EMSC06
2006, Bonn, Germany

THROUGH THE EVOLUTION OF PUBLISH/SUBSCRIBE SYSTEMS: Application case

Emiliano Casalicchio (casalicchio@ing.uniroma2.it)

Federico Morabito (federico.morabito@telecomitalia.it)

Application Case: Global Monitoring Infrastructure for Critical Infrasturcuture Protection

- The problem
- Requirements
- Infrastructure Architecture
- Discussions

(the problem) Motivation

- **Critical Infrastructures** have their own local
  - monitoring and control systems,
  - security and fault prevention procedure,

indispensable to guaranty the individual system functioning

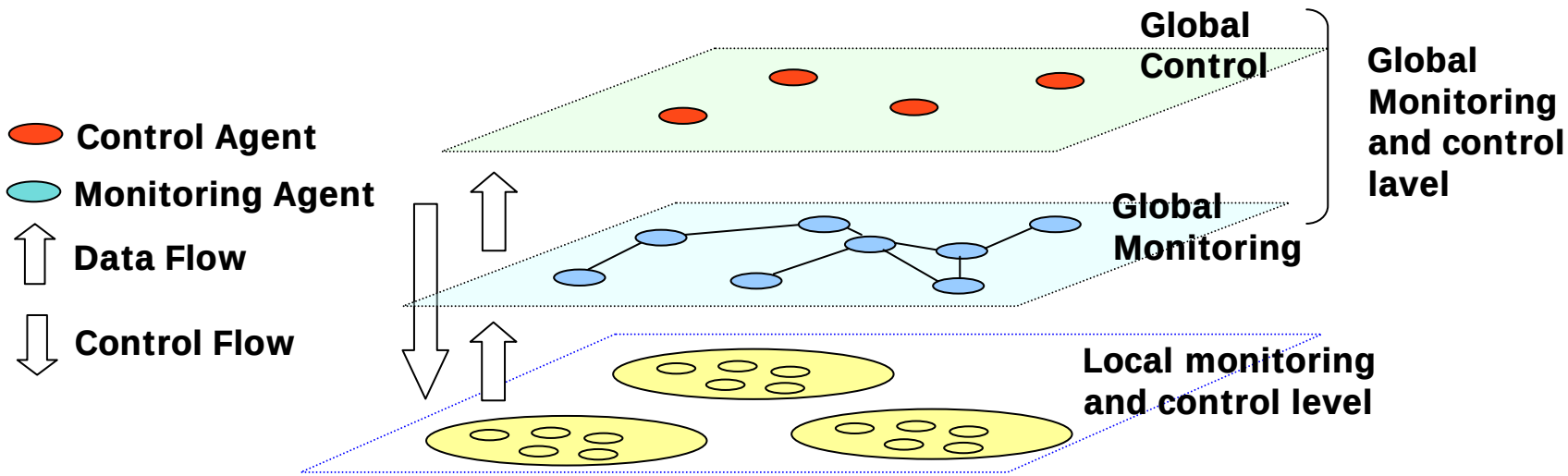
- There is the need for a ***Global Monitoring Infrastructure (GMI)***, with the goals of:
  - to catch early warning and faults events originated by single infrastructure;
  - to integrate existing monitoring and control systems;
  - to correlate and to infer the information obtained thus preventing or recovering cascading or escalating phenomena, and thus determine emergent phenomena, typical of the critical infrastructure interdependencies.

Global Monitoring Infrastructure: Performance Requirements

- *Scalability*, with respect to the number of events sources (and monitoring agents)
- *Fault tolerance*, with respect to failures of events monitoring agents, communication links, and control units
- *High speed events delivery* in order to allow the recovery actions
  - EDT << FPT, e.g. EDT~0.01FPT or EDT~0.01FPT
- *High Availability,* of monitoring functionality.
  - e.g. availability = 99.9999% => 31.5 sec. of downtime x year.
- *High Reliability of event delivery,*
  - *e.g. reliability* = 99.99% => 1/10000 lost event.
- *Security in Information delivery*
  - confidentiality of information
  - protection from malicious attacks.
  - trustiness and authentication of event sources (by control units)

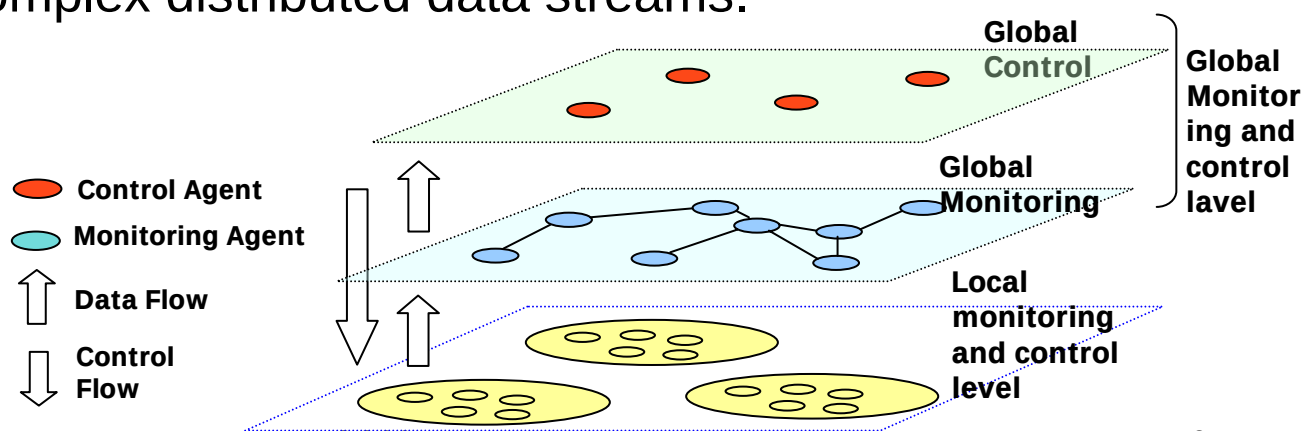
GMI architecture: high level view

- Local monitoring and control
- Global monitoring
- Global control



Global Monitoring Infrastructure: Functional Requirements

- **Continuous monitoring requirement** that is the need
  - to continuous monitor CI
  - to notify alarms (e.g. notify that some critical thresholds have been exceeded)
- **Correlation monitoring requirement**: that is the ability of the monitoring infrastructure
  - to involve more complicated, on-line manipulation, aggregation and inference over complex distributed data streams.



Candidate technologies

- The Events Notification Mechanisms: the publish-subscribe paradigm
- Communication mechanisms: the overlay networks
    - ALTERNATIVES????

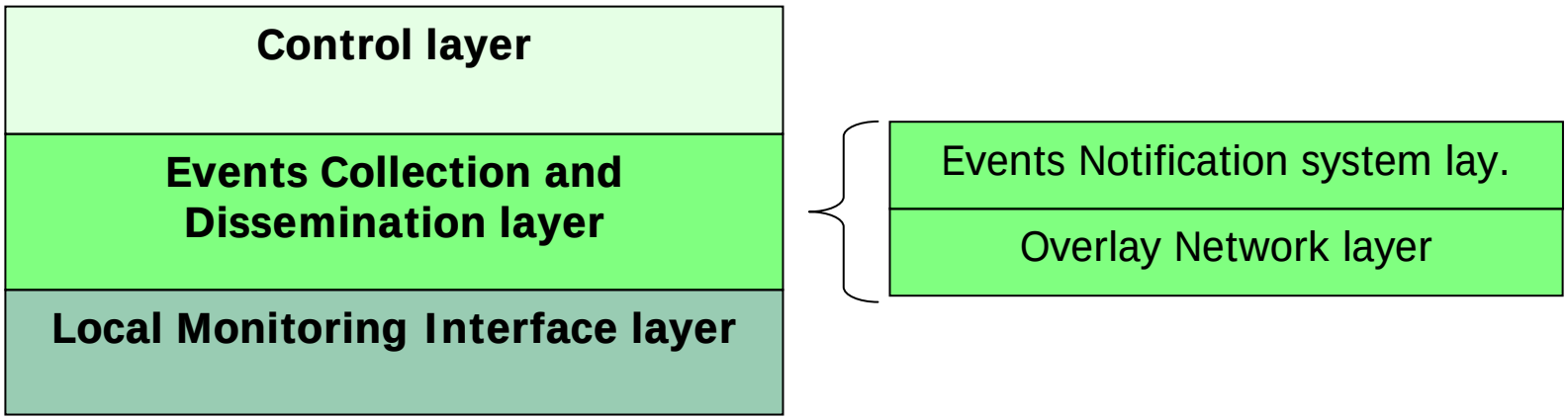
Events notification mechanisms

- Topic-based
  - Participants publish events and subscribe to individual topics selected from a predefined set.
  - The receivers for an event are known a priori
- Content-based
  - the events are classified according to the properties of the events themselves (i.e. the content).
  - Filters are defined usually in the form of name value pairs of properties and basic comparison operators.
  - The subscriptions are generic queries on an n dimensional events space, obtained expressing predicates that logically combine filters

Communication mechanisms: the overlay networks

- Broker overlay:
  - composed of a set of independent, communicating servers (broker).
  - Brokers typically communicate each other through an underlying transport protocol.
  - Clients can access the system through any broker and in general each broker stores only a subset of all the subscriptions in the system.
  - The topology of the overlay network is managed by an administrator (a broker overlay is inherently static).
- Peer-to-peer structured overlay:
  - is a self-organized application-level network composed of a set of nodes forming a structured graph over a virtual key space where each key of the virtual space is mapped to a node.
  - Distributed Hash Tables have emerged as infrastructures for efficient, scalable resource lookup in large peer-to-peer distributed networks.
  - Such systems are decentralized, scalable, and self-organizing (i.e. often as well, they automatically adapt to the arrival, departure and failure of nodes in the network).

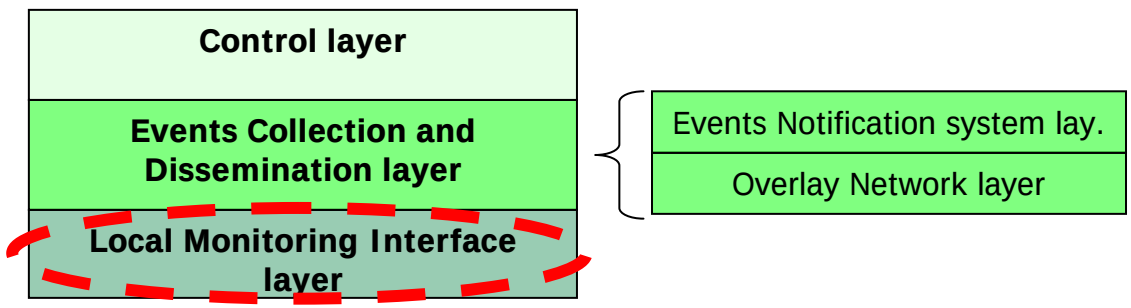
The GMI Architecture



- Local Monitoring Interface
- Events Collection and Dissemination
  - Event notification system
  - Overlay network layer
- Control layer

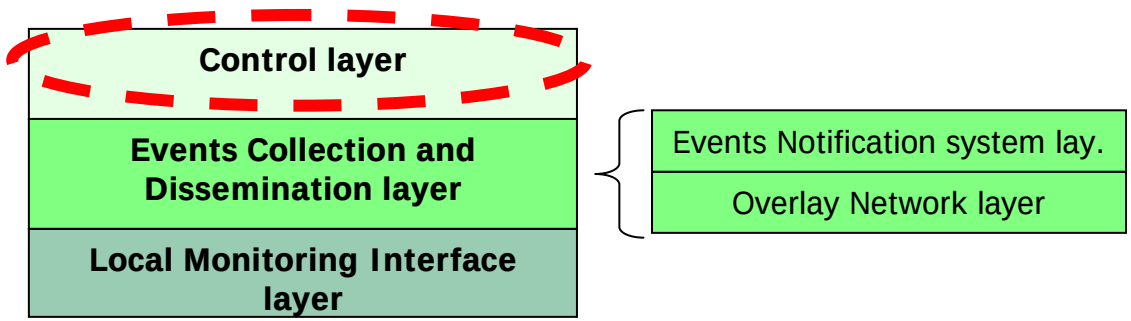
The GMI Architecture: Local Monitoring Interface

- directives for implementing the **interfaces** between the "local monitoring and control level" and the "global monitoring and control level"
- defines the **rules and technologies**
  - to export the system status information
  - to use the appropriate control feedback (from global controllers)
  - to manage the format of the incoming and outgoing data
  - to address the security level and policies required for protecting the confidential data



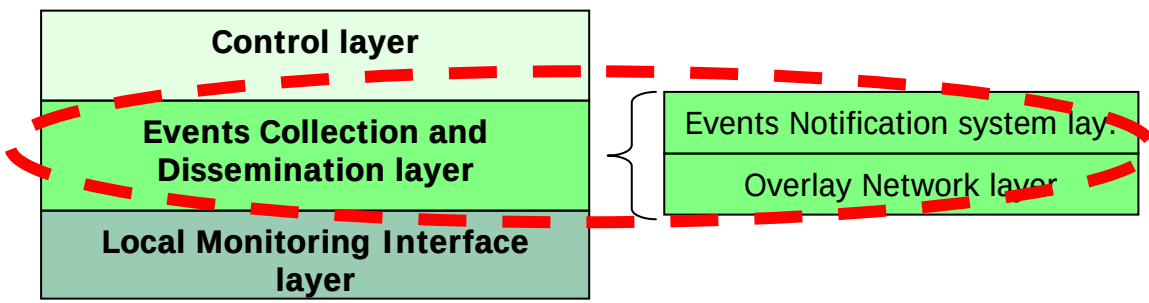
The GMI Architecture: Control layer

- the control procedures and policies are implemented here
  - Control procedure depends on the infrastructures involved in the crisis, on the gravity of the alarms and on the CI owners
- We imagine such layer as a network of software-human based systems



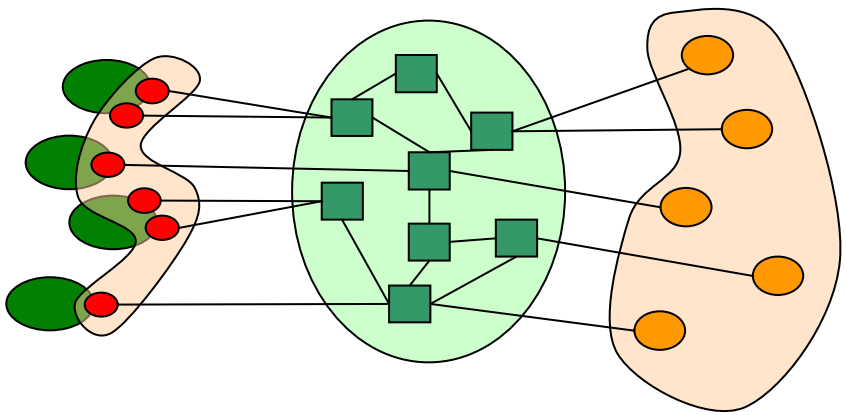
The GMI Architecture: Events Collection and Dissemination

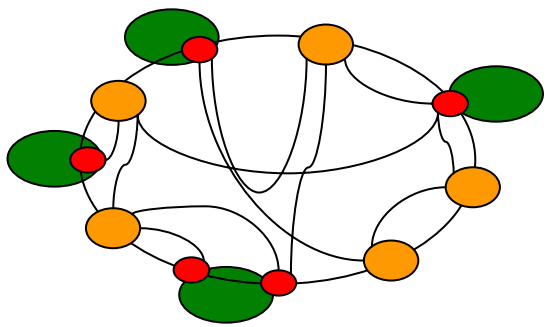
- Events notification system
  - defines the type (and the architecture) of the pub/sub interaction mechanism used to disseminate the collected information.
- Overlay network layer
  - defines the overlay network technology and the overlay network topology used by the events dissemination system.



Events Collection and Dissemination layer architecture

- Broker-based
- DHT-based





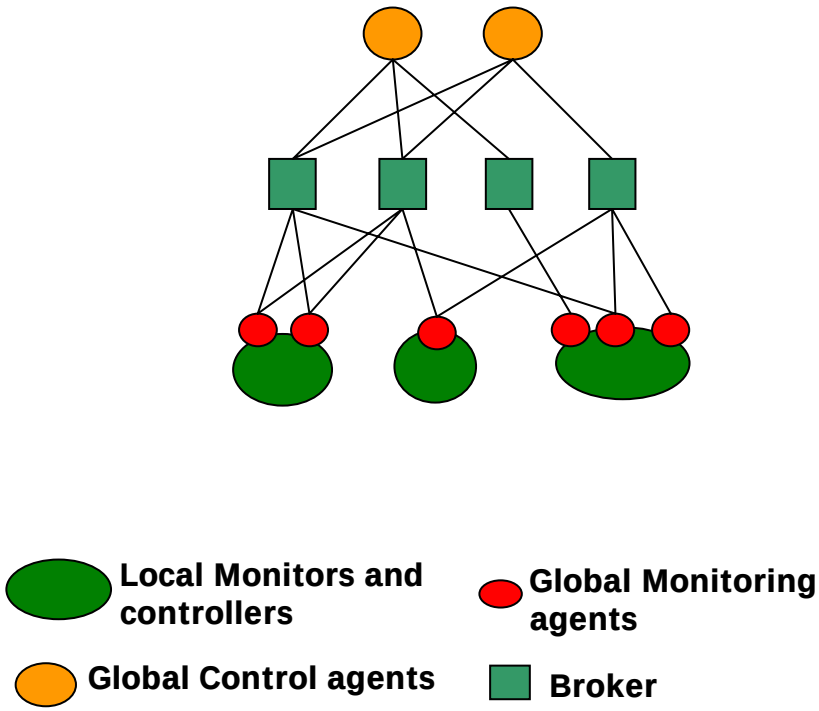
Local Monitors and controllers

Global Control agents

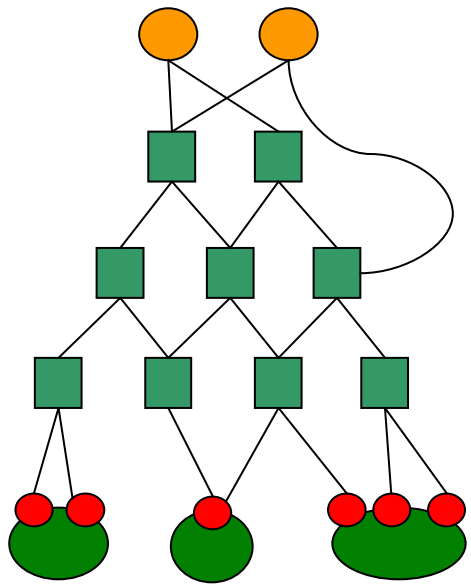
Global Monitoring agents

Broker-based architecture

- Flat



- Hierarchical



Qualitative comparison

- Functional Requirements: expressiveness of the event notification systems (interaction schema expressiveness)
  - Topic-based v.s. Content-based
- Performance Requirements: Overlay network architecture
  - Broker-based v.s. DHT-based

Interaction schema expressiveness

- Continuous monitoring requirement
  - Addressed by topic based systems
  - Alarms can be mapped in topics
  - Events can be continuously generated by every authorized entity
- Correlation Monitoring Requirement
  - Addressed by Content-based systems
  - Complex predicate can be defined over the set of events
  - Monitoring agents may be queried when needed

Overlay network architecture

	DHT-Structured overlay	Broker overlay
Scalability	Good scalability property, allowing to scale the system with respect to nodes and data	The scalability can not be easily addressed
Fault Tolerance	Self organizing mechanisms with respect to the nodes and links failures. System load self-balancing Mechanisms	Brokers are point of failures and can be also bottlenecks. The network of brokers must be designed with fault tolerance characteristics. The advantage is that the topology is well known and the brokers are managed by a unique entity.
High Speed Events Delivery	The efficiency of the information delivery depends strictly on the underlay networks infrastructures and on the actual node organization.	The static topology allow to set-up stable and high speed communications connections. By the way, low scalability of the architecture may results in very intensive traffic among brokers.
Availability	It relies on the replication of content on more than one node for improving the availability of content, enhancing performance.	Each broker can be a single point of failure and/or a bottleneck. High availability is not an intrinsic property, mechanisms must be explicitly set-up.
Security	Various cryptographic algorithms and protocols are employed to provide security for content published and stored in structured overlay networks. Authentication mechanisms can be based on access lists mechanisms and are performed at the single node. However security in DHT based overlay network is an open issue.	Brokers acts as intermediary for publisher-subscriber interaction and authentication. This introduce an higher level of security and may speed-up the authentication process. As drawback this poses an additional computational load on the brokers.

Concluding remarks

- The **continuous and correlation requirements** drive the selection of the type of pub/sub interaction paradigm:
  - Content-based permits to satisfy both requirements, thus enabling to capture the **emergent phenomena**
- The **performance requirements** define the chosen implementation of the underling overlay networks
  - **p2p structured overlay**
    - Advs.: intrinsic fault tolerant routing mechanisms, and efficient query functionalities
    - Drawbacks: the low level of security achievable, and the lack of control on the event dissemination time
  - **Brokers-based overlay**
    - Advs.: centralized system management and control, easy and efficient authentication, information control and security
    - Drawbacks: fault tolerance, availability and scalability are achievable but are not intrinsic properties