

An Approach to Security Analysis of Distributed Computing GRID Environment

*Vladimir Dimitrov, Zlatogor Minchev,
Dimitar Todorov, Hristo Turlakov*



Institute of Information and Communication Technologies
Bulgarian Academy of Sciences

www.iict.bas.bg

Sofia, Bulgaria

International Conference
AUTOMATICS & INFORMATICS '11

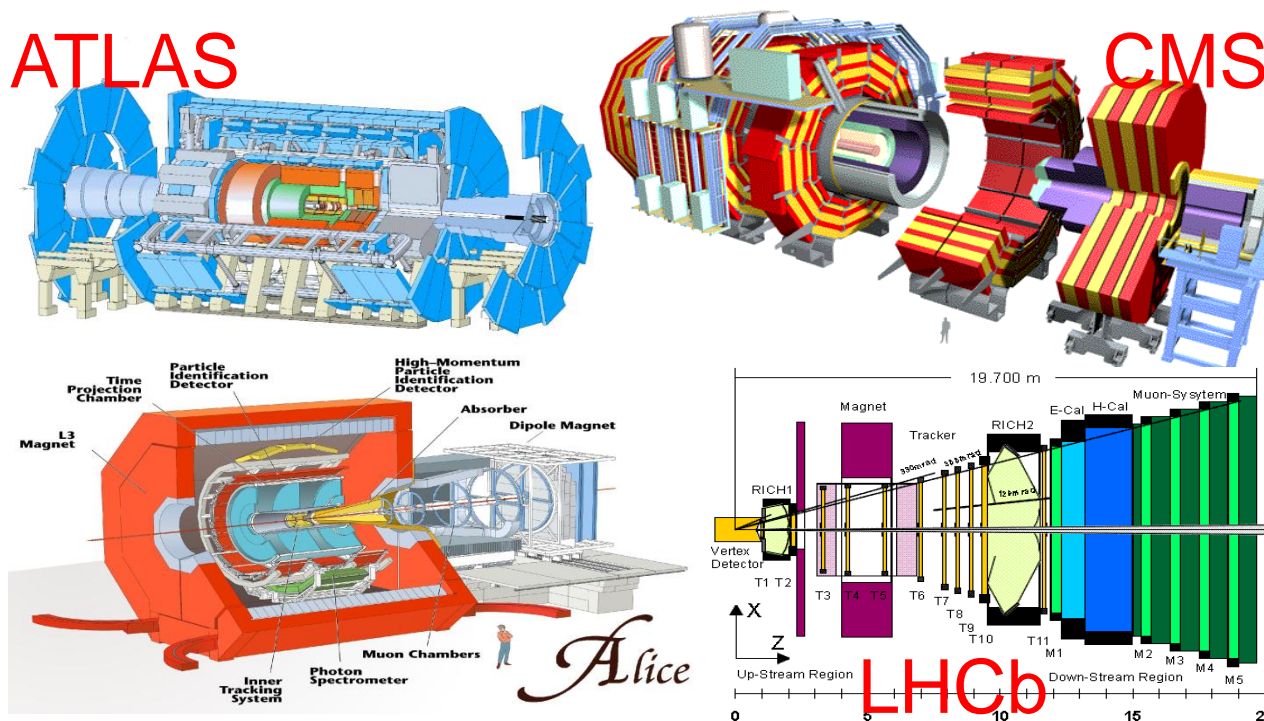
October 5, 2011

Contents

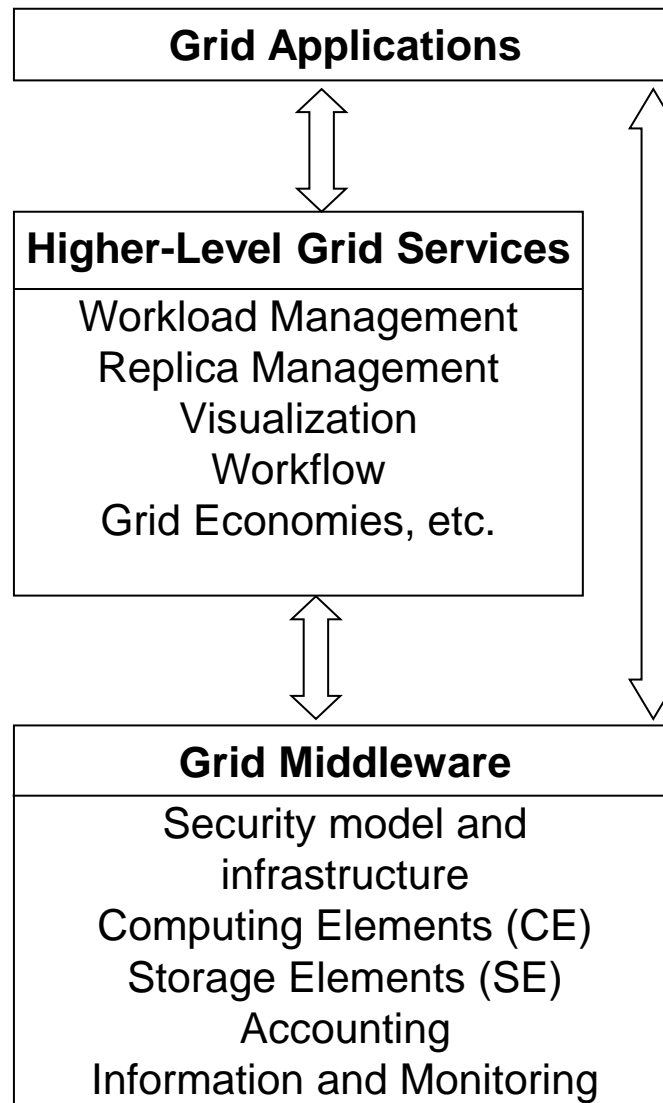
- ❑ **gLite Middleware Services**
- ❑ **Methodology**
- ❑ **gLite Threats Model**
- ❑ **Software implementation**
- ❑ **Discussion**

gLite Grid Middleware Overview

- Developed for processing the huge amount of data generated by LHC in CERN inside the EGEE series of FP7 projects.
- Now many other scientific areas rely on **gLite** services, such as: Biomedicine, Chemistry, Astrophysics, Earth sciences, Finances, Civil Protection, even Archeology etc.



gLite Middleware Services Main Idea



Grid System

The **gLite** is a middleware that makes a set of independent server clusters with high speed network connections suitable for virtual use as a unified resource in a way widely known as **Grid Computing**.

This middleware is currently deployed on several hundreds of server clusters known as Grid-sites. It enables a global e-science approach to a number of disciplines. There are tens of thousands of end-users and thousands of support and management staff using the Grid infrastructure with this middleware.

✓ The evolution of the Grid infrastructure and further development of gLite continues with **EGI-InSPIRE FP7 project** (Integrated Sustainable Pan-European Infrastructure for Researchers in Europe, 2010-2014).



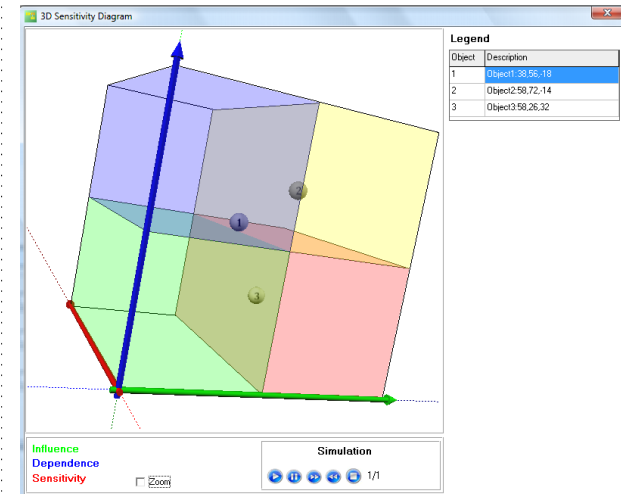
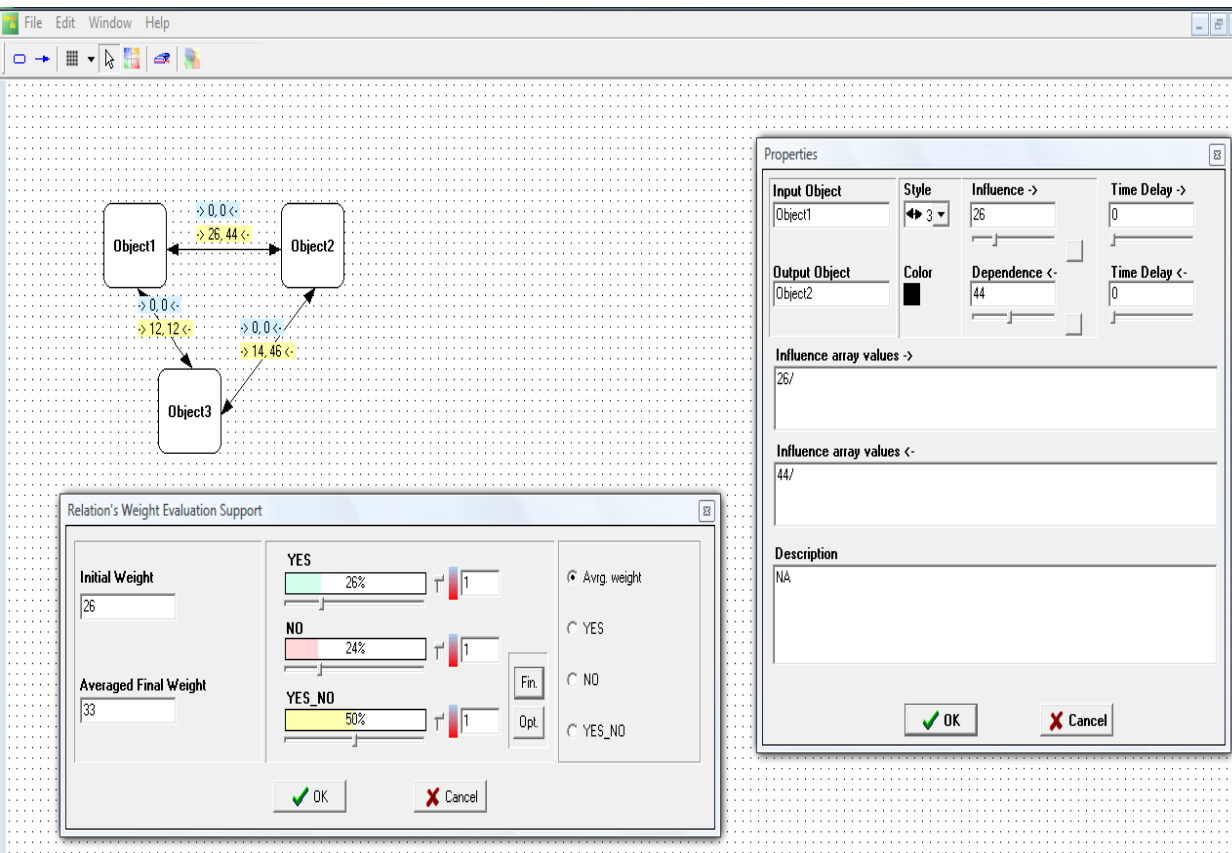
Methodology

- ❑ **Experts' knowledge extraction via brainstorming, discussions and Delphi questionnaires filling-up;**
- ❑ **Results representation via the E-R paradigm in the dynamical systems theory sense;**
- ❑ **System based sensitivity analysis.**

Software implementation



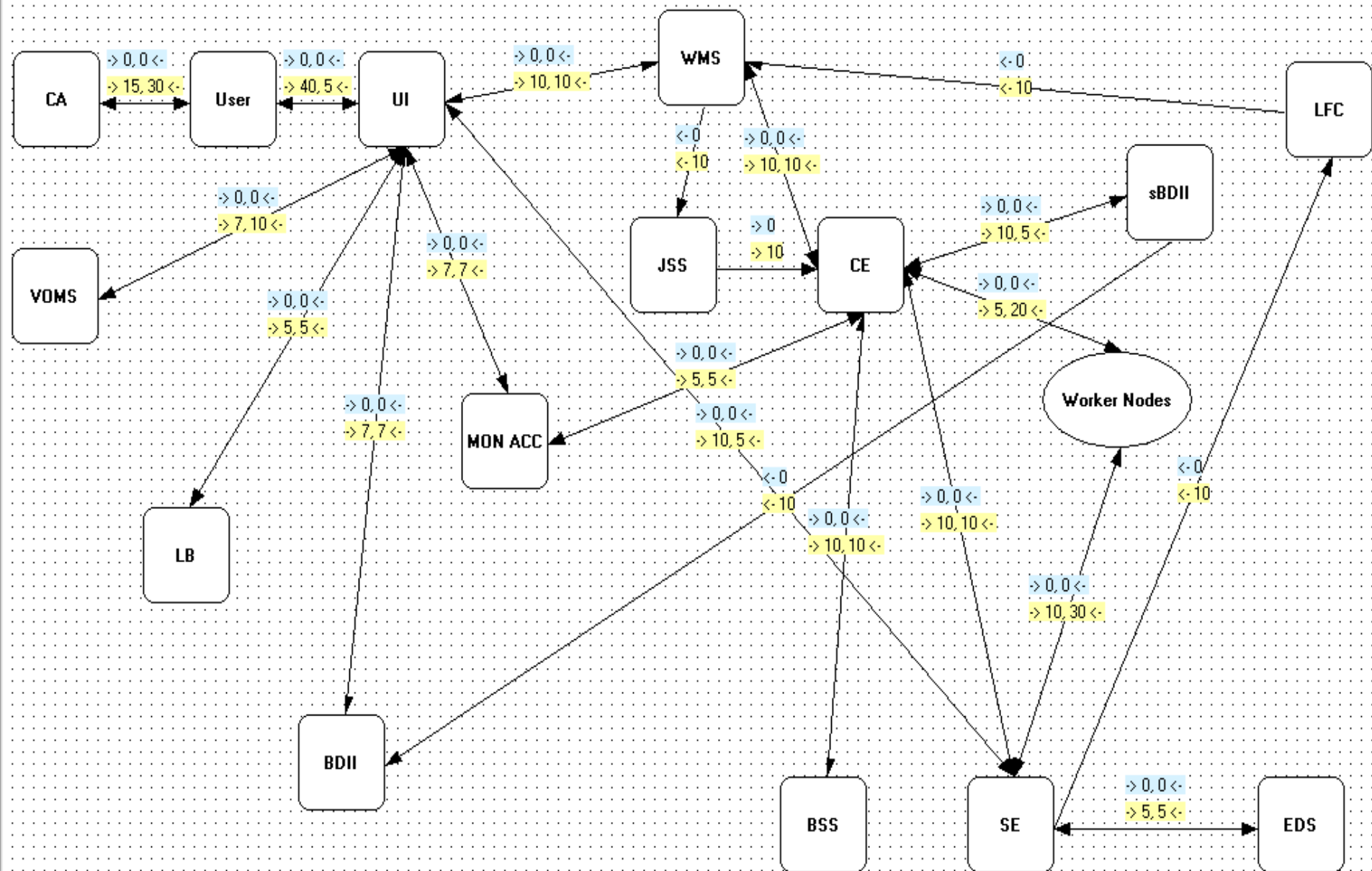
I-SCIP®



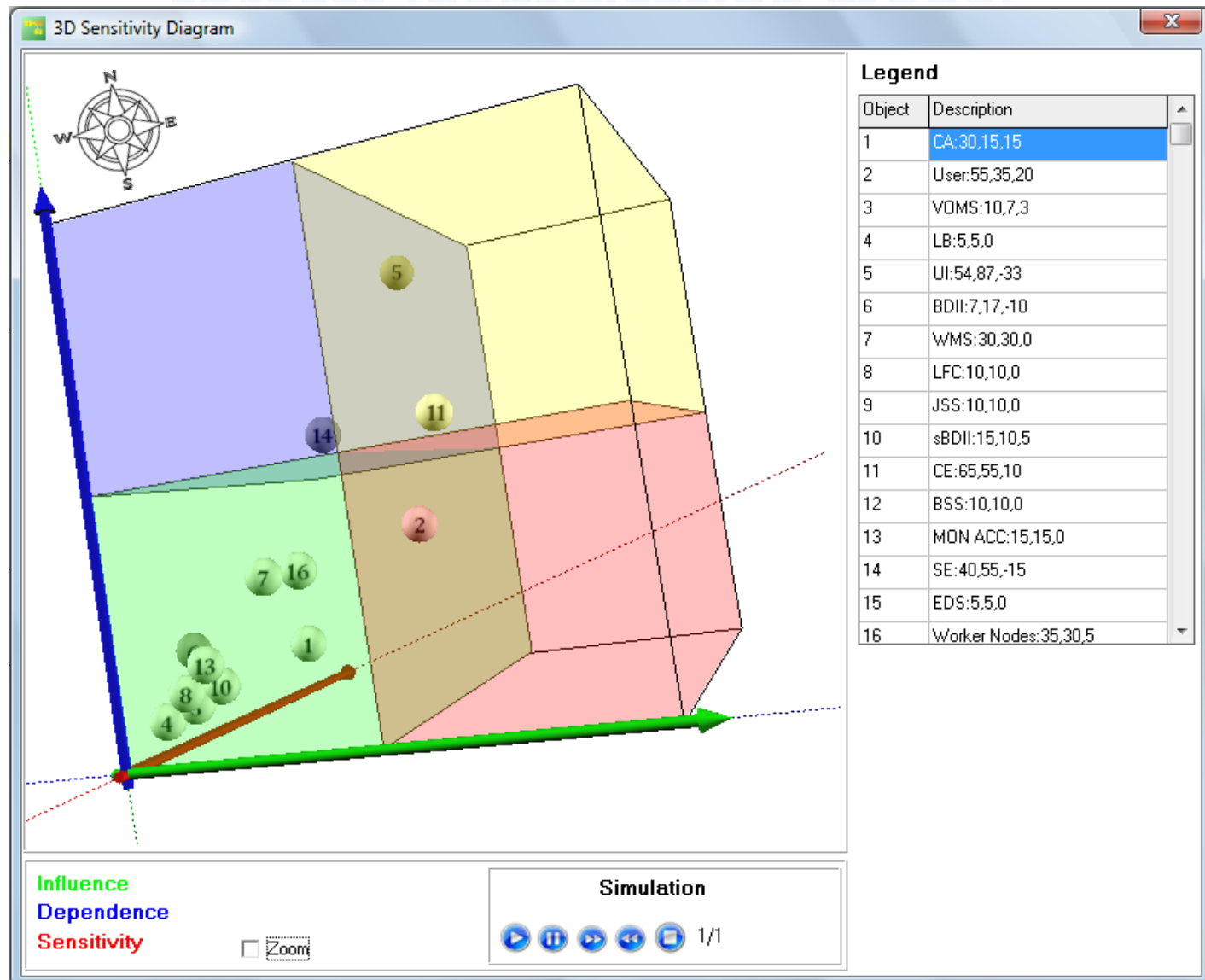
A typical scenario for using Grid

1. The User applies to the regional Certification Authority (CA) for a Grid certificate;
2. CA signs and publishes the certificate;
3. The user applies for membership in an appropriate Virtual Organization (VO) with this Grid certificate;
4. The VO management approves the membership;
5. The User installs and configures a computer with User Interface (UI) software;
6. The user develops a Grid application (job);
7. The user authenticates and authorizes himself/herself using the valid Grid certificate and VO membership credentials;
8. The User queries Berkeley Database Information Index (BDII) nodes for Grid resources currently available;
9. The User submits the job to appropriate Workload Management System (WMS) node;
10. The WMS manages and monitors the Grid job and submits it to an appropriate Computing Element (CE) node of Grid site for execution;
11. The CE puts the job on a BSS queue;
12. The job is executed in turn on a Worker node(s) belonging to this Grid site;
13. The User monitors the job status using Logging and Book-keeping (LB) capabilities during steps 10 to 12;
14. When the job is finished, the User retrieves the job output to UI. End of scenario.

gLite Threats Model



Sensitivity Diagram for gLite middleware threats identification model



Discussion

- ❑ The accomplished initial results do not show the detailed nature of the gLite threats but only outline a way how they could be identified, using experts' knowledge and the presented system based modelling;
- ❑ No universal solution for threats analysis is applicable without certain scenario context, though even in such case the uncertainty still stays an open problem;
- ❑ In our future plans we intend to extend the presented methodology and to implement it for Cloud environment system security studying;

EU Network of Excellence SysSec



Acknowledgements

This work was partially supported by the EU FP7 **project SysSec** – A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: Europe for the World under the agreement n° 257007 and FP7 **EGI-InSPIRE project**.

The authors also express their gratitude to the pilot group of experts for the fruitful discussions and the questionnaires filling-up.

Thank you for the attention!

Questions?

www.iict.bas.bg