

# Risk Management in Grids \*

Karim Djemame, Iain Gourlay, James Padgett  
School of Computing, University of Leeds, UK  
{karim,iain,jamesp}@comp.leeds.ac.uk

Kerstin Voss  
University of Paderborn, Germany  
kerstinv@upb.de

Odej Kao  
Berlin Technical University, Germany  
odej.kao@tu-berlin.de

May 7, 2008

## Abstract

Advances in Grid computing research have in recent years resulted in considerable commercial interest in utilizing Grid infrastructures to support commercial applications and services. However, significant developments in the areas of risk and dependability are necessary before widespread commercial adoption can become a reality. Specifically, risk management mechanisms need to be incorporated into Grid infrastructures, in order to move beyond the best-effort approach to service provision that current Grid infrastructures follow.

Consider a scenario in which an end-user is willing to pay a Grid resource provider for use of their resources to execute a task or process. The

---

\*This work has been partially supported by the EU within the 6th Framework Programme under contract IST-031772 "Advanced Risk Assessment and Management for Trustable Grids" (AssessGrid).

end-user may want to associate Quality of Service (QoS) requirements with such a request. For example, one such requirement may specify that the task be completed by a specified deadline and a penalty clause to cover financial losses if the requirement is not met. Alternatively, such tasks may generate large amounts of data, which, if lost or corrupted, will also result in financial loss for the end-user's organization. Consequently, end-users (or their organisations) may wish to negotiate Service Level Agreements (SLAs) which define all aspects of the relationship between themselves and a Grid resource provider(s) and specify all contractual obligations and liability limits. In particular, such SLAs need to specify the performance guarantees of the resource provider in addition to penalty fees for both end-users and providers, if either fails to deliver what is guaranteed.

Hence an infrastructure that supports SLA negotiation is clearly desirable. The importance of SLAs to Grid commercialisation has stimulated a drive to standardise automated SLA negotiation / agreement process within the Grid research community. However, both providers and end-users are cautious on adopting such an approach since agreeing to an SLA represents a business risk for both parties. From the provider's perspective, an SLA represents a commitment to meet the objectives specified therein and to pay a penalty if it fails to provide the guaranteed service. SLA violation can be caused by many events, such as resource or network failures, operator unavailability, or even a power cut. Without a means of formally evaluating the likelihood and expected impact of such negative events, a provider faces serious difficulties and potential risk in deciding to which SLAs it will commit. Similarly, end-users need to know the likelihood of an SLA violation in order to accurately compare SLA quotes and take appropriate decisions in relation to acceptable costs and penalty fees, since these too have a potential impact on their business.

These issues are addressed through risk management, a discipline which takes account of the possibility that future events may cause adverse effects. Risk management is important in a diverse range of fields including statistics, economics, biology, engineering, systems analysis, and operations research. Risk management has been extensively used in IT technologies but applying the concept to Grid infrastructures is still in its infancy. While risk is traditionally seen as a negative force, modern risk management recognizes its positive aspects and that, in contrast to risk-avoidance strategies, accepting certain risks can be beneficial. A typical modern day example is that of the insurance industry. For example, if a customer takes out insurance, then the risk of potential financial loss due to theft is transferred from the customer to the insurance company at the cost of a premium.

In the scenario mentioned earlier, risk management and assessment mechanisms are of value to resource providers, enabling them to make informed decisions regarding which SLA requests they wish to commit to, as well as building a resource management schedule through consideration of risk assessment information. Additionally, risk assessment and management enable a provider to identify infrastructure bottlenecks and mitigate potential risk, in some cases by initiating fault-tolerance mechanisms to prevent SLA violations. An end-user also benefits, since risk assessments can be used to determine if an SLA request will be made after an SLA quote has been analysed, based on its price, penalty, and Probability of Failure (PoF). Further, an end-user may make use of a broker, and its reliability and risk assessment mechanisms, to identify and negotiate with suitable providers. Risk assessment enables the broker to evaluate the risk involved in mapping a workflow consisting of a number of sub-jobs onto more than one resource provider, based on the providers' published PoFs. In addition, the functionality to evaluate the reliability of a provider's risk assessment, based on historical data, is useful and significantly enhances the service of a broker.

This chapter is outlined as follows: section 2 discusses background issues such as Grid SLAs, risk management and trust issues. Section 3 describes the integration of risk awareness within a Grid computing architecture. The AssessGrid project addresses the problem of risk management in Grid computing and forms the basis of this section 3. Section 4 examines potential economic issues in relation the AssessGrid architecture and its actors . end-user, broker, and provider.