

11th ICCRTS

Coalition Command and Control in the Networked Era

The Use of Information Principles for Engineering NEC

Analysis, Coalition Interoperability, Policy

Dr Ann Fitchett, Mr D McConnell, Mr Stuart Sowray

Integration Authority (UK MoD)
MoD Abbey Wood (#2308),
Bristol, UK. BS34 8JH
Tel +44 (0)11791 34166
ia2c@dpa.mod.uk

THE INTEGRATION AUTHORITY:

improving the DEFINITION and DELIVERY of Integrated Military Capability



NEC Themes

Effects Synchronization

Achieving the desired effects through the synchronization of activities within and between mission groups.

Agile Mission Grouping

Enabling the dynamic creation and configuration of task orientated mission groups that share understanding and that employ and co-ordinate available assets to deliver the desired effect.

Dynamic Collaborative Interworking

Enabling agile command and control within and between mission groups through the ability to concurrently plan and execute operations in a way that is dynamic, continuous and synchronized.

Shared Understanding

Enabling each user to generate an understanding of the battlespace that is appropriate and adequate to their task and consistent with the understanding of other users.

Full Information Accessibility

Enabling users to search, manipulate and exchange relevant information of different classifications (respecting security constraints) captured by, or available in, sources internal and external to the battlespace.

Resilient Information Infrastructure

Ensuring information is managed coherently across the battlespace and that the potential for secure and assured connectivity is provided to all battlespace users.

Inclusive Flexible Acquisition

Co-ordinating processes across MOD, OGDs and industry that promote the rapid insertion of new technologies, facilitates coherence between acquisition programmes and provides an incremental approach to delivering and maintaining 'net-ready platforms'.

- **Changing Nature of Threat**
 - Growth of Urban environment
 - Cultural and Psychological dimension

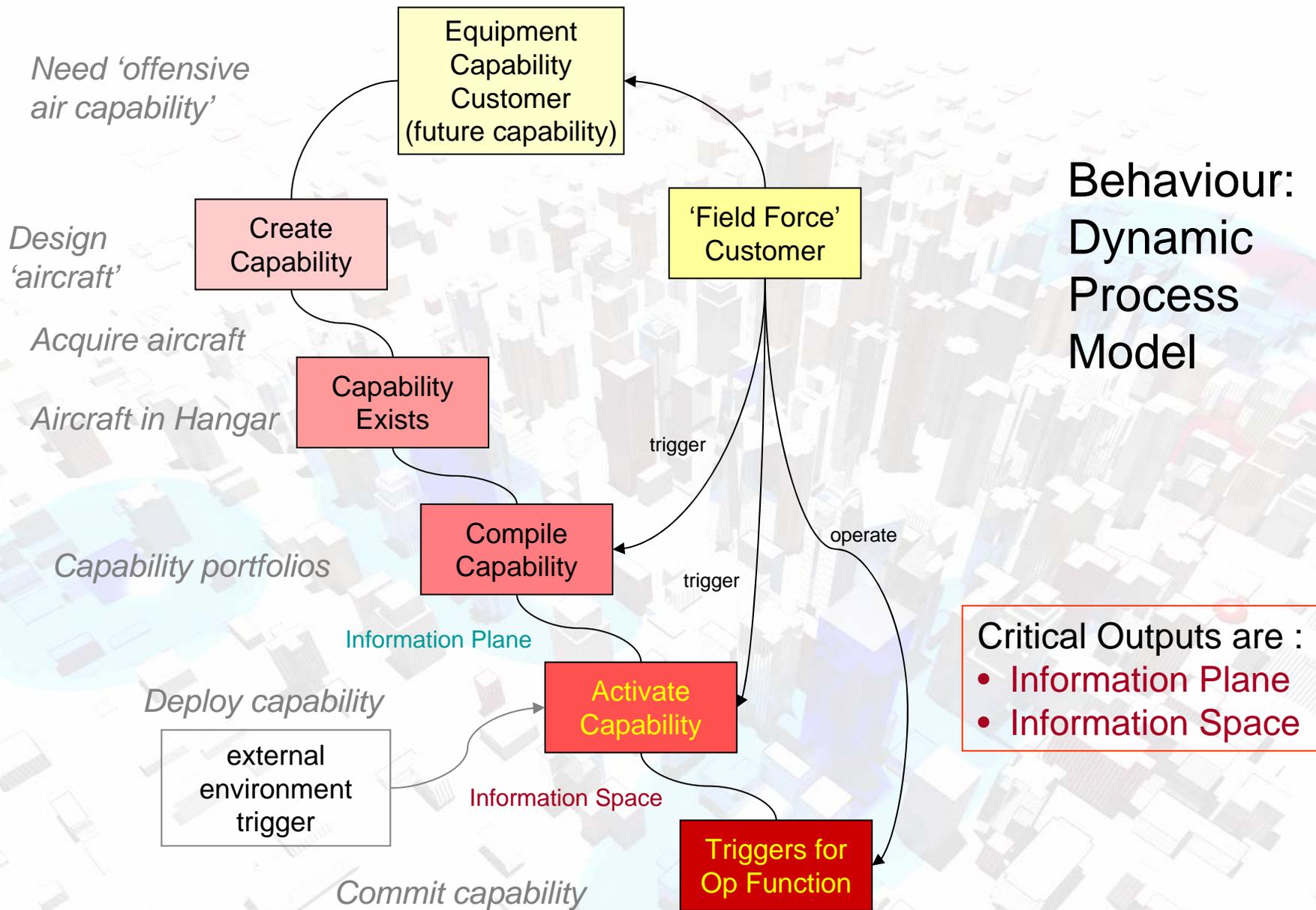
- **New Threats**
 - Asymmetric
 - Information Age

... the world's urban areas are increasing in size; by 2025 nearly 60 percent of the world's population will live in urban areas. Given this growth, it is prudent to assume ... forces will continue to be deployed to urban areas for combat and post-conflict stabilization operations for the foreseeable future.

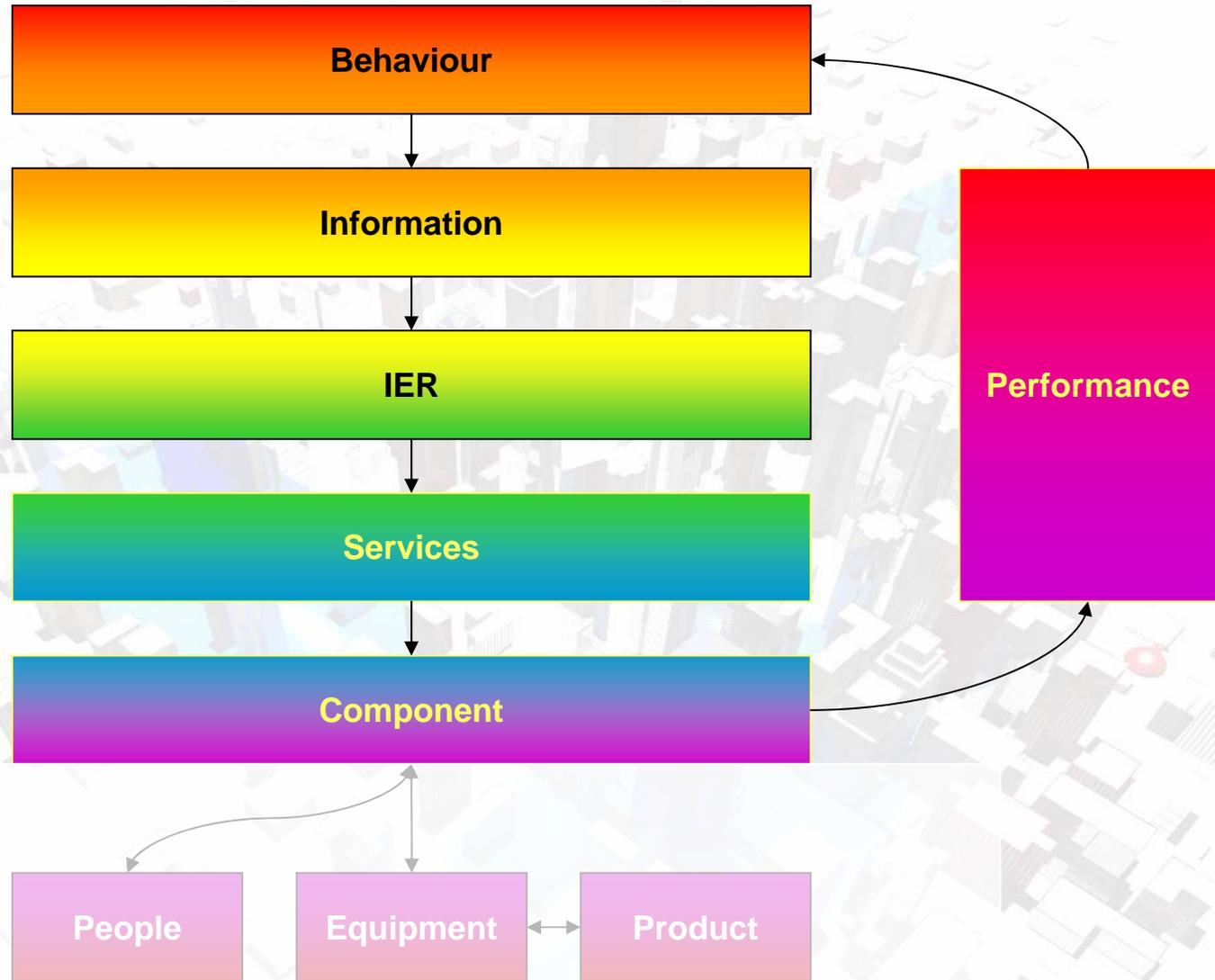
- **Enduring Characteristics**
 - Social
 - Organisation

- Command and control
 - Importance of ‘Social Dimension’
 - Cultural Inertia
 - Evolutionary rather than Revolutionary
- Security
 - Subjective
 - Transient
- Technology and Standards
- Legacy Capability

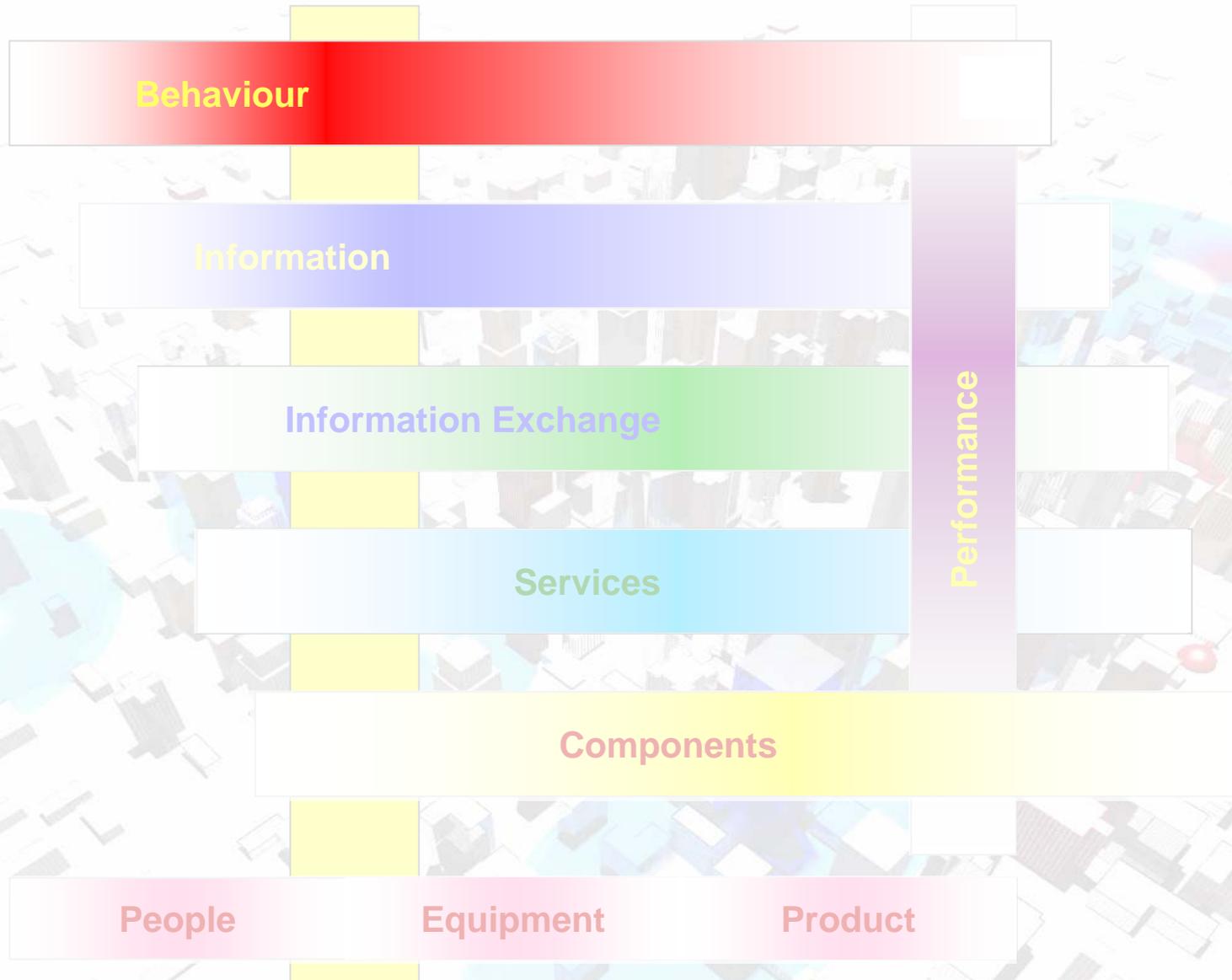
Capability Development – Design Process



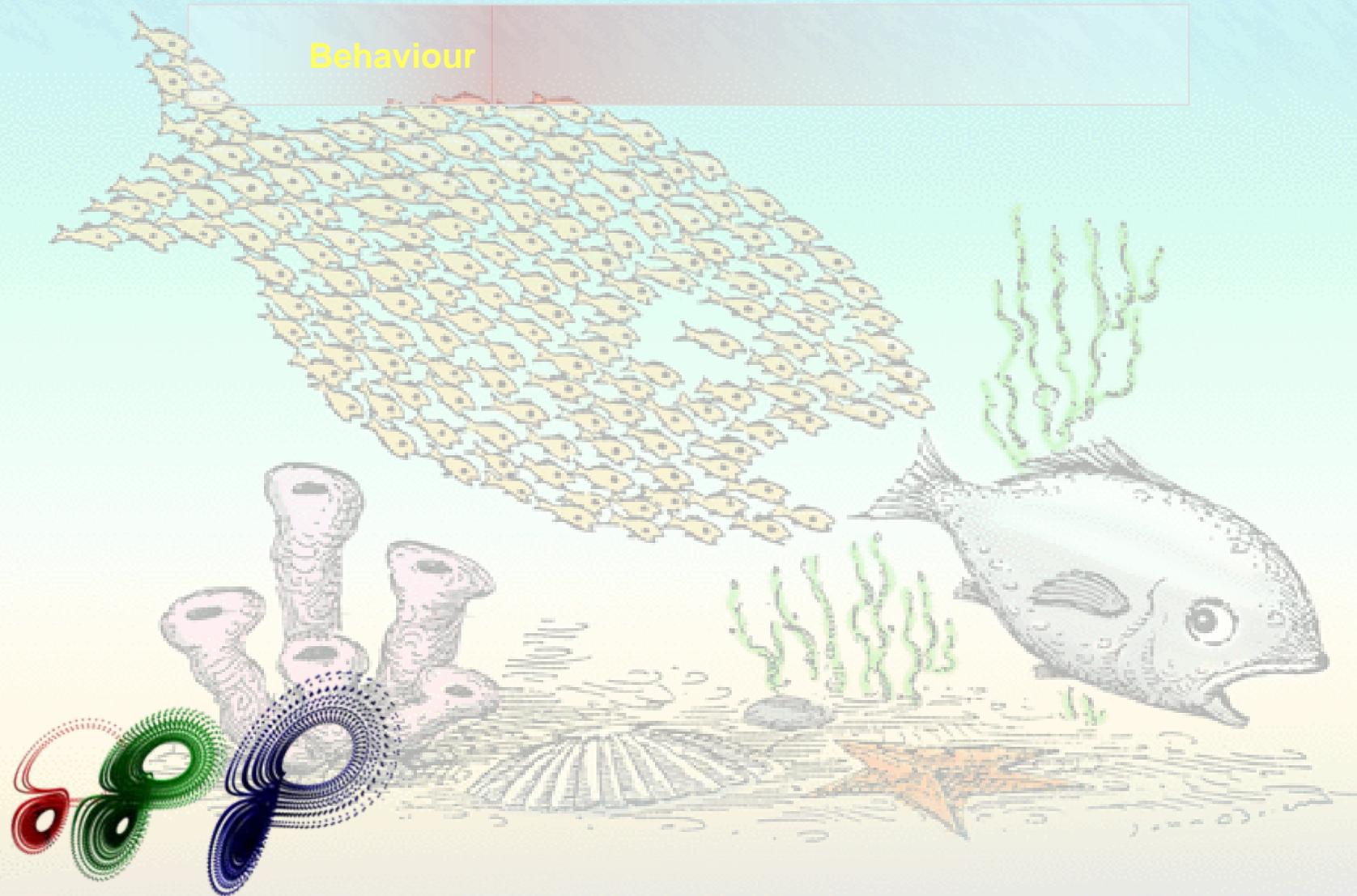
Design Framework



Design Framework - Behaviour

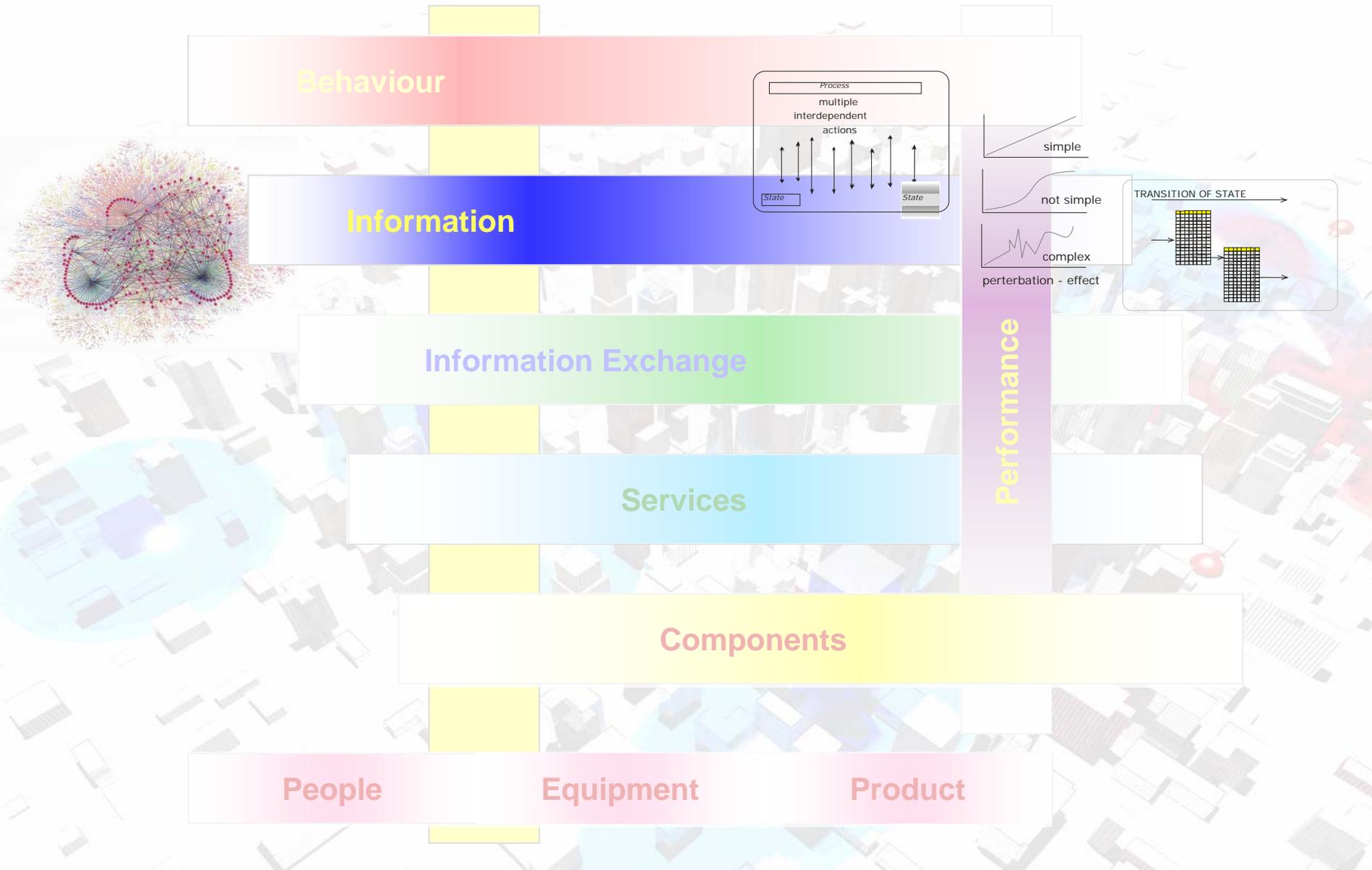


Behaviour Layer



Behaviour

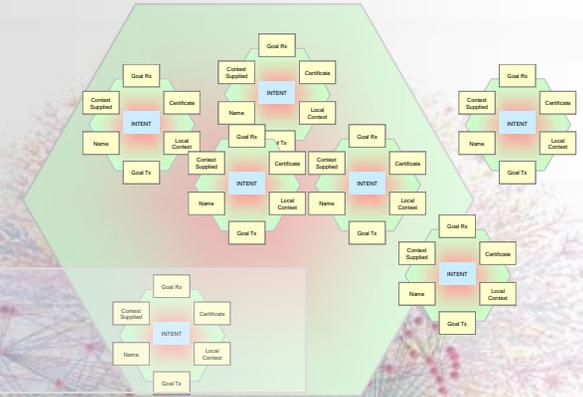
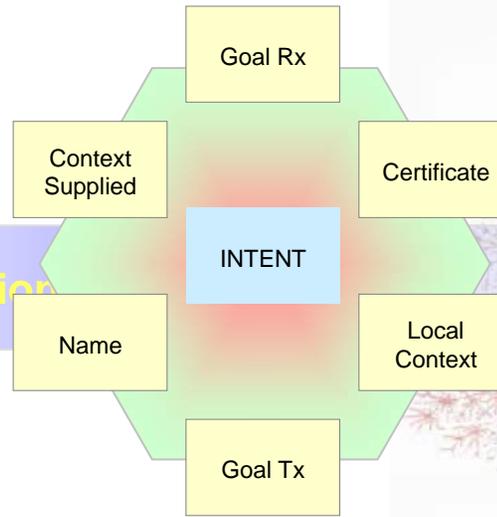
Design Framework - Information



Information Layer

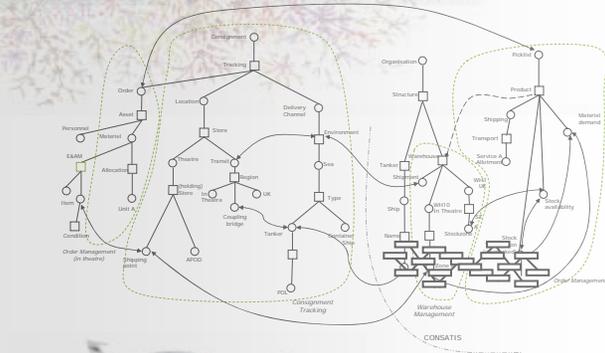
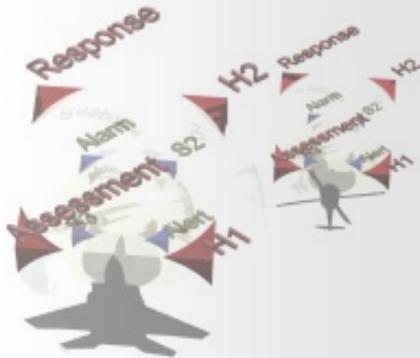


Information



Schema Elements

- Goal Received
- Context Supplied
- Goal Transmitted
- Local Context
- Name
- Certificate
- Intent



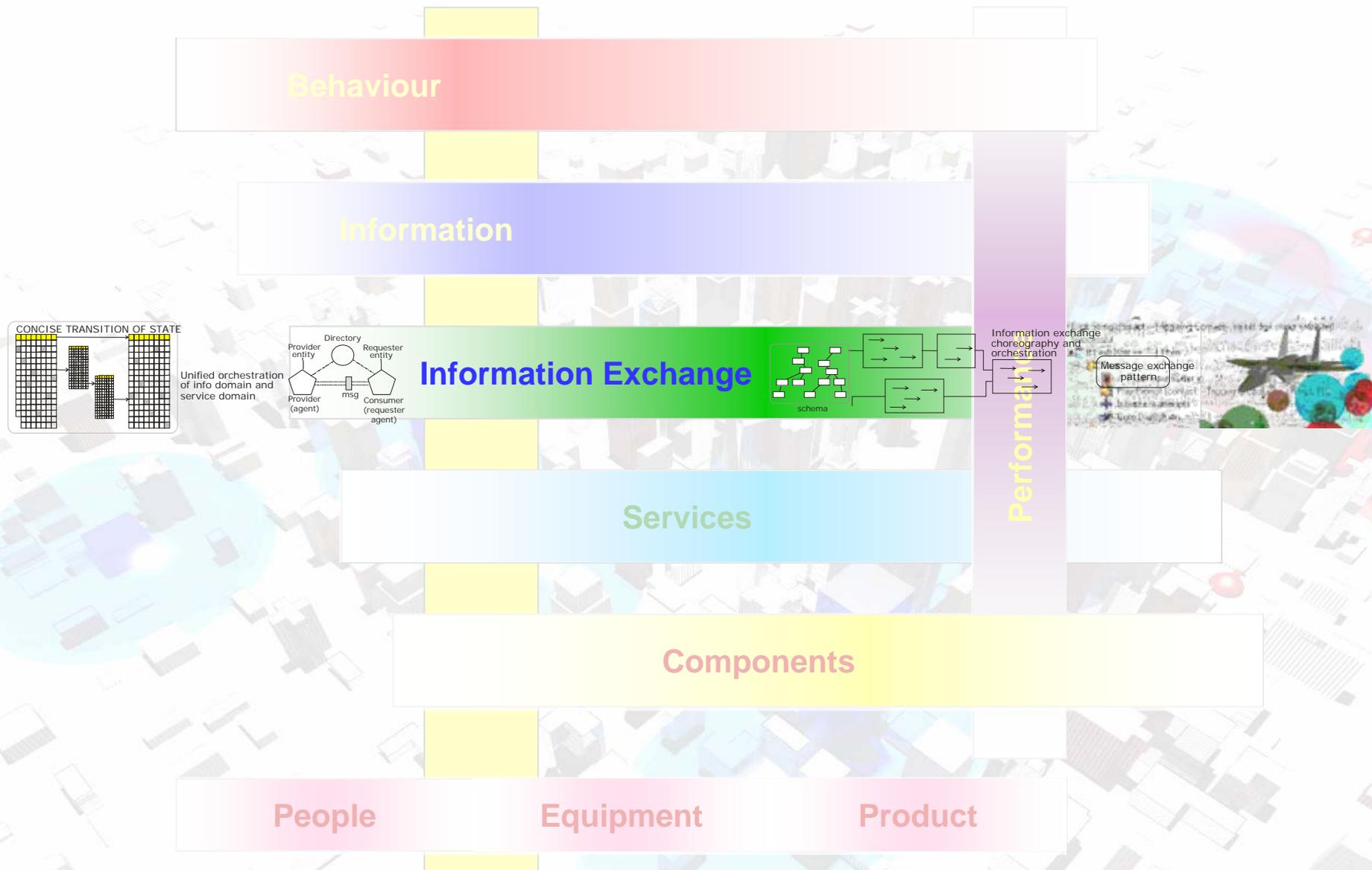
Design Framework - Information

Behaviour

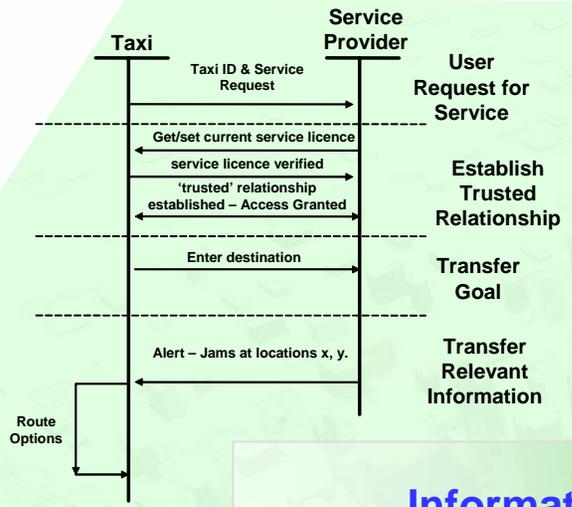
Information Information Principles

Ser	Principle	Elaboration
1	A stimulus shall have an ID and affective value set by the intent	
2	An alert is based on an affective value and is set in a CONTEXT	
3	A local CONTEXT can be generated by an entity. •Only an entity able to act as a CONTEXT ID Auth can generate a 'local' CONTEXT •The extent of the local context is defined by the entities identified	
4	The CONTEXT ID authority is responsible for: •generating an alarm in its own context •Managing the context	
5	Trust must be verified and GOAL must be validated at the global level •Establishment of trust at the local level, verification at the global level •ID auth must have mechanism for authentication before trust can be established •To have a goal there must be a command relationship (with the association-authentication) of this relationship	
6	Trust component in a relationship is the basis for authentication	
7	An ENTITY is given its 'goal' from a command entity. The goal is received from a trusted entity within its local context	
8	A GOAL sets domain to develop the global CONTEXT and resolves conflict (behaviour) for an ENTITY. Successful completion of a goal represents knowledge that can be applied to specific domains.	
9	The CONTEXT ID authority will interpret specific data ('facts') to represent an entity and relationships among entities. It will be able to infer, from specific data, changes needed to assignments, eg including identity of entities referred to in the CONTEXT.	
10	An ENTITY will be assessed in CONTEXT. CONTEXT may be nested to discover non-stereotypical activities.	
11	The CONTEXT ID authority will represent a concept that is consistent with current domain knowledge about the ENTITY, but does not exclude features that appear irrelevant until the concept is proven.	

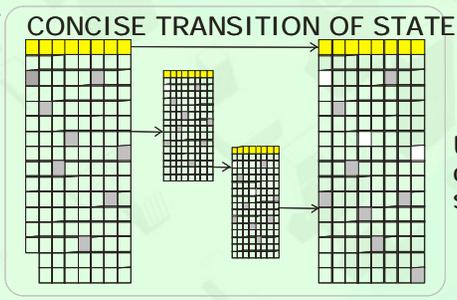
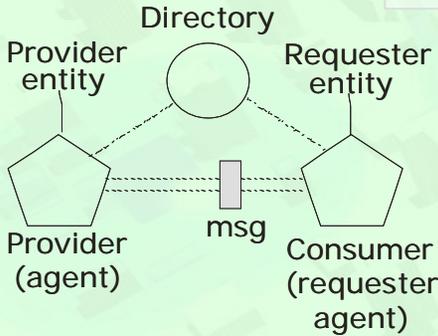
Design Framework – Information Exchange



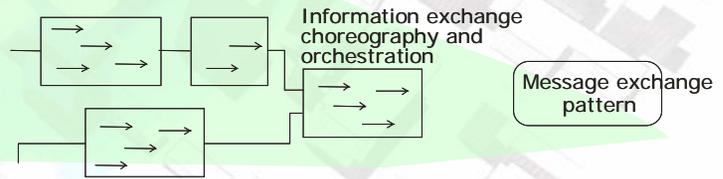
Design Framework – Information Exchange



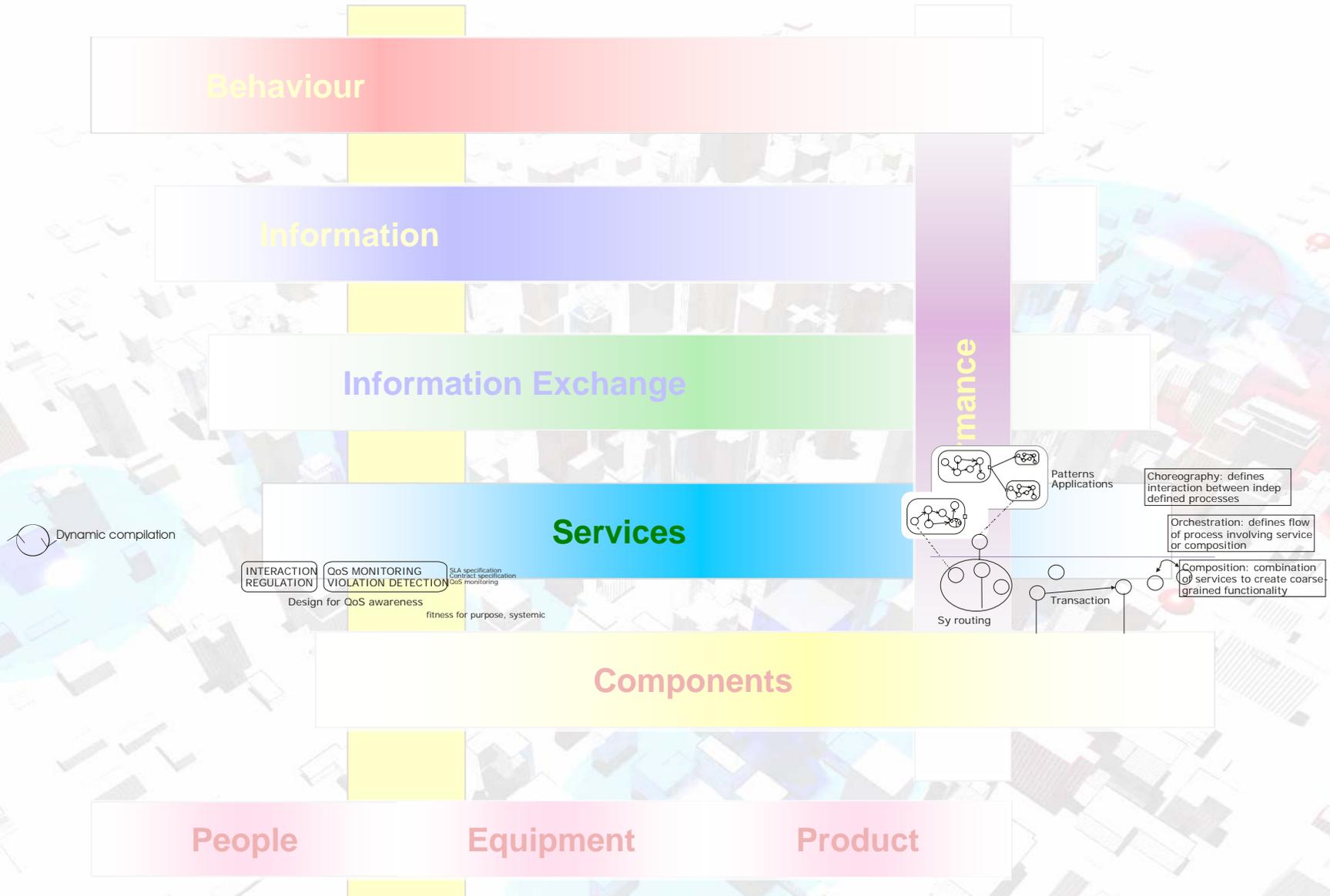
Information Exchange



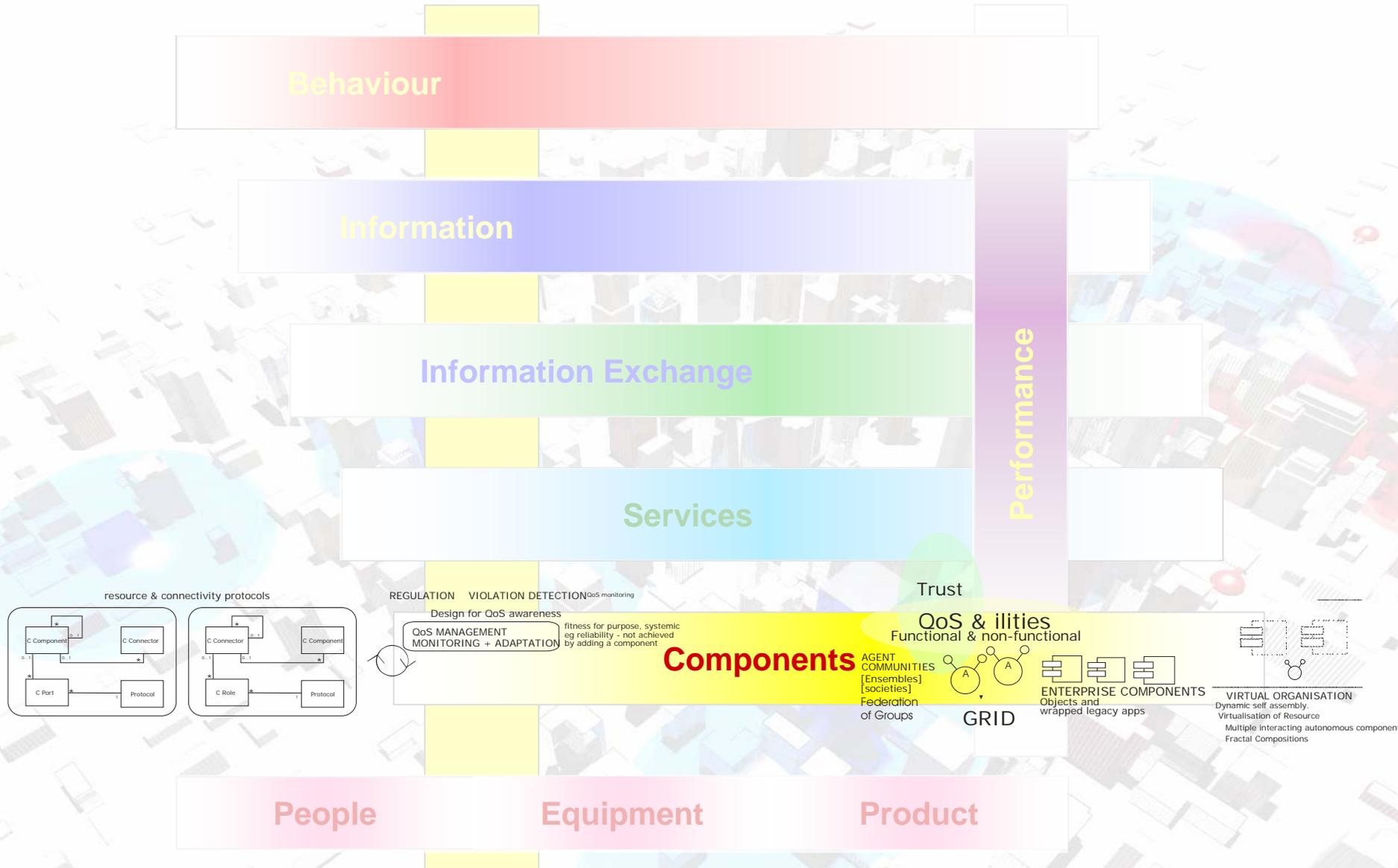
Unified orchestration of info domain and service domain



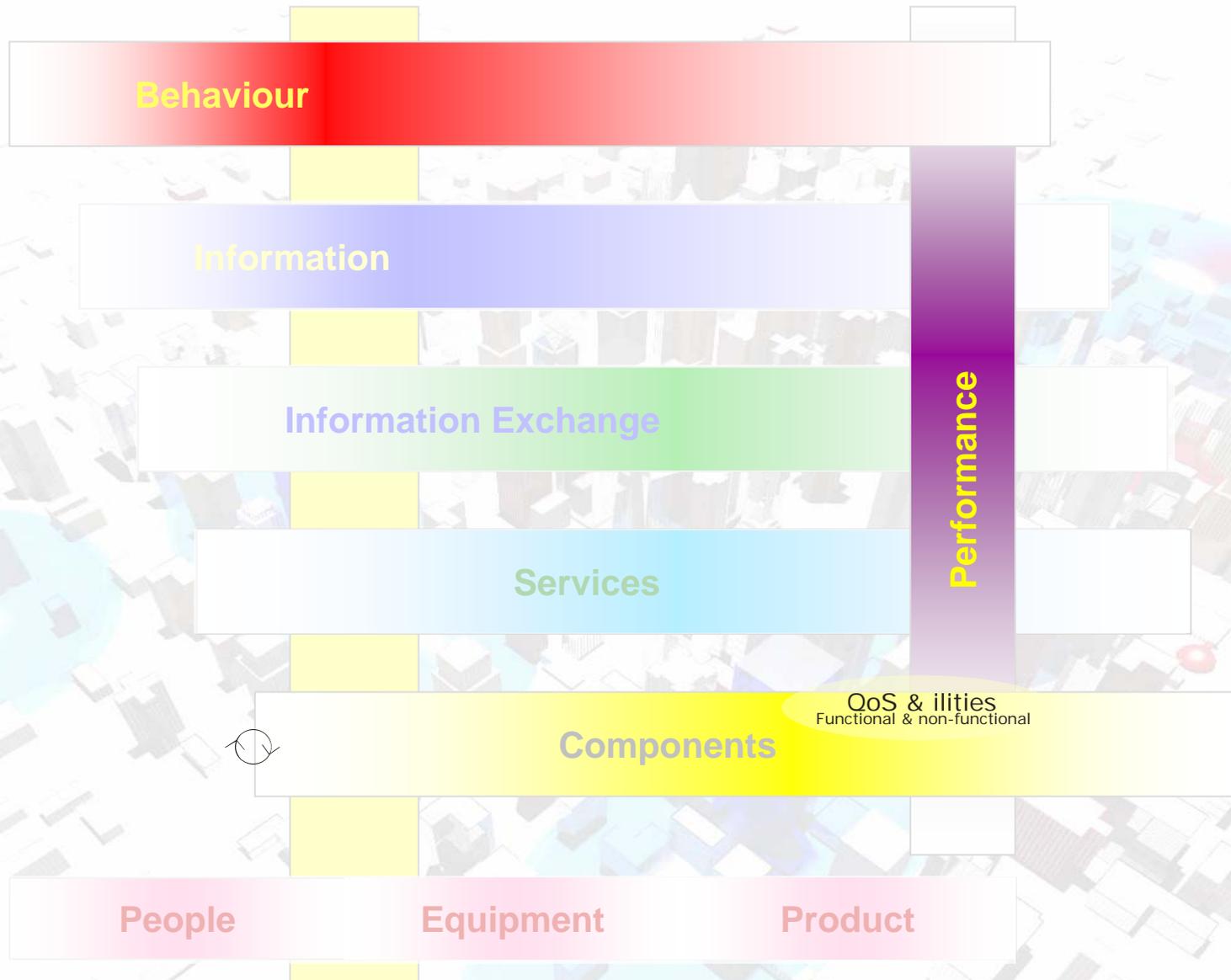
Design Framework - Services



Design Framework - Components



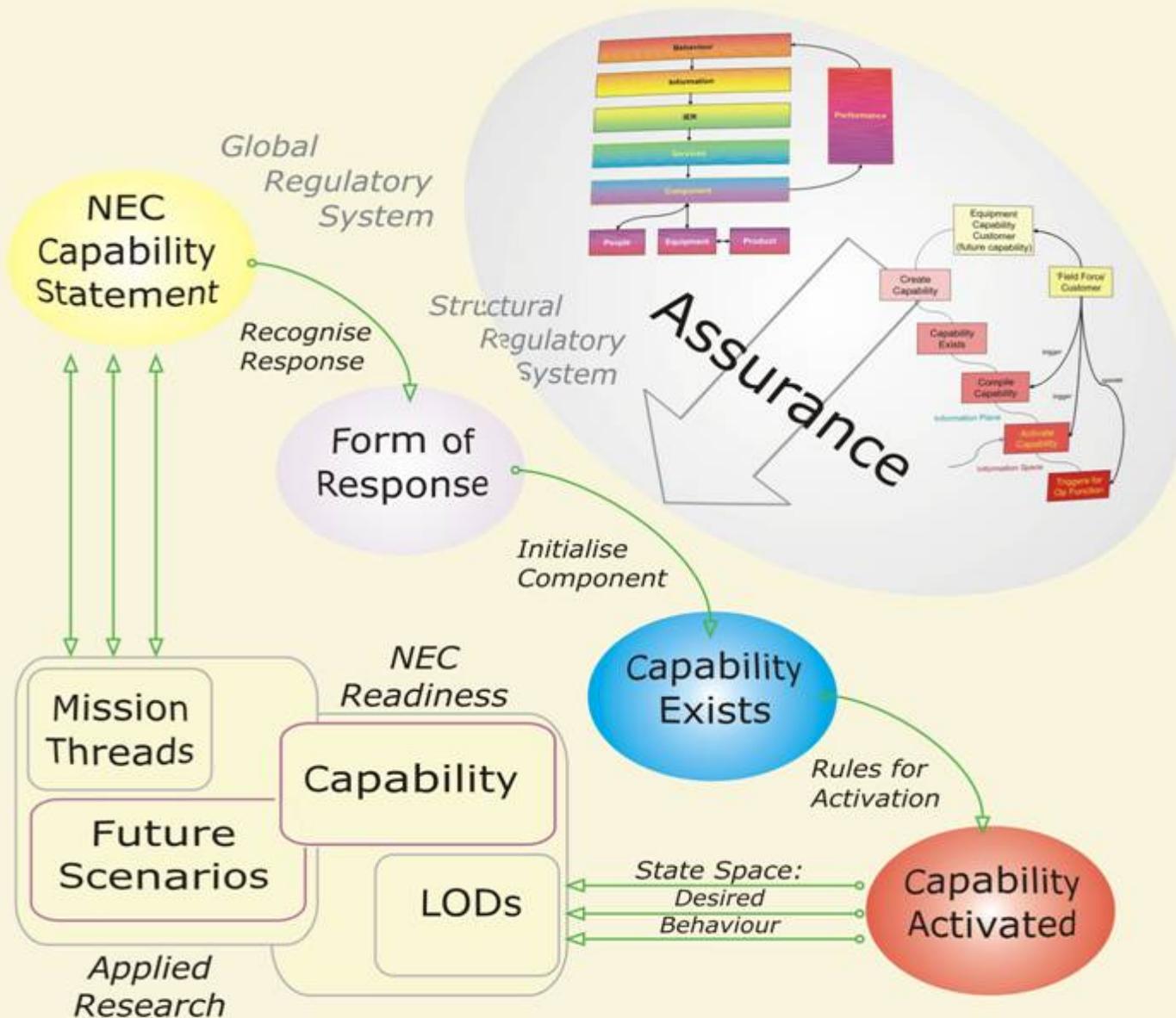
Design Framework - Performance



CONCLUSIONS

- Designing for Performance and behaviour
- Information Design
- Enabling Decision Superiority
- Effects-Based Decision Making
- NEC Entry Criteria
- Dynamically Reconfigurable Information Building Blocks
- Assured Delivery of Required Behaviour

Assurance – IA Core Business



Engineering for Performance and Behaviour in the NEC Era



Key integration requirements for NEC readiness, assured performance and behaviour in the NEC era

System Characteristics

Process
NEC enabled command and control (C2) is about assurance that planning organisational behaviour explicitly meets the demands of shared situation awareness and agile mission groups. A successful decision support planning process is characterised by the ability to generate options for the commanders' intent.

Information
Information to describe the commanders' intent must be represented within context that is maintained by the system of interest (SOI). The SOI must be scalable to reflect organisational needs for agility.

Technical
NEC enabled C2 is the driver for tailored technologies that will provide the service oriented overlay to enable the organisation to operate effectively in its environment. Process and information coherence assurance is maintained by the design framework, which supports the definition of enduring *capability building blocks* as a generic functional baseline.

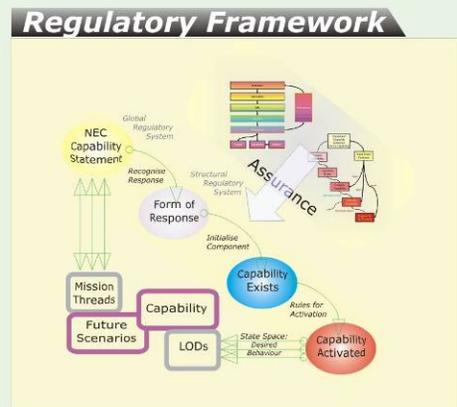
- ### Characteristics
- UK NEC Reference Architecture is a global concept that finds local expression in the Lines of Development
 - Assurance of effective performance will be facilitated by the use of generic components and generic state descriptors.
 - Structural components for best-performance systems must be able to provide differential which can be recognised and exploited by a global regulatory system.
 - Evolution towards NEC-enabled capability will follow a component (functional) model that is inclusive, non-prescriptive and maps to current practice.

System Properties

Integration Authority Role
The UK NEC Reference Architecture will provide rules and guidance throughout the programme life-cycle, against which the Integration Authority (IA) assurance role can be undertaken. Assurance provides validation of what is appropriate in development of NEC enabled capability, rather than what the design will support. The authority will conduct reviews and assessments at approval gates to ensure integration consistency and coherence across LODs.

Design Framework
The Design Framework provides a simplified description of a complex design process that underpins the UK NEC Reference Architecture. Its purpose is to generate the control mechanism that will assure desired organisation behaviour that realises NEC capability. The control mechanism is encapsulated in the regulatory system.

Capability Development
The capability development process produces an information Architecture as the baseline to generate the commanders' system of interest. The process is iterative and seeks to increase the commander's awareness of ground truth.



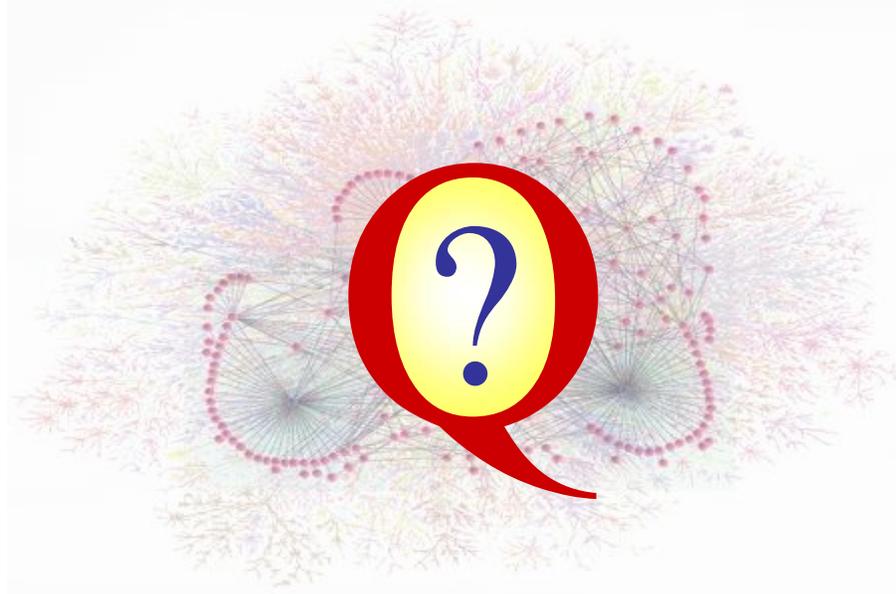
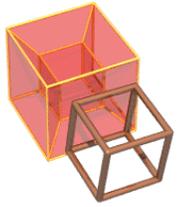
IA Sponsorship

Coherent NEC capability
Capability statements are generated that provide a high level explanation of the 'real picture for NEC' offered by the UK NEC reference Architecture characteristics and properties. Capability statements are mapped into capability requirements that will form the response to be provided by a type of system. The systemic approach promotes confidence as known boundaries are set, but can cater for new problems.

Integration Programme
The global regulatory system and NEC-enabled C2 structural regulatory components are managed as an integrated capability portfolio across the lines of development.

- ### Delivering
- NEC Epoch 2 is about integration across the LODs and has process emphasis.
 - The IA assurance function will provide the NEC context and sponsor the regulatory systems across the LODs.
 - The IA Authority will support adaptive gateway reviews of programmes. This recognises that programmes are unique and will change over the programme's life.



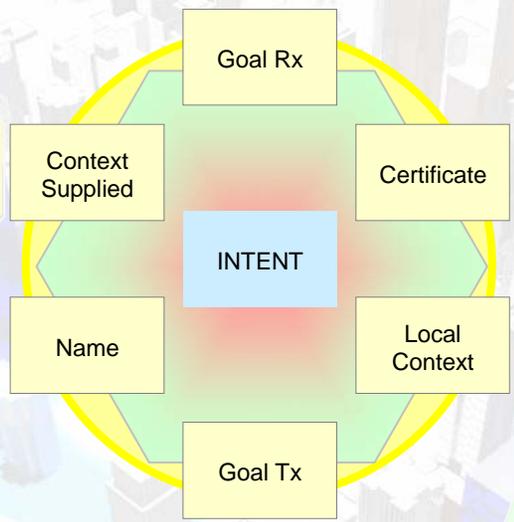
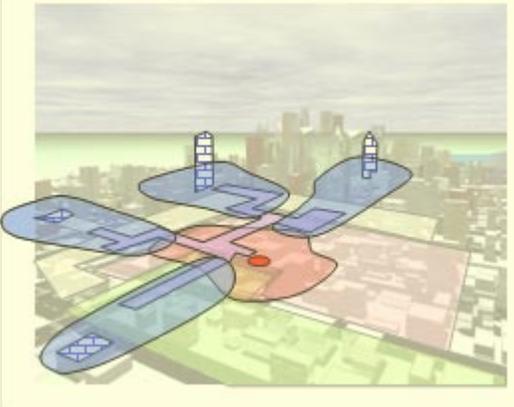
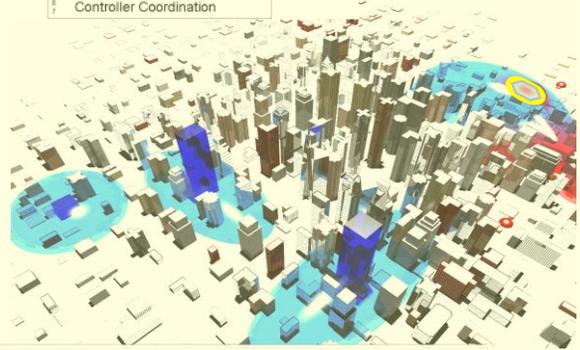
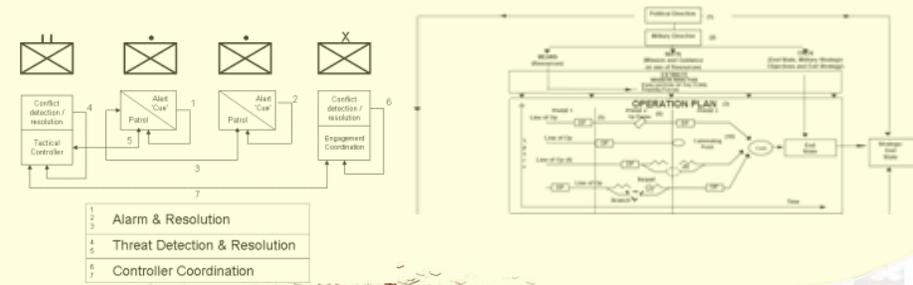


THE INTEGRATION AUTHORITY:

improving the DEFINITION and DELIVERY of Integrated Military Capability



Local and Global Context



Level 0 – Principles

Information Principles

Ser	Principle	Elaboration
1	A stimulus shall have an ID and affective value set by the intent	
2	An alert is based on an affective value and is set in a CONTEXT	
3	A local CONTEXT can be generated by an entity. <ul style="list-style-type: none">•Only an entity able to act as a CONTEXT ID Auth can generate a 'local' CONTEXT•The extent of the local context is defined by the entities identified	
4	The CONTEXT ID authority is responsible for: <ul style="list-style-type: none">•generating an alarm in its own context•Managing the context	
5	Trust must be verified and GOAL must be validated at the global level <ul style="list-style-type: none">•Establishment of trust at the local level, verification at the global level•ID auth must have mechanism for authentication before trust can be established•To have a goal there must be a command relationship (with the association-authentication) of this relationship	
6	Trust component in a relationship is the basis for authentication	
7	An ENTITY is given its 'goal' from a command entity. The goal is received from a trusted entity within its local context	
8	A GOAL sets domain to develop the global CONTEXT and resolves conflict (behaviour) for an ENTITY. Successful completion of a goal represents knowledge that can be applied to specific domains.	
9	The CONTEXT ID authority will interpret specific data ('facts') to represent an entity and relationships among entities. It will be able to infer, from specific data, changes needed to assignments, eg including identity of entities referred to in the CONTEXT.	
10	An ENTITY will be assessed in CONTEXT. CONTEXT may be nested to discover non-stereotypical activities.	
11	The CONTEXT ID authority will represent a concept that is consistent with current domain knowledge about the ENTITY, but does not exclude features that appear irrelevant until the concept is proven.	

Level 0 – Design Principles

Level 0 Design Principles

Ser	Principle	Elaboration
1	A stimulus will have a unique ID which can be used as a label in the system of interest the extended system	
2	All unique IDs shall comply with the corporate naming system.	
3	Syntax and Semantics must be global and not domain specific eg Sol	
4	There must be a method of maintaining specific focus at the Sol level, which must be consistent with Shared SA	
5	Establishment of 'trusted for goal' exchange must be global. GOAL shall form part of the extended system.	
6	Authentication of the command-trust relationship is global and pre-agreed	
7	A command-trust relationship for a goal must form part of Shared SA	
8	A goal must be consistent with a coherent global strategy / COA	
9	Local autonomy of action must be consistent with the goal	
10	Predicted behaviour must be recognised (ie feature in predicted data set)	
11	Datasets must be used to recognise salient features of entity behaviour.	

