“Some Operation Models”

Markus Schulz, IT-GD, CERN
markus.schulz@cern.ch

“Strawman to spark discussions”

Enabling Grids for E-science in Europe

1954-2004 CERN 50

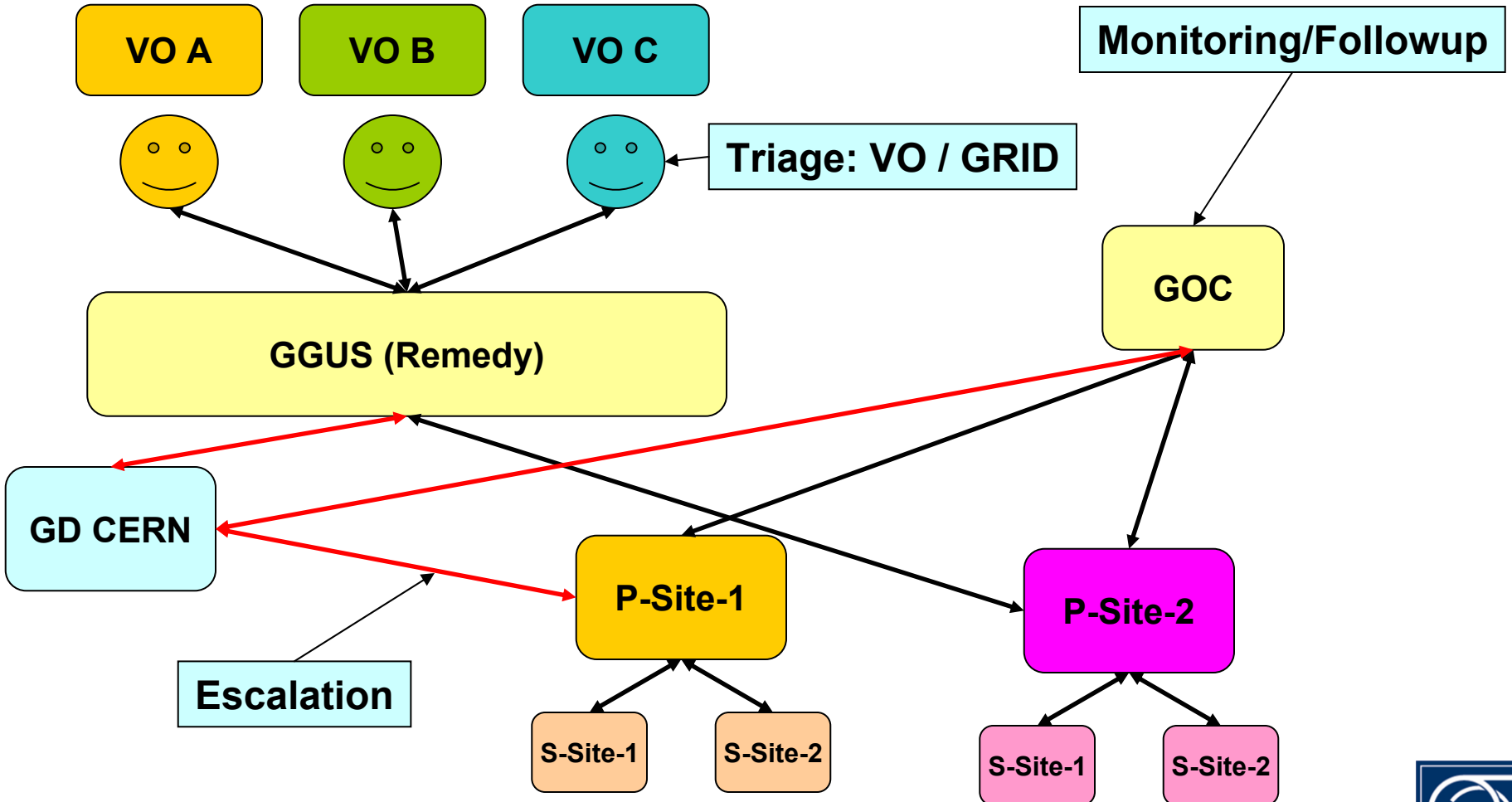
EGEE is a project funded by the European Union under contract IST-2003-508833

Outline

- Operating LCG
  - how it was planned
  - how it happened to be done
  - how it felt
- What's next?

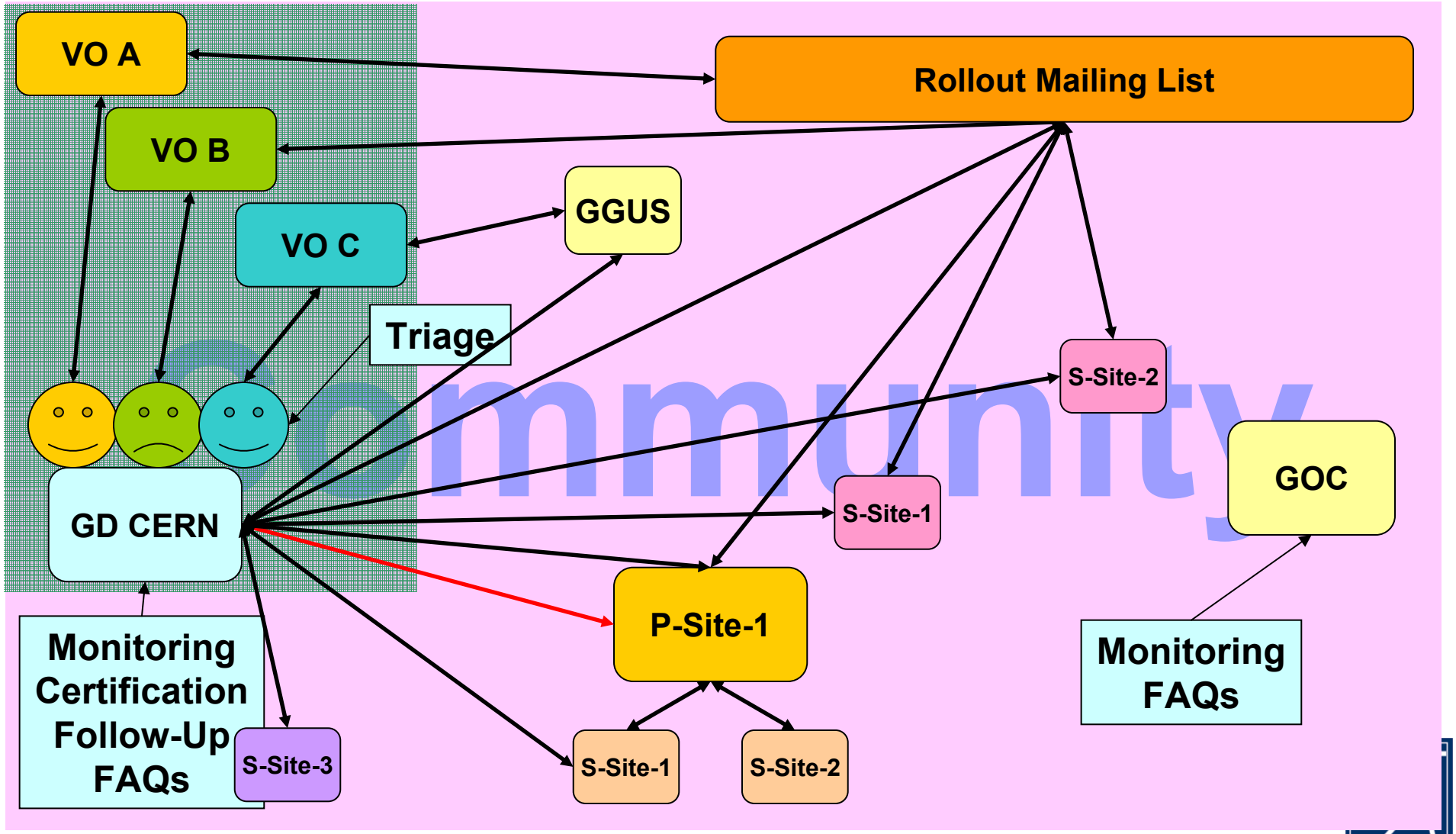
Problem Handling

PLAN



Problem Handling

Operation (most cases)



PART II

- Operation models
  - How much can be delegated to whom?
    - autonomy/ availability
  - What are the consequences?
    - cost for 24/7 with 8x5 staff
  - One/multiple models for all sites/regions?
  - One model for site integration, update, user support, security, operation?
    - latency, efficiency, distribution of workload …..
  - One size fits all?
  - Next slides are meant to stimulate discussions not give answers

CICs and ROCs and Operations

- Core Infrastructure Centers (CICs)
  - run services like RBs, Information Indices, VO/VOMS, Catalogues
  - are the distributed Grid Operation Center (GOC)
  - and more….
- Regional Operation Centers (ROCs)
  - coordinate activities in their region
  - give support to regional RCs
  - coordinate setup/upgrades
  - and more..
- Resource Centers (RC)
  - computing and storage
- Operation Management Center (OMC)
  - coordination

Model I Strict Hierarchy

- CICs locates a problem with a RC or CIC in a region
  - triggered by monitoring/ user alert
- CIC enters the problem into the problem tracking tool and assigns it to a ROC
- ROC receives a notification and works on solving the problem
  - region decides locally what the ROC can to do on the RCs.
    - This can include restarting services etc.
    - The main emphasis is that the region decides on the depth of the interaction.
    - ===> **different regions, different procedures**
  - CICs NEVER contact a site
    - .====> ROCs need to be staffed all the time
  - ROC does it is fully responsible for ALL the sites in the region

Model I Strict Hierarchy

- Pro:
  - Best model to transfer knowledge to the ROCs
    - all information flows through them
  - Different regions can have their own policies
    - this can reflect different administrative relation of sites in a region.
  - Clear responsibility
    - until it is discovered it is the CICs fault then it is always the ROCs fault
- Cons:
  - High latency
    - even for trivial operations we have to pass through the ROCs
  - **ROCs have to be staffed (reachable) all the time. $$$$**
  - Regions will develop their own tools
    - parallel strands, less quality
  - Excluded for handling security

Model II Direct Com. Local Contr.

- ROCs are active in:
  - the follow-up of problems that take longer to handle
  - setup of sites
- CICs are active in:
  - handling problems that can be solved by simple interactions
    - communicated directly between CICs and RCs
      - **ROCs are informed on all interactions between CICs and RCs**
      - **all problems are entered into the problem tracking tool.**
    - restarting of services, etc. are handled by the RCs

Model II Direct Com. Local Contr.

- **Pros:**
  - Resources are not lost for trivial reasons
  - Principe of local control is maintained
  - ROCs are in the loop,
    - but weak ROCs can't create too severe delays
  - No complex tools for communication management needed
    - mail + IRC sufficient
- **Cons:**
  - RCs need to be reachable at all times
    - not realistic, and very expensive ~~€€€€€€€€€€~~
  - CICs have to be aware of the level of maturity of O(100) RCs
  - ROCs have to monitor what is going on to learn the trade
  - Language problems between the CICs and sysadmins
  - Unclear responsibility
    - "This was reported" / "Why didn't the CICs fix it them self"

Model III Direct Com. Direct Contr.

- Like Model II with some modifications
  - CICs have access to the services on the RCs
    - can, if the RC is not staffed, manage some of the services
    - site publishes at any time
      - **whether the local support is reachable or not**
      - **what actions are permitted by the CICs.**
    - all interactions are logged and reported to RC and ROC
      - **Some tools that allow very controlled (limited) access like this are under development (GSI enabled remote SUDO)**
- Variation with ROCs only interaction (IIIa)

Model III Direct Com. Direct Contr.

- **Pros:**
  - Resources are not lost for trivial reasons
  - ROCs are in the loop,
    - but weak ROCs can't create too severe delays
  - One set of tools for remote operation
    - some uniformity ---> chance for better quality
  - Site decides at any time on balance between local/remote operation
  - RCs can be run for (short) time unattended
- **Cons:**
  - Set of tools for secure limited remote operation respecting the sites policies has to be put in place
  - ROCs have to monitor what is going to learn the trade
  - Unclear responsibility
    - "This was reported" / "Why didn't the CICs fix it them self"

Sample UseCases

- User reports jobs failing on one site
- User reports jobs failing on some/all sites
- Monitoring shows site dropping in and out of the IS
- An acute security incident
- Upgrading to a new version
- Post mortem after the security incidents
- …….

- Good preparation for the Operations Workshop