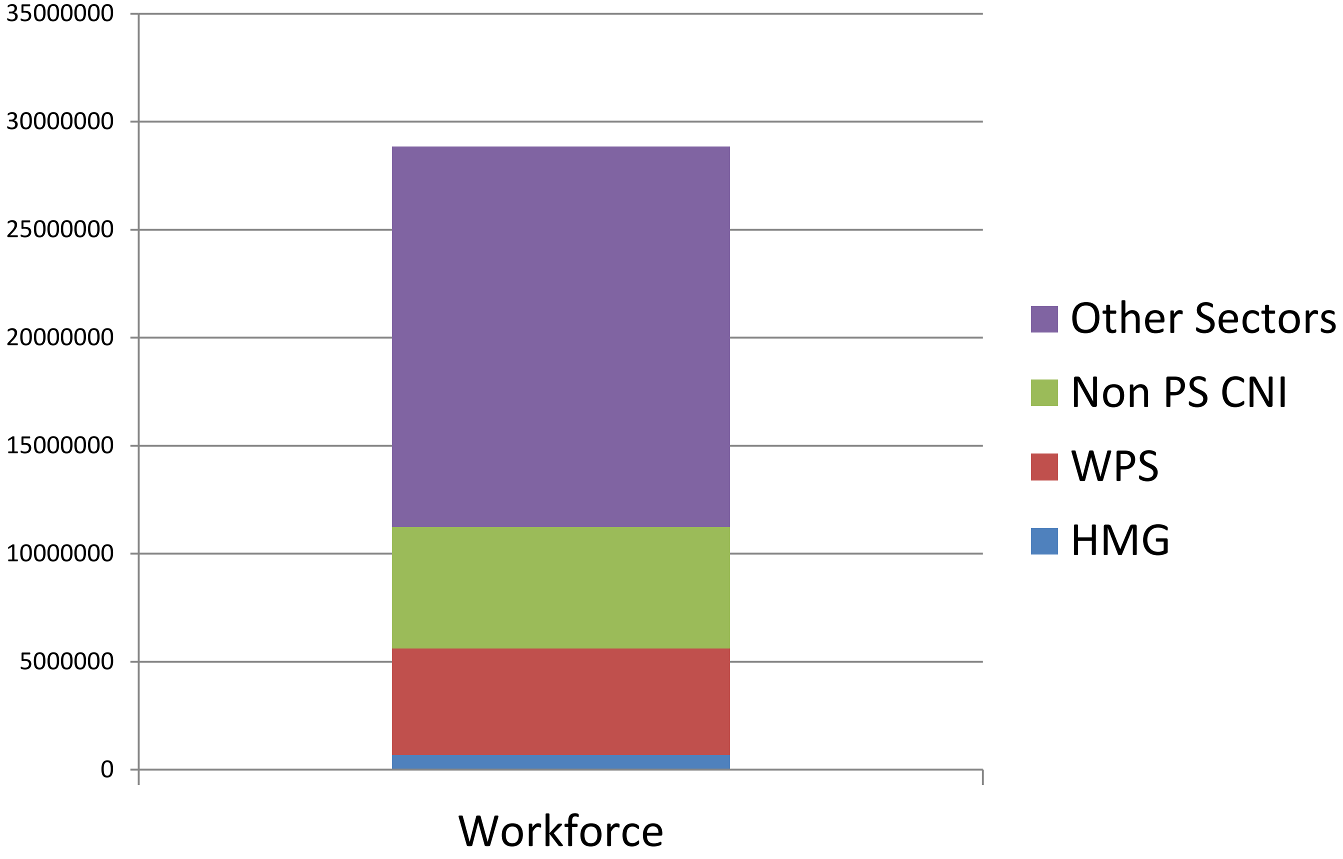
UK Economic Sectors



Source: GIPSI / Cabinet Office (2004)

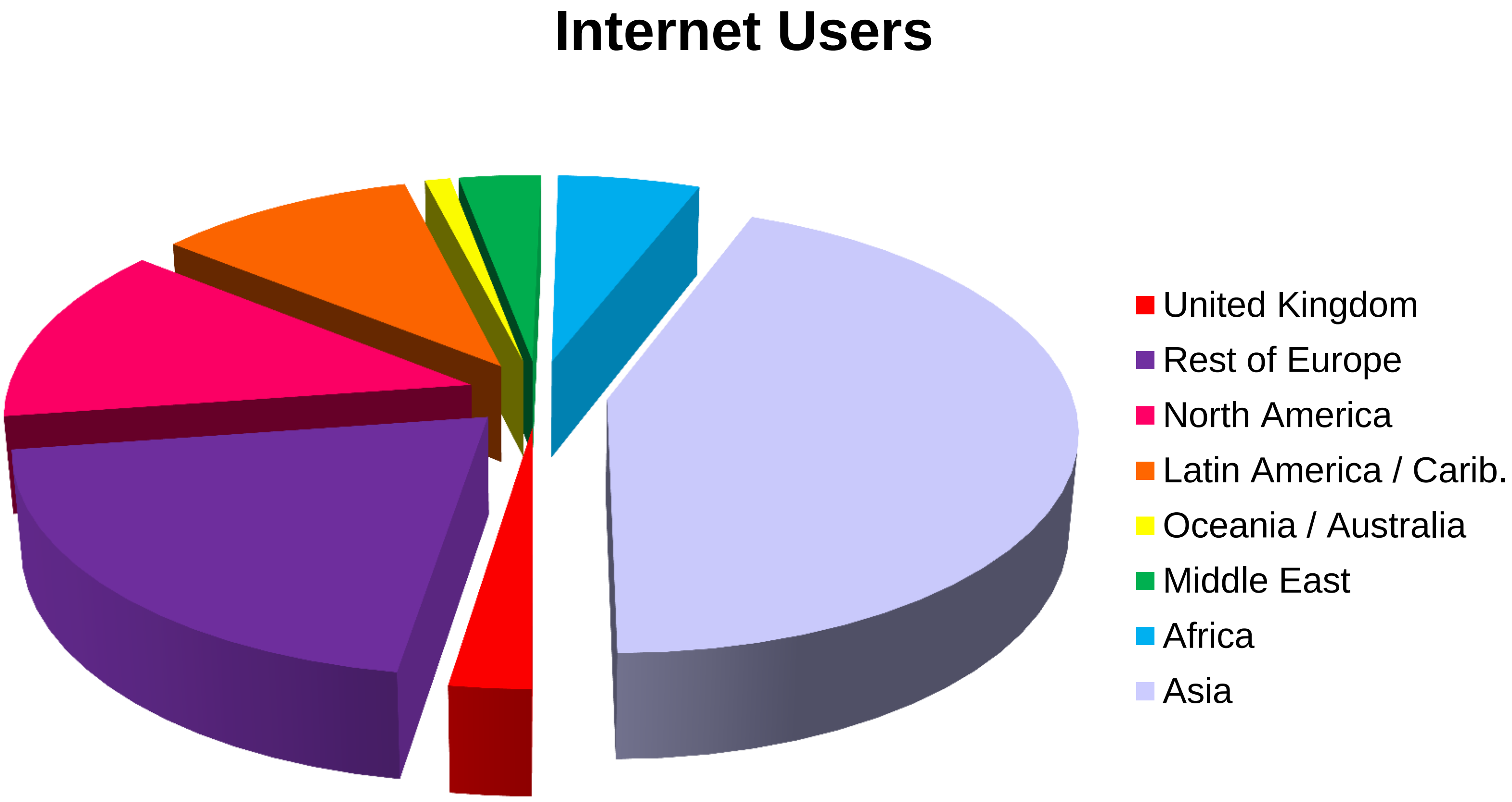
S S D R I : *UK's public-private partnership for Making Software Better*

UK Potential Audiences



Not forgetting that 60m+ Citizens would also benefit from more trustable ICT

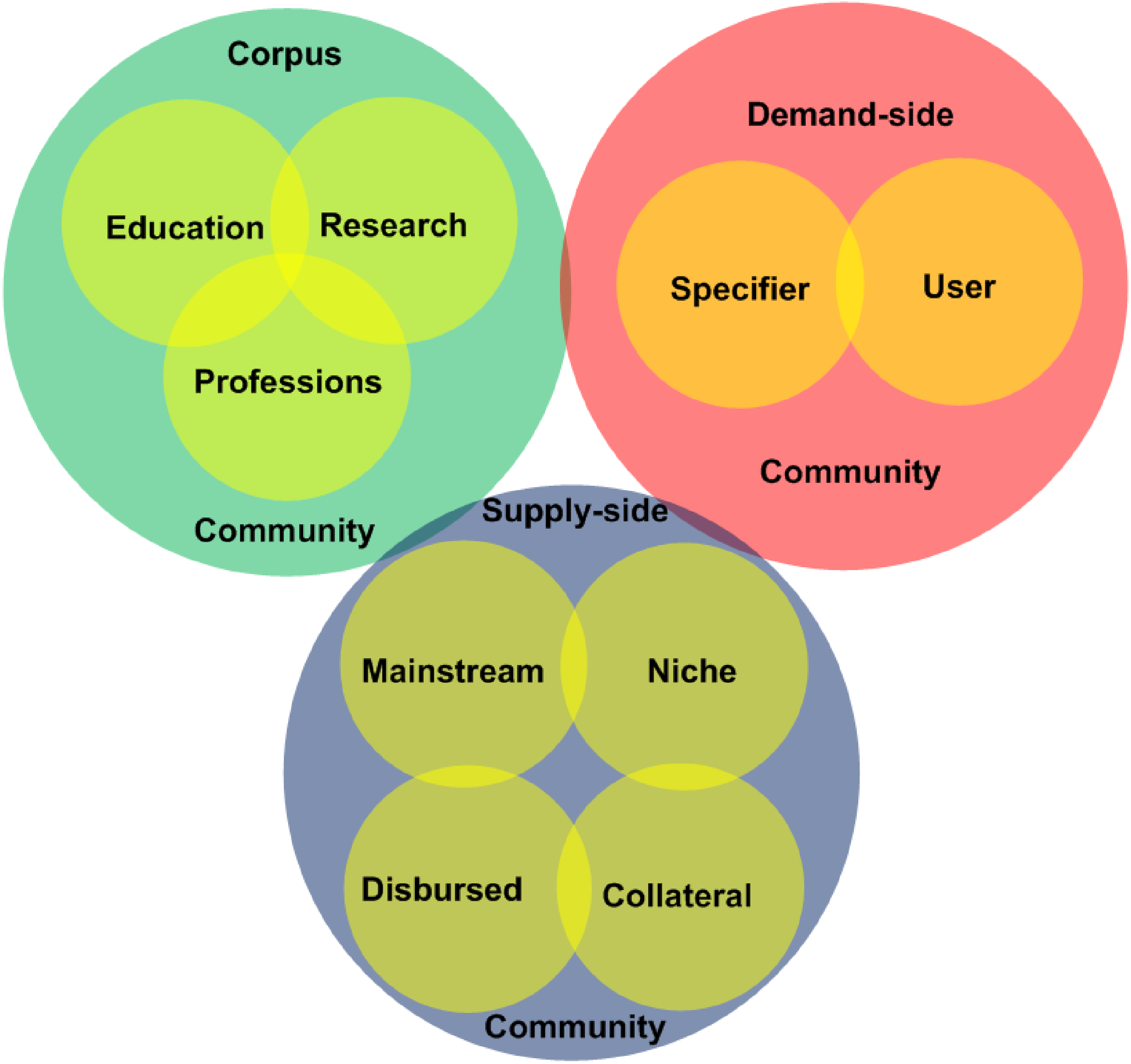
The International Dimension



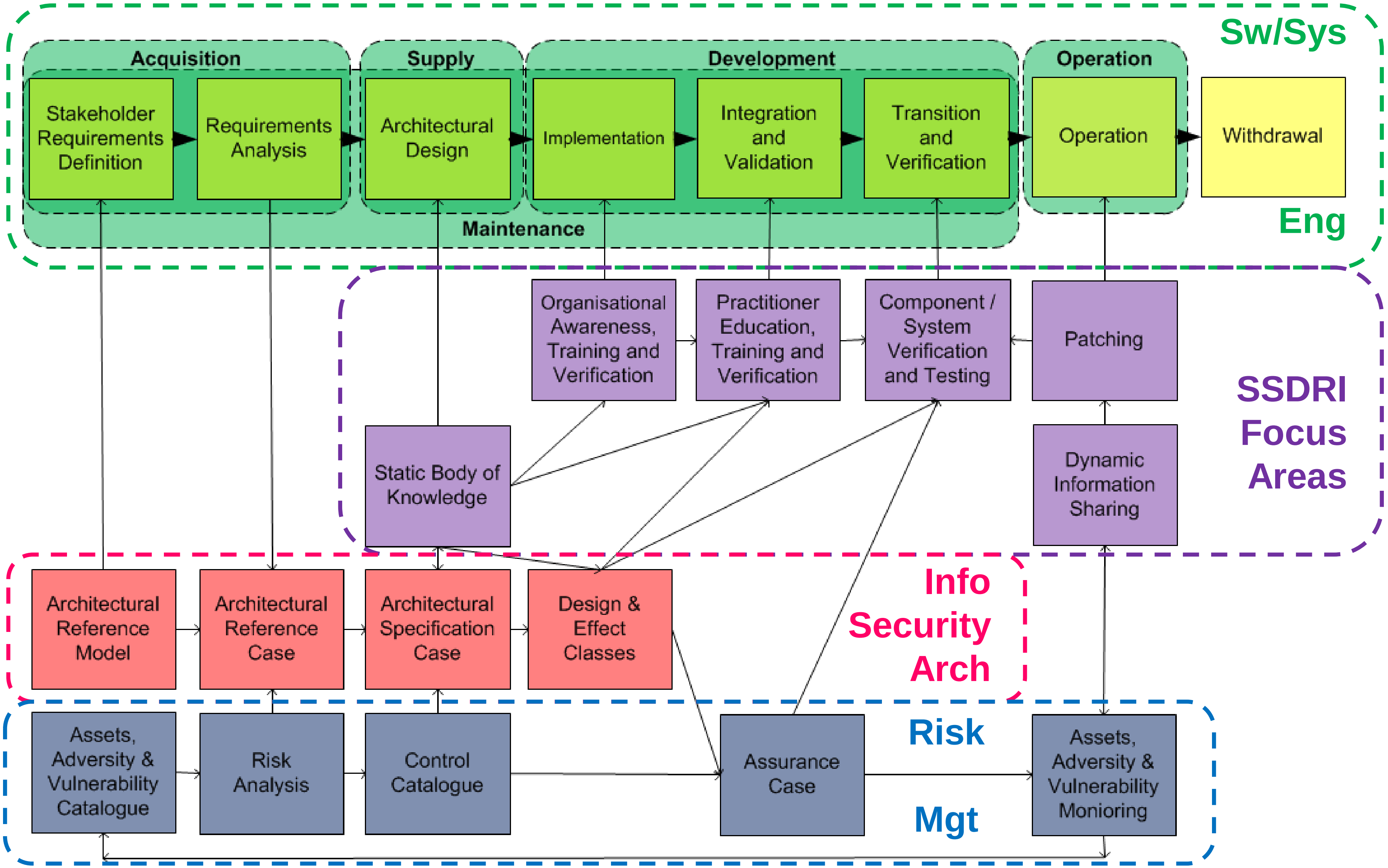
Source: National IA Forum (2010)

S S D R I : *UK's public-private partnership for Making Software Better*

SSDRI Audiences

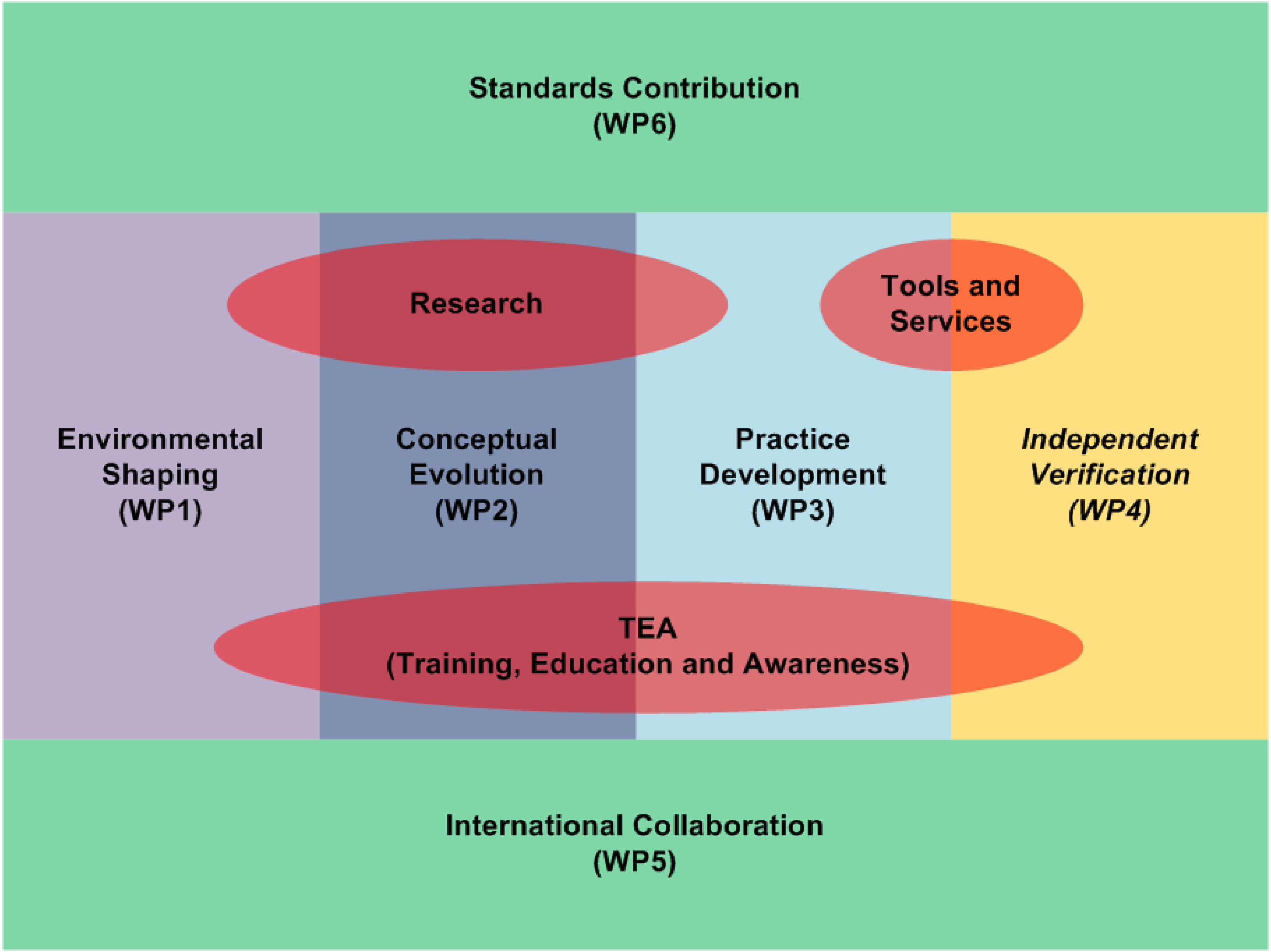


SSDRI Context: Lifecycle and Dependencies


Sw/Sys
Eng
Acquisition
Supply
Development
Operation
Stakeholder Requirements Definition
Requirements Analysis
Architectural Design
Implementation
Integration and Validation
Transition and Verification
Operation
Withdrawal
Maintenance
SSDRI Focus Areas
Organisational Awareness, Training and Verification
Practitioner Education, Training and Verification
Component / System Verification and Testing
Patching
Static Body of Knowledge
Dynamic Information Sharing
Info Security Arch
Architectural Reference Model
Architectural Reference Case
Architectural Specification Case
Design & Effect Classes
Risk
Mgt
Assets, Adversity & Vulnerability Catalogue
Risk Analysis
Control Catalogue
Assurance Case
Assets, Adversity & Vulnerability Moniroing

S S D R I : *UK's public-private partnership for Making Software Better*

SSDRI Work Packages and Effort Clusters



SSDRI Approach

- Many of concepts and practices needed for software Security / Dependability / Resilience have existed in specialist domains for many years
- Challenge is to “bake in” to **all** software, recognising that implementations may vary with Audiences and Functional / Assurance Requirements
- Focus of SSDRI on Pareto (“*80:20*”) approaches to *Making Software Better*, iteratively using learnings from specialists domains and interpreting them for the common good
  - c.f. “Public Health”: Prevention now avoids Treatment later

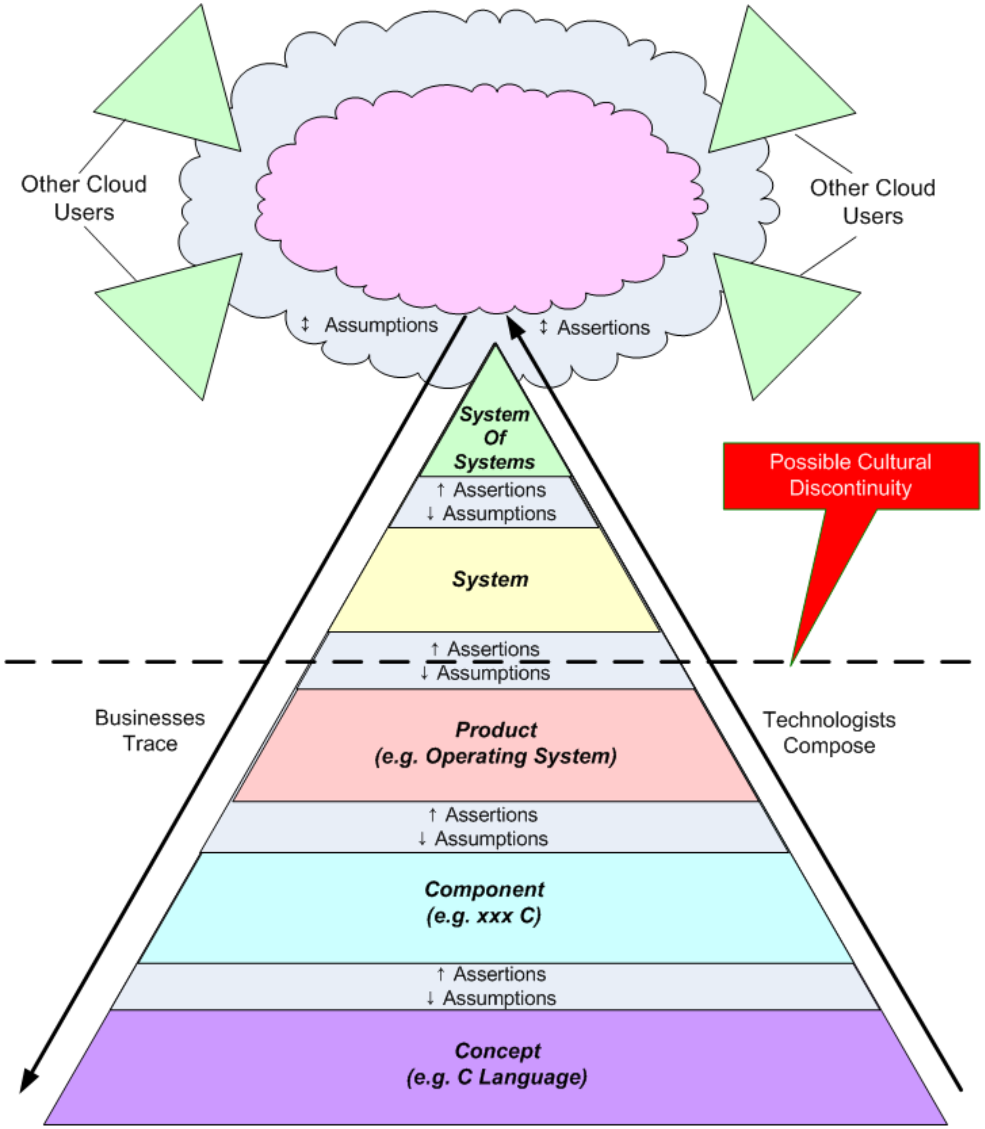
SSDRI WP1: Environmental Shaping
SSDRI WP3: Practice Development

- In “mature” industries (e.g. Aviation Engineering), **all** practitioners intrinsically responsible for producing trustable outputs
- We need SSDR embedded at all levels so it becomes “part of the Culture”:
  - **T**raining of current workforce
  - **E**ducation of future workforce
  - **A**wareness of all producers and consumers

SSDRI WP2: Conceptual Evolution

- Software SDR requires research and innovation in :
  - Situational Awareness – Horizon Scanning
  - Governance (e.g. Metrics, Trusted Information Sharing)
  - Human Factors (e.g. Stakeholder Behaviours)
  - Technical (e.g. New Techhologies and Attacks, Trustable Failure Modes, Compos ability and Traceability, Multicore Technologies)
- A particular challenge is Composability and Traceability

SSDRI: Composability and Traceability Challenge



- Assertions (↑) & Assumptions (↓):
  - Can be Positive (+ve) and/or Negative (-ve)
  - How should this be modelled ?
  - Who should be responsible ?
  - How should this be documented ?
    - Updates to Standards
    - Artefacts need to be in both System and IA terms
- Become Bidirectional Assertions (↕) & Assumptions (↕) for Composed System linking to Cloud
- An area for further study

SSDRI WP4: Independent Verification

- Product and Service Assurance splits (roughly) into 2 segments
  - "Due Diligence" by Independent Black Box testing
  - "High assurance" with preference for Formal Methods
- Also Maturity Model(s) needed for Supply Chain Assurance
- ***This Work Package is currently in abeyance whilst new schemes for Information Security Products and Services evolved by CESG***

SSDRI WP5: International Collaboration

- Software SDR is not a "UK plc" problem
- International Collaboration is therefore an essential element of efforts
  - Multinational involvement was intrinsically part of the precursor "Paris Workshop"
- Initial International Collaboration options
  - International Standardisation through BSI IST/033
  - Bilateral collaboration with US peer organisation, the Software Assurance (SwA)

SSDRI WP6: International Standardisation

- No standardisation of Standards Development Organisations (SDO) !
- Leading UK recognised SDO in SSDR area would be ISO/IEC JTC1, with multiple active projects in SC7 / SC22 / SC27 / SC38
- Some work in ITU-T
- Also need to keep eye on *de facto* standardisation through other bodies, such as Mitre and OWASP

SSDRI and UK Cyber Security Strategy

- 2010 UK National Security Strategy (NSS) gives “Cyber” (attacks and shortcomings) as one of 4 “Tier One” Risks
- Amplified by UK Cyber Security Strategy (UKCSS) in 2011, which include Actions for:
    - Raising awareness of needs for protection, including supply chain dependencies (**UKCSS 1.23; 4.11 ➔ SSDRI WP1**)
    - Anticipating technological, procedural and societal behaviour developments that affect cyberspace, identifying Centres of Excellence in research **(UKCSS 4.1; 4.10 ➔ SSDRI WP2)**
    - ➢ **Improving education at all levels, including higher and postgraduate level** (**UKCSS 4.3 ➔ SSDRI WP3**)
    - Working closely with the European Commission to encourage greater coherence within the EU on cyber issues (**UKCSS 3.10 ➔ SSDRI WP5**)
    - Stimulating the development of international, regional and national standards that are readily used and understood (**UKCSS 1.13; 1.24; 3.6 ➔ SSDRI WP6**)

Any Questions ?

Contact Details

Ian Bryant

Technical Director S S D R I

SSDRI Office
Gateway House pp4.30
De Montfort University - Cyber Security Centre
The Gateway, Leicester, LE1 9BH, England

ian.bryant@ssdri.org.uk   secretariat@ssdri.org.uk

+44 79 7312 1924   +44 33 0001 0479

www.ssdri.org.uk

(Twitter: @ssdriuk)