EUROPEAN COMMISSION
DIRECTORATE-GENERAL
Joint Research Centre

Joint Research Centre

ICT Vulnerabilities of the power grid: trade-offs of reviewing vs. upgrading current control architectures

Alberto Stefanini, Marcelo Masera, EC – DG JRC
and R. Matthew Gardner, INPG

ICT architectures and networked critical infrastructures

- Industrial + business applications
  - Different environments: real-time, office
  - Many interconnections
  - Multi-proprietary
  - Legacy + new applications
- Across jurisdictions
  - Several actors (owners, designers, operators)

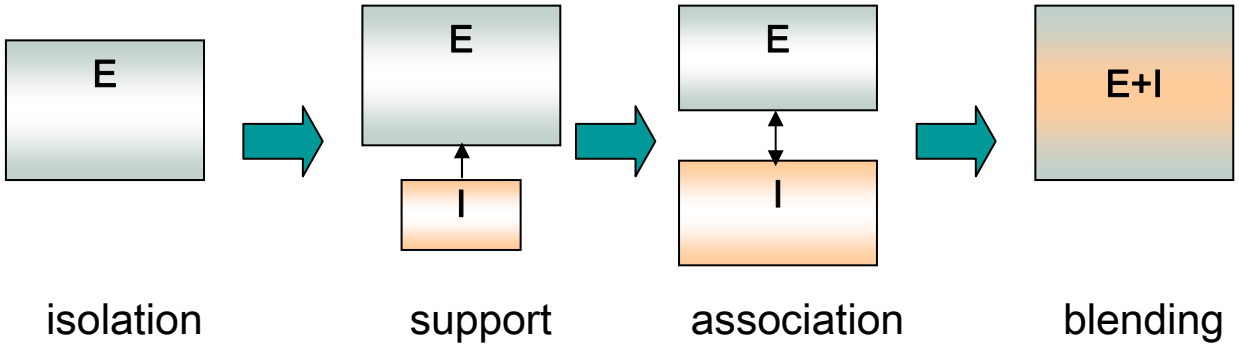
- Therefore:
  - Important dependability and security concerns
  - But, who owns the problem?

Evolution of the power infrastructure

Growing vulnerability

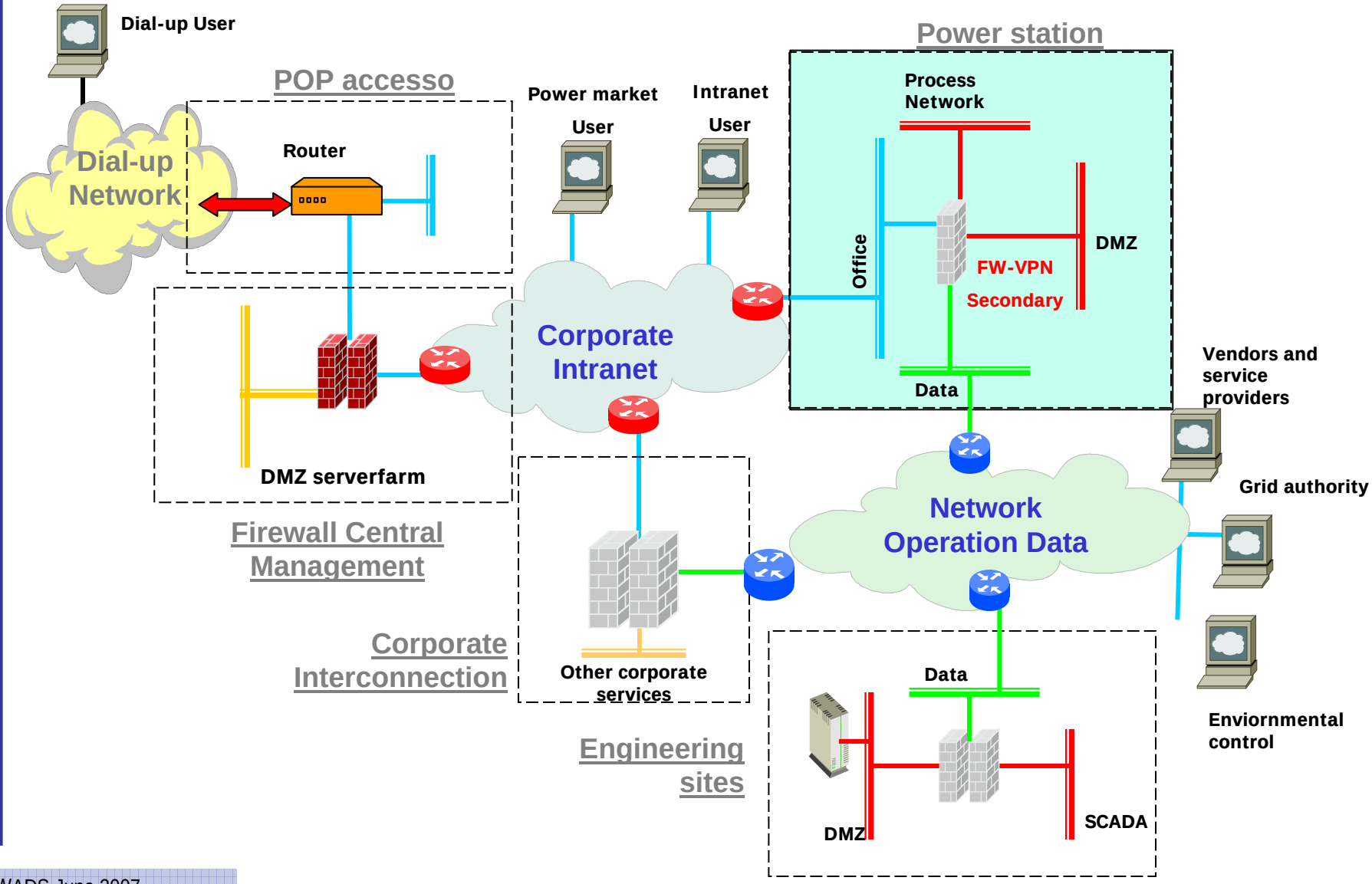
- Liberalisation and integration of EU energy market:
  - Demand is growing and cannot be easily faced anytime
  - Transactions increase - operators forced to use grid capacity to the limit
  - *Control system complexity grows - responsibilities are being partitioned among a growing number of different subjects*
- Emergence of cyber threats:
  - due to extended use of open IC infrastructures

The E+I paradigm



- The electric power infrastructure is information-based:
  - Within each company: operations, maintenance…
  - In relation with customers: energy information services…
  - Among companies: congestion, contingencies…
  - In the electricity market

Example: power plant



The GRID project (2006-2007)

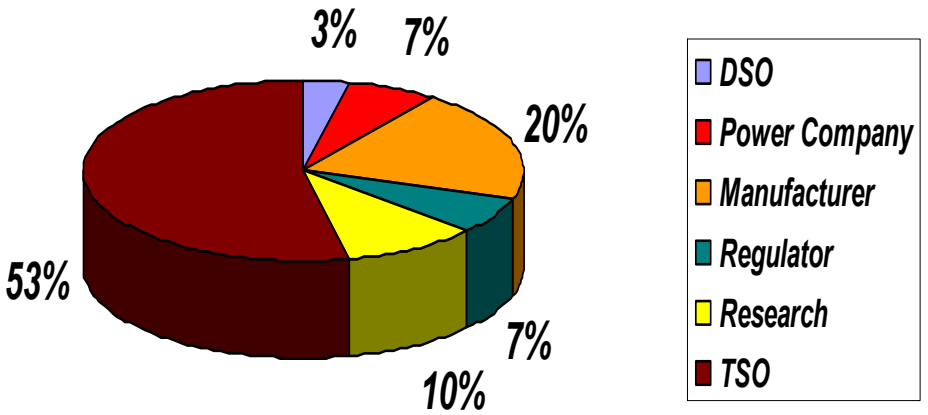
- Establish consensus at the European level on the key issues involved in ICT vulnerabilities in power systems
  - Roadmap on most urgent and significant R&D needs
  - Raise awareness on security concerns
- Methodology: *Dialogue with stakeholders*
  - Regulators, transmission system operators, electric utilities, R&D institutions, manufacturers
  - Representative associations (Eurelectric, UCTE, ETSO)
  - National authorities and European Commission

GRID steps

- *Stakeholders Conference*
  - *Stavanger, Norway on June 15, 2006*
- *Questionnaire for consultation of Stakeholders*
- *Workshops:*
  - Leuven (B) - November 14, 2006
  - Paris (F), June 20, 2007

The Questionnaire

- Diffused July 2006 to:
  - Approximately 600 members of industry and research
- 57 total responses (~10%)
  - 35 industry
  - 22 research
- 19 countries represented
  - 18 European countries
  - United States



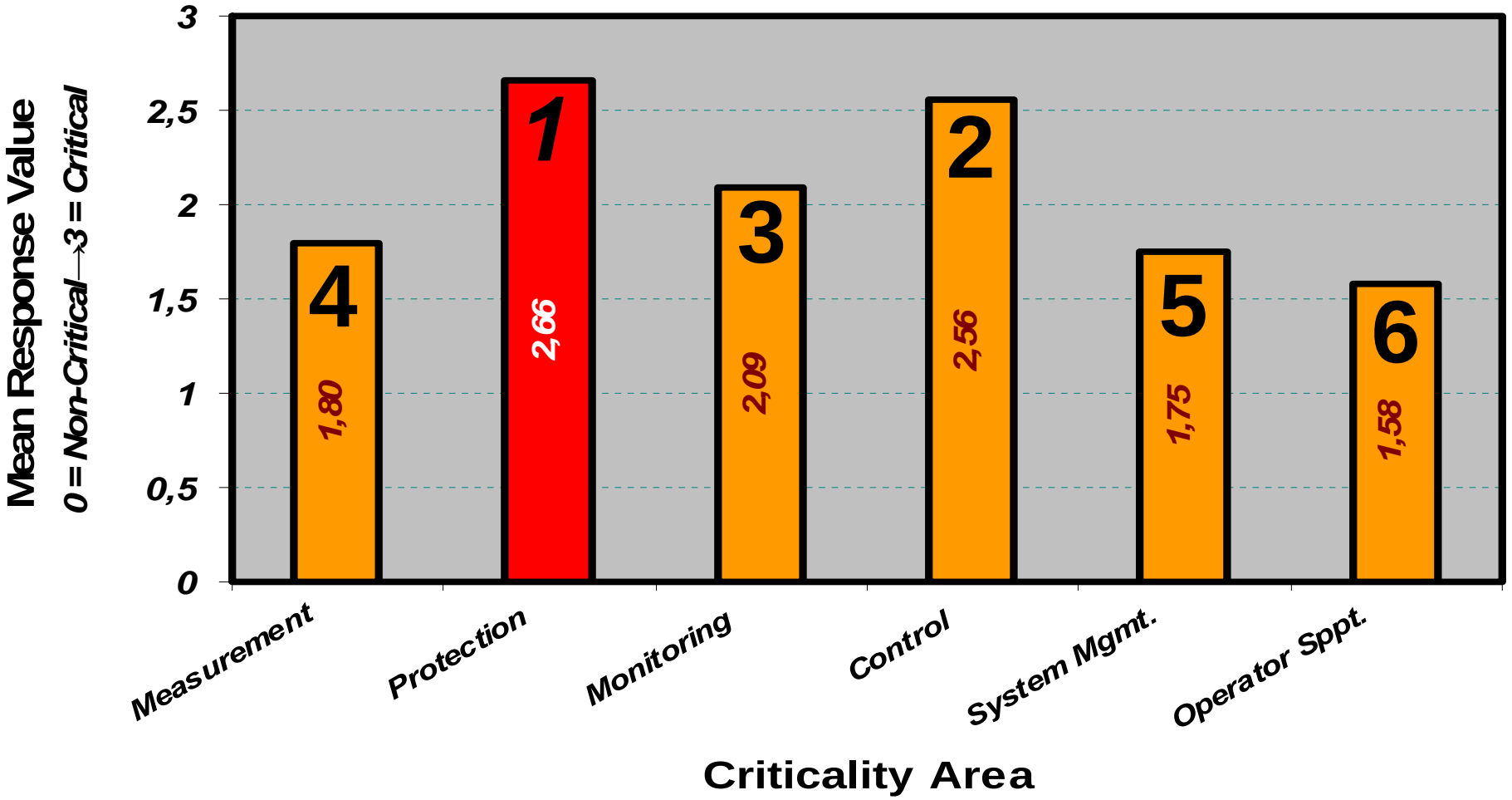
The questionnaire: focus on ICT dependent functions

Rank (0-3) the key ICT dependent functions of power systems concerning *criticality* and *vulnerability*:

- Measurements
- Protection
- Monitoring
- Control
- System Management and Coordination
- Operator Decision Support

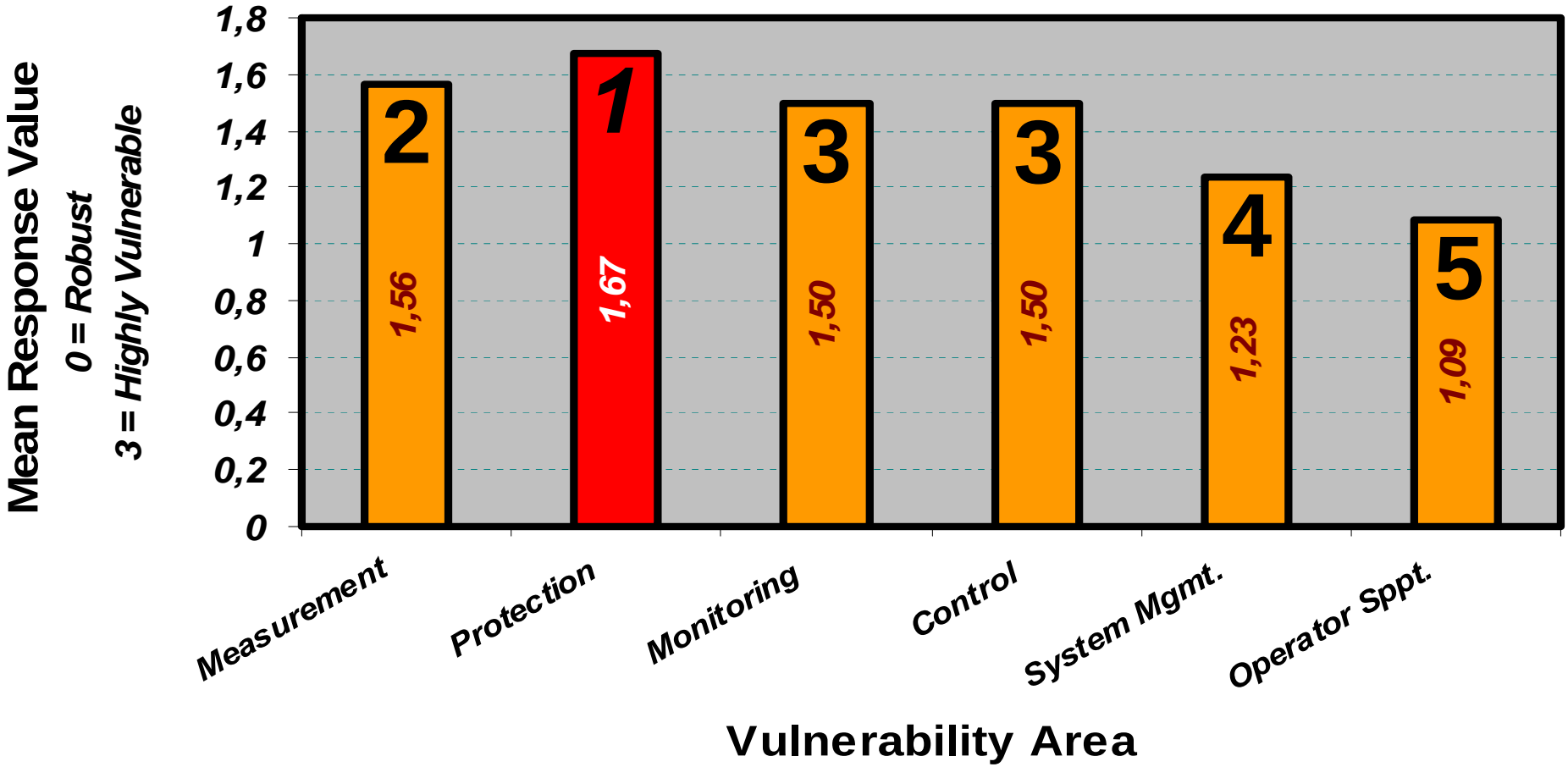
EUROPEAN COMMISSION
DIRECTORATE-GENERAL
Joint Research Centre

Criticality Response



EUROPEAN COMMISSION
DIRECTORATE-GENERAL
Joint Research Centre

Vulnerability Response



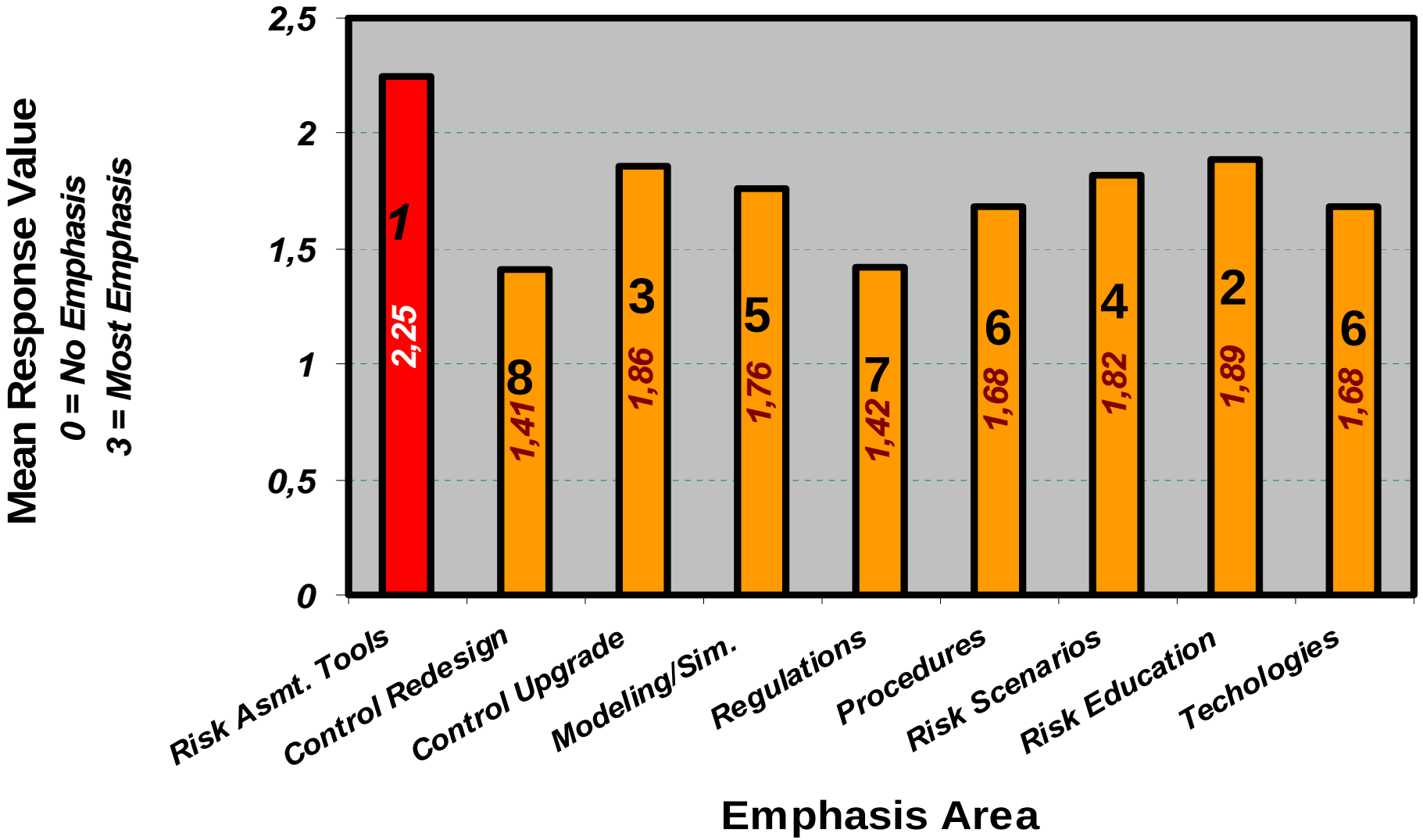
The questionnaire: emphasis areas

For increasing the robustness of the power system put emphasis (0-3) on:

- Risk and Vulnerability Assessment Tools and Methods
- Redesign of Control Architectures and Technologies
- Upgrading Control Architectures and Technologies
- Modeling and Simulation Tools
- Regulations
- Procedures
- Risk Scenarios
- Education on Risk
- Technologies

EUROPEAN COMMISSION
DIRECTORATE-GENERAL
Joint Research Centre

Emphasis Response



Questionnaire outcome

- What level of ICT based control and protection can be deployed?
  - Redundant/reliable exchange of data among TSOs
  - Software testing
  - Communication diagnostics/interference detection
  - Holistic security assessment tools & methods
- Simulation of critical situations over the whole of Europe
- Development of a framework of laws, procedures, and standards for ICT security

Questionnaire outcome vs Stavanger

- Stavanger Conference focus:
  - massive adoption of emergent technologies
    - likely to introduce enhanced cyber problems
    - enormous amount and flow of data
    - need to integrate those and made the situation intelligible
- Questionnaire:
  - Control Redesign is considered the last workable option
  - Control Update preferred

Questionnaire vs Stavanger (ct.)

- Stavanger:
  - paradigmatic shift in the way the EMS architecture is organised
  - deeply contrasting with the current architecture of control systems
  - difficult to integrate new vision with existing legacy systems
- Questionnaire and workshops: more conservative view
  - emphasis on risk assessment
  - diagnostics
  - control update methodologies (design, testing)

Thank you

GRID web site:

http://grid.jrc.it