EGEE2 Technical Overview: SA1 and SA3

Ognjen Prnjat, Kostas Koumantaros

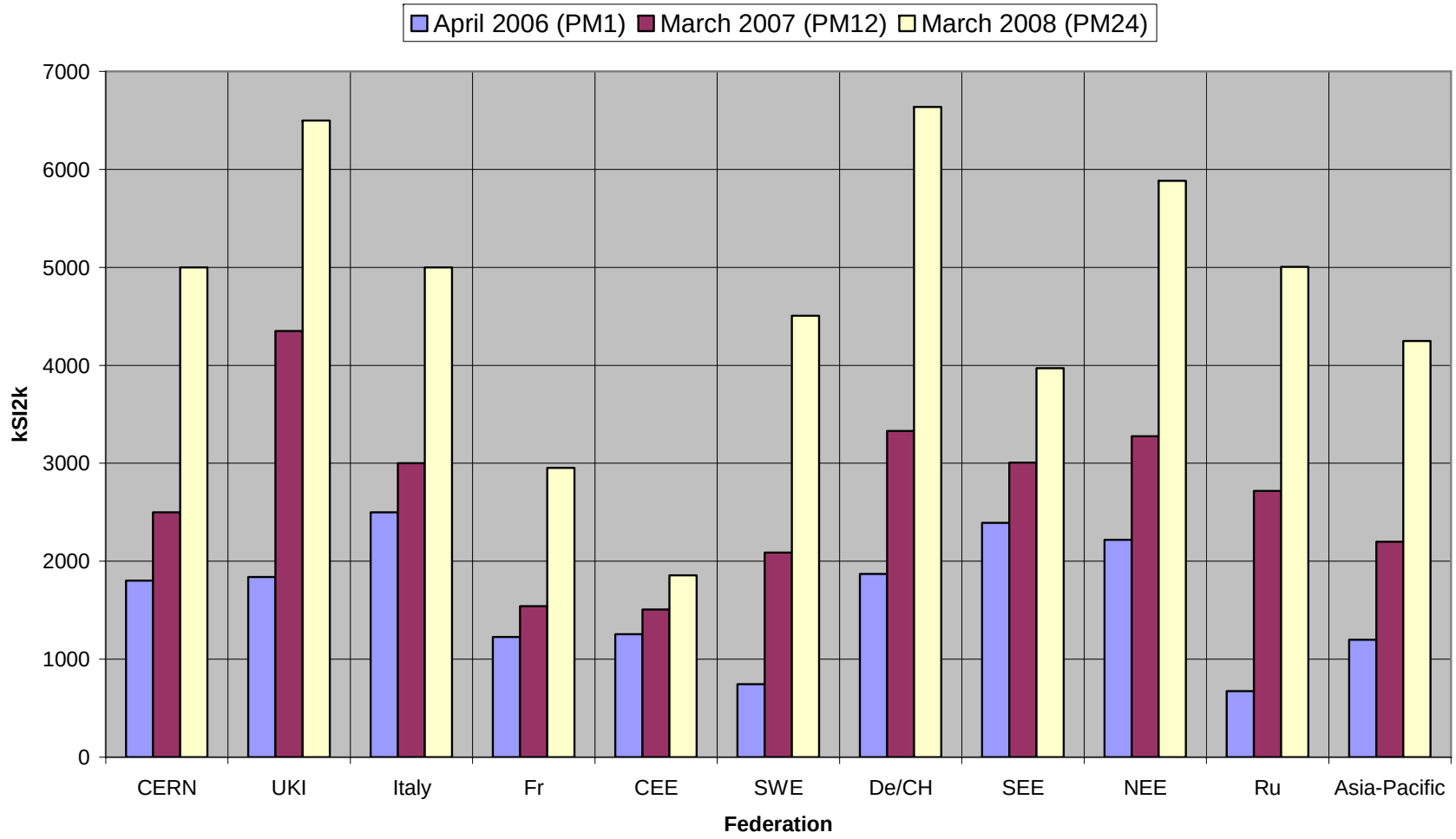
EGEE-HellasGrid Coordination meeting,
Athens 12-13/3/2006

www.eu-egee.org

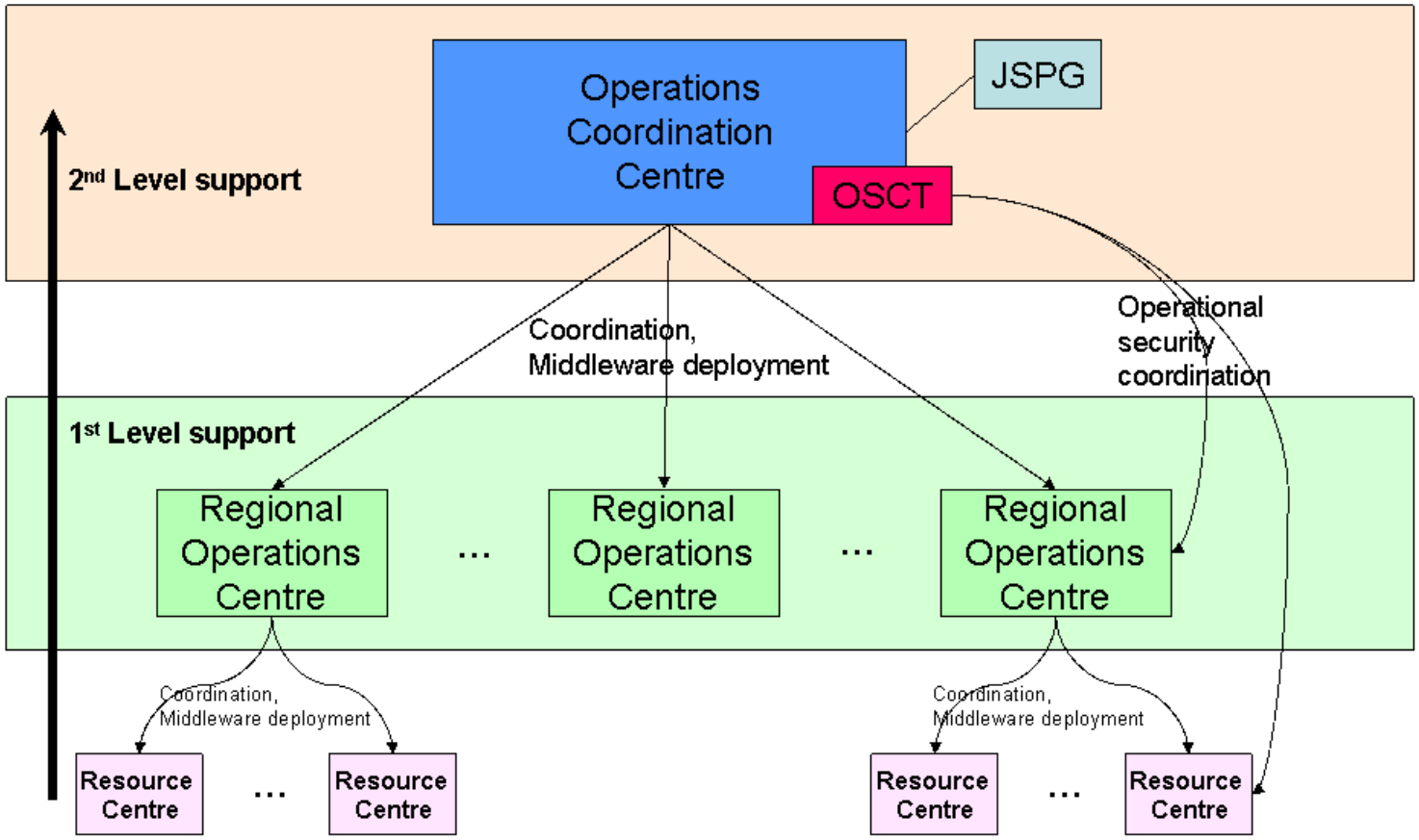
Information Society and Media

- **No distinction between ROCs and CICs: all ROCs**
- **SEE is the LARGEST ROC with:**
  - 7 countries
  - 35+ planned sites with total of comparable resources to others
  - 31 FTEs
    - (CERN 20, CE 20, UK 15, FR 25, It 30, etc.)
    - (focused teams above 5 are not manageable)

Resources: snapshot



Overall organization



More distributed operations

- **More responsibilities for country-level Operations Centres: taking role of what central ROC does now**
  - Registration
  - Site certification (SFTs run in Greece), debugging by countries
  - Deployment coordination
  - Full responsibility for operational problems (chasing tickets, fixing problems)
  - Country reps chasing sites for **weekly report**

Common tasks: each country

- Production
- VO support, integration support (also from NA4)
- User and site admin training
- Contribution to GGUS support teams: global operational and user support
- Local SLA management
- Local accounting and metrics coordination

SA1: cluster operations

- **Must have a dedicated person performing this work**
- **Basic cluster operations**
  - Fabric, OS, middleware
  - m/w certification; porting, customisations if necessary
  - Site installation, testing and certification.
  - Documentation
  - Operational support
  - Local monitoring service for the cluster
  - Resource utilization and SLA monitoring
  - Host and co-manage necessary core GRID services
- **Technical contributions in:**
  - Operations-related extensions to middleware, fabric management tools, middleware installation tools, monitoring tools, operational tools, metrics probes, etc. Need pro-activeness!
  - Providing expertise for common EGEE pool of operational-oriented as well as user support teams.
  - Provide input and logistical support for operators training; also support to other cluster administrator groups.

Specialized tasks

- **Pre-production in Greece, Romania, Israel**
- **Operational coordination and pro-active monitoring:**
  - First COD Bulgaria (short-term solution)
  - Will try to support non-hierarchical COD solutions i.e. leave it up to federation. Then we will setup our local COD.
- **Running essential Grid services**
  - Regional (ie regional SEE VO; infrastructure services)
  - For specific VOs
  - All sites, front line Israel, Cyprus, Greece
- **Security and incident response**
  - Greece, Bulgaria
- **ROC Helpdesk: Romania**
  - But supporters from all countries!

Further specialization: Greece

- **Security – Auth**
  - VO services, security coord., additions to security services, etc
- **Core operations service – ICCS**
  - Support for m/w deployment, site certification, operations, operational tools development
- **Monitoring and accounting coordination – FORTH**
  - Mon tools, accounting server, accounting and metrics collection
- **User support coordination – CTI**
  - Coordination of front-line support for the users; helpdesk oversight, TPMs, support for VO integration (operational)
- **Application support - Demokritos**

- **Pre-production - UoM, UoPatras**
  - Larger clusters, more dynamic deployment, f/b to developers

SA3: Overview

- SA3 will provide certified distributions of middleware ready for deployment by SA1 on the infrastructure.
- The middleware components will be drawn from EGEE/JRA1 and from external projects, with the goal of satisfying user application and operational requirements;
- Provide missing “glue” components and tools, and focus on debugging and analysis of problems;
- Make the middleware work effectively as a complete system;
- Certification of distributions with a full set of testing activities covering all aspects of functionality, reliability, security, etc.

SA3: Greek involvement

- **Running a local branch of certification testbed**
- **Mainly focused on the MW Certification process which includes:**
  - Validate that middleware components function according to their specification, including backward compatibility where needed;
  - Validate that the integrated middleware distribution functions as required;
  - Validate the security model;
  - Test security vulnerabilities;
  - Test a broad range of installation and deployment scenarios;
  - Performance and stress testing, including reliability and robustness;
  - Test management and operational functionality of the components;
  - Test interoperation with other middleware, ensure that upgrades do not break what is already achieved