



**Poseidon House
Castle Park
Cambridge CB3 0RD
United Kingdom**

TELEPHONE:
INTERNATIONAL:
FAX:
E-MAIL:

**Cambridge (0223) 323010
+44 223 323010
+44 223 359779
apm@ansa.co.uk**

ANSA Phase III

Engineering model for dependability (Nov 93 TC presentation)

List of author names goes here

Abstract

Need some instructions here.

APM.1087.00.02

Draft

11 February 1994

Request for Comments (confidential to ANSA consortium for 2 years)

Distribution:

Supersedes:

Superseded by:

The sponsors of the ANSA Workprogramme have agreed to allow access by companies which have signed an agreement with Bellcore in respect of the Workprogramme of telecommunications research currently known as TINA-C to permit said companies access to and use of certain documents, software, information and deliverables arising from the results of the ANSA Workprogramme. This information will be made available by the ANSA sponsors either as paper copies or through the medium of electronic file transfer from the information storage system operated by Architecture Projects Management Limited on behalf of the ANSA sponsors.

This is one such document and access is allowed in strict confidence on the understanding that the user accepts these conditions and on the sole basis that it will be restricted to those persons involved in the DPE work package of the TINA-C Workprogramme and that it will not be disclosed to any other person, firm or corporation.

The use of this information is restricted to its use only for the purposes of the carrying out of the DPE workpackage of the TINA-C Workprogramme and only at the site provided by Bellcore for that Workprogramme. No licence or permission for its use in any other part of the TINA-C Workprogramme or for its subsequent exploitation is granted and the ownership and copyright of all such documents, software, information and deliverables is expressly retained by Architecture Projects Management Limited for and on behalf of the sponsors for the time being of the ANSA Workprogramme. In the event of a company leaving the TINA-C Workprogramme or resigning from its bilateral agreement with Bellcore, then that company shall promptly and without demand return to Architecture Projects Management Limited all copies of any information, documents, software or other IPRs obtained under these provisions.

The access granted by these provisions is on the understanding that the TINA-C consortium and the sponsors for the time being of the ANSA Workprogramme intend to and shall promptly enter into a suitable formal agreement for access to information and interavailability of IPRs (including software) for the purposes of the carrying out of the ANSA and TINA-C Workprogrammes.

With regard to any company which is participating in the TINA-C Workprogramme and which is also a sponsor of the ANSA Workprogramme, the obligation of confidentiality and the use restrictions contained in these provisions shall be subject and without prejudice to the obligations undertaken by, and the rights granted to, such company under the ANSA sponsorship agreement.



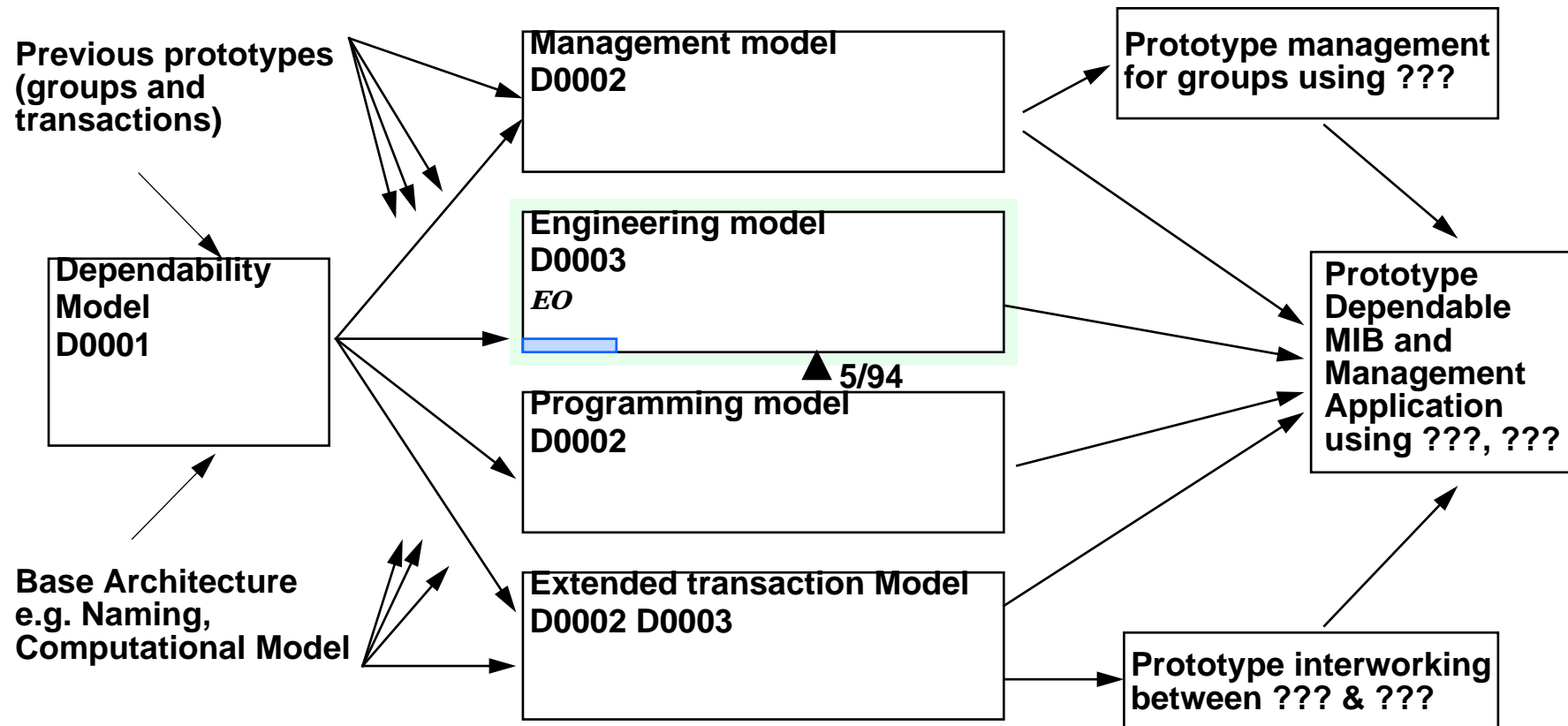
Engineering Model for Dependability

Work in progress

Ed Oskiewicz

Dependability Group

Dependability outline plan

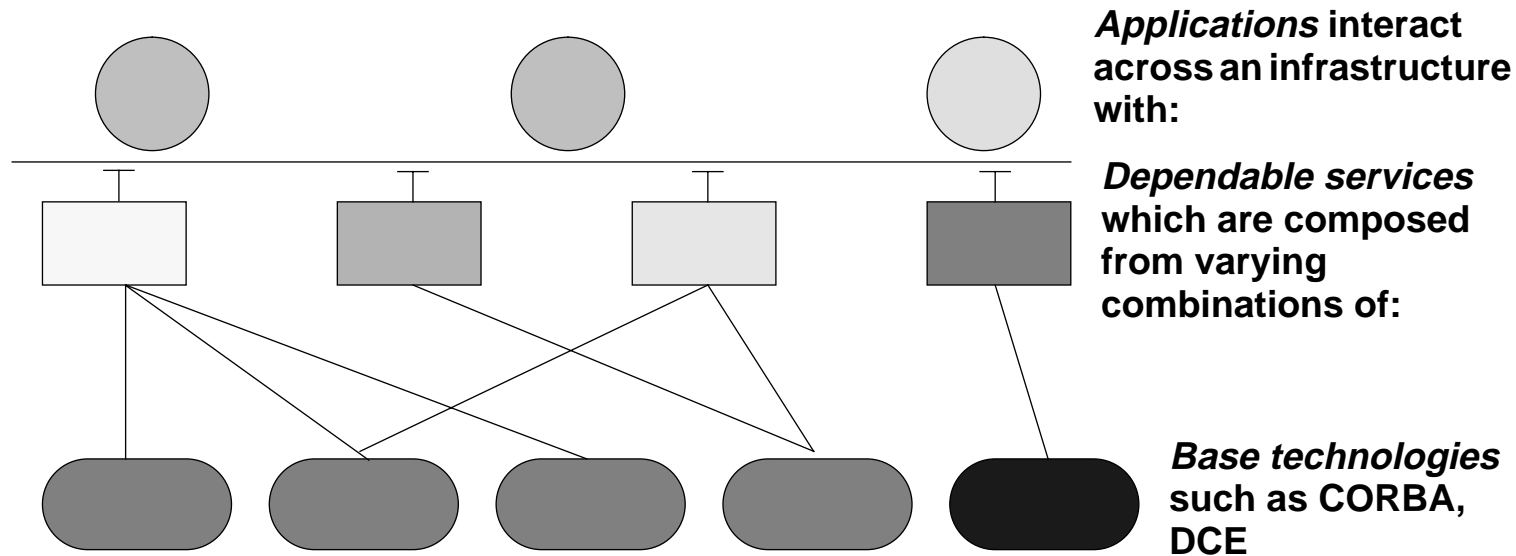




Objectives of this talk

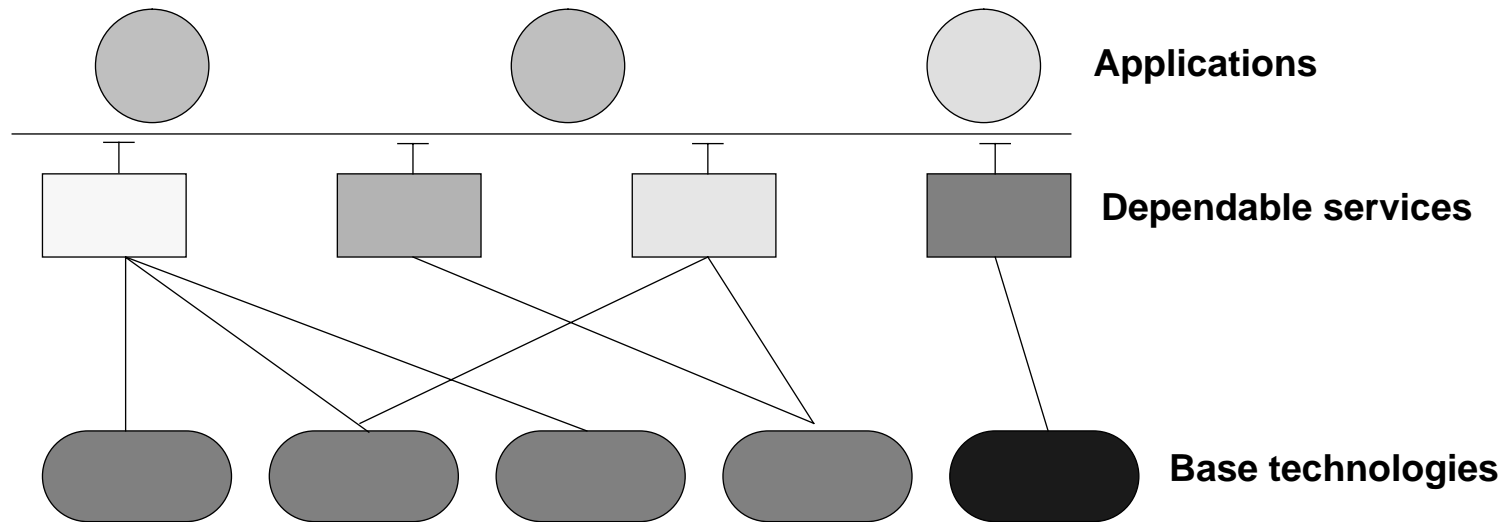
- **To motivate the need for an engineering model for dependability**
- **To describe some of the major issues and concerns**
- **To show why development of the model should be aligned with a credible application scenario**

Structure of the engineering model for dependability



- **Applications have expectations of other applications and of the infrastructure**
- **Dependable infrastructure services isolate applications from details of the underlying technology**

Satisfying application requirements



- **The engineering model must provide a vocabulary and taxonomy to be able to choose and compare technologies and services**
- **Do applications need sight of the details of base technologies?**



Scope of the engineering model for dependability

- **Concentrate on computationally significant features**
- **Is largely about the engineering of selective transparency**
- **Dependable infrastructure services can transparently enhance dependability**
 - **communications**
 - **applications**
- **Must be able to enhance pre-existing (*legacy*) applications**



Engineering approaches

- **Two extreme approaches**
 - *fault avoidance*, e.g. type checking, formal design methods
 - *fault tolerance*, e.g. replication and transactions
- **These are complementary approaches *not* alternatives**
 - fault avoidance may someday be able to produce fault-free components
 - fault tolerance is necessary to survive unpredicted or external failures
 - many techniques are a mixture of fault avoidance and tolerance
- **Fault tolerance is the initial emphasis of the engineering model for dependability**

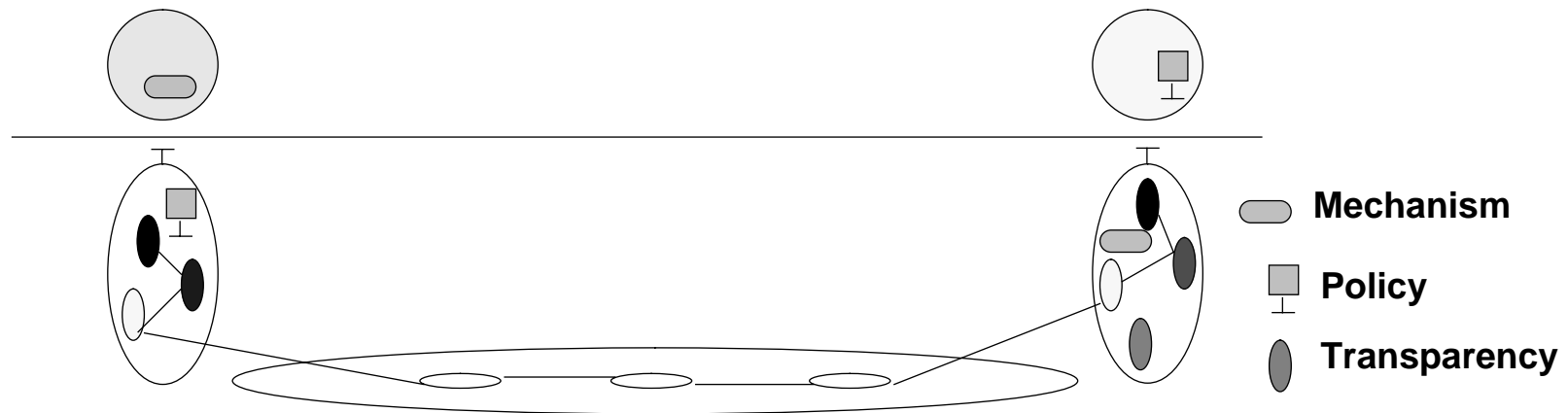


Phases of fault tolerance

- **Fault detection: *observing and testing expectations***
 - can observe the passage of time
make inferences about the non-occurrence of events
 - can exploit redundancy
 - implicit redundancy requires semantic knowledge
 - explicit redundancy exploits extra storage/processing/communications
 - this gives a basis for a taxonomy
 - can be provided in space and/or time
- **Fault recovery: *re-establishing expectations***
 - about management and reconfiguration - will be covered in later tasks
 - engineering model for dependability must encompass interaction with management

Transparency

- **Compensating for, or masking, unwanted aspects of an interaction**



- **The engineering model for dependability must define standard interfaces, composition rules and permit standard configurations**
- **There are also equivalence rules and compatibility problems**

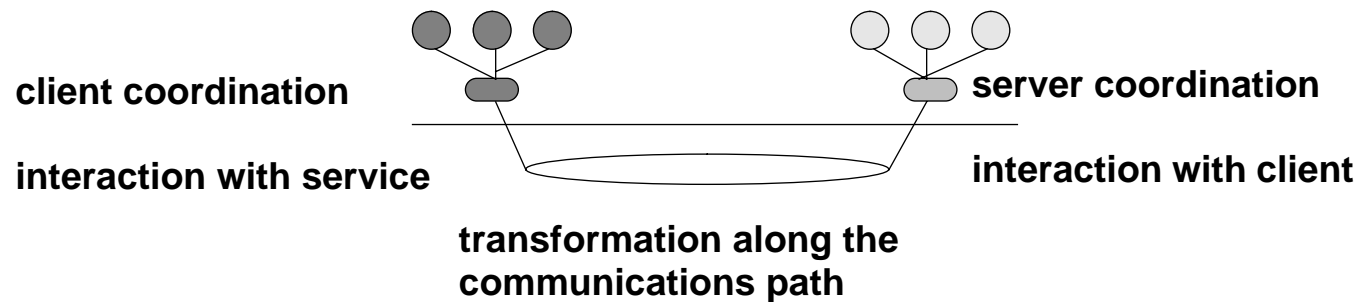


Implementation options

- **Dependability may be provided transparently or non-transparently**
 - clients and servers need not have the same view
- **Non-transparent users are able to influence the provision of dependability**
 - *indirect* - can adjust management parameters
 - *direct* - can actively participate in dependability processing
- **Options for the placement of dependability processing**
 - in the application
 - in the local infrastructure
 - along the communications path

Structure of a dependable interaction

- **Five distinct activities**



- **The client view**

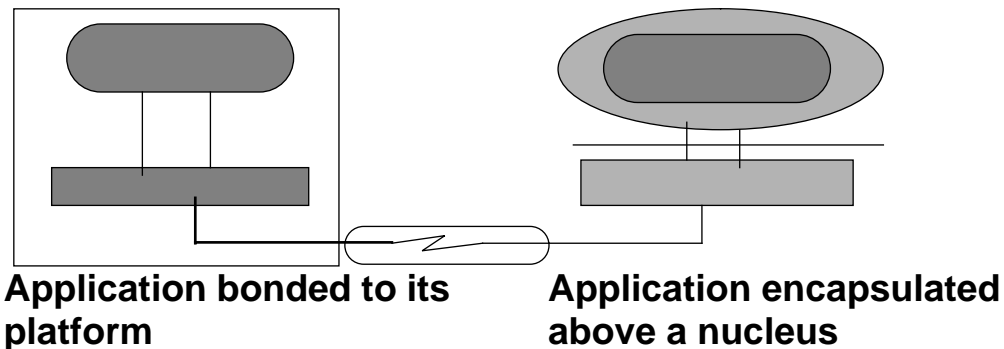
- able to pre-select most suitable service
- can detect server failure and initiate corrective action

- **The server view**

- has less control over invokers
- must detect and protect itself against client failure

Making legacy applications dependable

- **There are fewer opportunities to engineer entirely from scratch**
 - legacy applications *are* designed without regard to distribution
 - dependability enhancement must be transparent and externally applied
 - Message interception requires no platform changes
 - Encapsulation enables the application to migrate to a new platform



- **Can only achieve so much - inherent limitations of original application**
- **Many naming issues**



Interaction between legacy and non-legacy applications

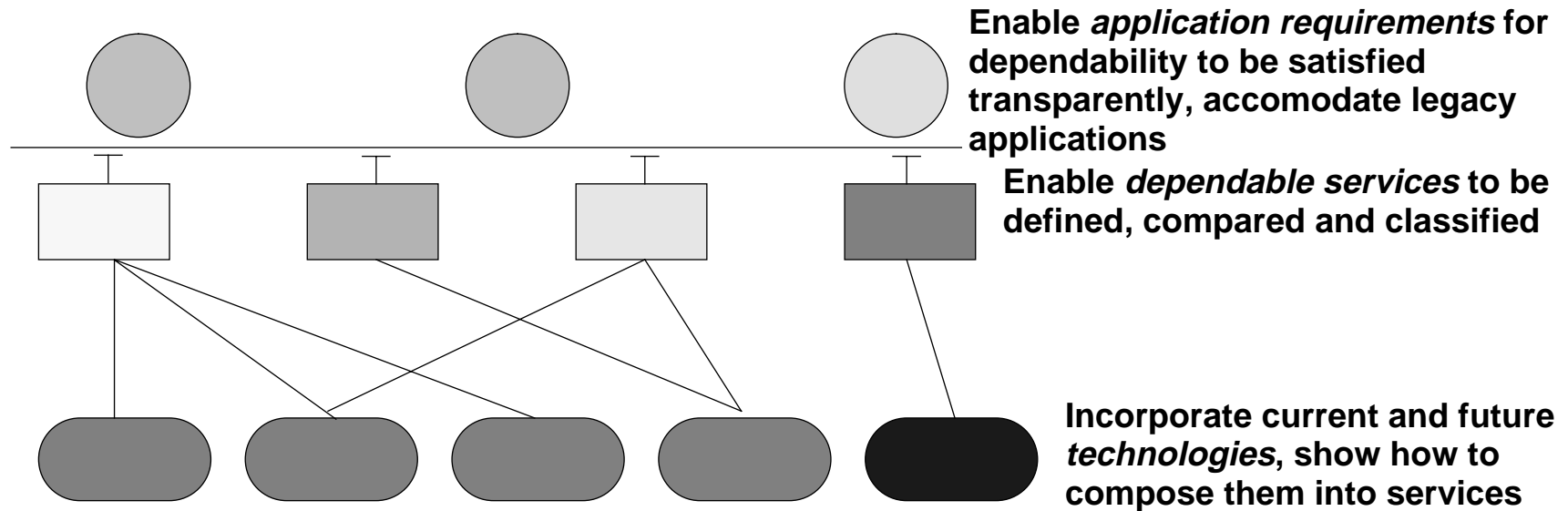
- **Legacy clients**
 - **determine interface corresponding to client usage**
 - **perform trader interactions**
 - **cope with opening, interacting with, closing service**
 - **assign a name which the service can use for e.g. charging**
- **Legacy servers**
 - **determine interface corresponding to server functionality**
 - **detect/manage conflict between multiple clients**
 - **assign suitable client names**



Aligning the engineering model with a scenario

-

Summary



- **The scenario keeps this grounded in credible, realistic requirements**