ERA System Design Review

Day Four

May 12, 2005

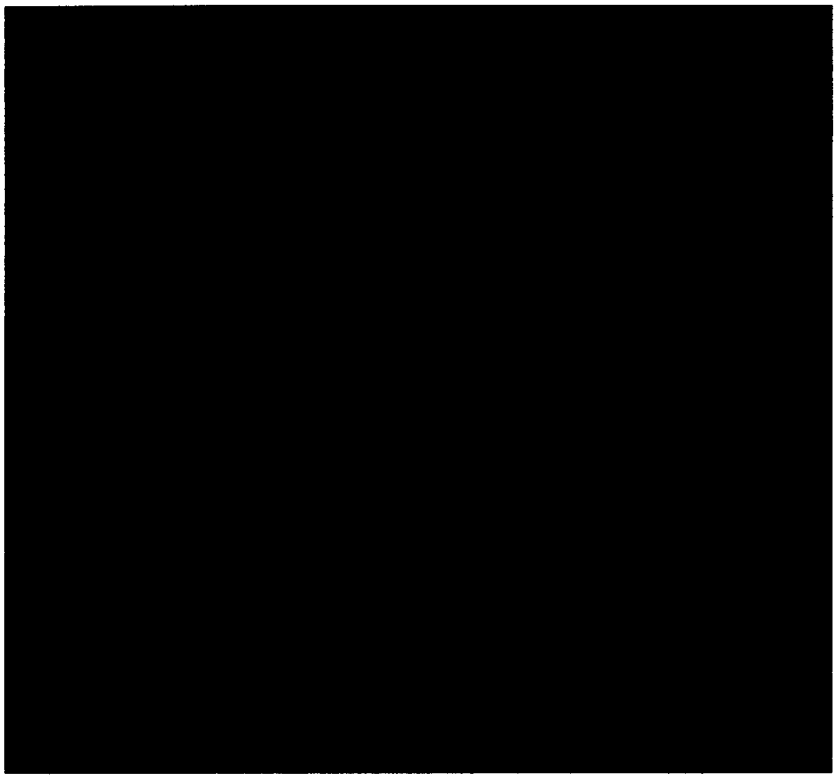
ERA SDR – DAY FOUR

Security Design

[redacted]

May 12, 2005

Security Design - Agenda

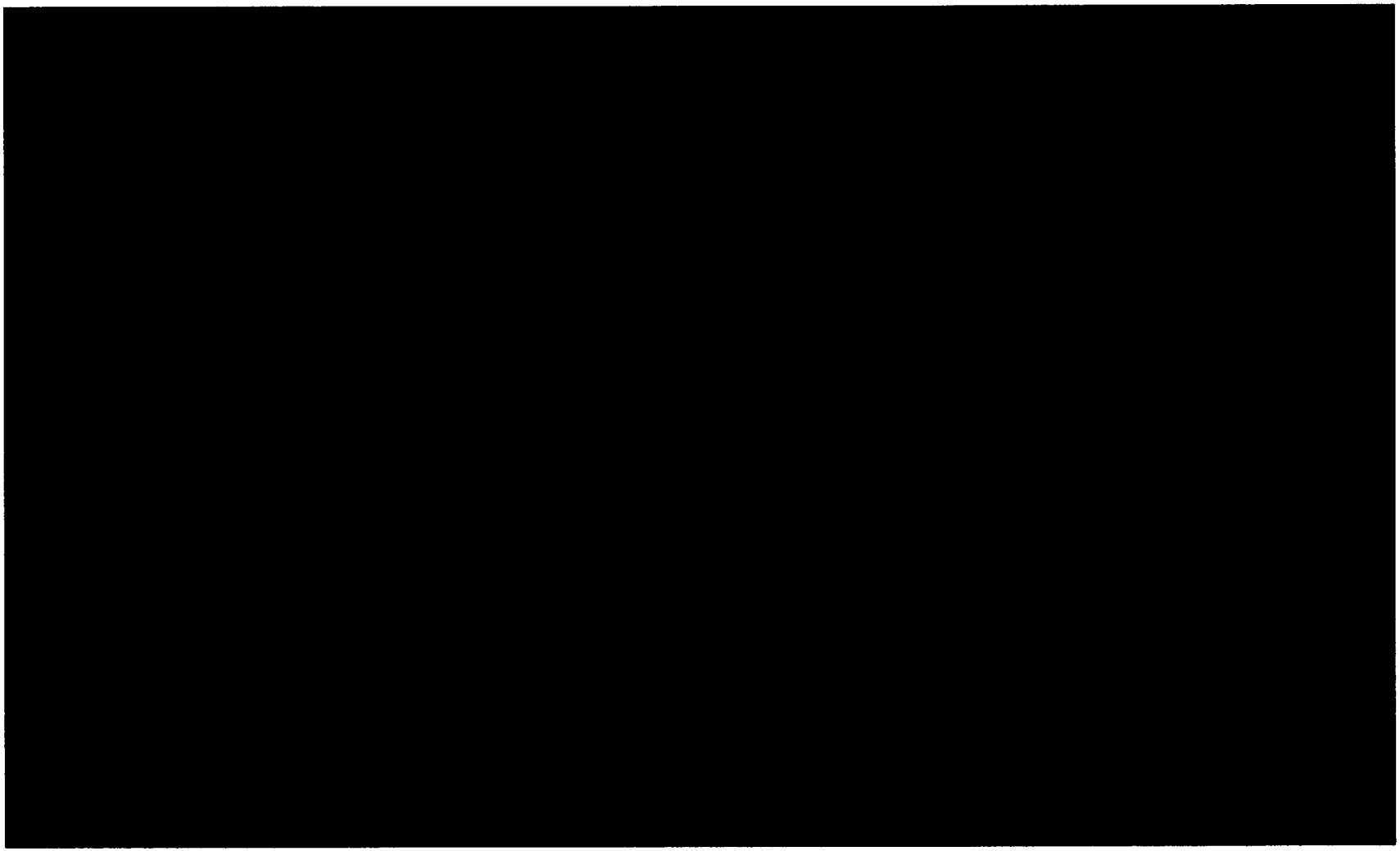


Security Description

Security Driving Requirements

Security Design Goals

Security Design Principles



Major Design Impacts

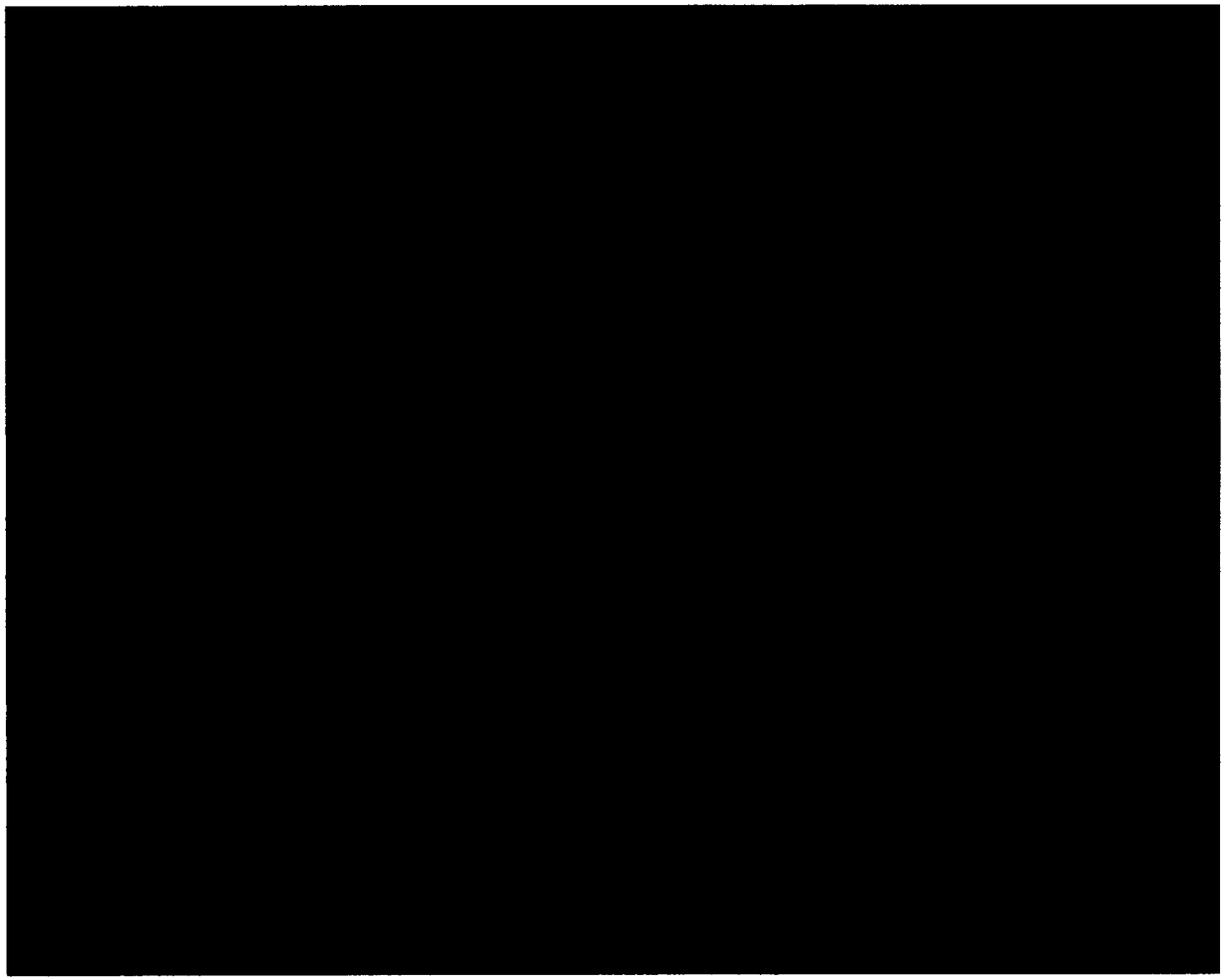
Isolation of Federations

Access Control - Restrictions for Assets

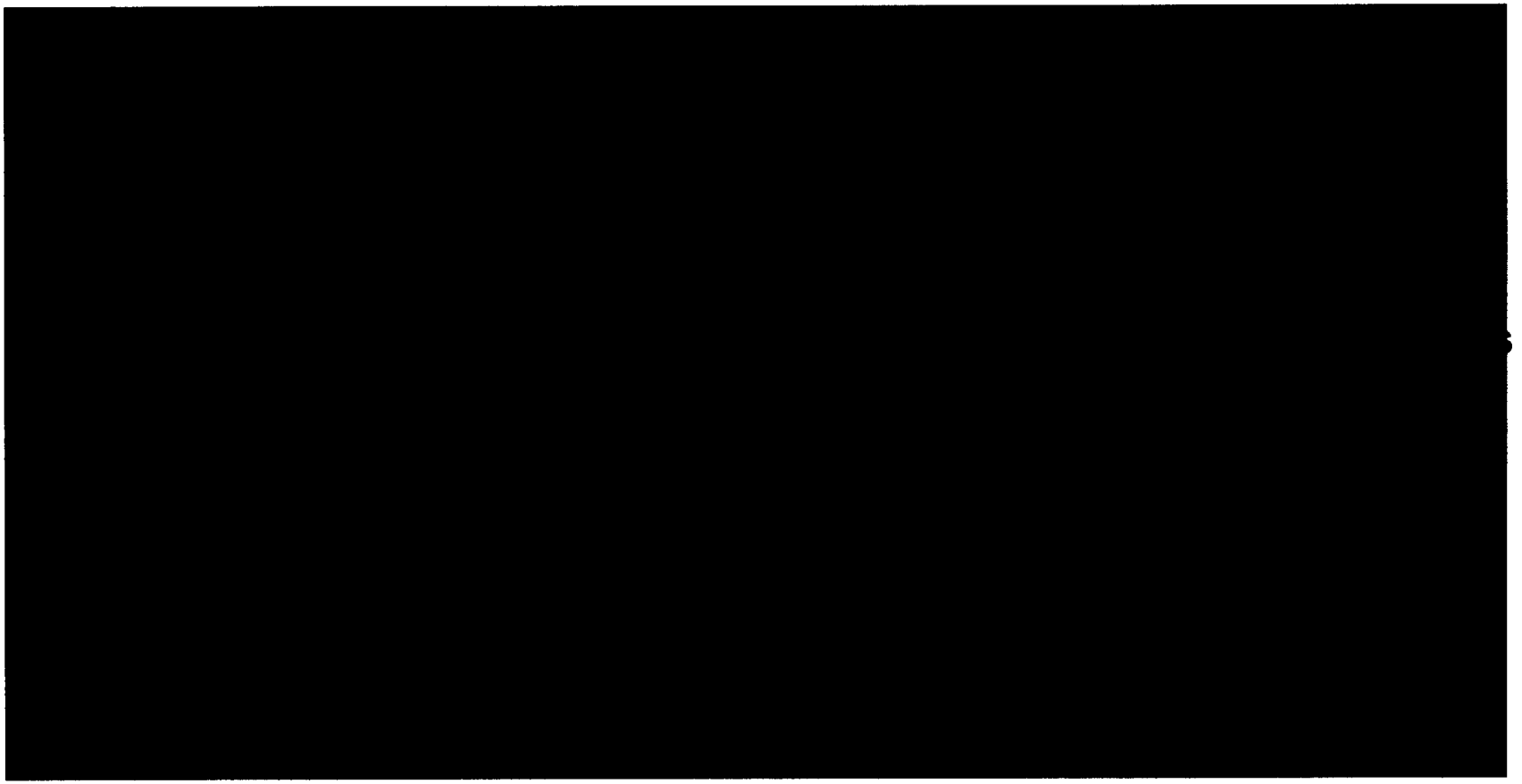
Access Control - Permissions

Access Permissions Example

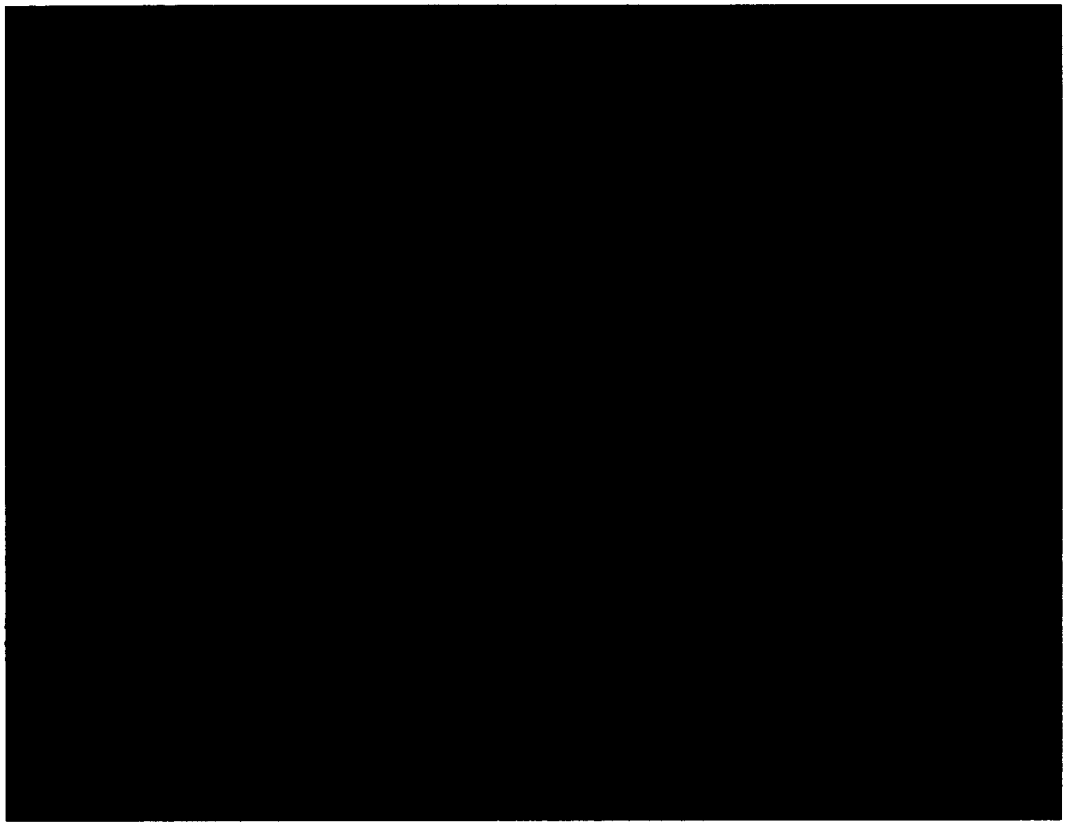
Security Specifics



Registration of Users



Logon and Assignment of Permissions



Accessing Functions and Data

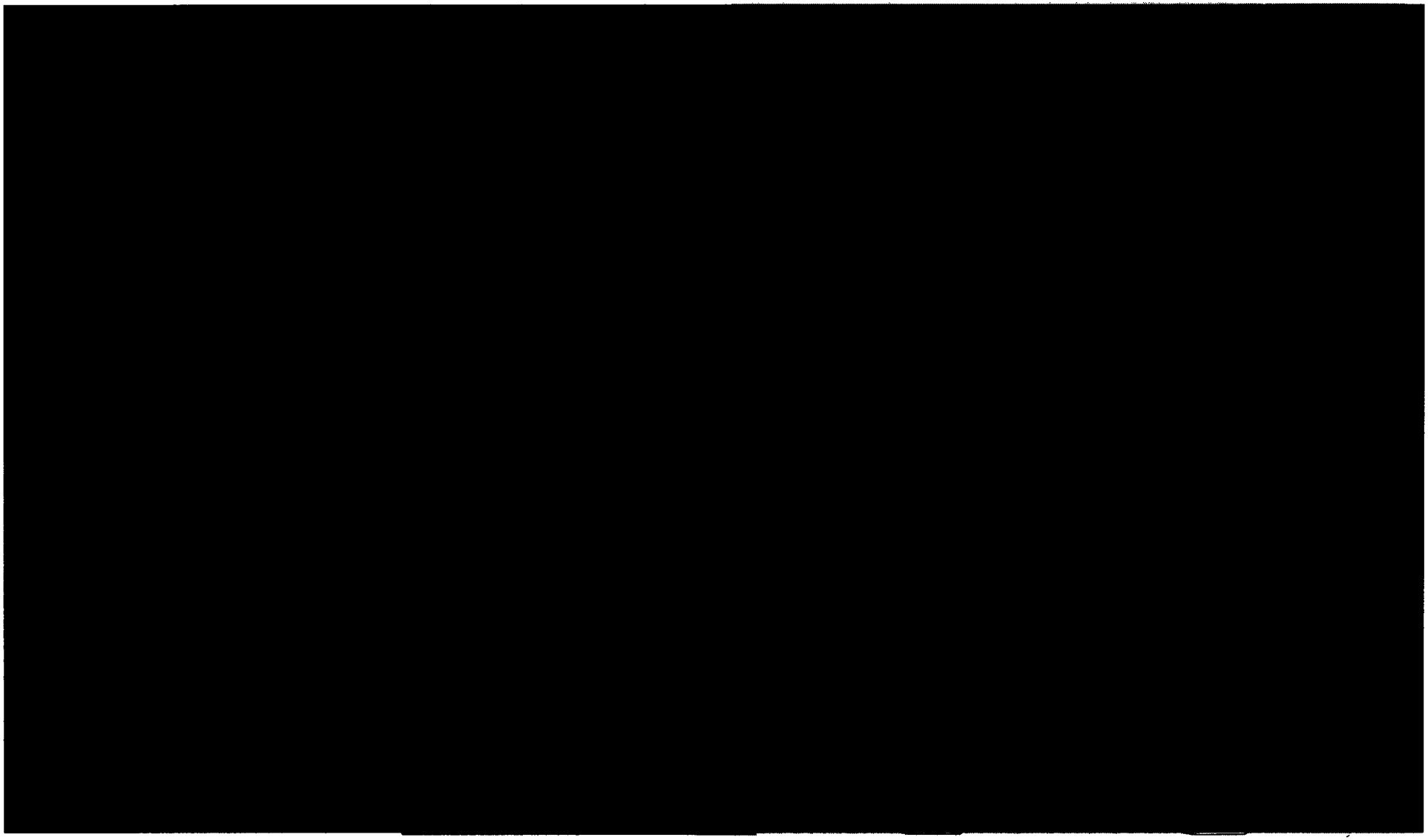
Auditing

Extracting a Record

Misclassified Records

Virus Control

Volumes Restricted by Access Restrictions



Sharing Among Federations

Sharing Among Federations

Span of Control of Administrators

Security Environment

Facility Security

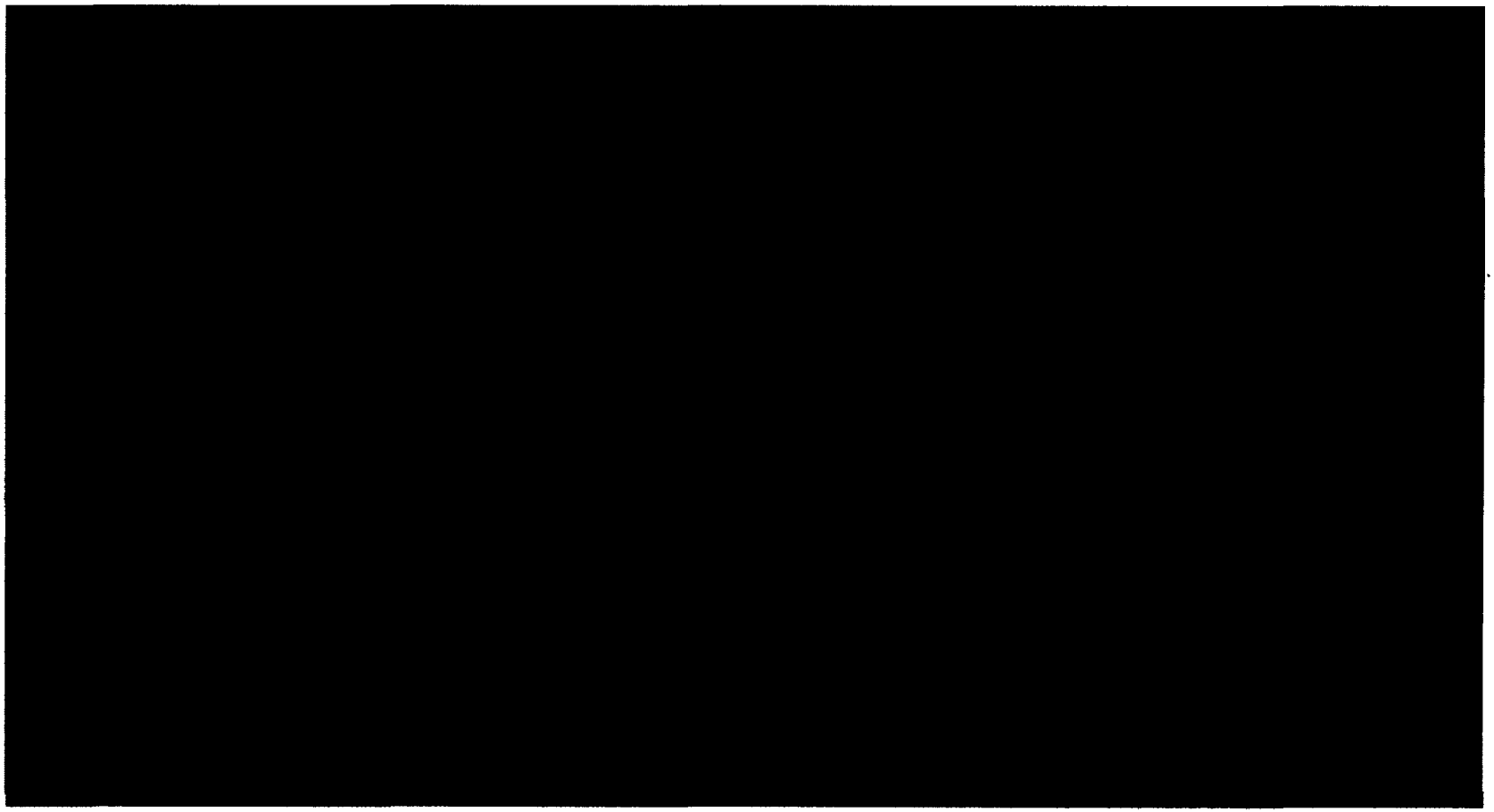
Network Security

Personnel Security

Distribution Of Media

Certification and Accreditation

C&A Process

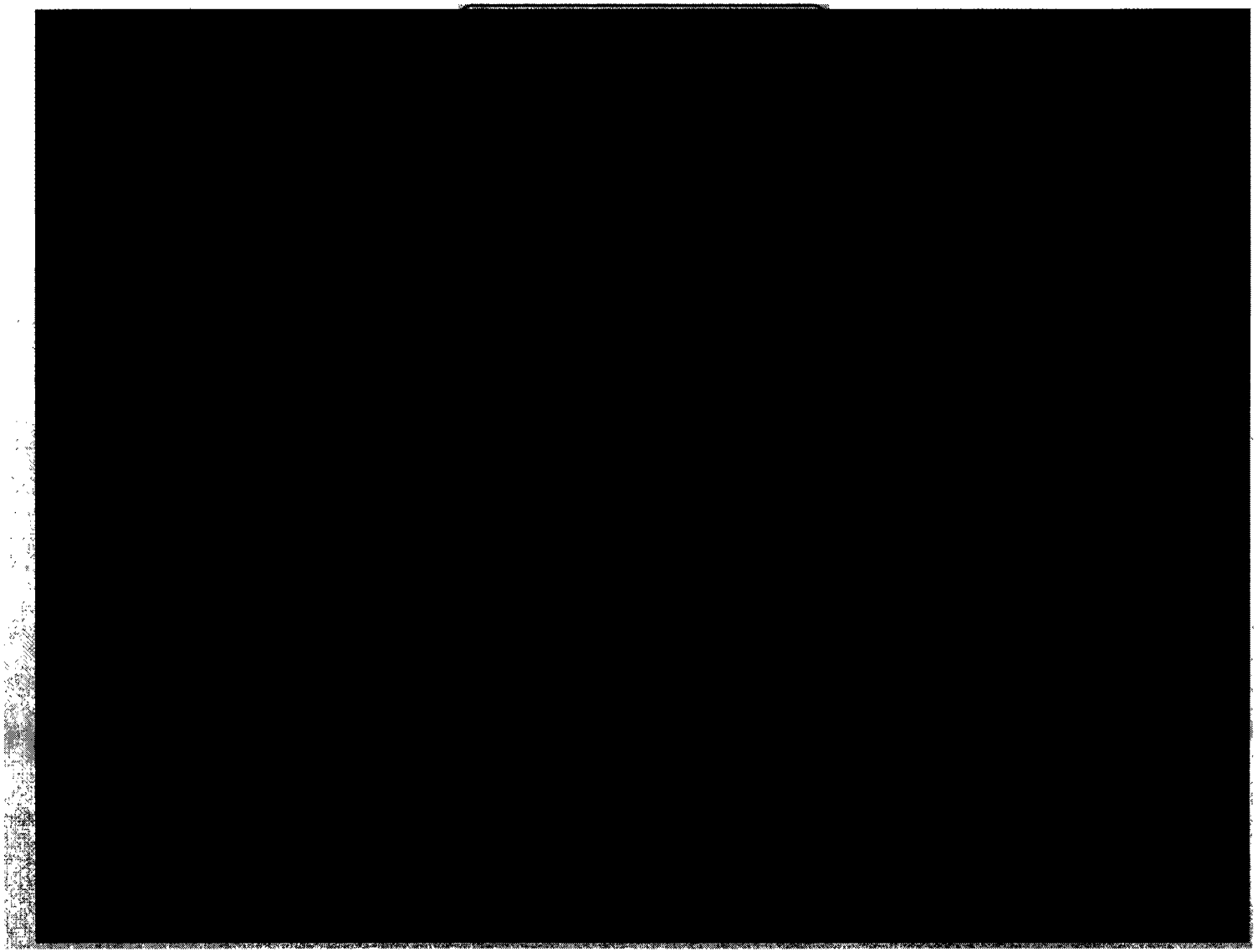


Design Components

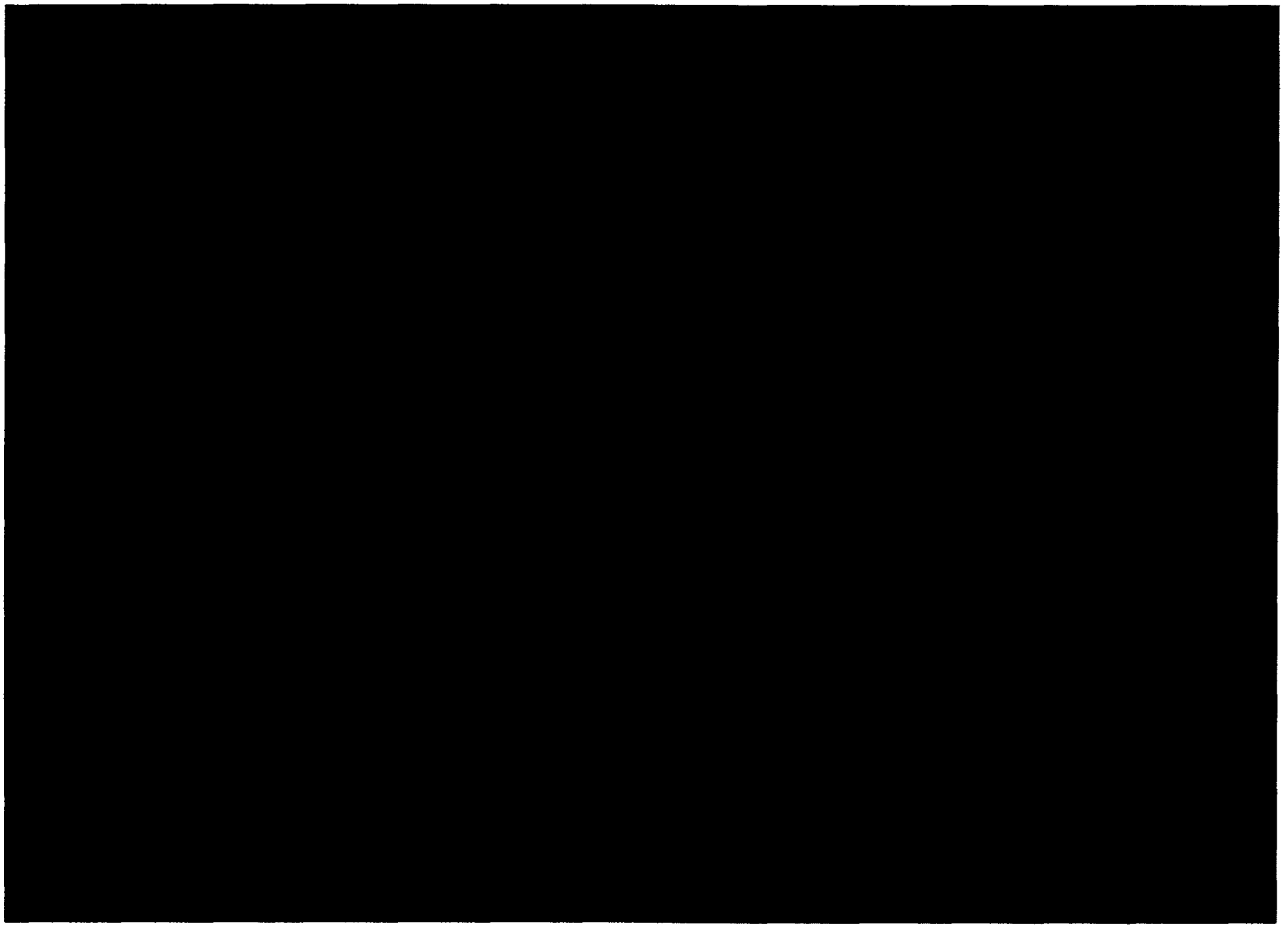
Top-level Security Architecture

Identification and Authentication

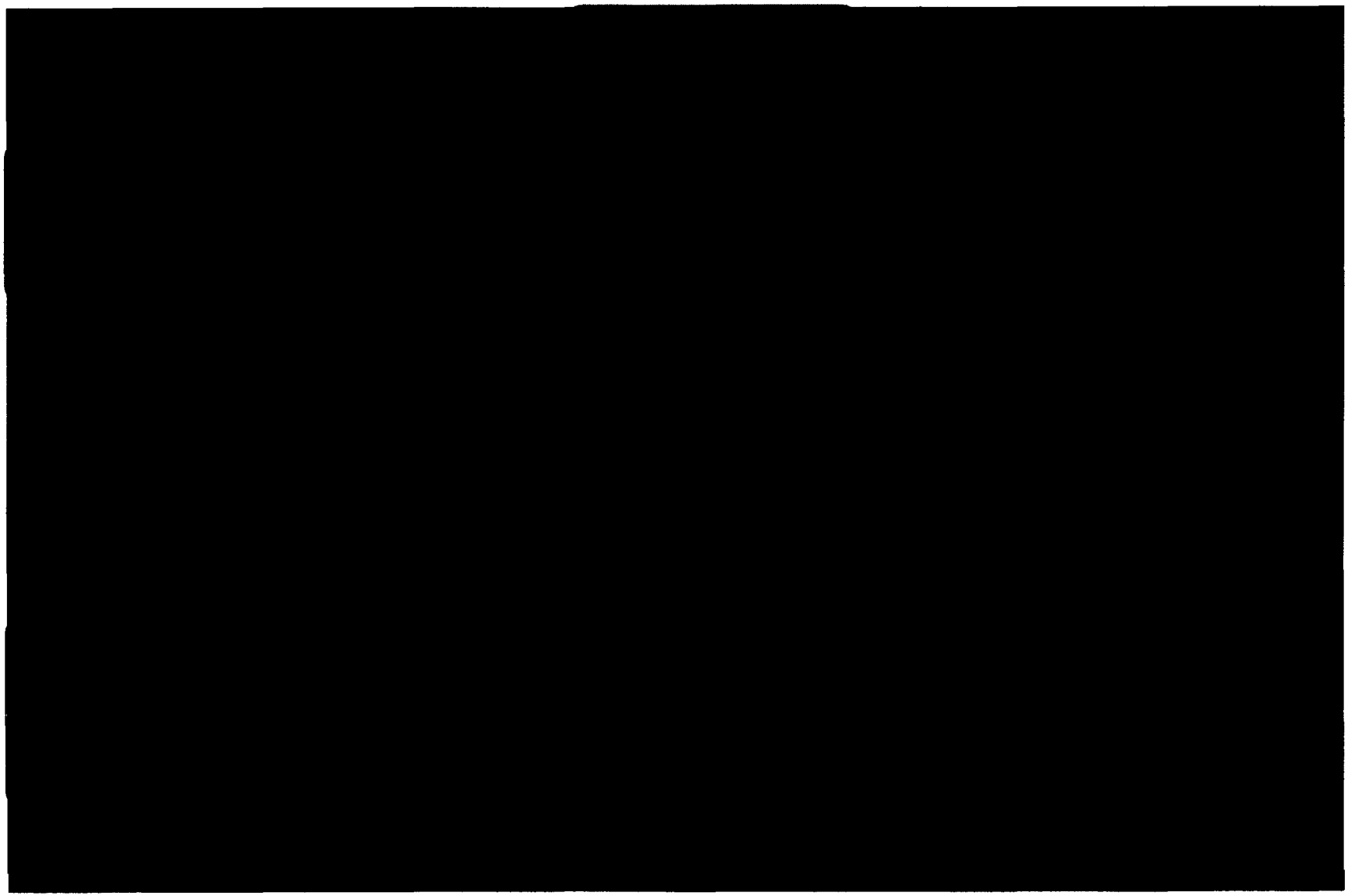
Access Control



Accountability



Availability



Security – Forward Plan/Conclusions

Security RIDs

[redacted]

BREAK

ERA SDR – DAY FOUR

Performance Modeling

[redacted]

May 12, 2005

Performance Modeling – A&D Phase Objectives

Predict required resources to achieve performance requirements

Investigate performance implications of different design decisions

Modeling Activities:

- **Network usage**
- **Ingest services**
- **Ingest temporary working storage**
- **Volume of data to be stored in archival storage**
- **Search indices**
- **Performance requirements**

Performance Modeling - Influence on Design

SOA means that performance time budget can be allocated for each step of a multi-step workflow

- Performance of each service can be independently specified and assessed
- Performance budget can be traded between services
- Performance budget can be traded between computation and communications

Search modeling:

- Confirms that for description/keyword searches, permanent indexing of the entire ERA records catalog will satisfy performance requirements
- Confirms that for Content-based searches, neither permanent indexing nor on-demand indexing will exclusively satisfy performance requirements in a cost-efficient manner
- Confirms that for content-based searches, the balance between permanent and on-demand indexing will require optimization based upon frequency of repeated hits

Influence on Design (continued)

Storage modeling:

- Quantifies the relative cost of tape and cache storage
- Quantifies the growth of internal storage driven by the need to migrate data to new media and formats
- Confirms that the complete catalog should be held at all Instances within Federations

Ingest modeling:

- Shows need to isolate physical issues of transferring and saving electronic data files from the intellectual tasks of Archivists
- Confirms that restricting the amount of temporary Ingest storage for cost efficiencies imposes limitations on when submissions can be accepted and on the maximum submission size

Performance Modeling – Additional Specifications Required

Log-on & authorization, and account status checks

- Number of valid and invalid user accounts
- Number of subscription services available
- Number of pending transactions and requests

Search

- Proportion of assets returned
- Proportion of assets returned that must be withheld from the requestor

Media Distribution

- Bounds of the order and confirmation process

Technical Performance Measurements (TPMs)

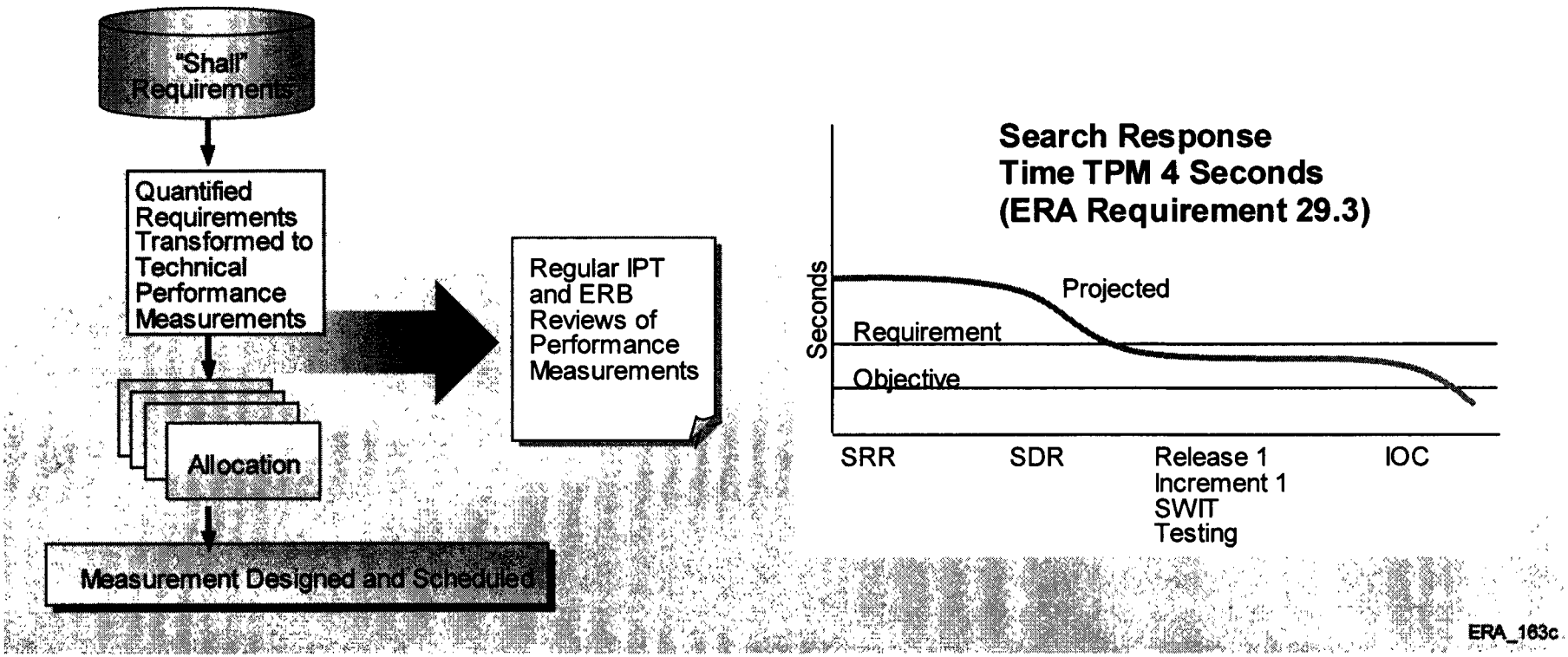
Established for each performance requirement

Assessed periodically throughout system development life cycle

- **Support the quantifiable measurement of progress toward achieving performance requirements**
- **Provide early warning of potential system design problems**

Allocation of performance "budget" to component orchestrations/services will occur as product design progresses

Tracking Technical Performance Measurements



Modeling – Forward Plan

Performance Models
- To identify tasks that are performance bottlenecks.

Persistence Models
- To improve sizing estimates.

Search Models
- To predict the price-performance characteristics for the different options.
- To assess full-text search capabilities.

Network Models
- Improvements to inter-site scale.
- Modeling of intra-site scale.

System Load Models
- To model performance under varying load

Media Failure Models
- To feed into lifecycle cost and performance models

System Simulations
- To allow different system management strategies to be evaluated

All Models will be updated to reflect measured values as the implementation proceeds.

LUNCH

ERA SDR – DAY FOUR

Availability Modeling and Analysis

[redacted]

May 12, 2005

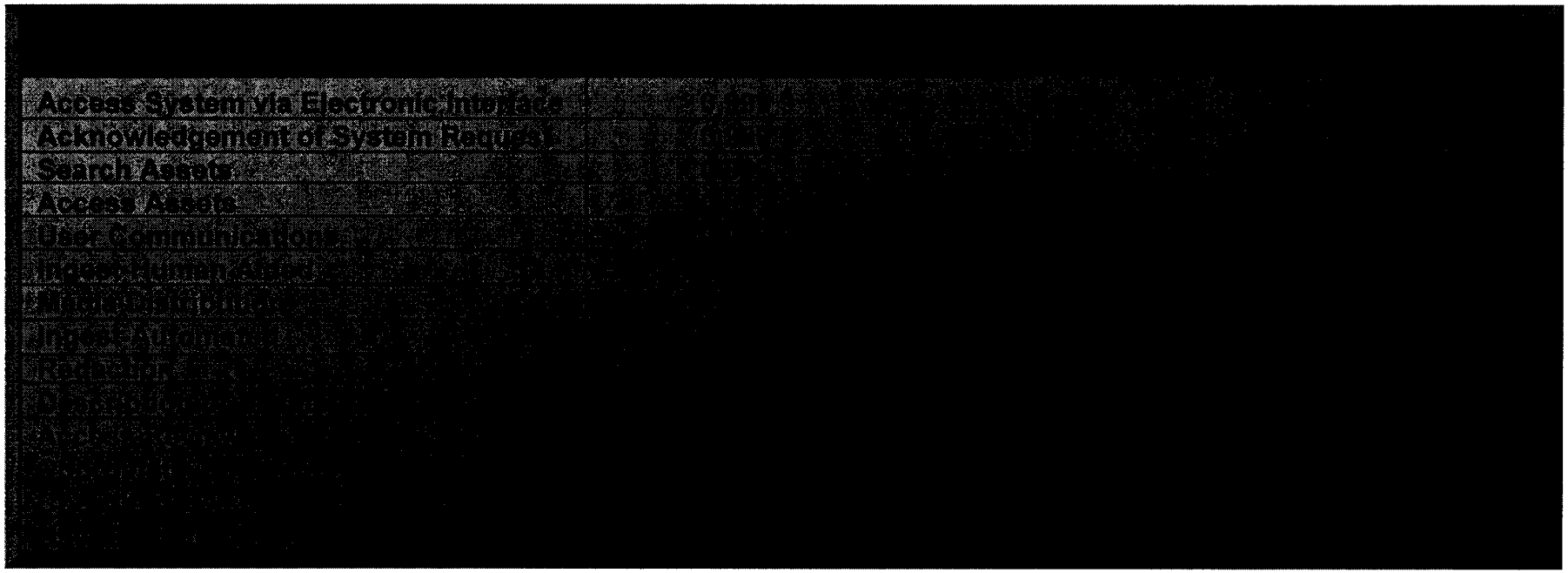
Agenda

Availability Modeling

Failure Mode and Effects Analysis (FMEA)

Availability Modeling

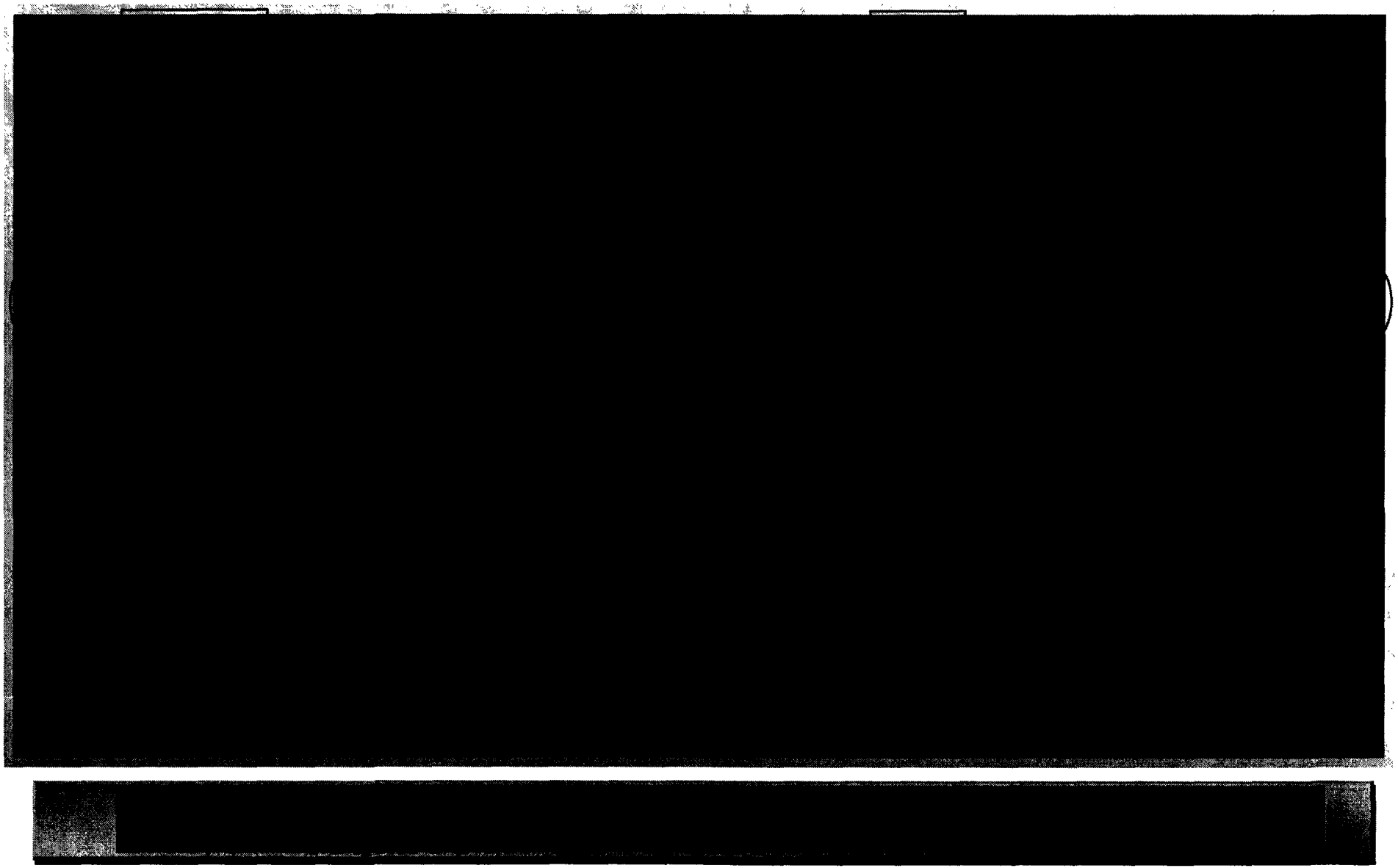
Availability Requirements and Results



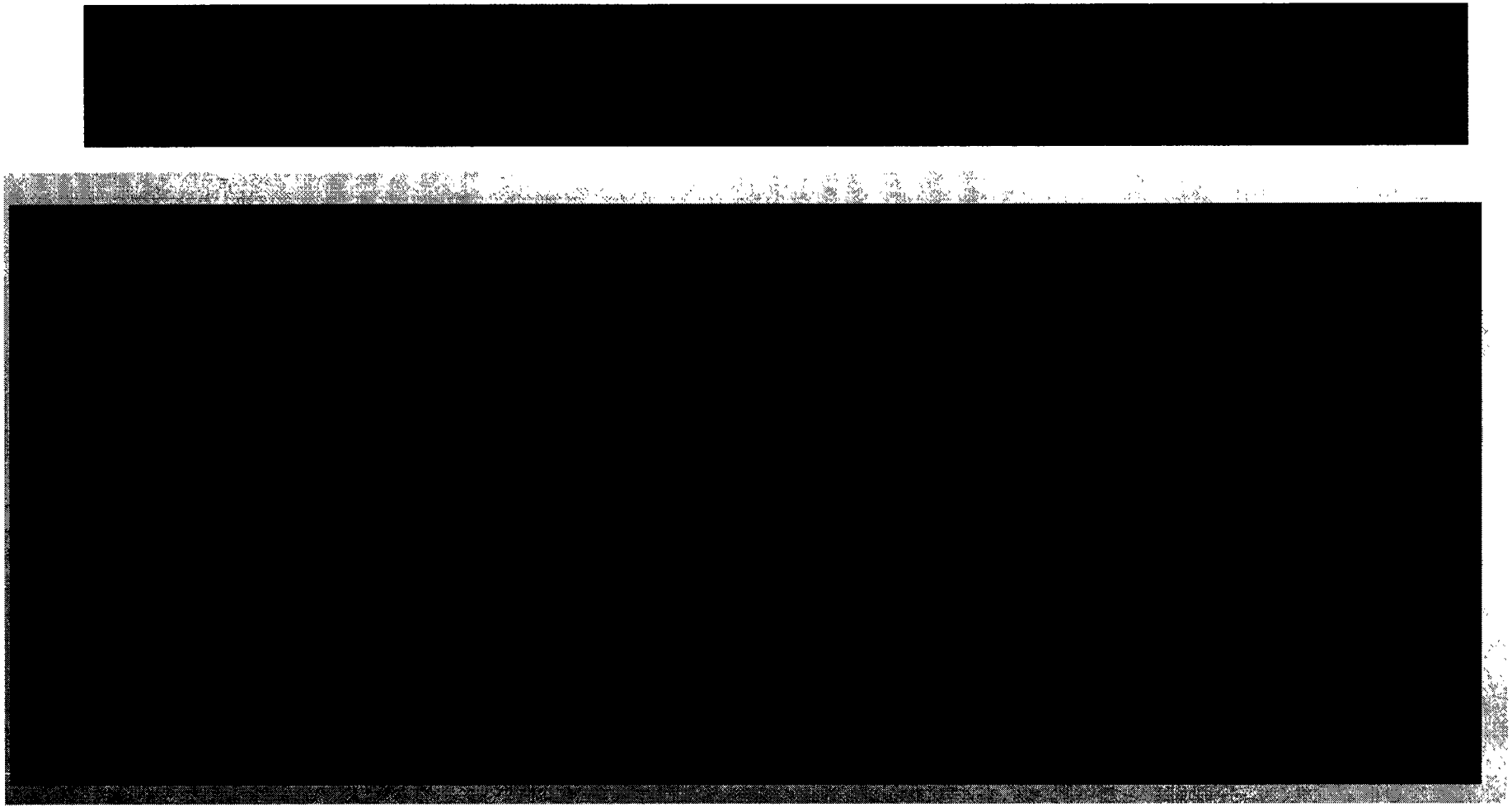
The Predicted Service Availability is driven by the no single point of failure requirement (LM32.2)

Availability Block Diagram (ABD) Sample

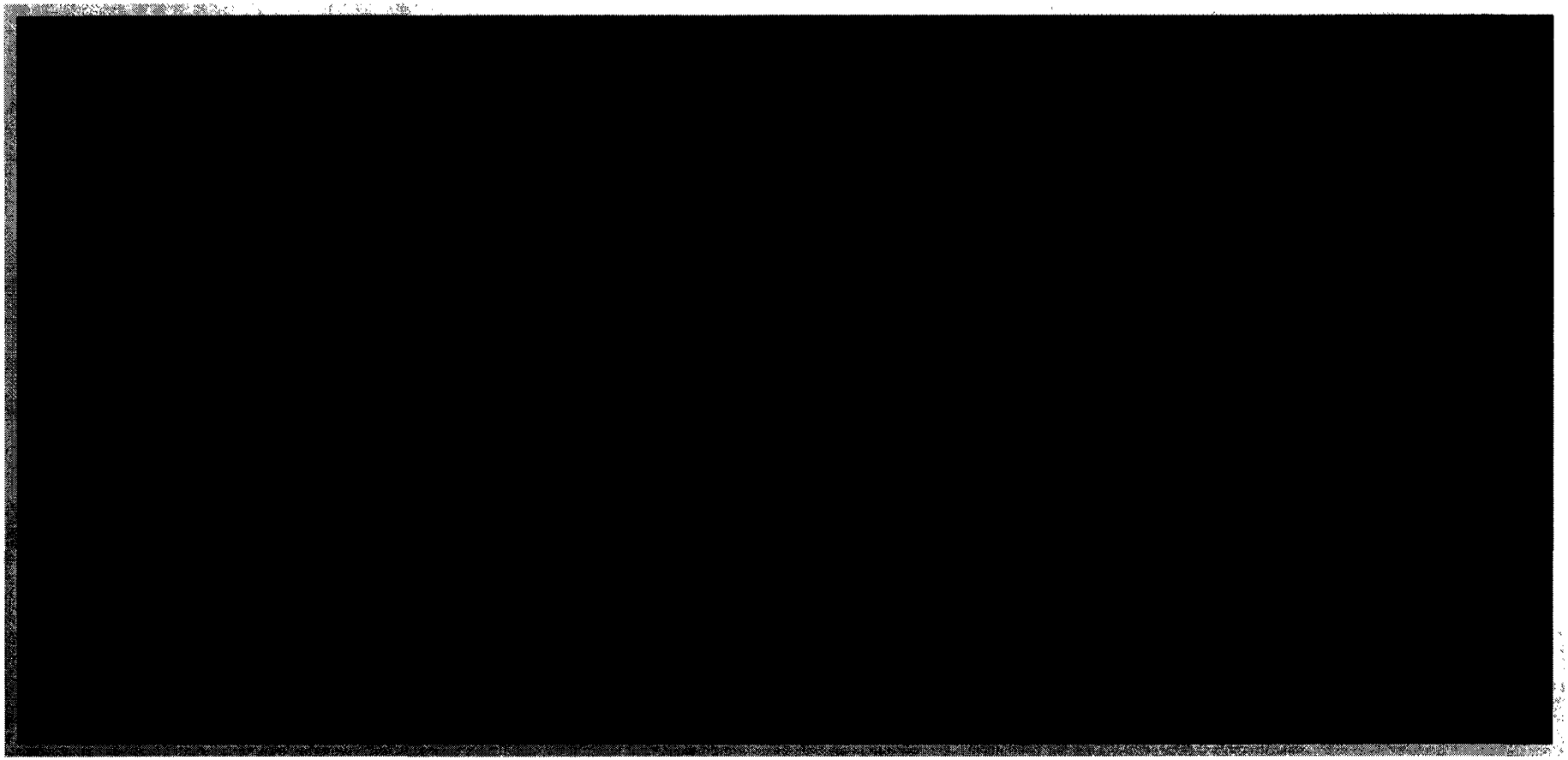
ABD Sample - LS&C Package for Access System Service (1 of 2)



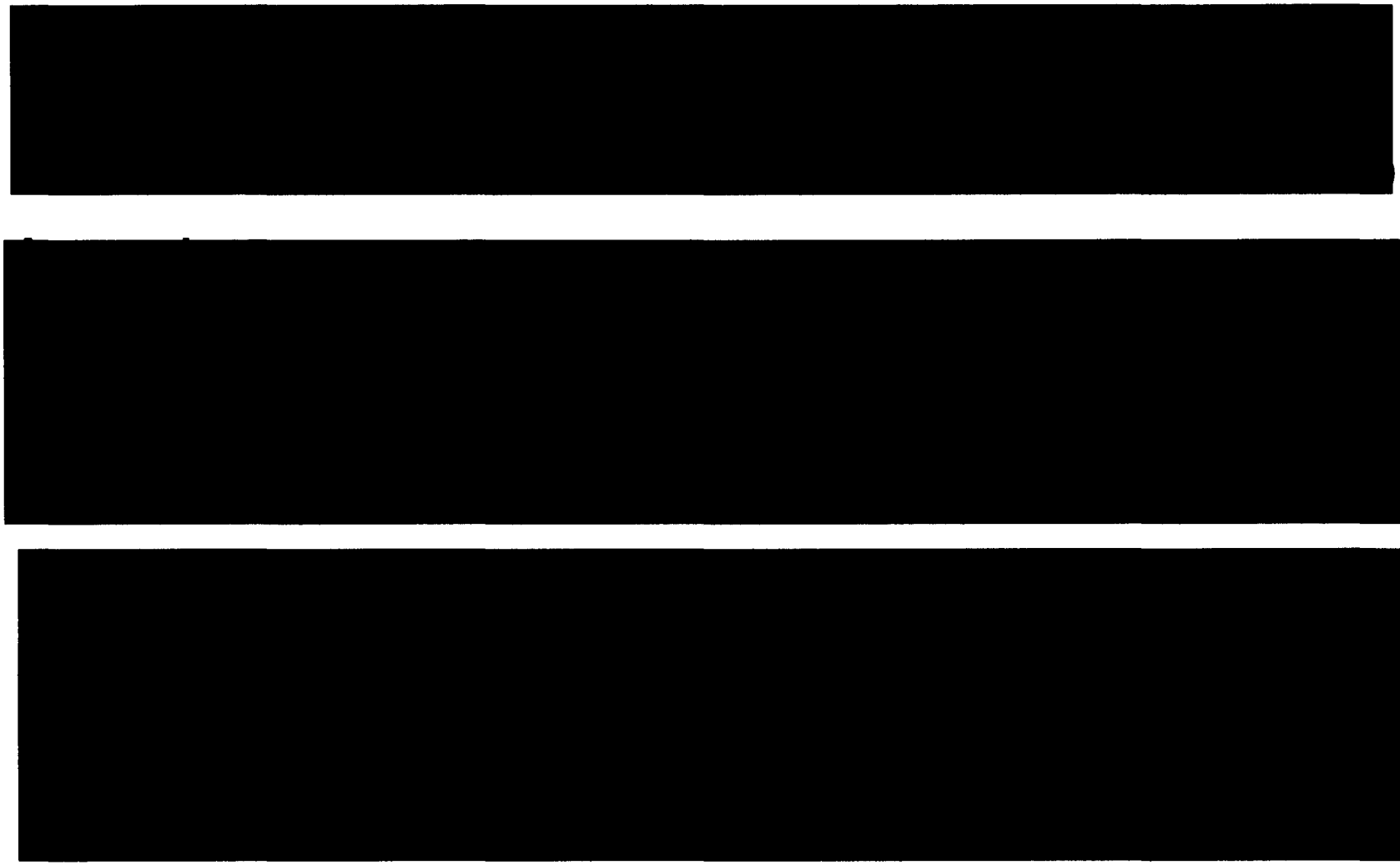
ABD Sample - LS&C Package for Access System Service (2 of 2)



ABD Sample - Access System Service



Failure Mode and Effects Analysis (FMEA)



FMEA Sample – Ingest

Item / Functional Identification	Function	Failure Mode	Failure Effects		Failure Detection Method	Compensating Provisions
			Local Effects	End Effect		
LAN Switch	Provides functional interconnection for Ingest items/components	a.) Total loss of function due to Interface to Operational System (IOS) fault	Total loss of interconnection capability			
		b.) Loss of function at one port due to module failure	Loss of interconnection capability at one port			
Input Server	Ingest records from physical media (tapes, CD, etc.)	a.) Total loss of function	Total loss of capability			

Sample from FMEA worksheets that form the basis of the ERA FMEA

FMEA Sample – Ingest (cont.)

Item / Functional Identification	Function	Failure Mode	Failure Effects		Failure Detection Method	Compensating Provisions
			Local Effects	End Effect		
Ingest Server	Transfers are received into ERA and files transferred into Ingest Working Storage after they are screened.					
	1) Receive and segregate electronic records based on potential access restrictions	a) Loss of Ingest Working Storage				
		b) Simultaneous loss of both Ingest Server operating system common mode failure				
	2) Packaging submitted files and templates with SIP and into Ingest Working Storage	a) Loss of Ingest Server				

Availability Modeling – Forward Plan

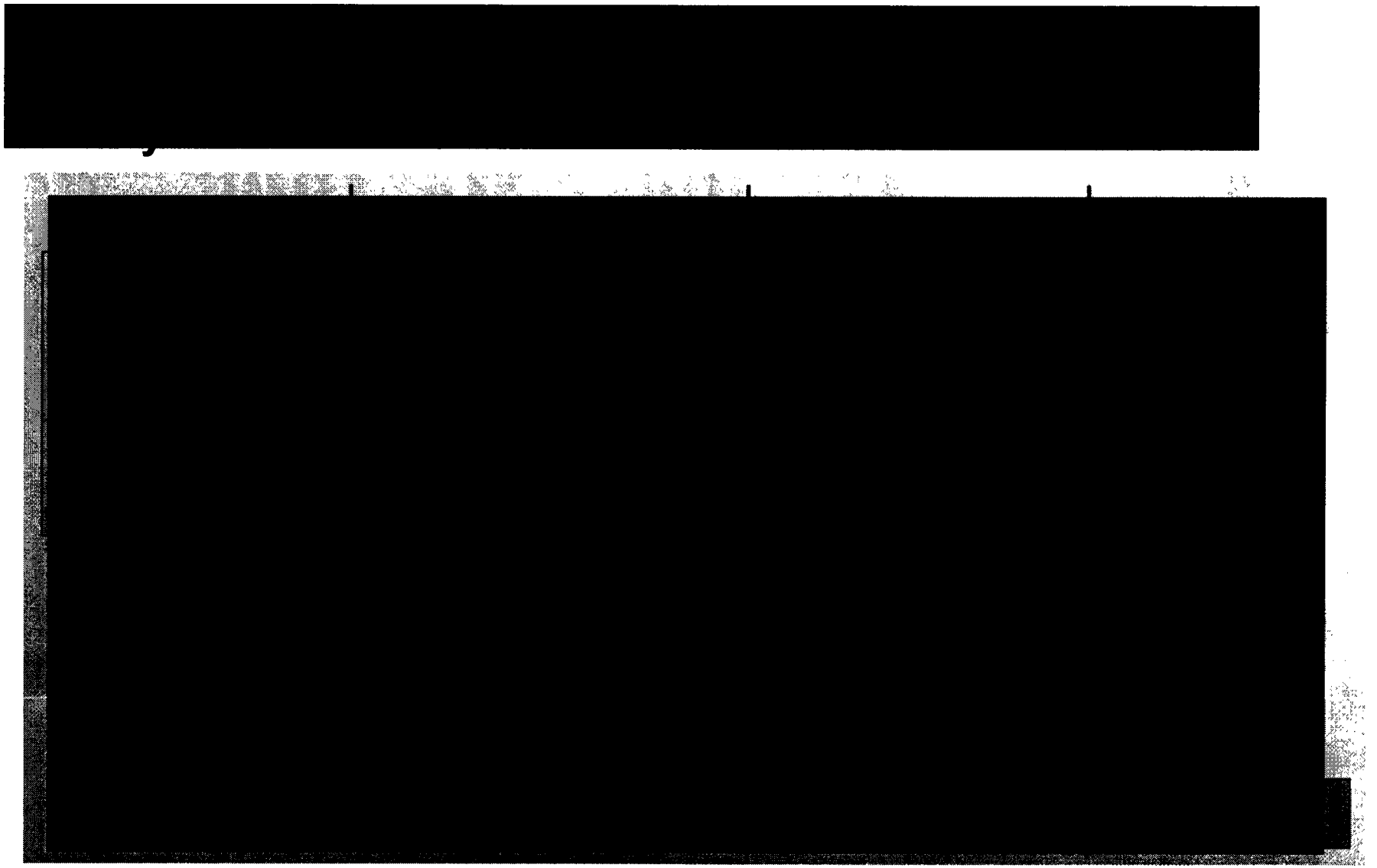
Update availability modeling throughout product design to ensure continued compliance with availability requirements

Capture measured data from previous Increments

Provide Availability Modeling and Prediction Report (CDRL L63) prior to each Increment CDR

Assess any SyRS requirements changes for impact to compliance with availability requirements; ensure appropriate architecture/design changes as required

FMECA - Forward Plan



ERA SDR – DAY FOUR

Integration and Test

[redacted]

May 12, 2005

Agenda

Test Involvement in Architecture & Design

ERA System Design Features for Test

Levels of Integration and Test

Integration and Test Approach
- SWIT
- System Integration

Integration and Test Environment

Iterative Test Approach

Test Artifact Hierarchy

Preliminary Test Procedures

Forward Plan

Test Involvement in Architecture & Design

Identification of ERA System features required for Integration and Test program

Revalidation of verification methods

Assessment of architecture and design components

Initial test planning

- **Master Test Plan (CDRL L31)**
- **System Integration Plan (CDRL L56)**

ERA System Design Features for Test

External Interface Testing
- Emulator Test Tool to generate messages and responses

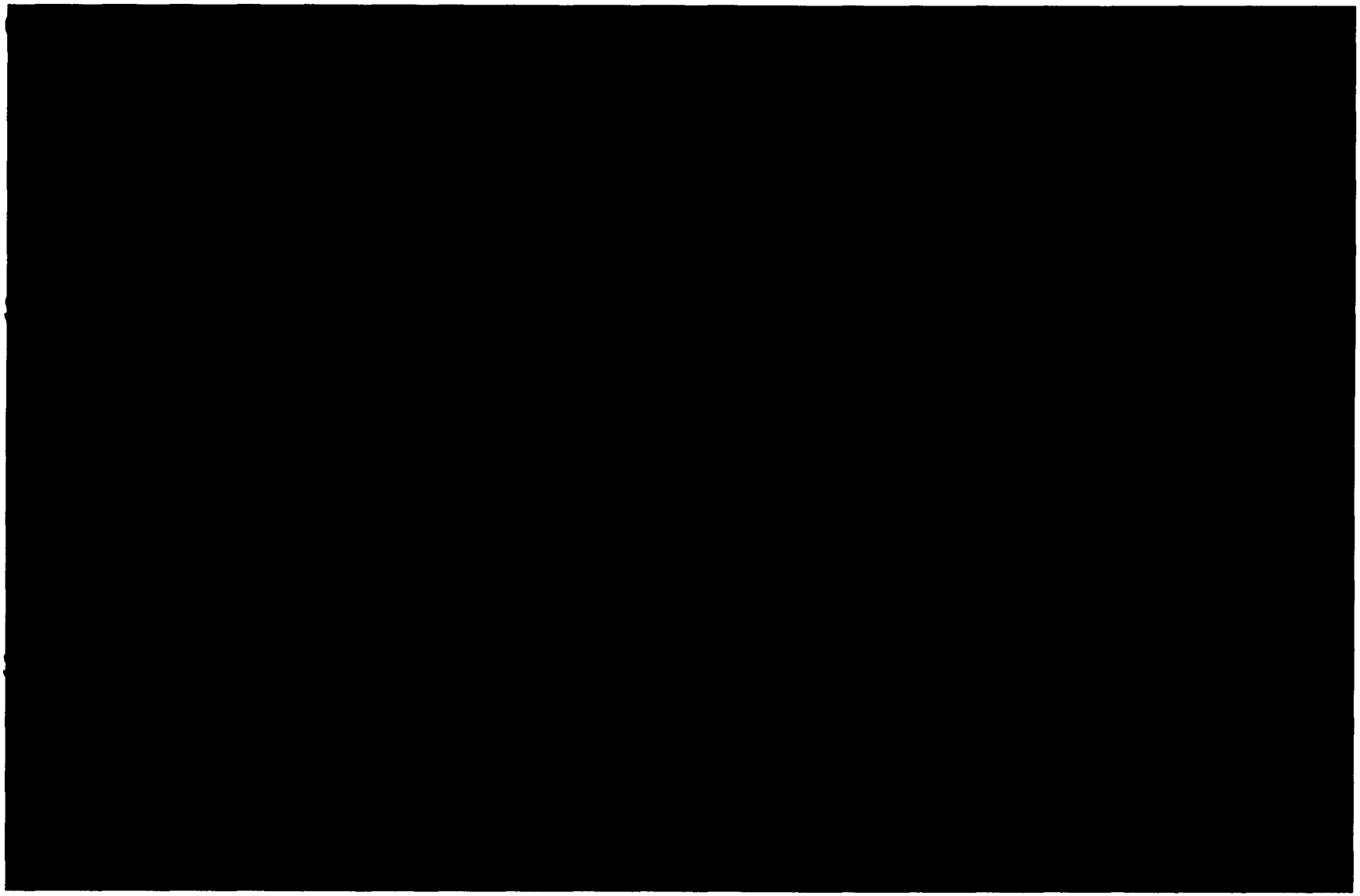
Identification, isolation and purging of test data and associated artifacts

Performance Testing
- Automatic generation of system load data
- "Hooks" within software for measurement of response times and internal processing times
- Enabling/disabling performance measurement "hooks"

Data Recording, Reduction and Analysis
- Specification of data to be logged
- Enabling/disabling of data logging
- Data report generation

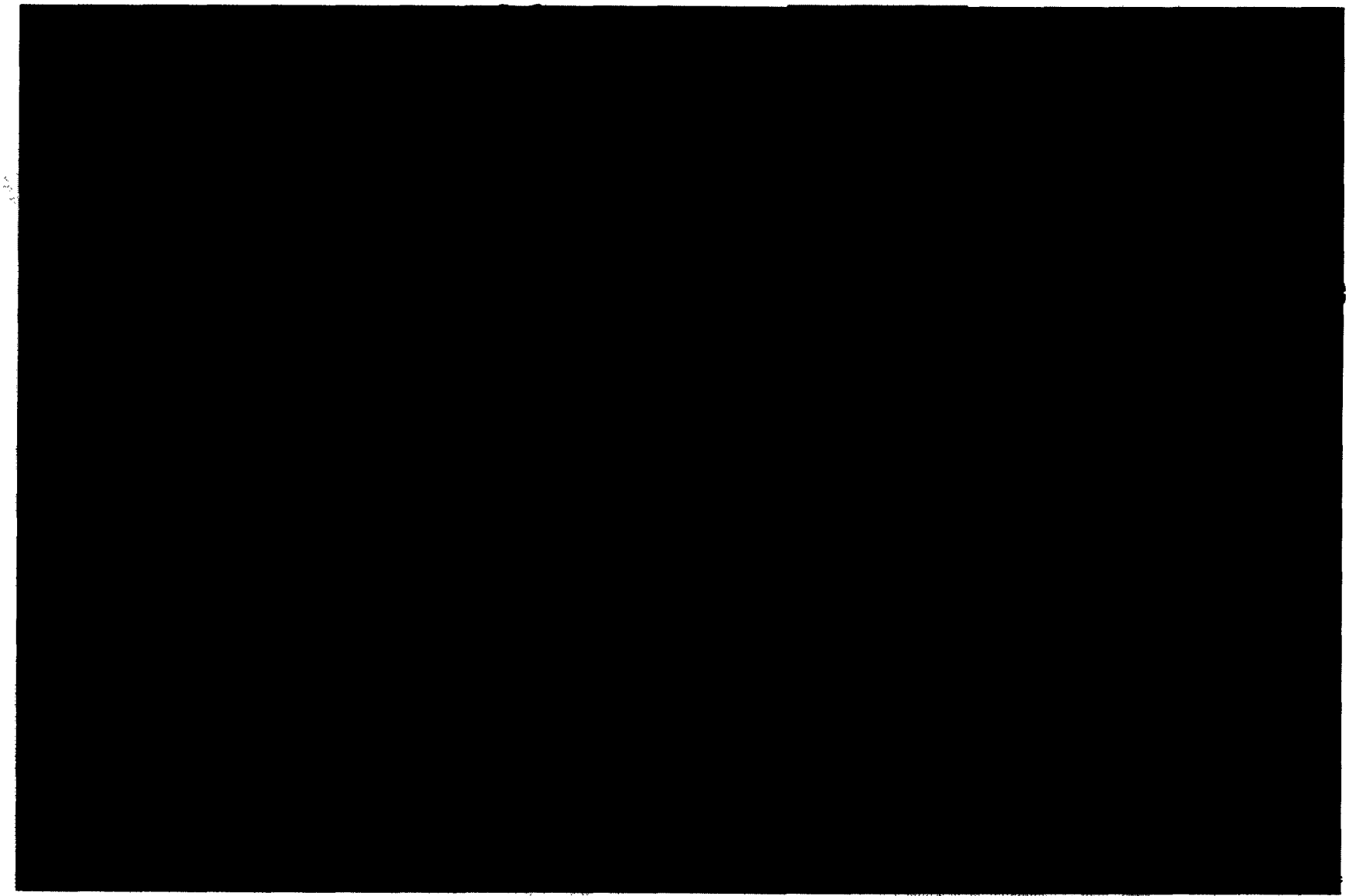
Levels of Integration and Testing

Integration and Test Approach - SWIT

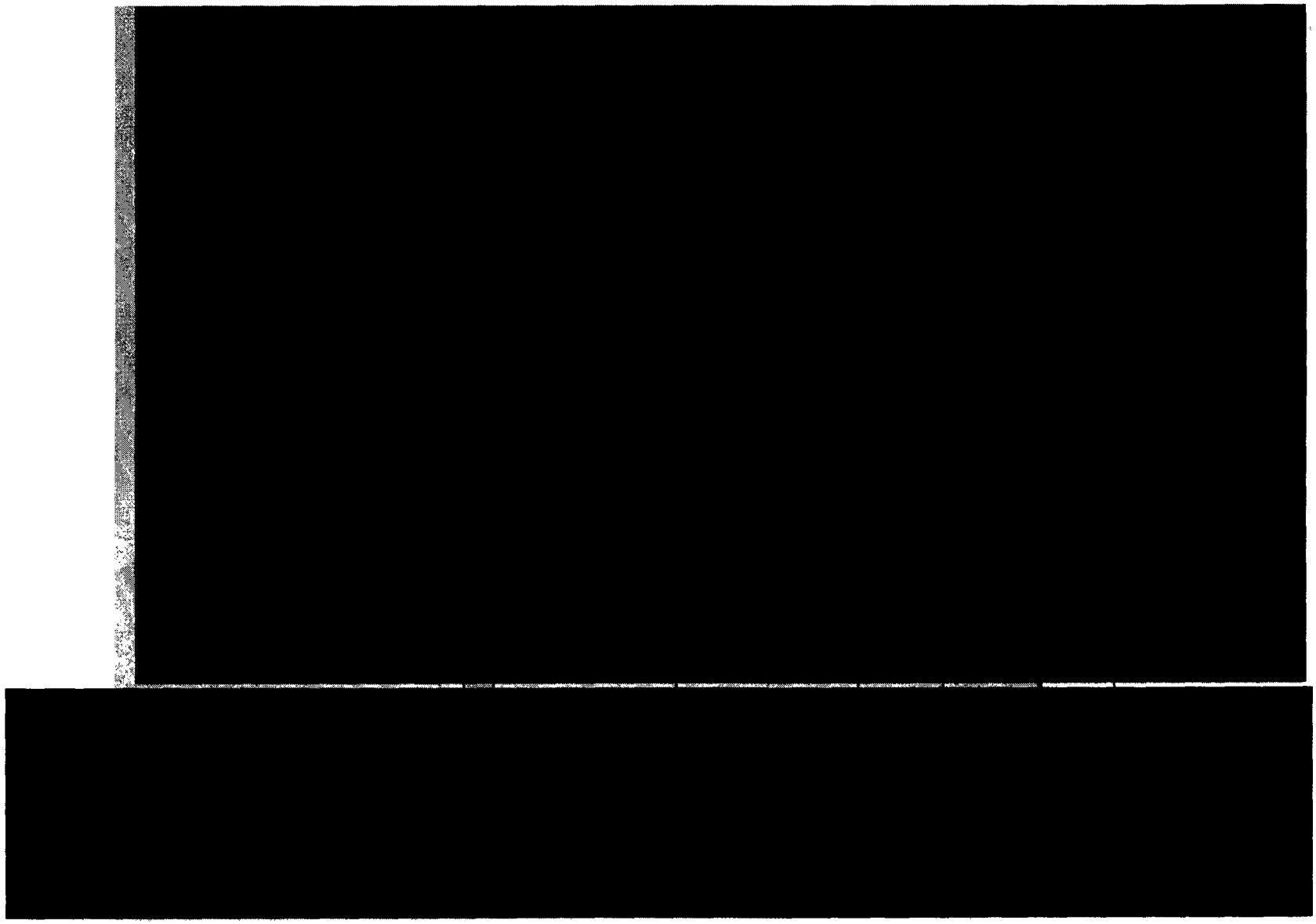


Integration and Test Approach – System Integration

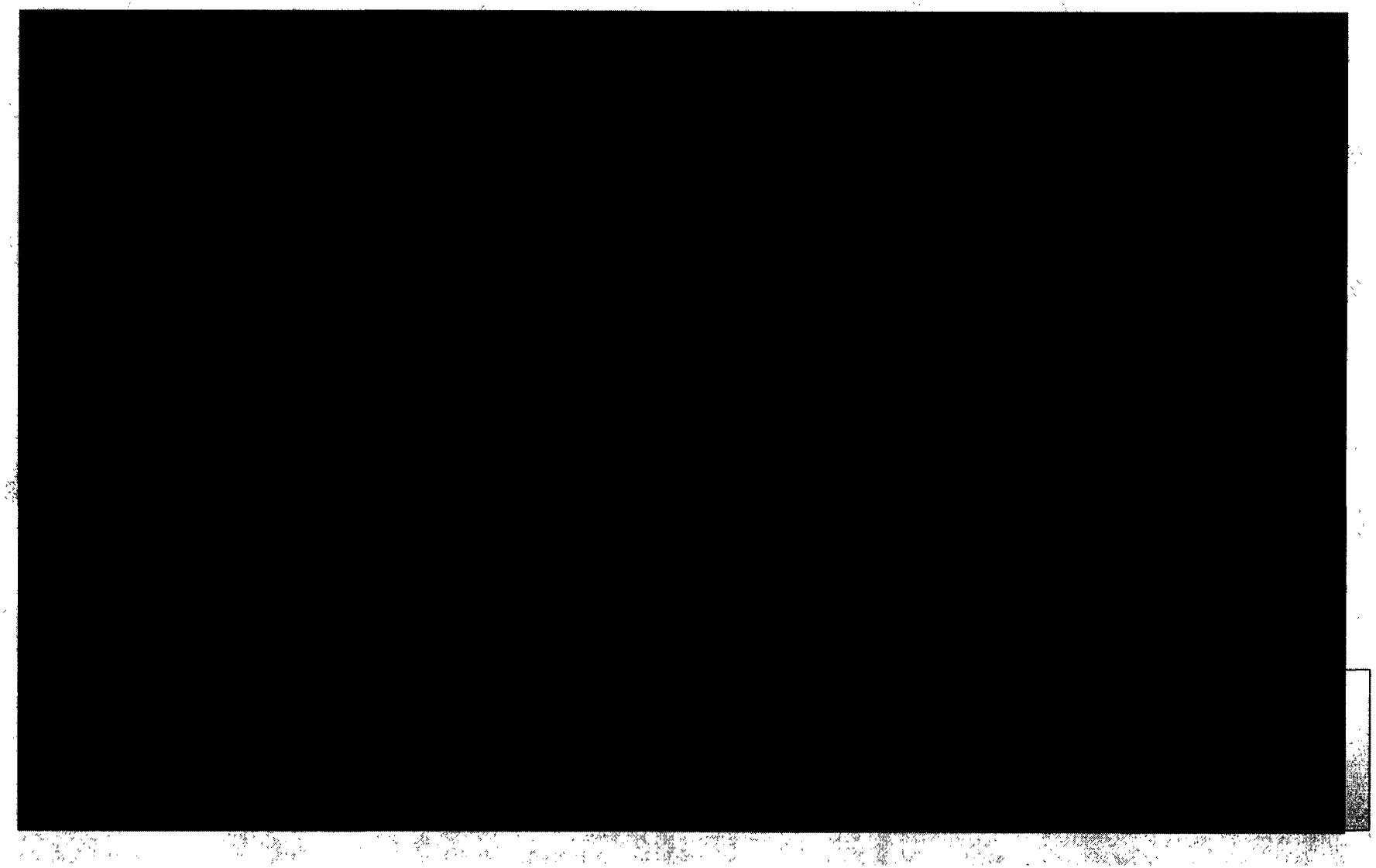
Integration and Test Environment



Iterative Test Approach



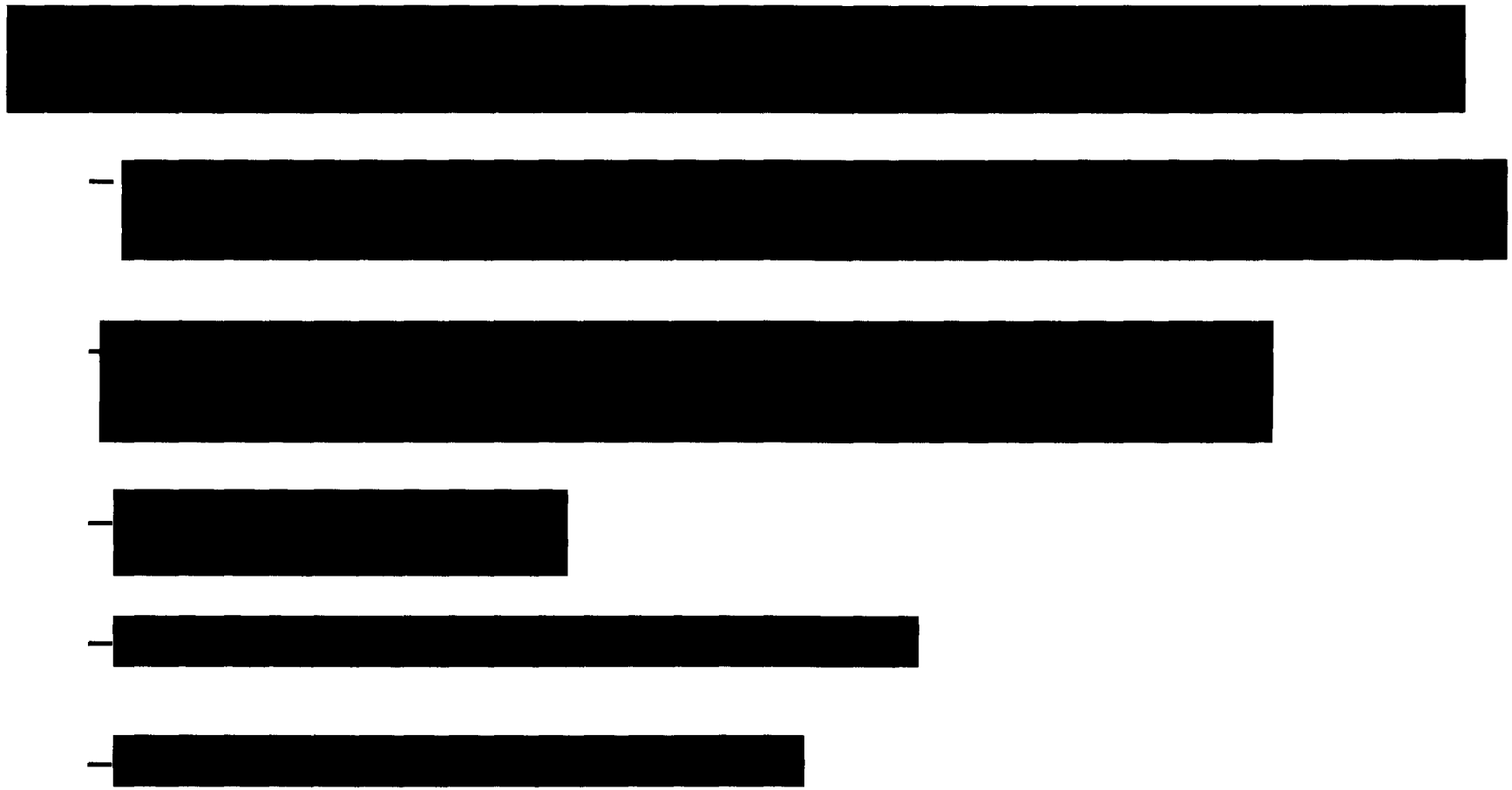
Test Artifact Hierarchy



Preliminary System Test Procedures

Preliminary Installation Acceptance Test Procedures

Integration and Test – Forward Plan



BREAK

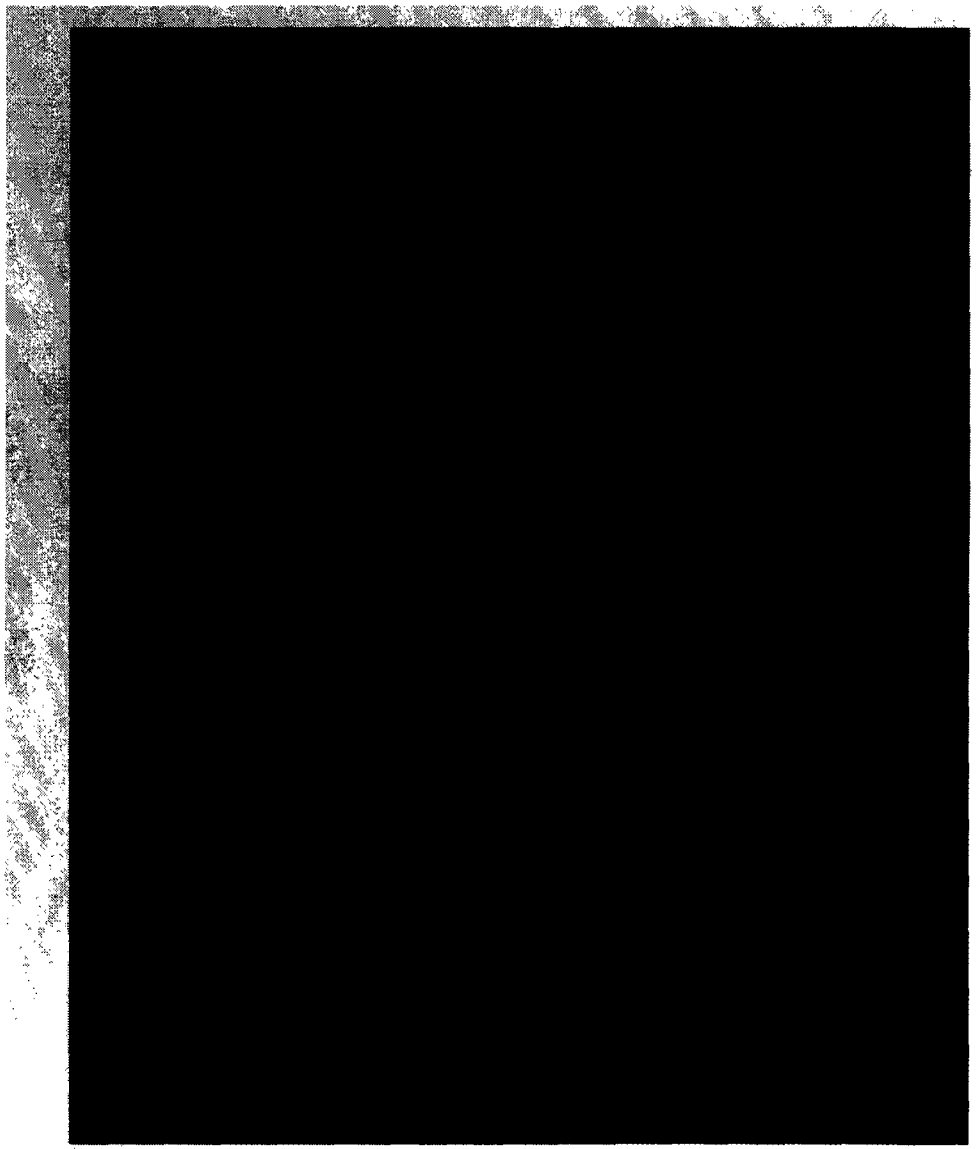
ERA SDR – DAY FOUR

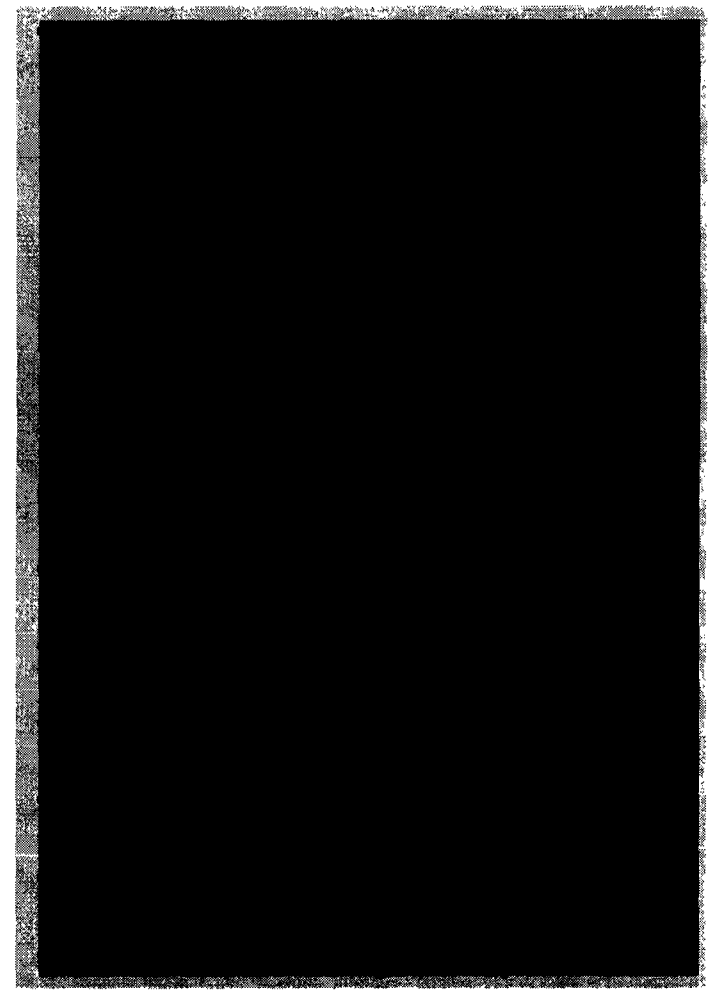
Trade Studies Summary

[redacted]

May 12, 2005

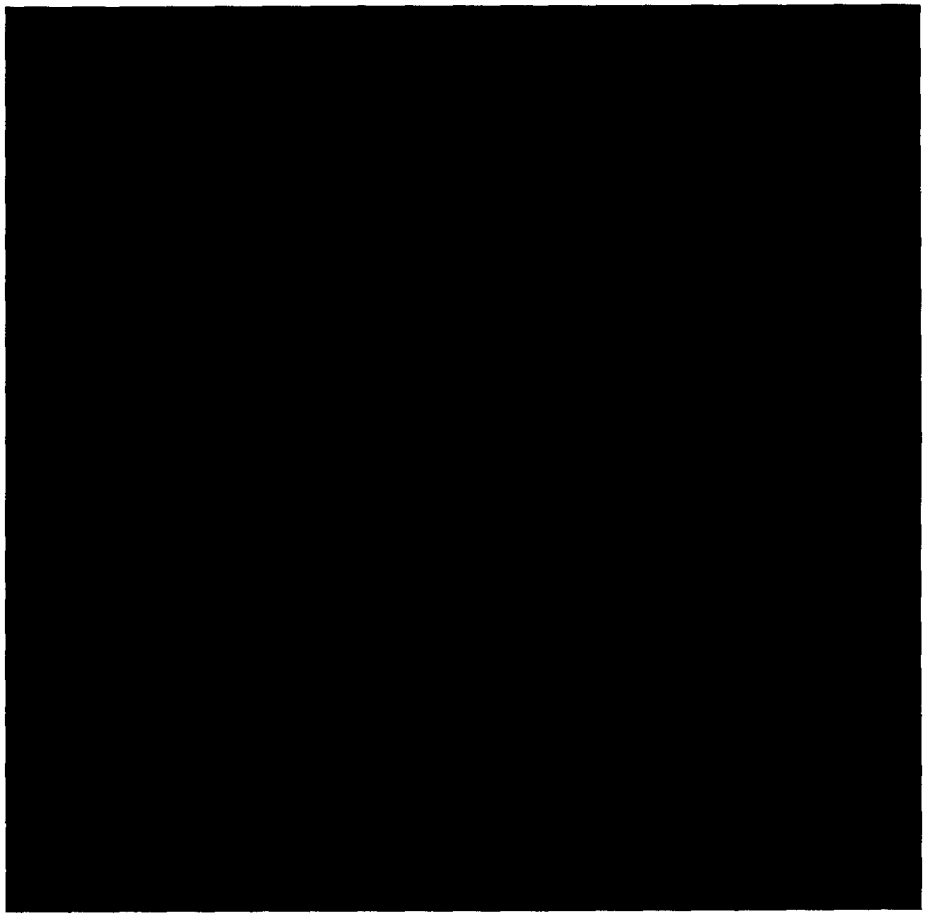
Trade Studies Methodology

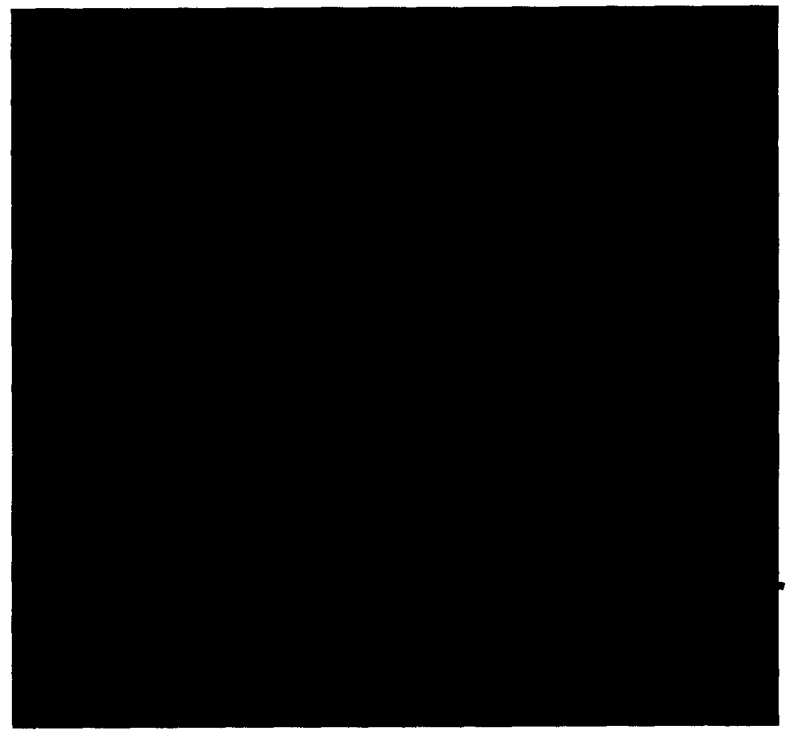




Methodology – Evaluation Criteria

Trade Studies – Status





Enterprise Infrastructure Software

Storage Management Software

Database Software

Enterprise Identity Management Software

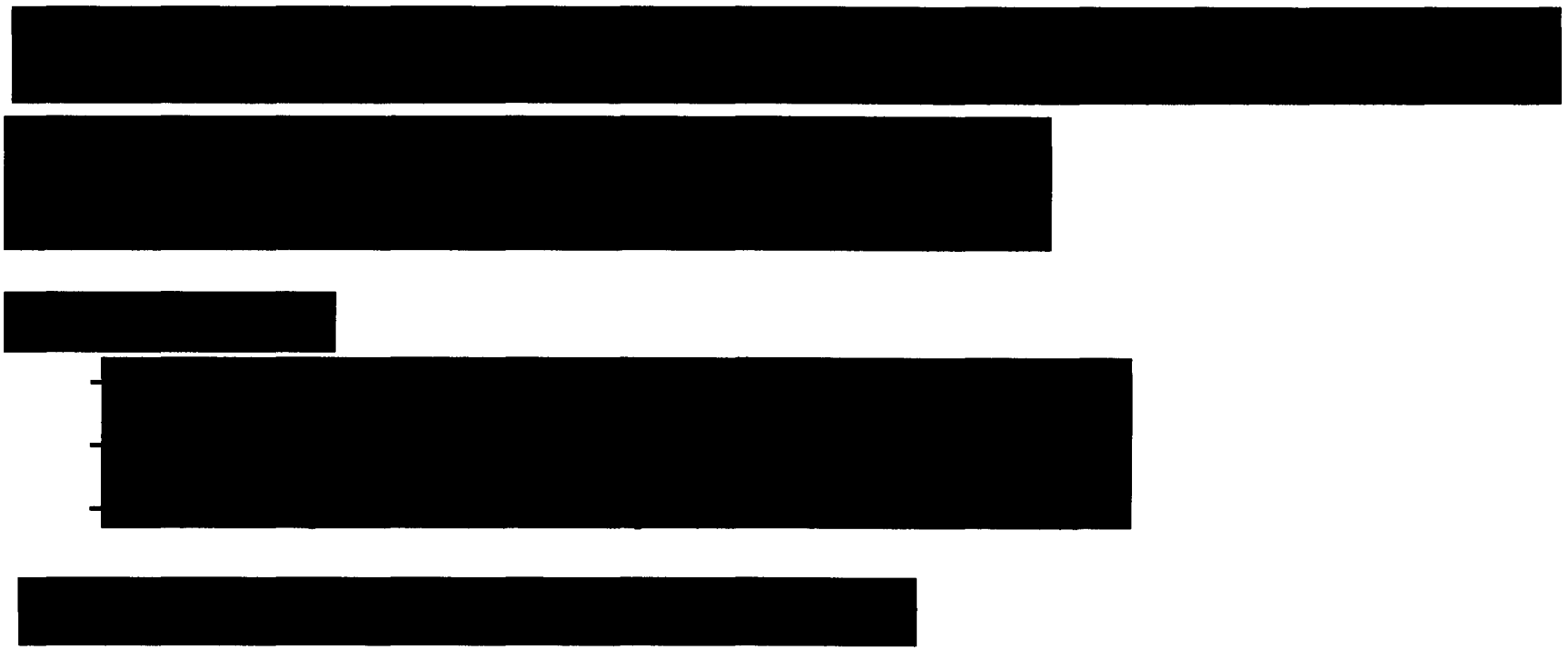
[redacted]

Search Software

[redacted]

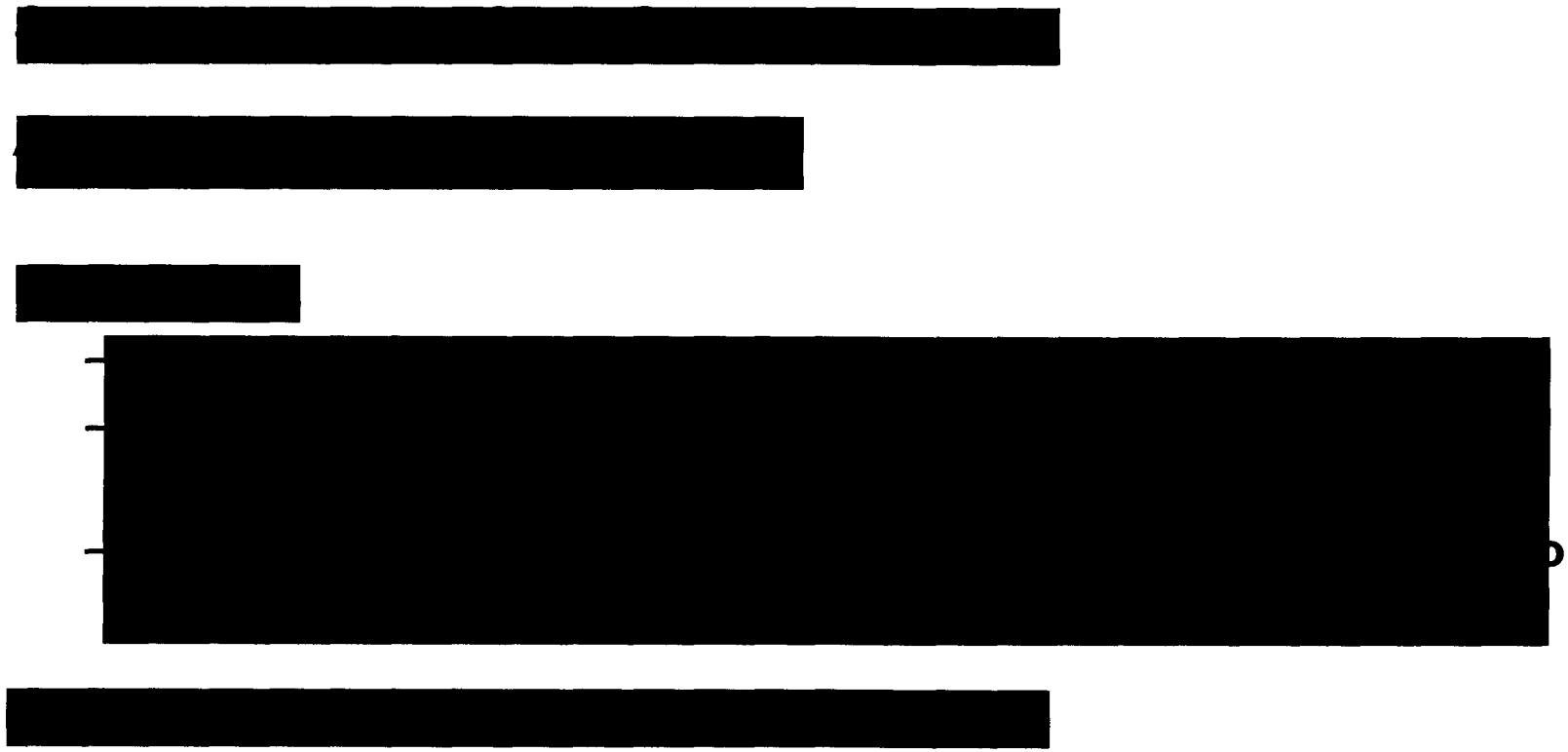
Security Compliance Management Software

Network Devices



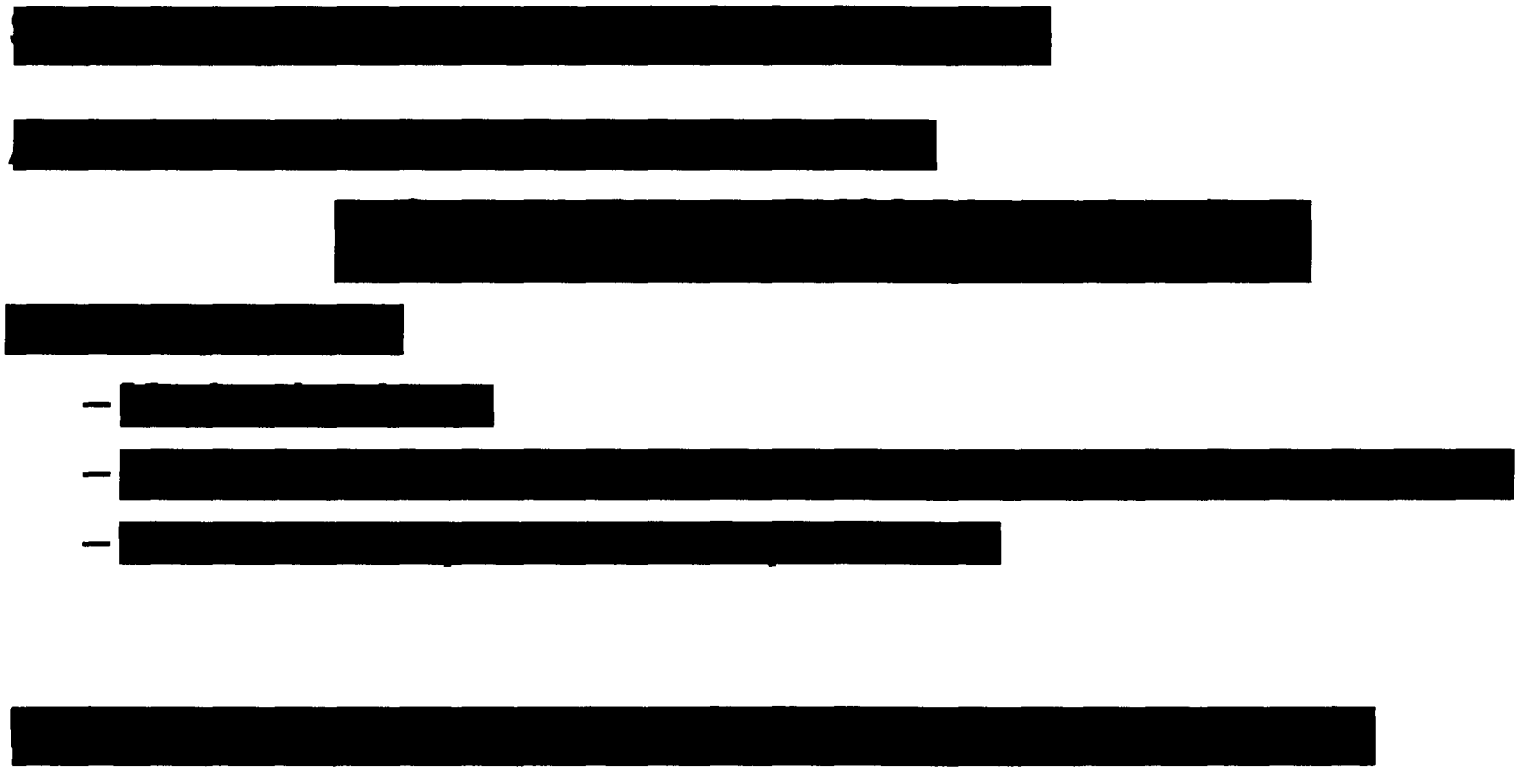
Sever Hardware & Operating System

Development Environment



Automated IT Management Software

Configuration Management Software



Trade Study – Forward Plan

Trade Study – RIDs

[redacted]

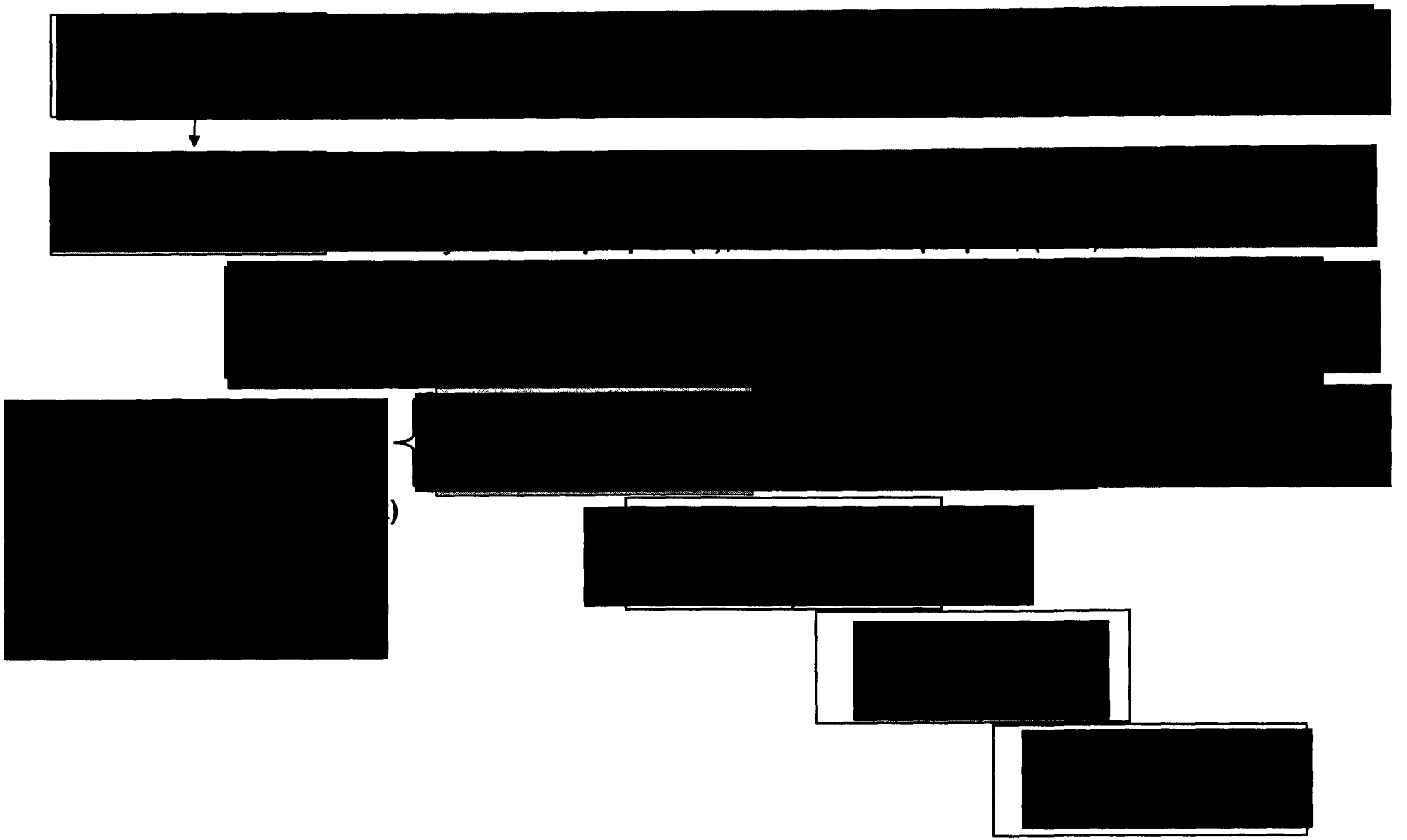
ERA SDR – DAY FOUR

Increment/Release Requirements & Design Reviews

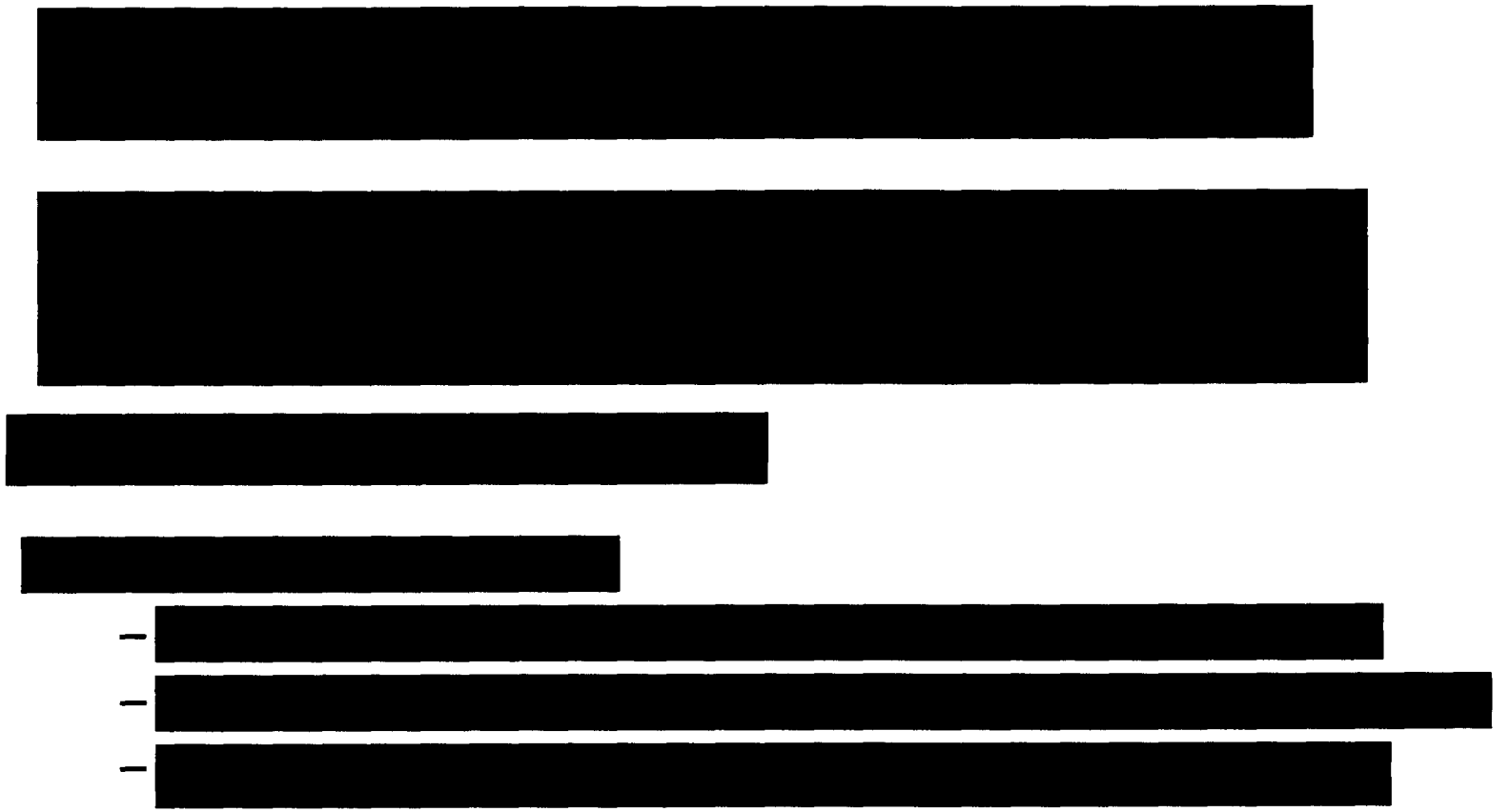
Bill Harris

May 12, 2005

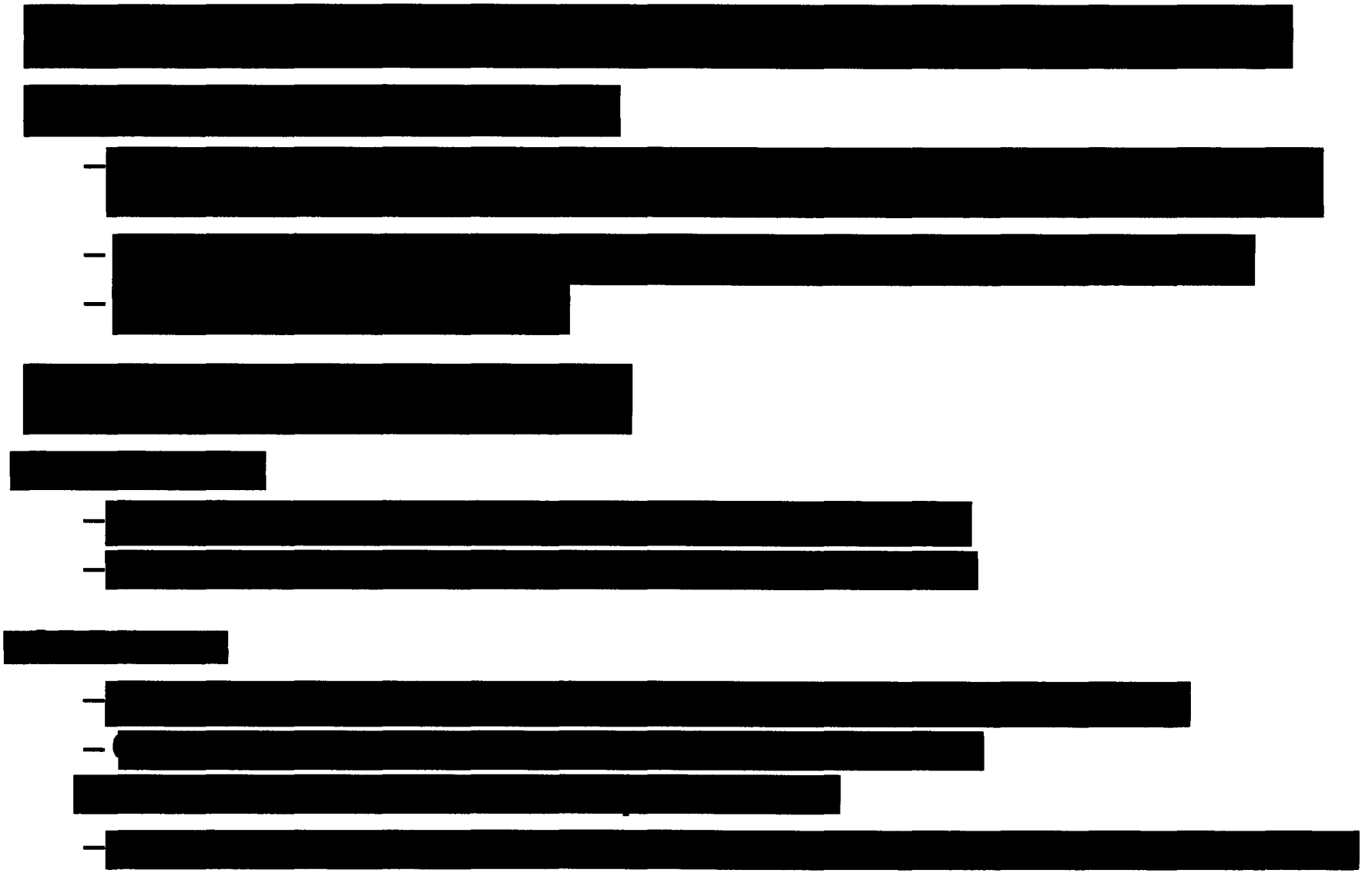
Engineering Methodology



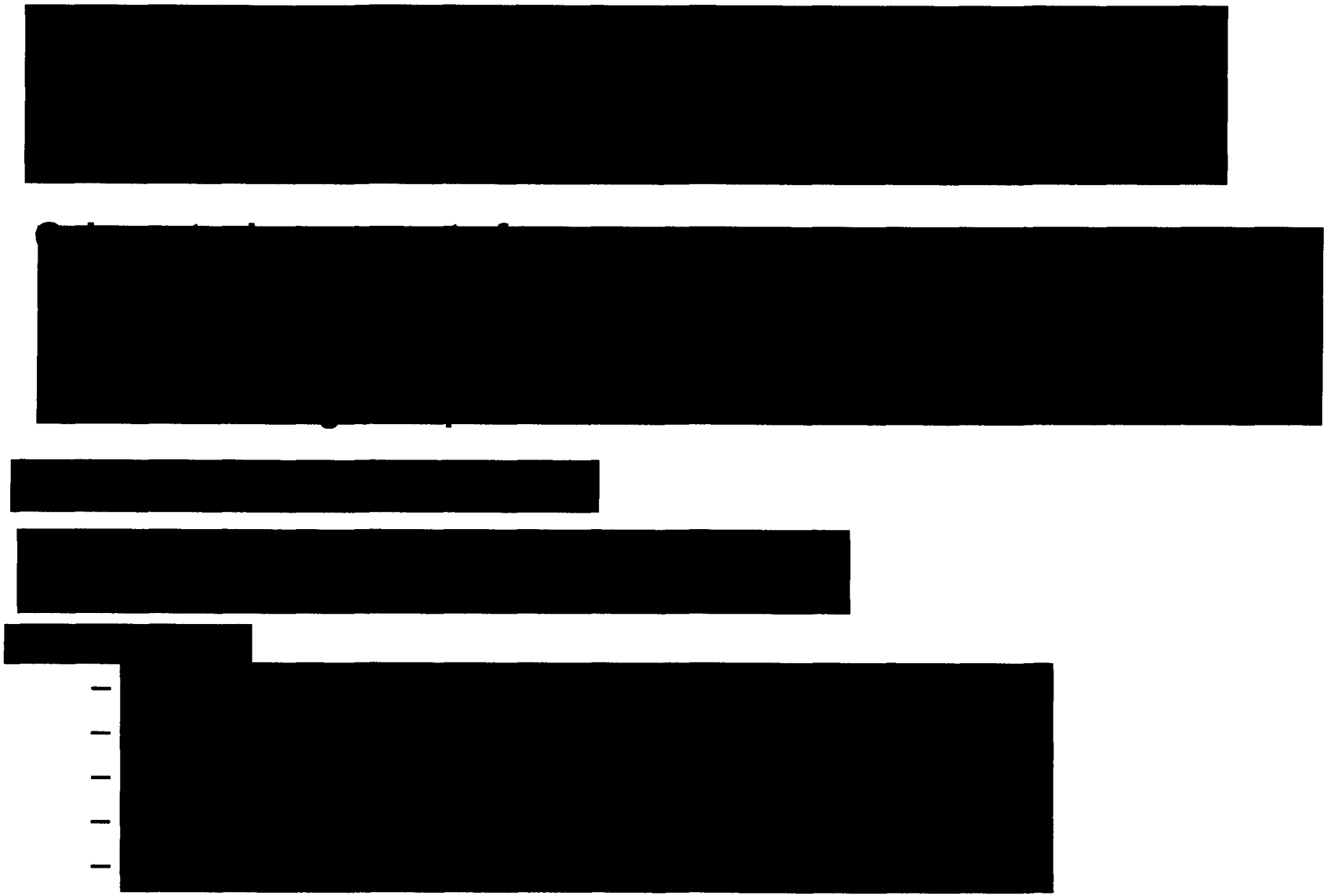
System Requirements Review (SRR)



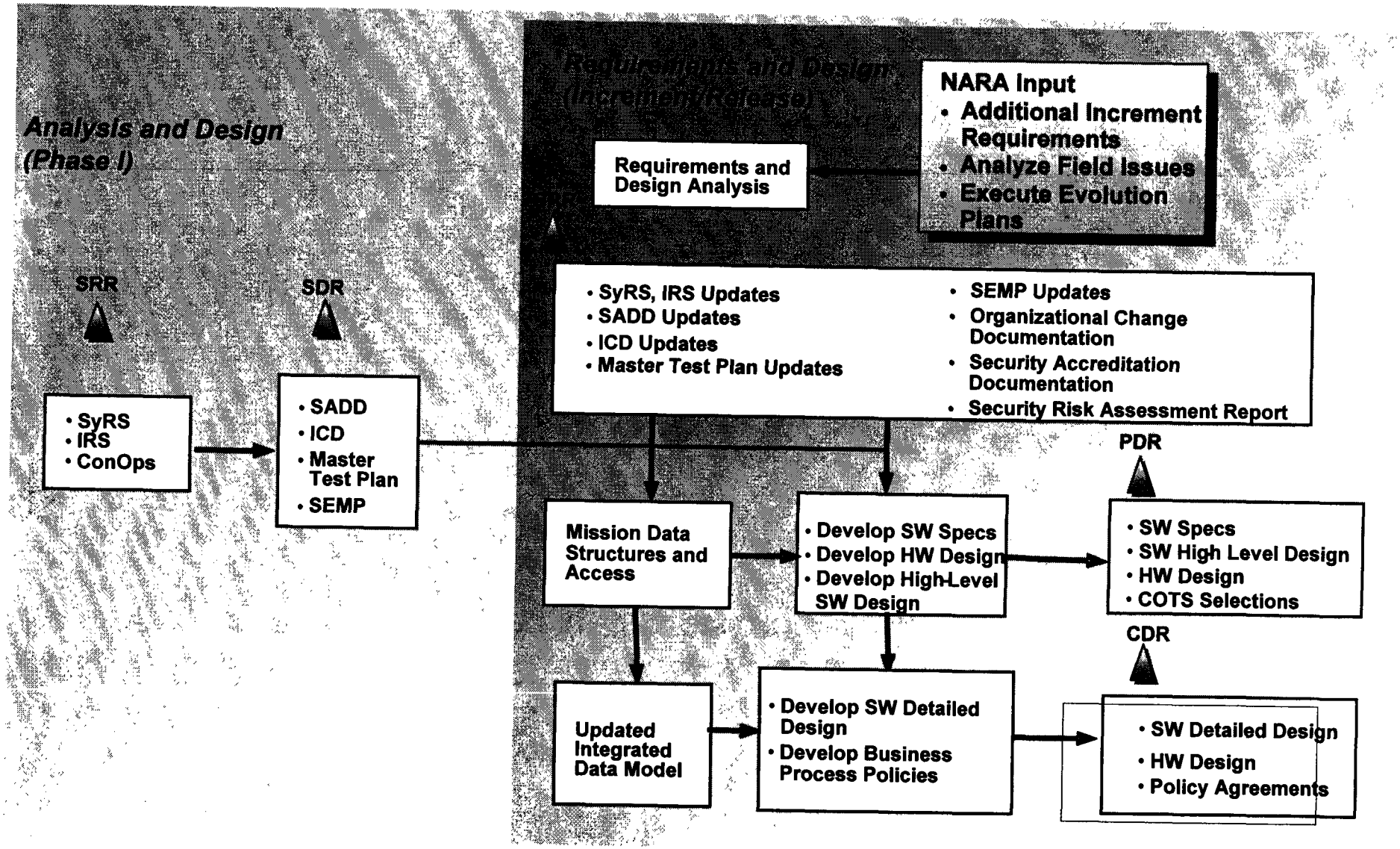
Preliminary Design Review (PDR)



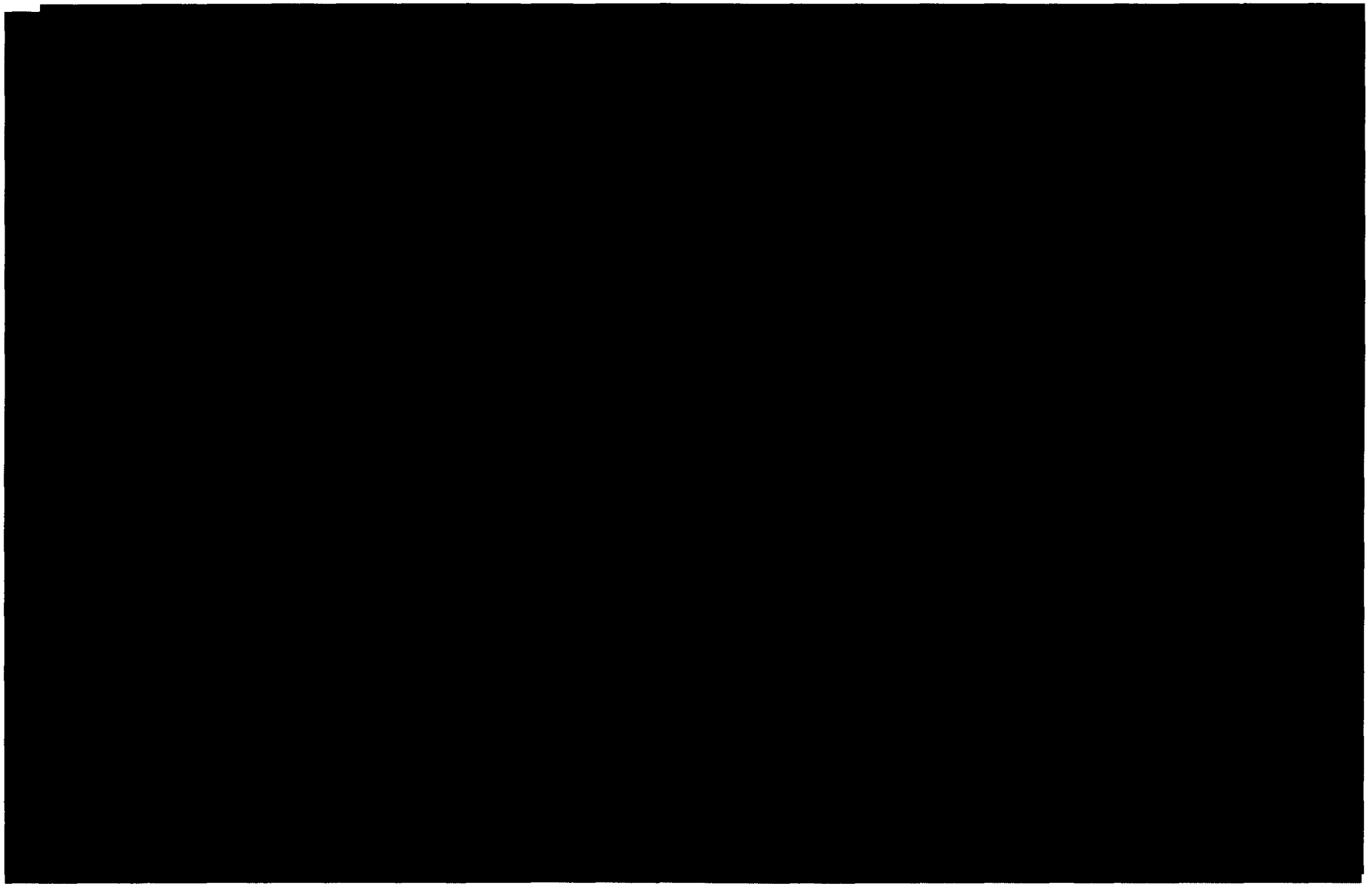
Critical Design Review (CDR)



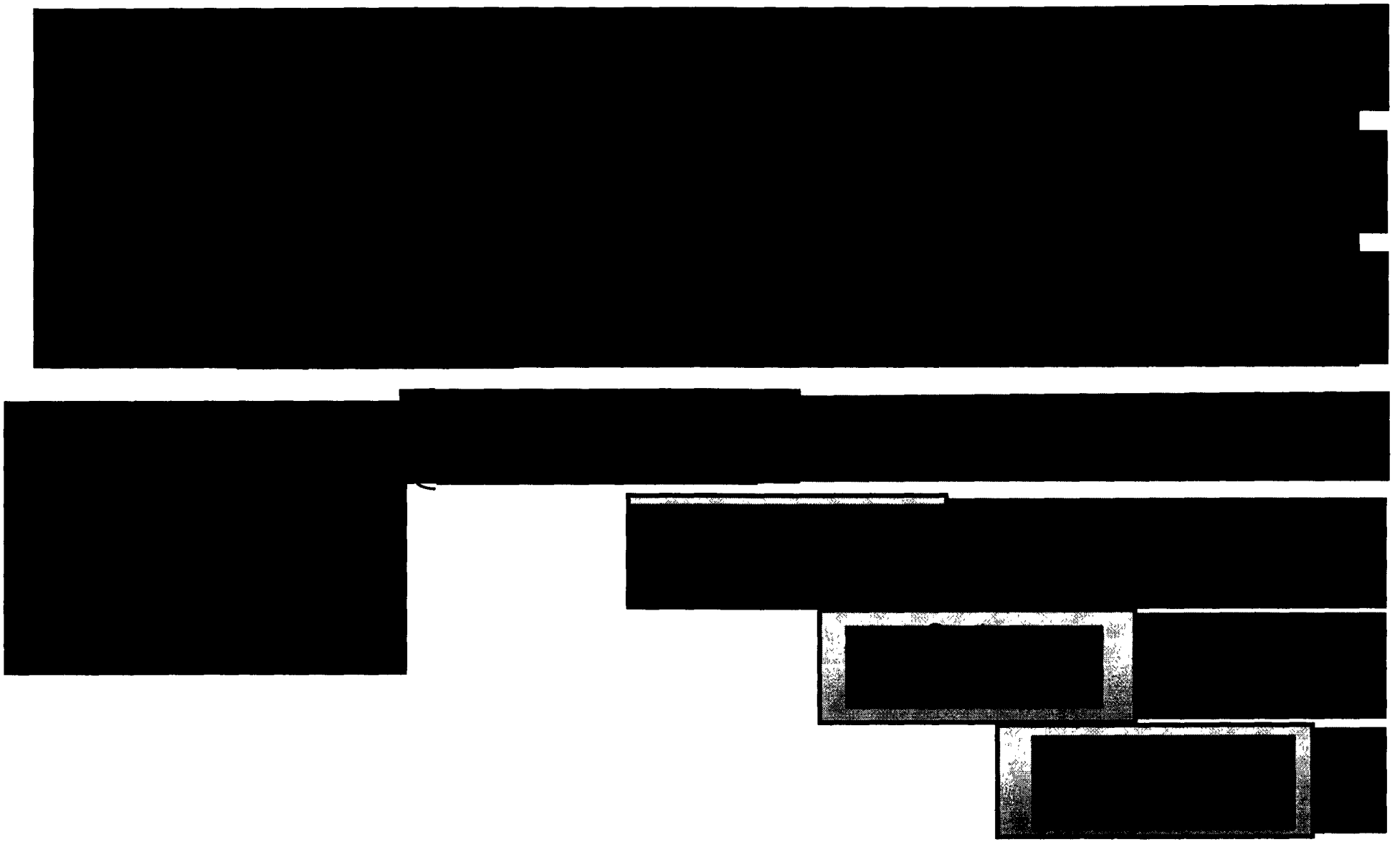
Increment/Release Requirements and Design



Specification Tree



Following Increment Requirements and Design



Closing Remarks