Distributed
European
Infrastructure for
Supercomputing
Applications

DEISA security overview

Jules Wolfrat (SARA)
OSCT
Amsterdam
23 March, 2010

www.deisa.eu

SEVENTH FRAMEWORK PROGRAMME
e-infrastructure
RI-222919

Agenda

Advancing the European HPC Infrastructure and Services

- Objectives and Strategy
- Inventory of Services and Resources

Organization as a Virtual Distributed HPC Centre

Security

- Policies
- General security policies
- Organization

Objectives & Strategy for HPC in Europe

Distributed
European
Infrastructure for
Supercomputing
Applications

EU FP6 objective

European Strategy Forum
on Research Infrastructures

ESFRI

EUROPEAN ROADMAP
FOR RESEARCH
INFRASTRUCTURES

Report 2006

EU FP7 objective

Establishing a persistent European HPC ecosystem that integrates national (tier-1) HPC centres and new large European Petascale (tier-0) centres

DEISA strategy

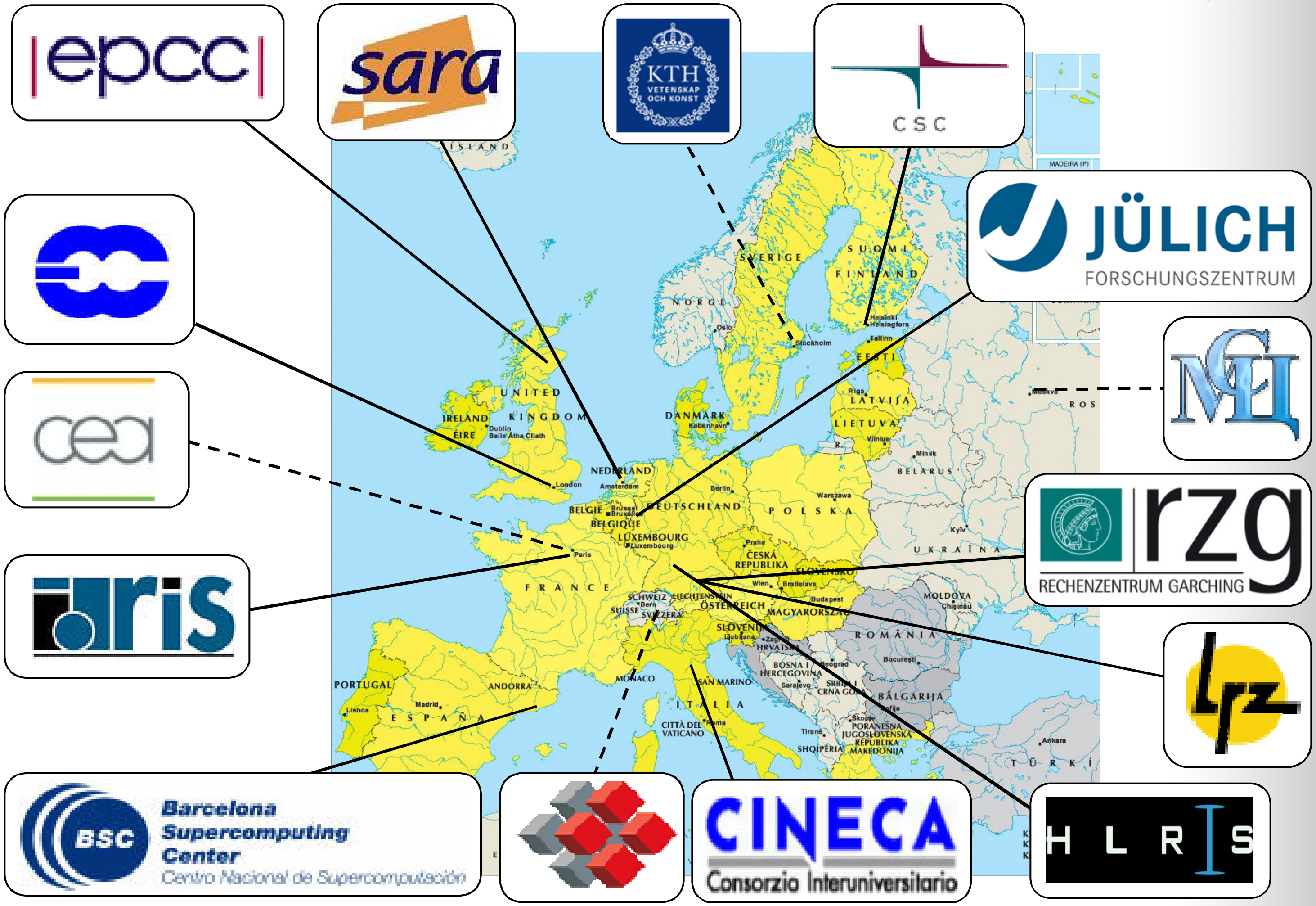
building a European HPC Service on top of existing national HPC services. This service is based on the deployment and operation of a persistent, production quality, distributed supercomputing environment with continental scope

DEISA2 strategy

Consolidate the existing DEISA HPC infrastructure and services and **deliver a turnkey ready operational solution for the future European HPC ecosystem**

Distributed
European
Infrastructure for
Supercomputing
Applications

DEISA Partners



15 partners, 10 countries, EC support 2004-2011

DEISA Supercomputers

State-of-the art supercomputers

> 2 PF aggregated peak performance

- Cray XT4/5, Linux
- IBM Power6, AIX / Linux
- IBM BlueGene/P, Linux
- IBM PowerPC, Linux
- SGI ALTIX 4700, Linux
- NEC SX9 vector system, Super UX
- Bull & NEC Intel Nehalem clusters

Fixed fractions of resources dedicated to DEISA usage

Core Infrastructure and Services

Dedicated High Speed (10Gb/s) Network

Global Data Management

- High performance I/O and data sharing with a global file system (IBM GPFS)
- high performance transfers of large data sets (gridFTP)

Common AAA

- Single sign on (gsi-ssh, Middleware)
- Common Project and User Administration
- Accounting
- Project progress monitoring and controlling

User-related Operational Infrastructure

- DEISA Common Production Environment (DCPE)
- Job management service
- Common user support and central help desk

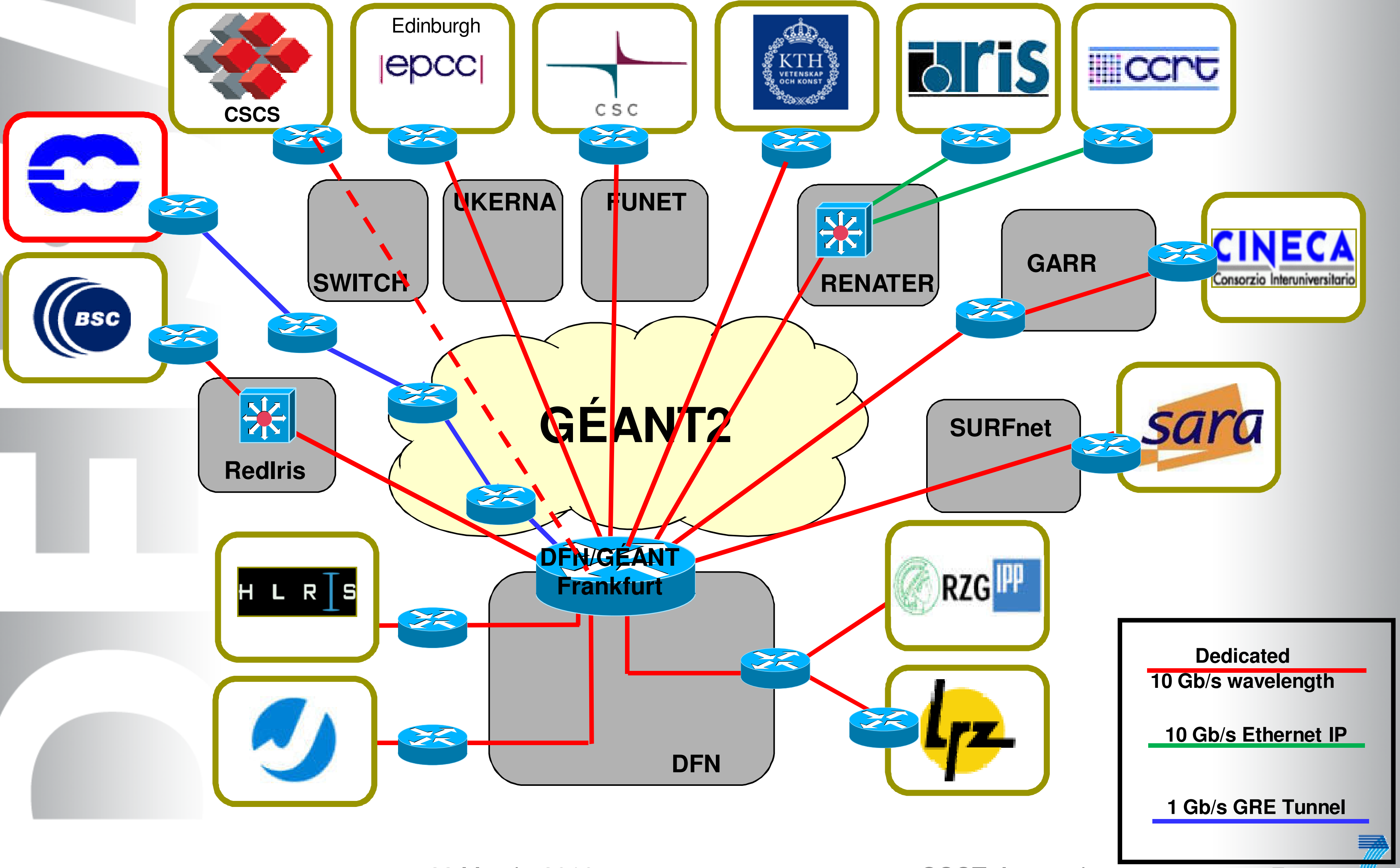
System-related Operational Infrastructure

- Common monitoring and information systems
- Common system operation

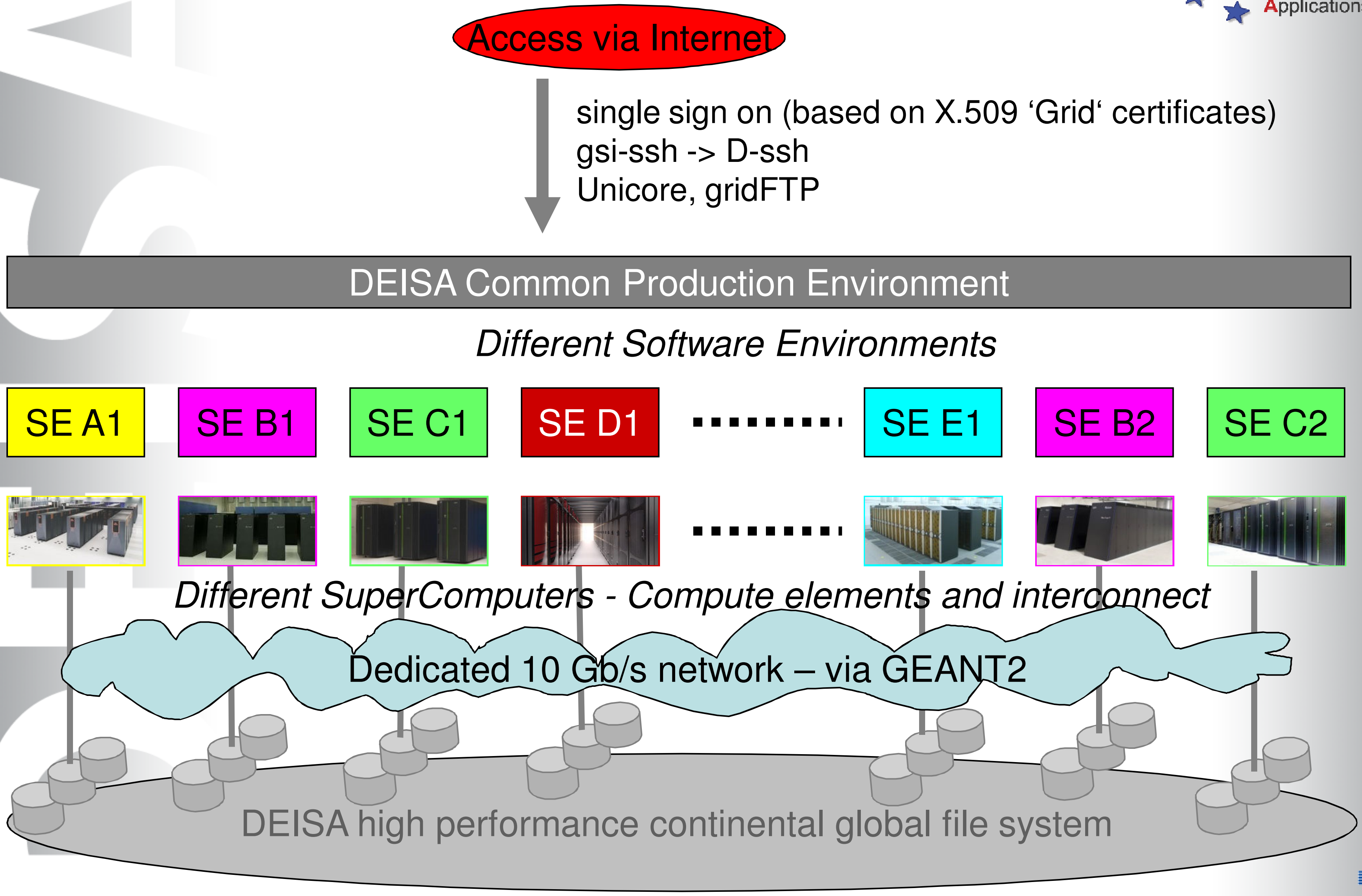
Global Application Support

Global Project and Resource Allocation Management

Dedicated high speed network (10 Gb/s)



Unified Access and Use of HPC Resources



Access via Internet

single sign on (based on X.509 ‘Grid‘ certificates)
gsi-ssh -> D-ssh
Unicore, gridFTP

DEISA Common Production Environment

Different Software Environments

SE A1 | SE B1 | SE C1 | SE D1 | .... | SE E1 | SE B2 | SE C2

Different SuperComputers - Compute elements and interconnect

Dedicated 10 Gb/s network – via GEANT2

DEISA high performance continental global file system

DEISA Extreme Computing Initiative

Projects from DECI calls 2005, 2006, 2007, 2008, 2009

Involvement of over 180 research institutes and universities from 25 European countries:

Austria Belgium Cyprus Denmark Finland
France Germany Greece Hungary Ireland
Italy Latvia Norway Poland Portugal
Romania Russia Slovac Rep. Spain Sweden
Switzerland Netherlands Turkey Ukraine UK

with collaborators from four other continents

North America, South America, Asia, Australia

Projects and Science Communities

DECI call 2005	
29 proposals accepted	12 mio core-h granted*
DECI call 2006	
28 proposals accepted	12 mio core-h granted*
DECI call 2007	
45 proposals accepted	30 mio core-h granted*
DECI call and Science Communities 2008	
42 proposals accepted	50 mio core-h granted*
3 communities	5 mio core-h granted*
DECI call and Science Communities 2009	
50 proposals accepted	60 mio core-h granted*
7 communities	12 mio core-h granted*

*) Core-h normalized to IBM P4+@1.7GHz

DECI: DEISA Extreme Computing Initiative
Yearly call for proposals

Communities: Virtual Scientific Communities

Distributed
European
Infrastructure for
Supercomputing
Applications

Science Communities Support

Life Sciences

VIROLAB

Virtual Physiological Human
network of excellence

Fusion Energy Research

EFDA
EUROPEAN FUSION DEVELOPMENT AGREEMENT

EUFORIA

Space Science / Cosmology

esa planck

VIRGO

Climate Research

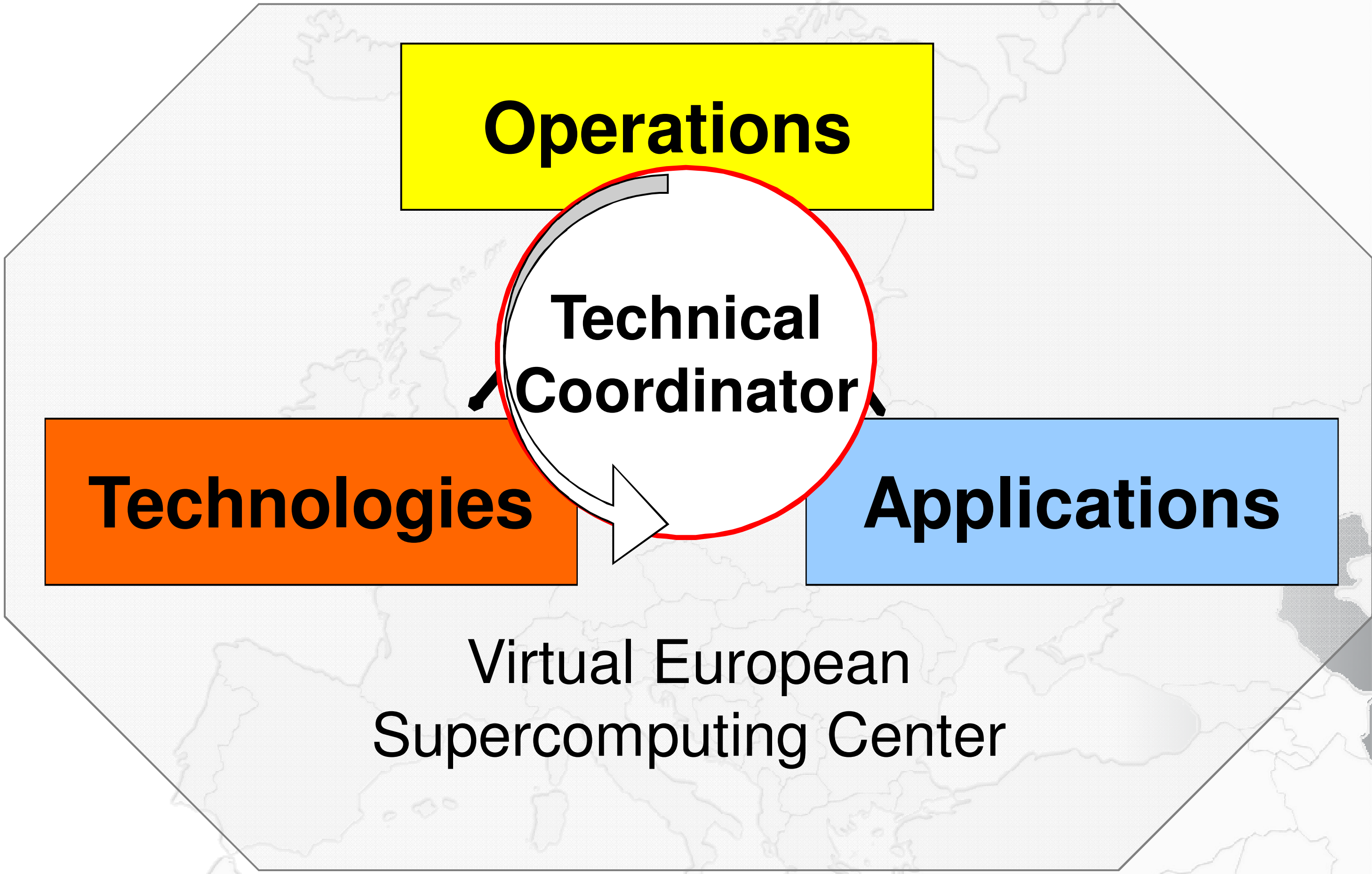
enes
European Network for Earth System Modelling

2008 3 communities 5 mio core-h granted*

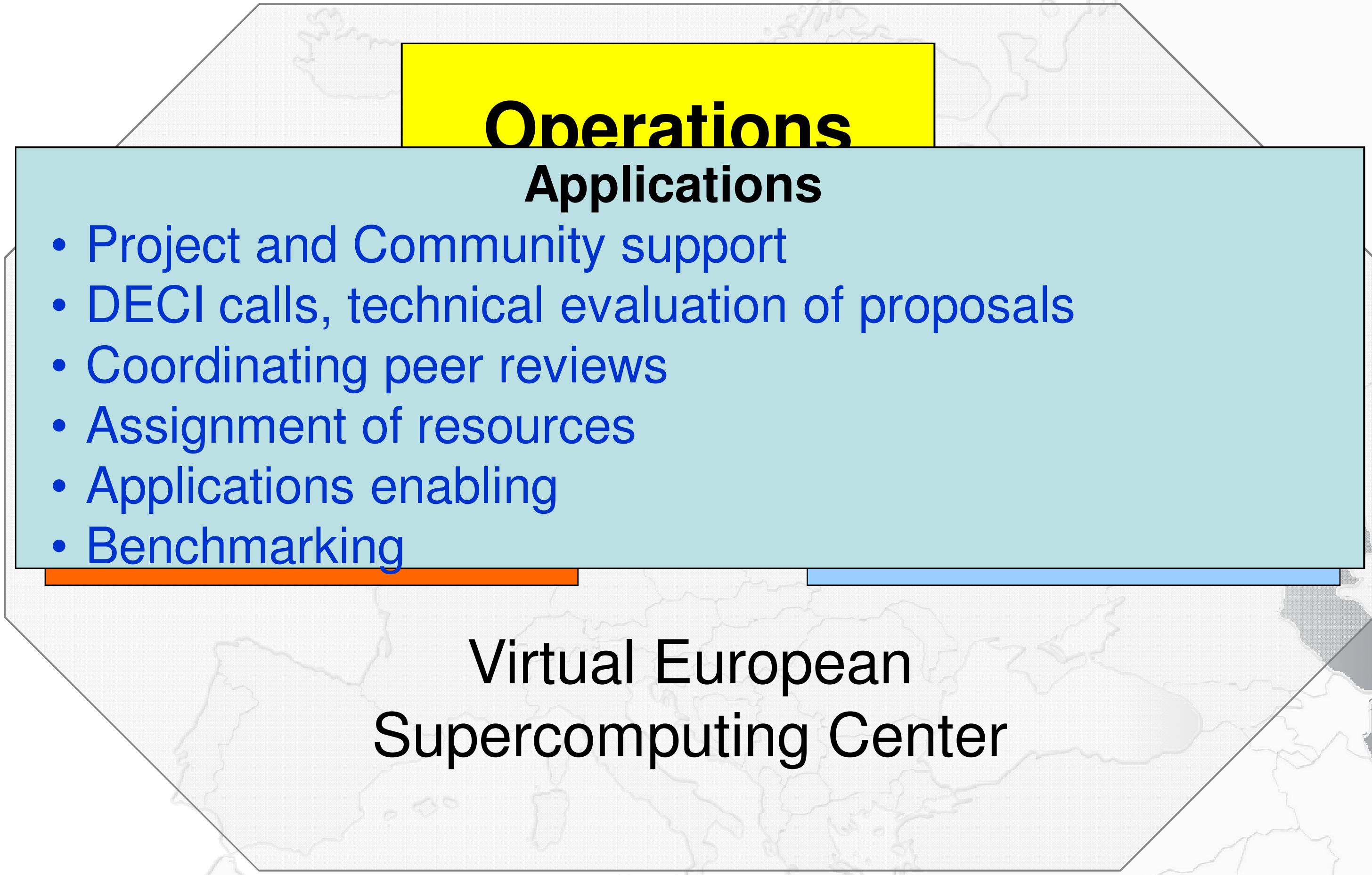
2009 7 communities 12 mio core-h granted*

Virtual European Supercomputing Centre

Technical Coordinator



Virtual European Supercomputing Centre



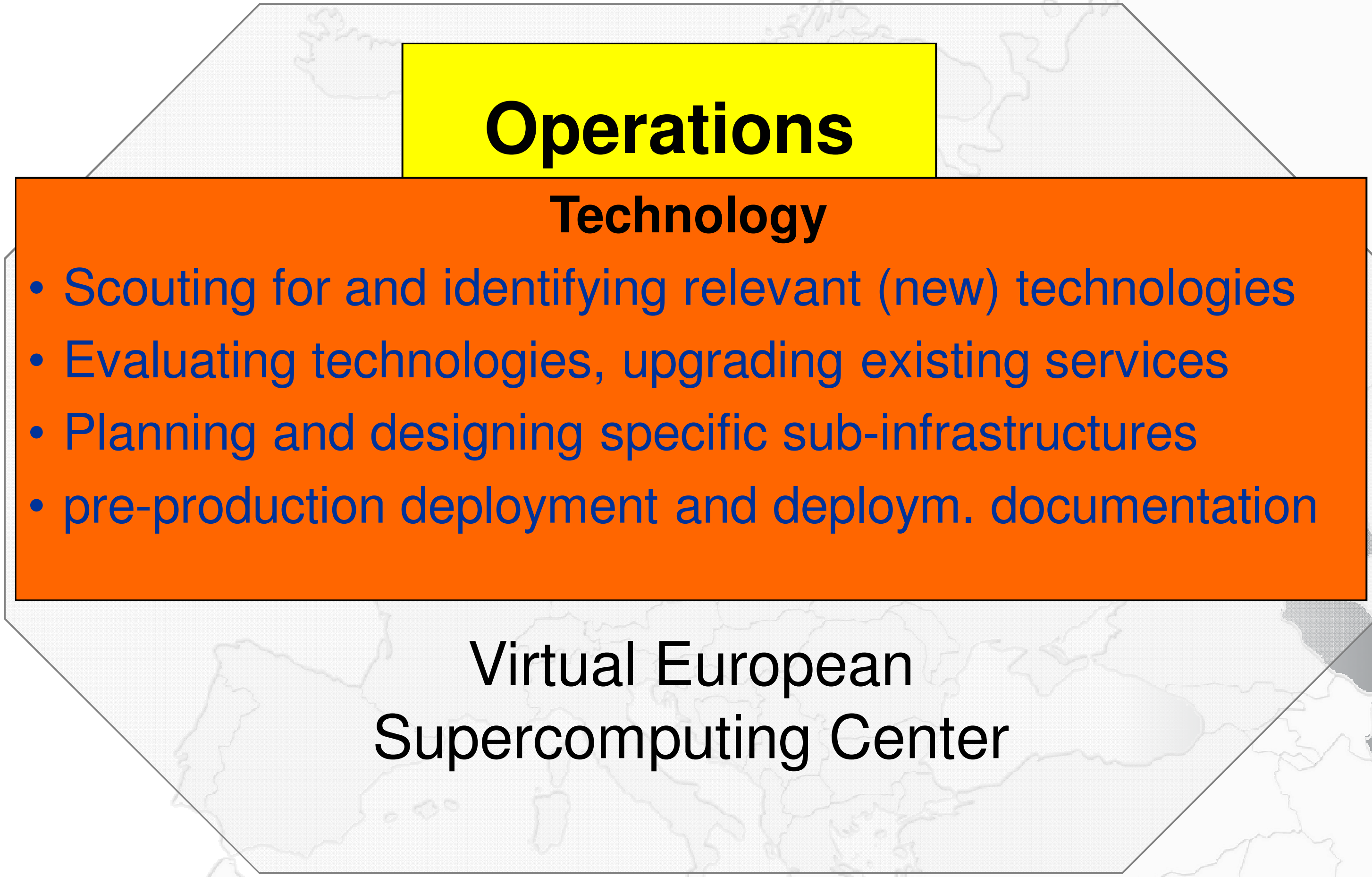
Operations

Applications

- Project and Community support
- DECI calls, technical evaluation of proposals
- Coordinating peer reviews
- Assignment of resources
- Applications enabling
- Benchmarking

Virtual European
Supercomputing Center

Virtual European Supercomputing Centre



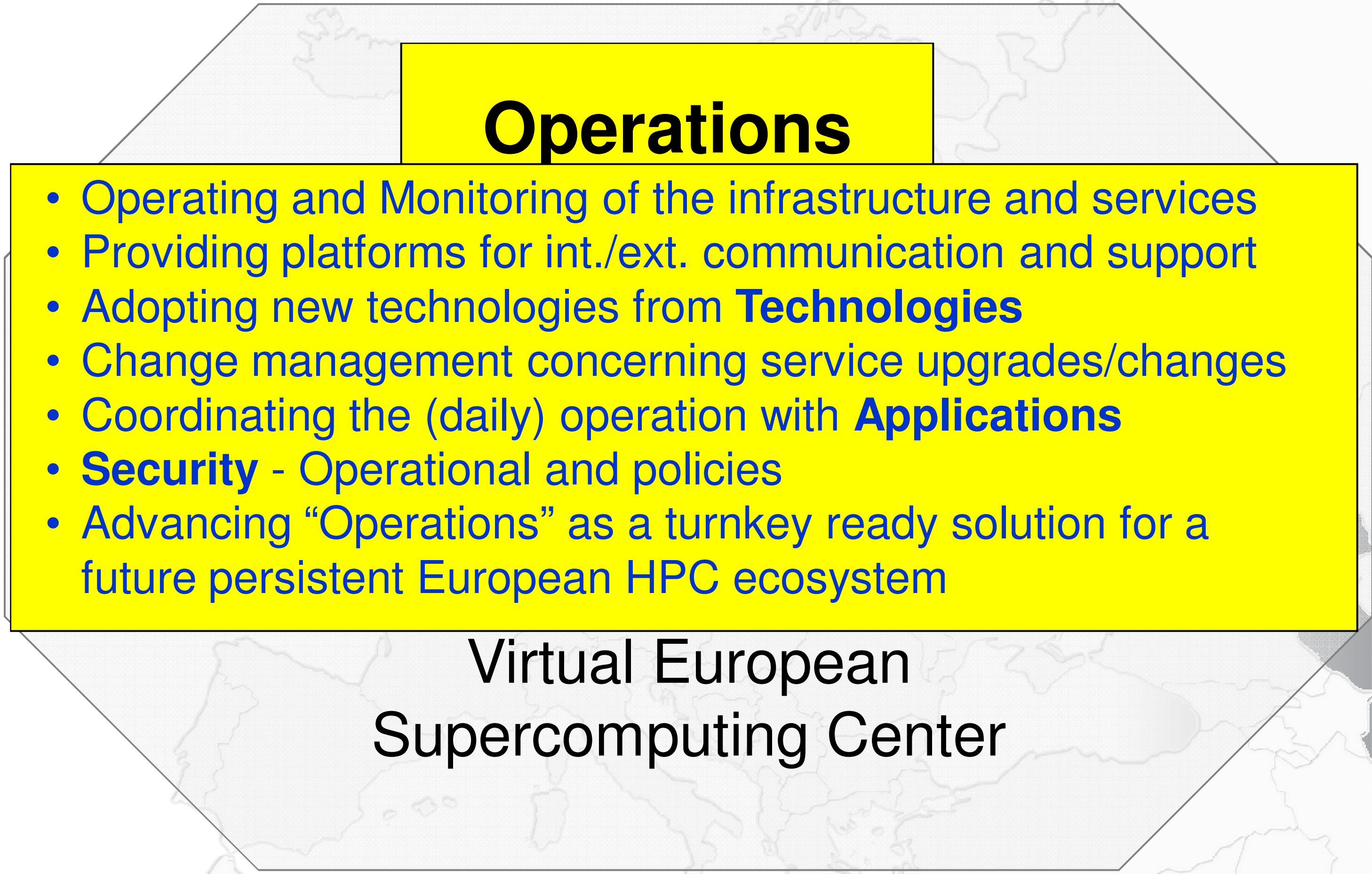
Operations

Technology

- Scouting for and identifying relevant (new) technologies
- Evaluating technologies, upgrading existing services
- Planning and designing specific sub-infrastructures
- pre-production deployment and deploym. documentation

Virtual European
Supercomputing Center

Virtual European Supercomputing Centre



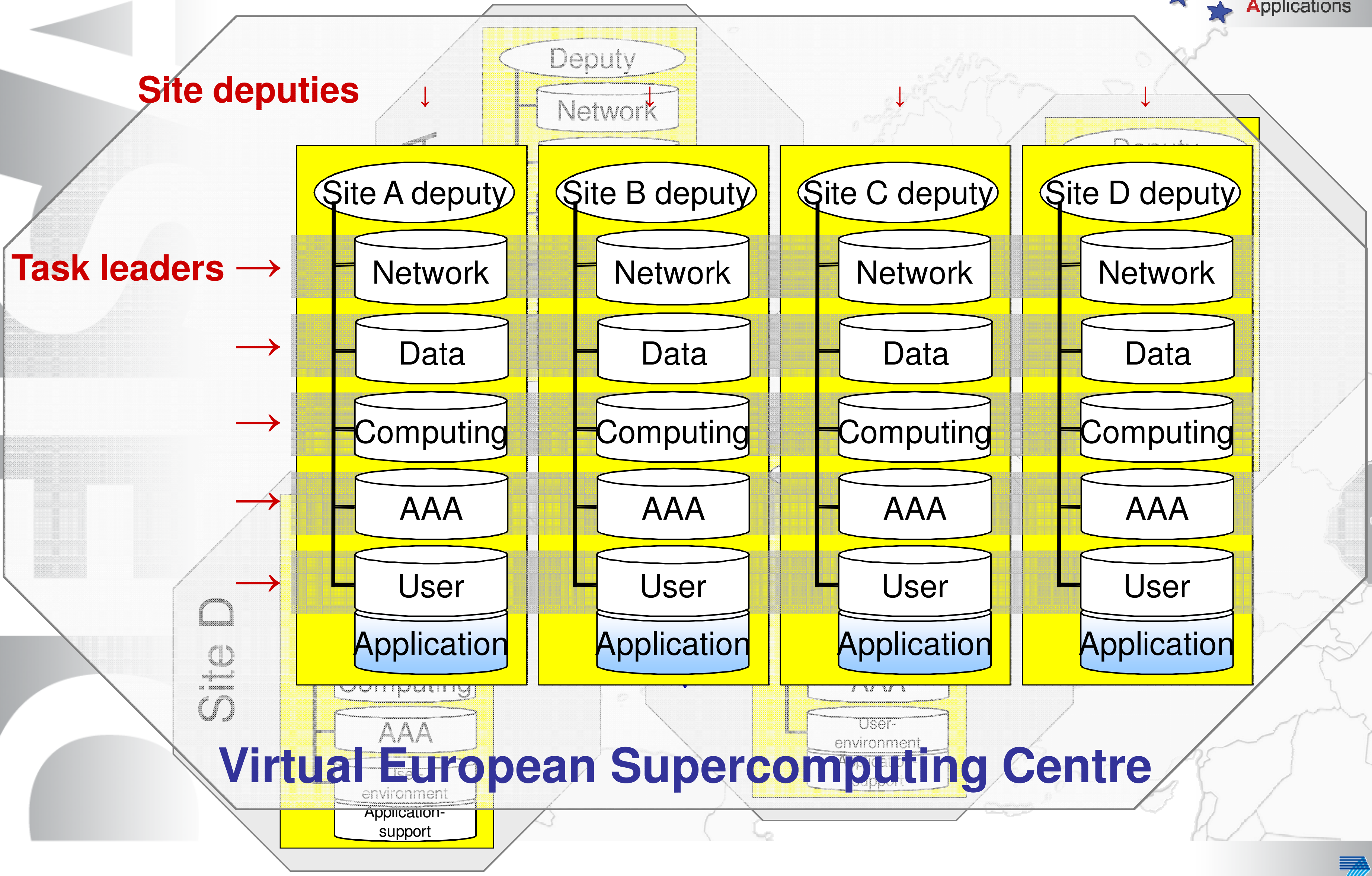
Operations

- Operating and Monitoring of the infrastructure and services
- Providing platforms for int./ext. communication and support
- Adopting new technologies from **Technologies**
- Change management concerning service upgrades/changes
- Coordinating the (daily) operation with **Applications**
- **Security** - Operational and policies
- Advancing "Operations" as a turnkey ready solution for a future persistent European HPC ecosystem

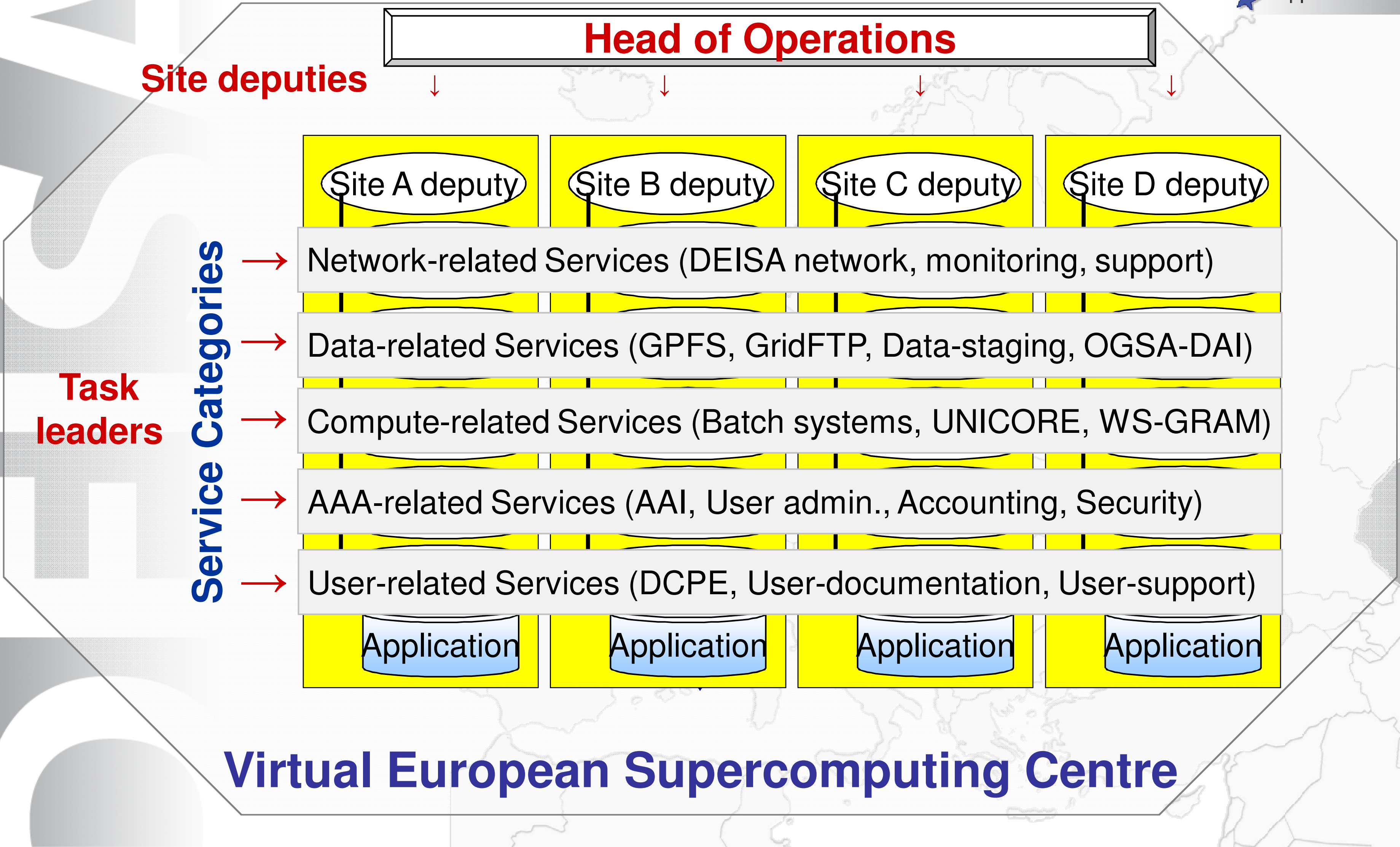
Virtual European
Supercomputing Center

Federated Operation of DEISA

Distributed European Infrastructure for Supercomputing Applications



Federated Operation of DEISA



Head of Operations

Site deputies

Site A deputy

Site B deputy

Site C deputy

Site D deputy

Task leaders

Service Categories

Network-related Services (DEISA network, monitoring, support)

Data-related Services (GPFS, GridFTP, Data-staging, OGSA-DAI)

Compute-related Services (Batch systems, UNICORE, WS-GRAM)

AAA-related Services (AAI, User admin., Accounting, Security)

User-related Services (DCPE, User-documentation, User-support)

Virtual European Supercomputing Centre

Security

Policies

Acceptable Use Policy - based on JSPG version

- On top of local policies (contract between user and partner)

User administration policy – counterpart of VOMS administration policy

Change management

- Policy for adopting new technologies or technology upgrades

General Security Policies

General security policies (1)

- Definition of a policy framework
- Based on three basic principles

1. Trust between partners
   - It is expected that each partner already has implemented a security policy which guarantees a certain level of reliable services. This has been the assumption from the start of DEISA because nobody expects that one of the centers can afford it to be exposed to vulnerabilities, although the level of acceptable risks may differ between partners.

General security policies (2)

2. Common policy (Consensus)
   - Any consortium of individual organizations, like DEISA, working closely together, will need political decisions and service level agreements, which have to be based on information exchange on hardware and software changes. This information exchange is essential for any local IT security analysis and policy decisions.
   - Changing hard- and/or software at one site may influence IT security risks at other sites. Decisions on accepting increased security risks can not be imposed on sites. The common security policy of the whole consortium has to be defined and accepted by all sites.

General security policies (3)

3. Limited scope of risk assessments
   - Though one can argue that any new or changed software and/or service can and will generate new risks, and therefore any change has to be analyzed and discussed, it should be clear that there are a lot of software changes which do not need any detailed analysis, since they do not impose new risks. Examples for those changes which are out of scope are for instance software updates and mostly all upgrades to existing software components (if they do not include any additional functionality).

Roles and responsibilities

- Site Security Officers
  - responsible for security policy at a partner site
- DEISA OSCT (Operational Security Coordination Team)
  - site security representatives for DEISA
  - Responsible for risk review of changes
    - Must approve any change before production
- Policy WG – review and prepare policy documents
- DEISA CERT – For security incident response
  - Internal phone and e-mail contacts for all sites
  - Each partner is responsible to report any incident which may impact the DEISA infrastructure

  - Video Conference can be scheduled on short notice too.

Planning

- A dedicated one day security meeting with all partners was organised in February. Objectives:
  - Enhancing the trust between partners
  - Improving policies and procedures
- Internal follow up actions
  - Improvement of the procedure for incident handling
  - Use of intrusion tools in DEISA infrastructure
  - Set up of security audit procedures
- Privacy is an issue if exchange of (log) information is discussed

External relations

- Sharing of policy documents and procedures
  - Participation in JSPG
  - AKIF in Germany?
- Collaboration on operational security
  - Other infrastructures
  - National CSIRTs
- PRACE is also setting up a security forum
  - Large overlap in partners between DEISA and PRACE, so proposal will be to have common teams and to share policies and procedures

Access to DEISA infrastructure

- Not all systems at partner sites are part of the DEISA infrastructure and not all users at sites are DEISA users.
- Remote job submission (UNICORE, Globus WS-GRAM)
- Interactive access is granted for users on all systems on which they are expected to run jobs (authZ is on system level).
- Access provided preferably with gsi-ssh. Internally between systems and through gateway nodes
  - Certs can be revoked!
  - However users don’t like certs, so put ssh keys on systems (if allowed). Enhances risks.
  - Much need for improvement of procedures for certificate requests, i.e. federation based facilities and tools