Managed by

European Research Consortium for Informatics and Mathematics
ERCIM

Security Requirements Analysis

Formal Models, Policy Derivation, and Security Rationales

Syed Naqvi

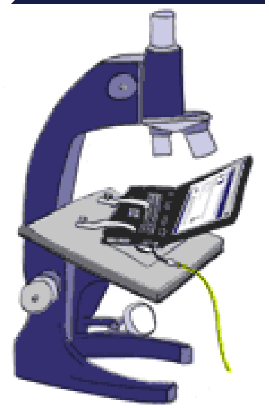
Research Fellow (CETIC Belgium, CCLRC United Kingdom)
CoreGRID European Network of Excellence
snaqvi@ieee.org

Definition of ‘Requirement’

- In engineering, a requirement is a singular documented need of what a particular product or service should be or do. It is most commonly used in a formal sense in complex systems.
- In systems engineering, a requirement is a description of what a system must do. This type of requirement specifies something that the delivered system must be able to do.
- A security requirement is complementary to the functional requirement of a system. It should be based on an analysis of assets and services to be protected and the security threats from which these assets and services should be protected.

How to Express Requirements ?

Specification language understandable by all the actors



KAOS : Knowledge Acquisition in autOmated Specification

Anti-Goal (Threats) Model

- Goal Model
- Responsibility Model
- Operations Model
- Constraints Model

http://www.objectiver.com

http://www.cetic.be/internal220.html

Dardenne A., Lamsweerde A. and Fickas S., *Goal-Directed Requirements Acquisition*, Science of Computer Programming Vol. 20, North Holland, 1993, pp. 3-50.

http://www.info.ucl.ac.be/Research/Publication/1993/SCP.ps.gz

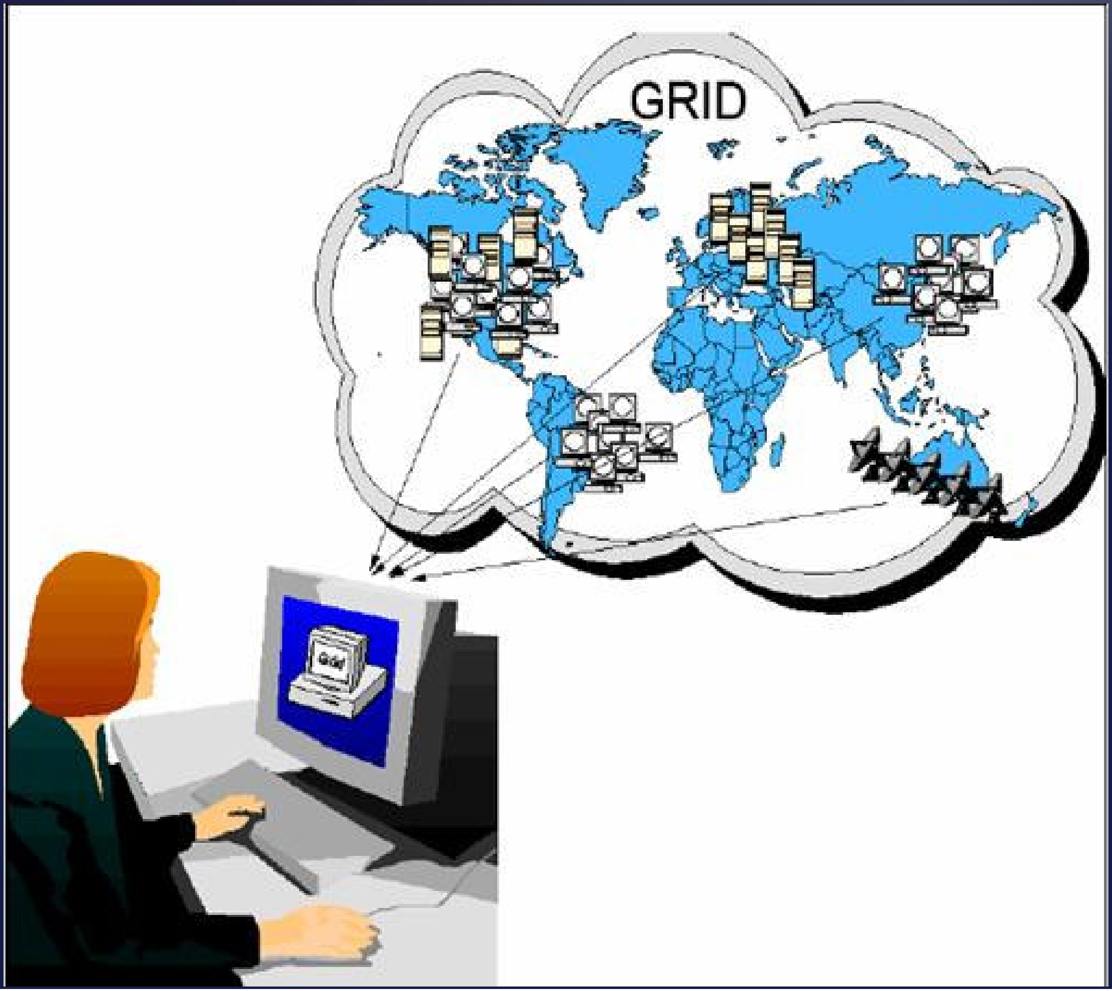
Lamsweerde A., *Elaborating Security Requirements by Construction of Intentional Anti-Models*, Proceedings of ICSE’04, 26th International Conference on Software Engineering, Edinburgh, May. 2004, ACM-IEEE , pp 148-157.

http://www.info.ucl.ac.be/Research/Publication/2004/avl-Icse04-AntiGoals.pdf

CASE STUDY

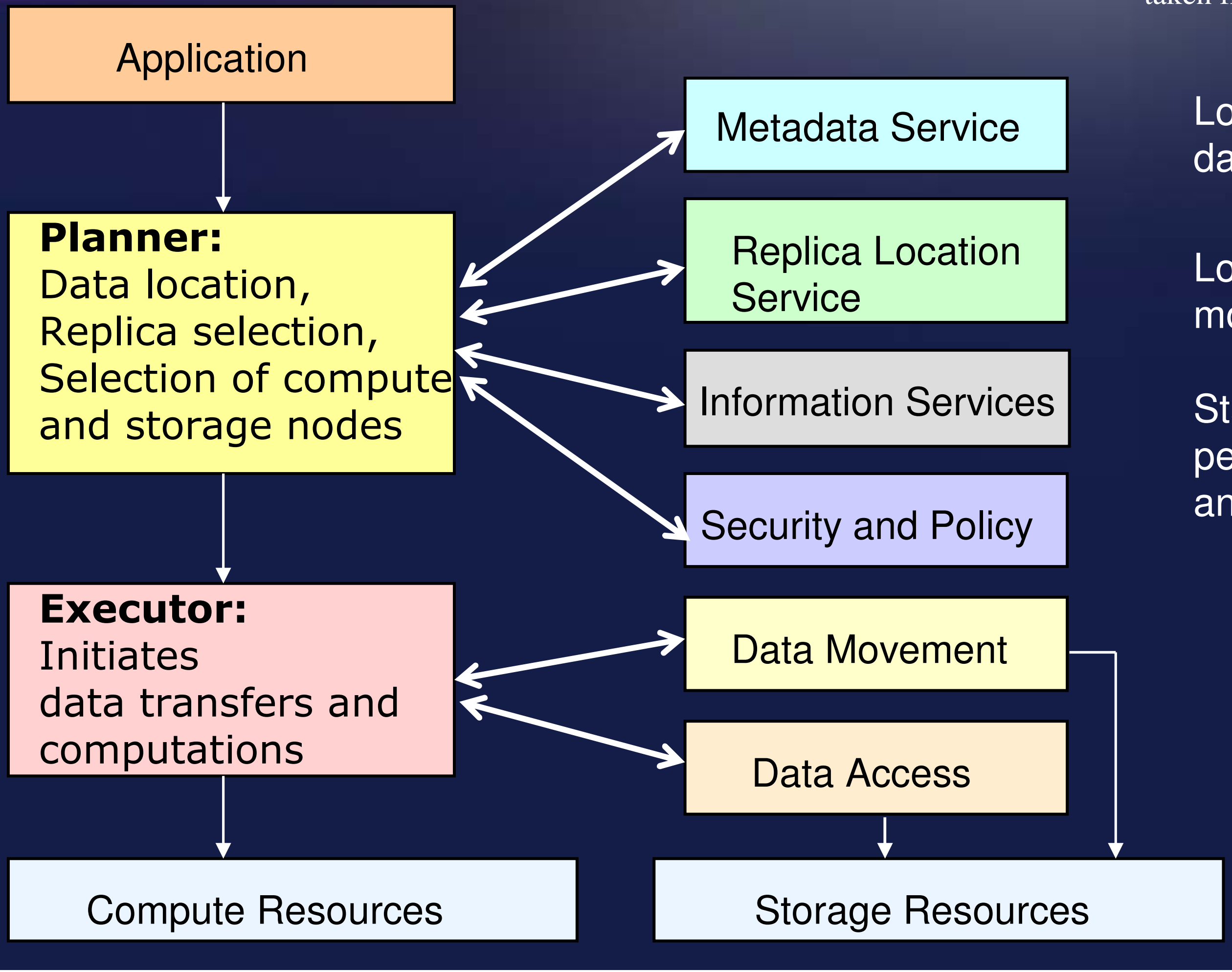
Security Requirements Model of Grid Data Management System (GDMS)

The GRID



Functional View of Grid Data Management

taken from www.twgrid.org



Application

Planner:
Data location,
Replica selection,
Selection of compute and storage nodes

Executor:
Initiates data transfers and computations

Metadata Service

Replica Location Service

Information Services

Security and Policy

Data Movement

Data Access

Compute Resources

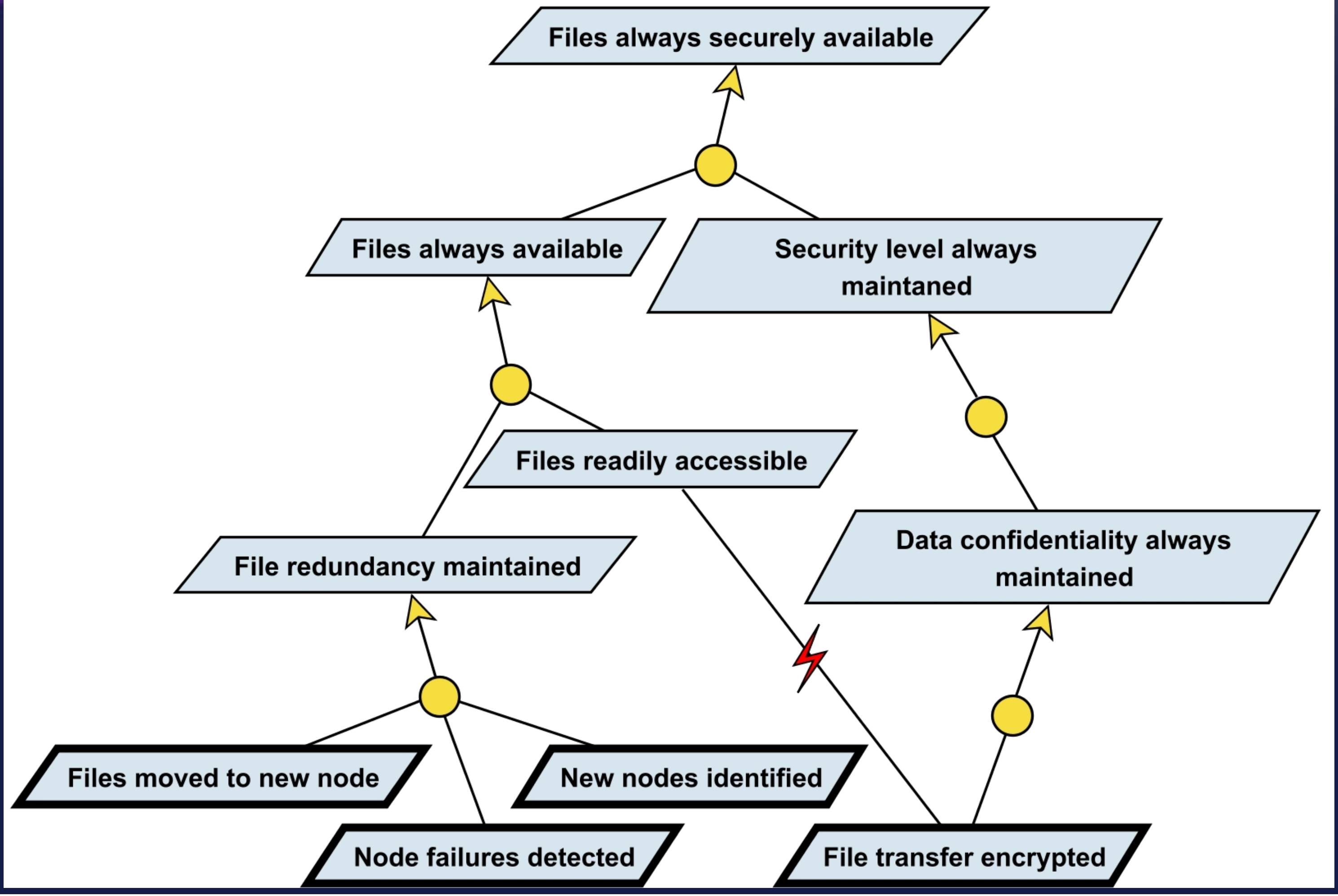
Storage Resources

Location based on data attributes

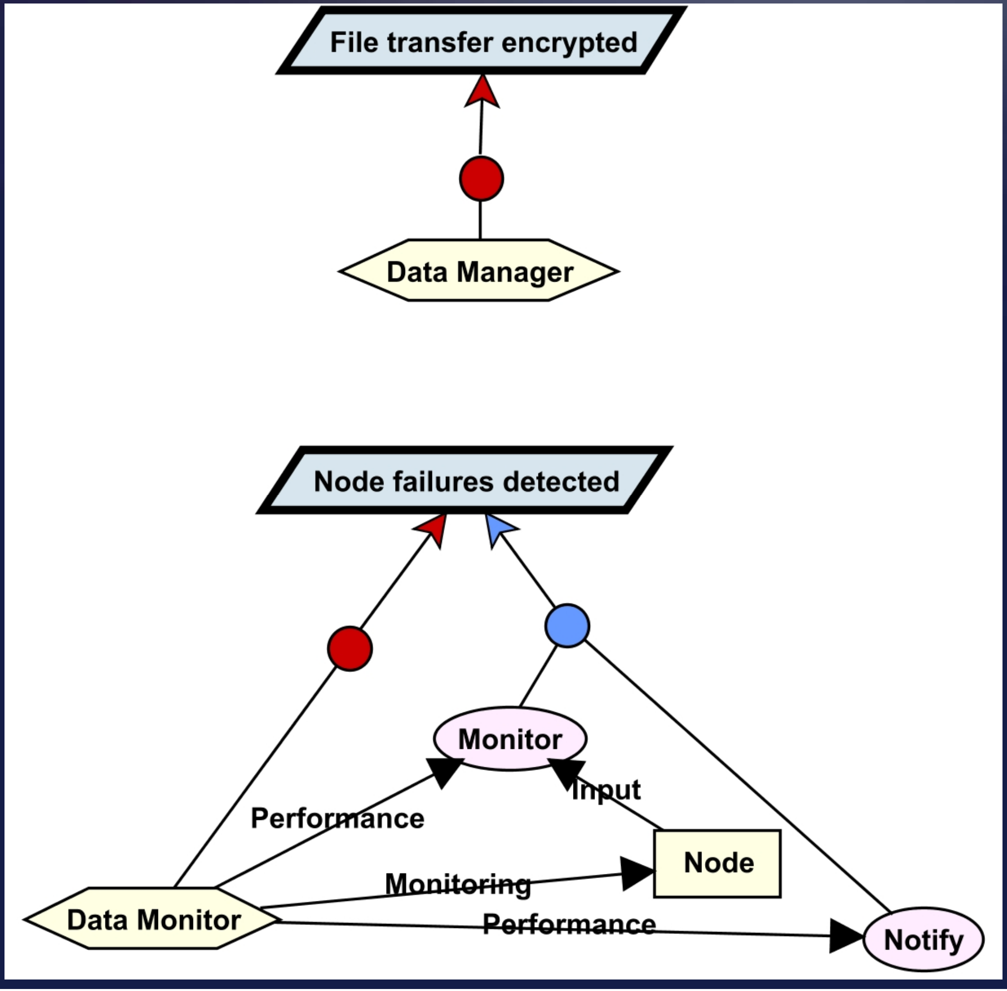
Location of one or more physical replicas

State of grid resources, performance measurements and predictions

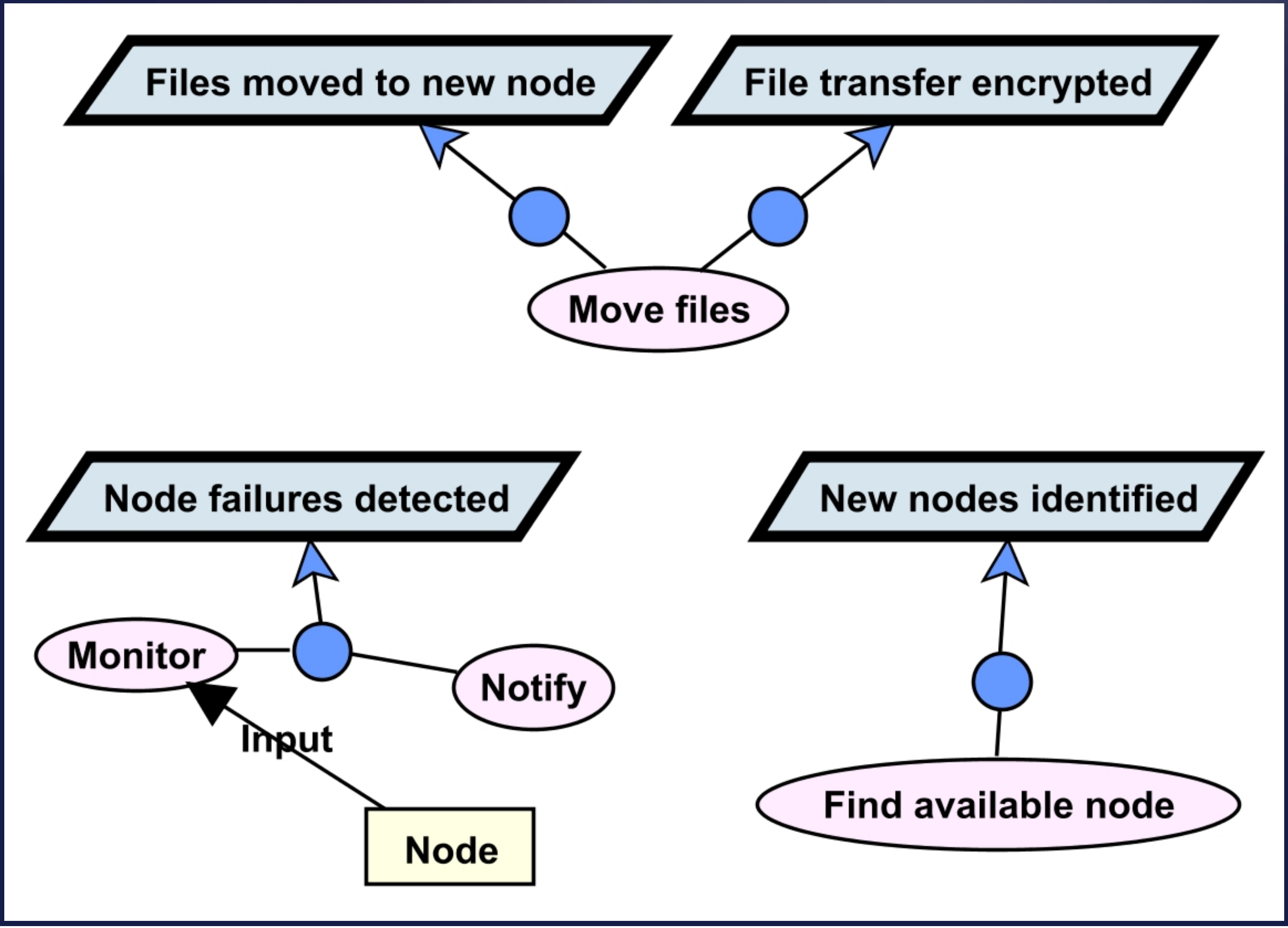
Goal Model


Files always securely available
Files always available
Security level always maintaned
Files readily accessible
File redundancy maintained
Data confidentiality always maintained
Files moved to new node
New nodes identified
Node failures detected
File transfer encrypted

Responsibility Model



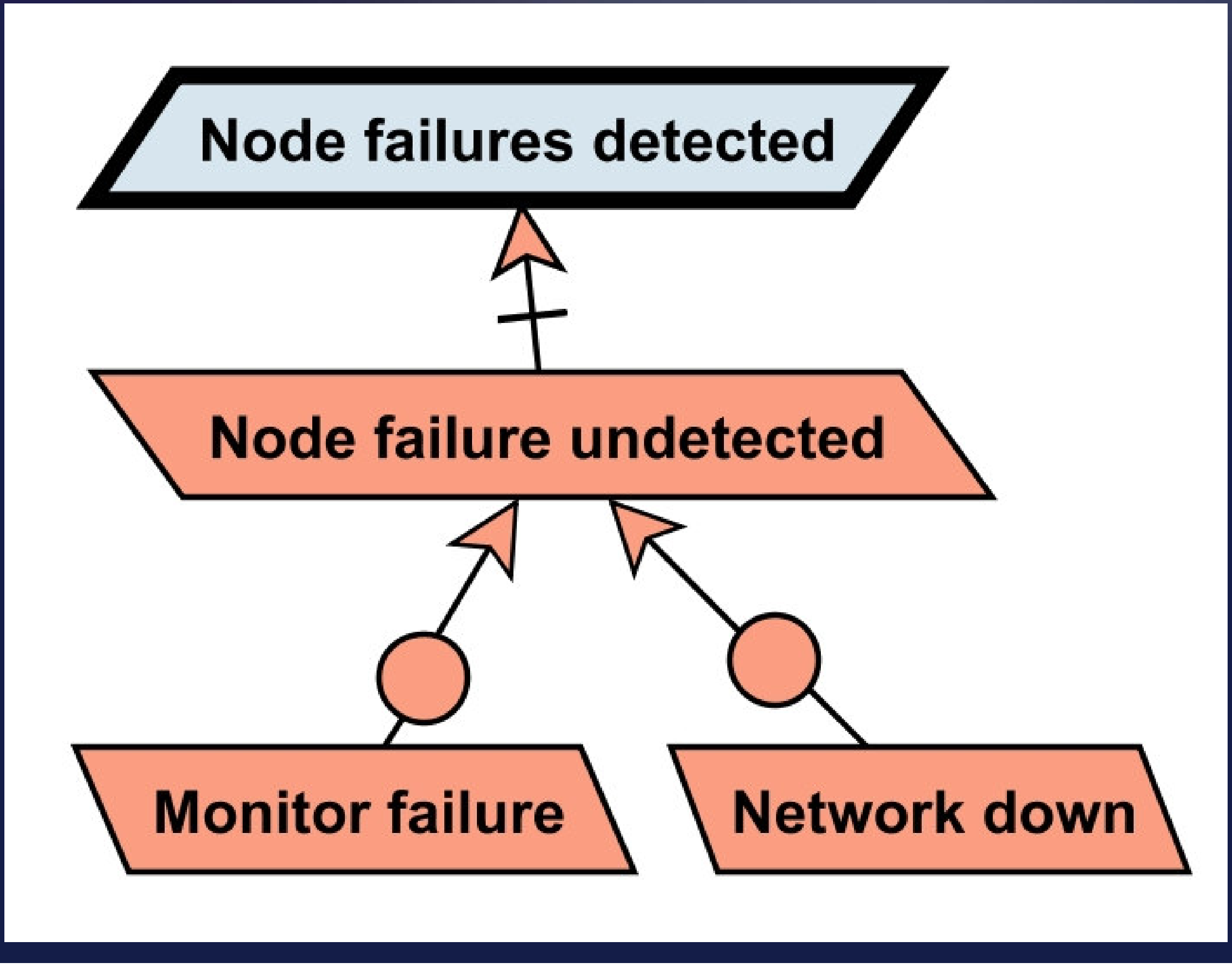
Operations Model



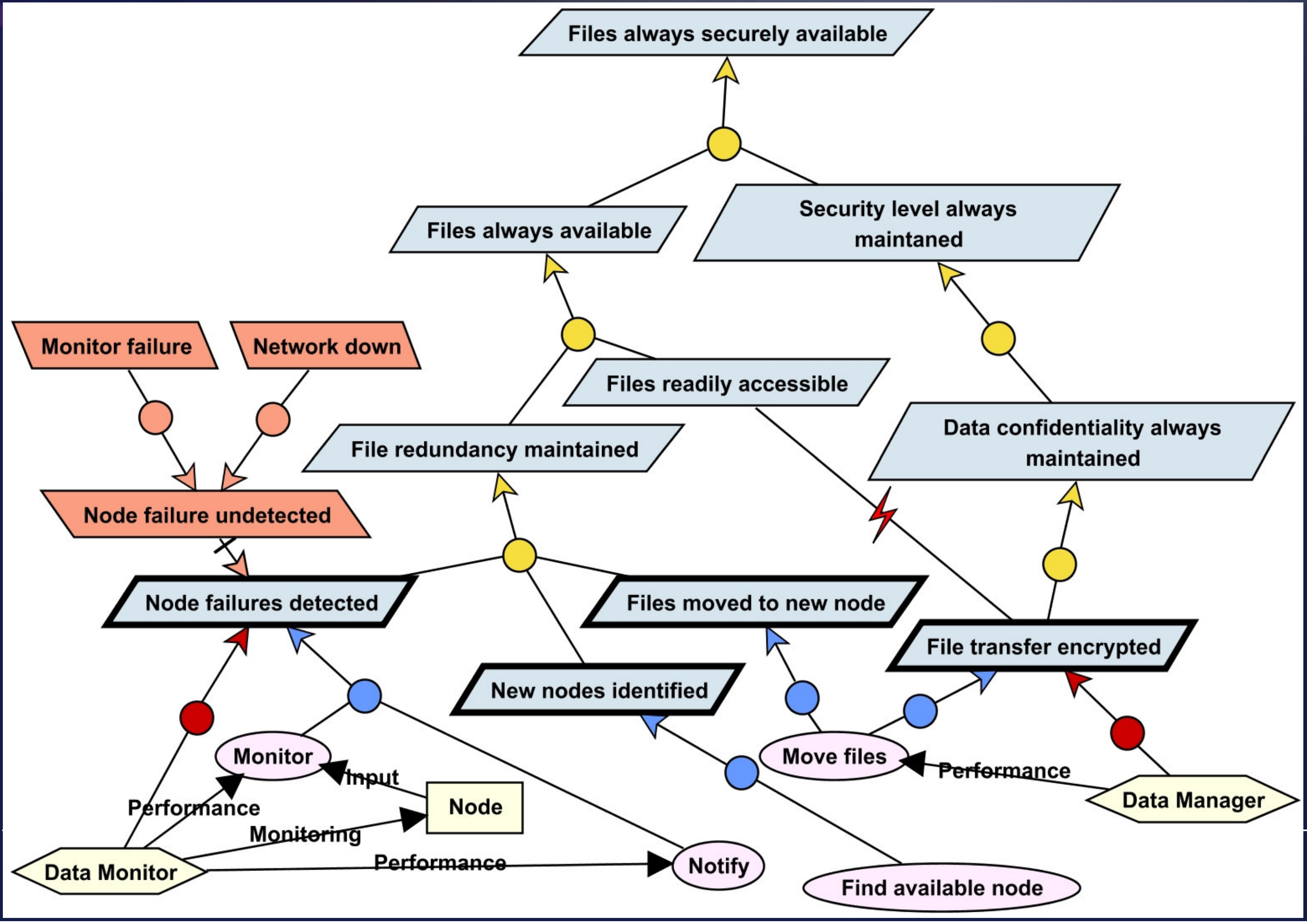
Information Society Technologies

CoreGRID

Constraints Model



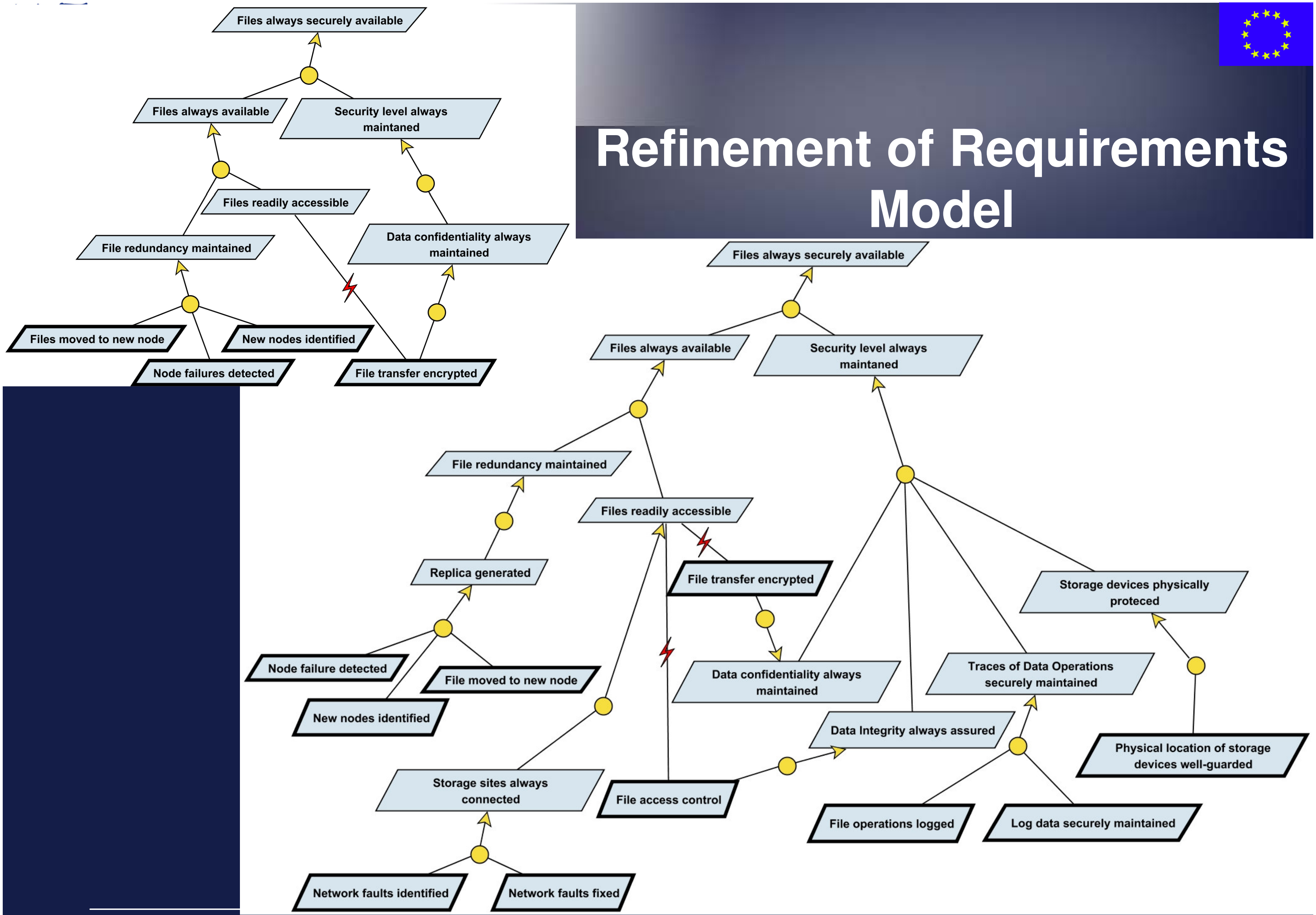
Overall Model



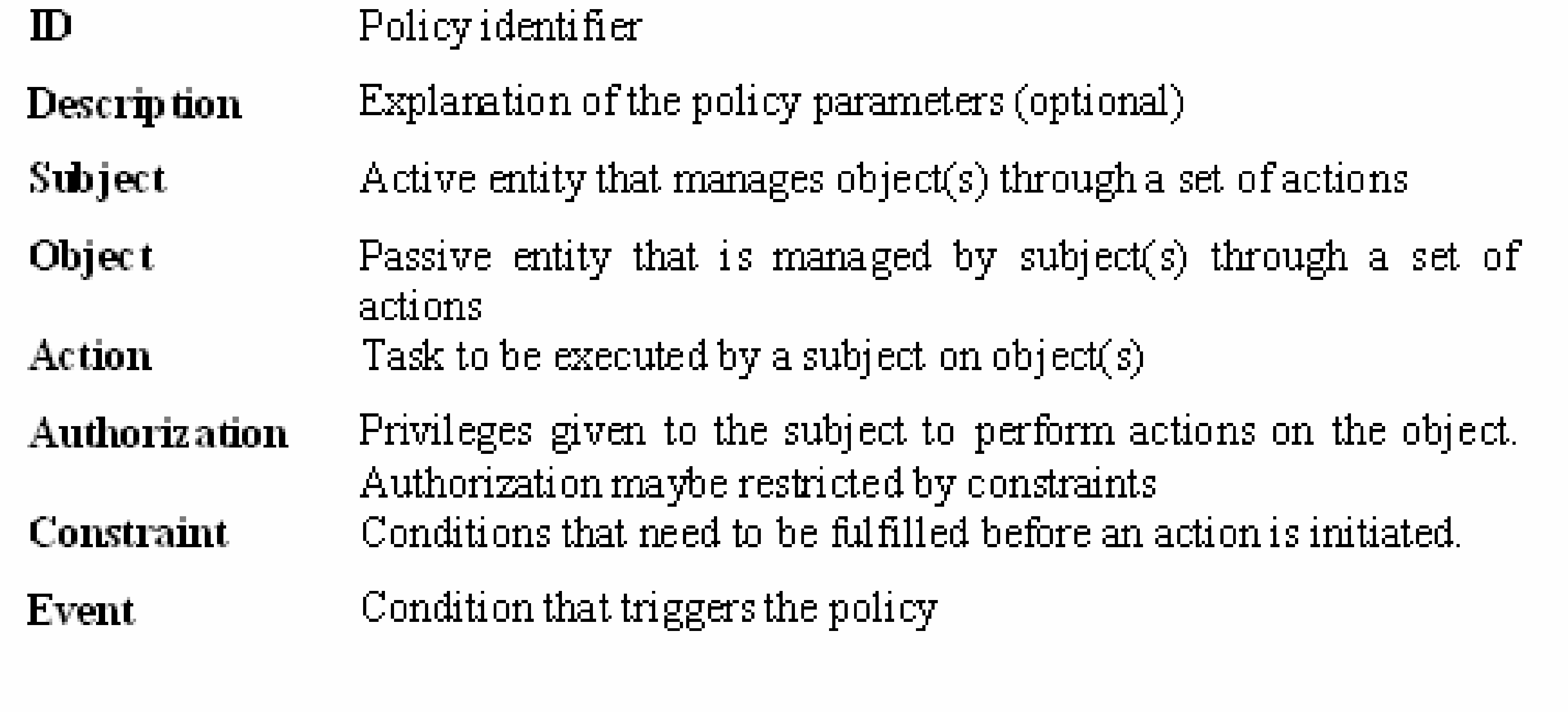
PERSPECTIVES

Derivation of Security Policies
Security Rationales

Refinement of Requirements Model


Files always securely available
Files always available
Security level always maintaned
Files readily accessible
File redundancy maintained
Data confidentiality always maintained
Files moved to new node
New nodes identified
Node failures detected
File transfer encrypted
Files always securely available
Files always available
Security level always maintaned
File redundancy maintained
Files readily accessible
Replica generated
File transfer encrypted
Storage devices physically proteced
Node failure detected
File moved to new node
New nodes identified
Data confidentiality always maintained
Traces of Data Operations securely maintained
Data Integrity always assured
Physical location of storage devices well-guarded
Storage sites always connected
File access control
File operations logged
Log data securely maintained
Network faults identified
Network faults fixed

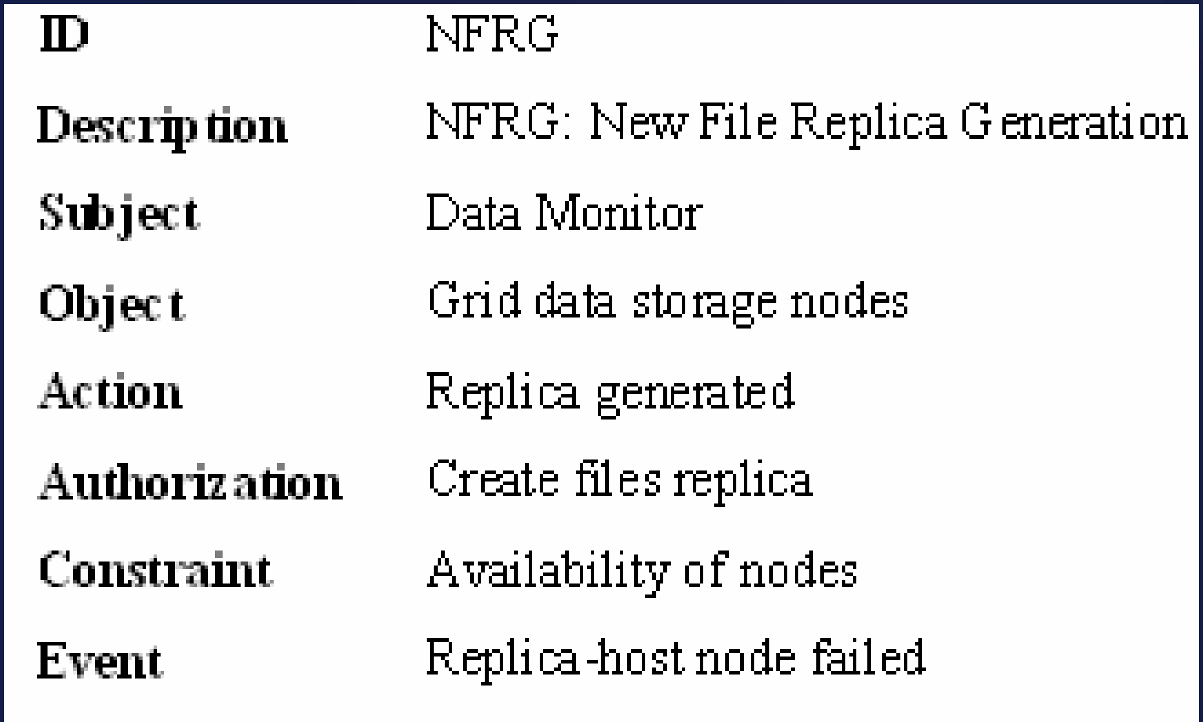
Policy Templates



ID	Policy identifier
Description	Explaration of the policy parameters (optional)
Subject	Active entity that manages object(s) through a set of actions
Object	Passive entity that is managed by subject(s) through a set of actions
Action	Task to be executed by a subject on object(s)
Authorization	Privileges given to the subject to perform actions on the object. Authorization maybe restricted by constraints
Constraint	Conditions that need to be fulfilled before an action is initiated.
Event	Condition that triggers the policy

Example Policy

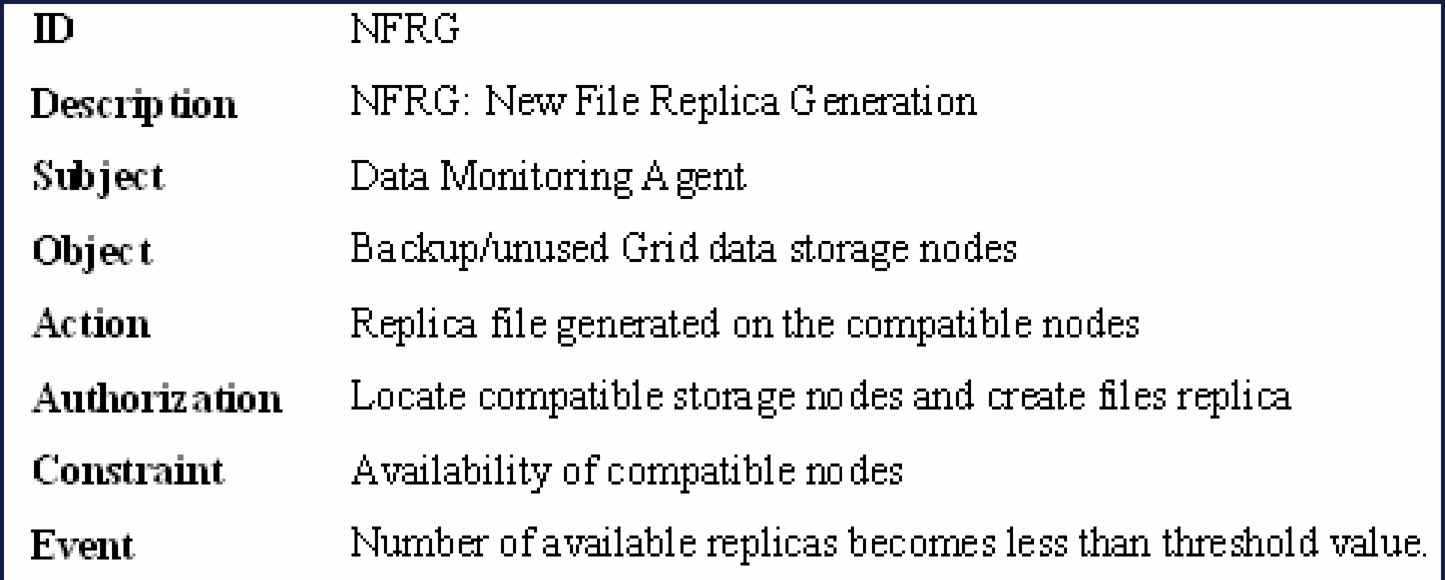
New replica of file is generated when an existing storage node is failed



ID	NFRG
Description	NFRG: New File Replica Generation
Subject	Data Monitor
Object	Grid data storage nodes
Action	Replica generated
Authorization	Create files replica
Constraint	Availability of nodes
Event	Replica-host node failed

Towards refinement …

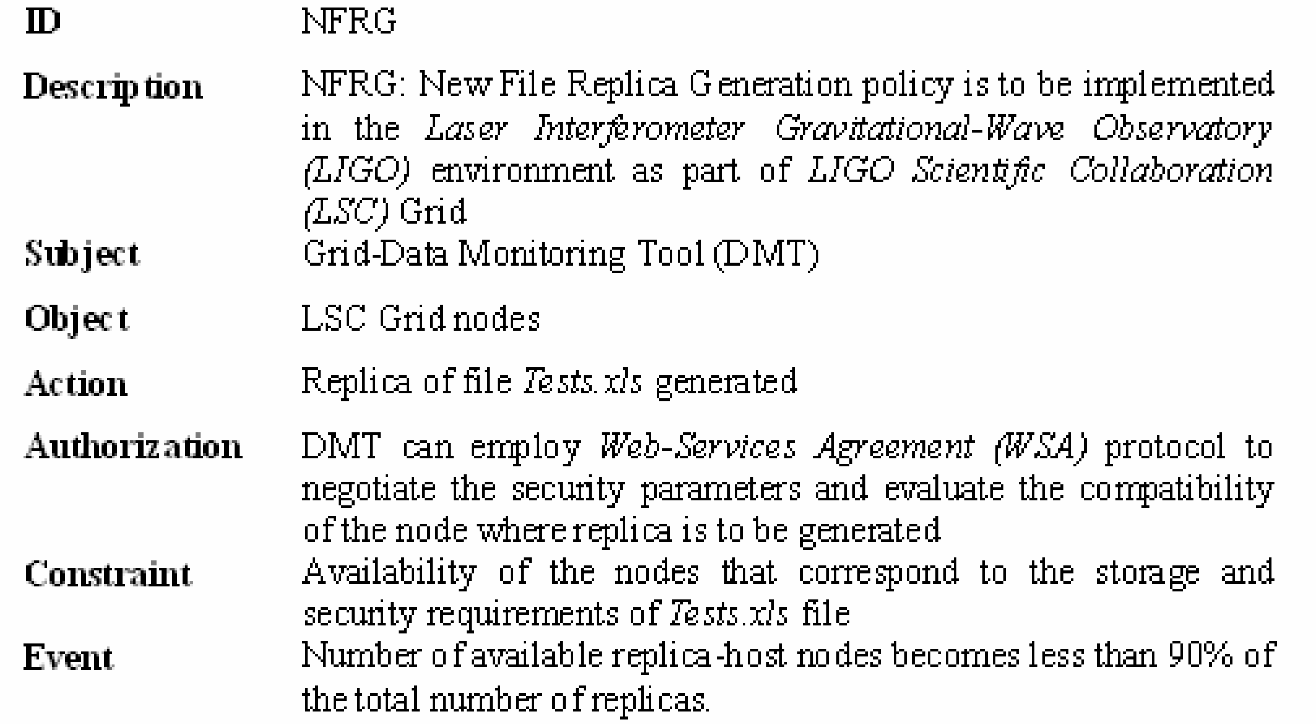
When the number of available file replicas becomes less than the threshold number, the monitoring agent will generate new replica by negotiating the security compatibility of the nodes with the file security requirements.



ID	NFRG
Description	NFRG: New File Replica Generation
Subject	Data Monitoring Agent
Object	Backup/unused Grid data storage nodes
Action	Replica file generated on the compatible nodes
Authorization	Locate compatible storage nodes and create files replica
Constraint	Availability of compatible nodes
Event	Number of available replicas becomes less than threshold value.

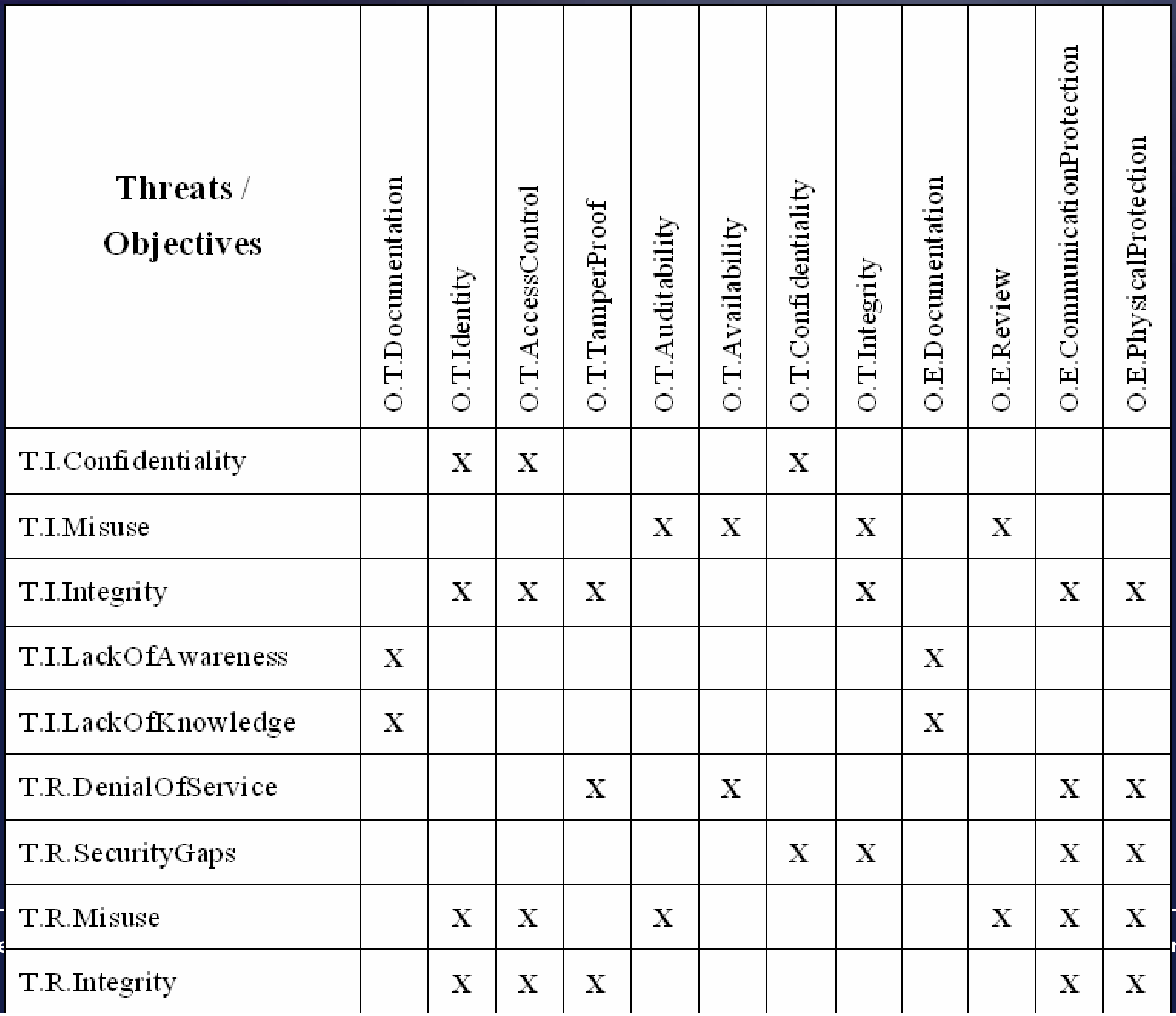
Implementation Policy

When the number of available replicas of Test.xls file becomes less than ninety percent of the total number of replicas over the LCS gird, the Grid Data Monitoring Tool will generate new replica by negotiating the security compatibility of the nodes with the security requirements of Test.xls file by using the Web-Service Agreement protocol.



ID	NFRG
Description	NFRG: New File Replica Generation policy is to be implemented in the *Laser Interferometer Gravitational-Wave Observatory (LIGO)* environment as part of *LIGO Scientific Collaboration (LSC)* Grid
Subject	Grid-Data Monitoring Tool (DMT)
Object	LSC Grid nodes
Action	Replica of file *Tests.xls* generated
Authorization	DMT can employ *Web-Services Agreement (WSA)* protocol to negotiate the security parameters and evaluate the compatibility of the node where replica is to be generated
Constraint	Availability of the nodes that correspond to the storage and security requirements of *Tests.xls* file
Event	Number of available replica-host nodes becomes less than 90% of the total number of replicas.

Security Rationales



Threats / Objectives	O.T.Documentation	O.T.Identity	O.T.AccessControl	O.T.TamperProof	O.T.Auditability	O.T.Availability	O.T.Confidentiality	O.T.Integrity	O.E.Documentation	O.E.Review	O.E.CommunicationProtection	O.E.PhysicalProtection
T.I.Confidentiality		X	X				X					
T.I.Misuse					X	X		X		X		
T.I.Integrity		X	X	X				X			X	X
T.I.LackOfAwareness	X								X			
T.I.LackOfKnowledge	X								X			
T.R.DenialOfService				X		X					X	X
T.R.SecurityGaps							X	X			X	X
T.R.Misuse		X	X		X					X	X	X
T.R.Integrity		X	X	X							X	X

“Security is like adding brakes to cars. The purpose of brakes is not to stop you: it’s to enable you to go fast!”

Gene Spafford