Architecture, Modelling and Tools for increasing dependability and security of Information Systems

The Objectives of DESEREC project

25 – 26 September 2006

Wroclaw University of Technology, Poland

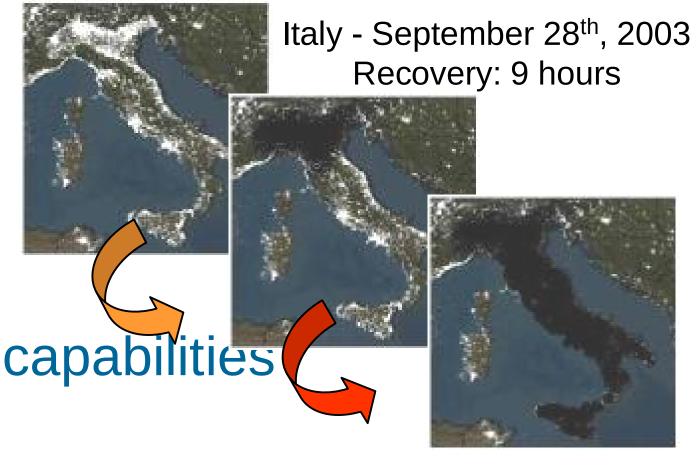
Presentation Synopsis

- DESEREC project objective
- Project organisation and schedule
- Achievements and work under progress
- The next steps
- Training workshop objective
- Project contact points

Objective: Dependability concerns

- The everyday life of European citizens relies on critical activities supported by networked Information Systems (I.S.):
  - Communications (telephone, Internet)
  - Energy & fluids (electricity, gas, water)
  - Transportation (railways, airlines, road)
  - Health and emergency response

- So far, limited taken actions let these I.S.
  - not failure-proof enough to face:
    - Software & hardware faults
    - Malicious actions: intrusion, virus
  - with poor self-healing capability
    - and therefore sensitive to cascading effects
  - suffering long recovery time



Italy - September 28th, 2003
Recovery: 9 hours

- The DESEREC project aims to leverage those capabilities
  - in new <u>and</u> existing Information Systems

Objective: DESEREC Research
A multi-tiered response driven by three objectives

First objective - ***prevent***

- keep every incident local

Second objective - ***react***

- sustain or quickly resume the critical applications

Third objective – ***plan***

- reallocate optimally the resources to recover the full range of services

Objective: The approach proposed by DESEREC

- Keep as much as possible every failure local
  - By containment of compromised or failed devices
    - Early detect: distributed monitoring
    - Identify the suspicious area: scope shaping
    - Contain the incident: cut off on the insulation border
- Plan the most probable under-nominal modes
  - With an optimal use of available resources
    - Simulation runs validate modelling
  - Deployment process
- Enable recovering capabilities
  - To resume quickly the most critical applications
    - By re-allocating the available resources
    - Even in unpredictable situations
  - Planning and simulation tools to restore full services
    - With partial resources

Containment

Planning

Reconfiguration

Objective: A multi-tiered response infrastructure

delay

Incident

1 sec

Detection

Counter-measures

Incident cleared, OK

Incident still present

10 sec

Containment

Scope shaping

No critical impact, OK

A critical service has stopped

10 min

Reconfiguration

Select an existing configuration
OR
Build an emergency configuration

Emergency configuration applied

hours

Modelling

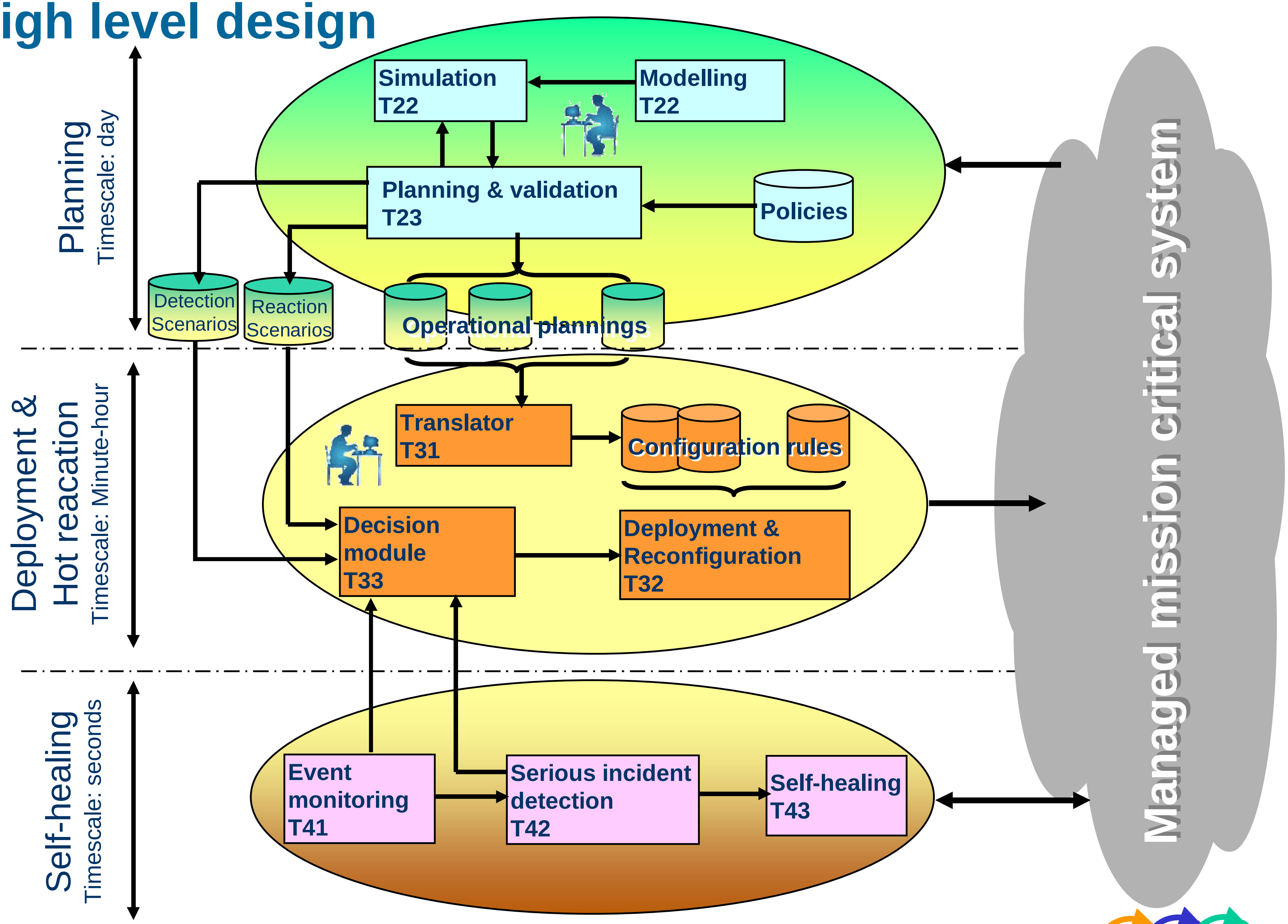
Run simulation

Configuration is optimal, OK

Optimal configuration applied

Reconfiguration

High level design



Planning
Timescale: day

Simulation T22

Modelling T22

Planning & validation T23

Policies

Detection Scenarios

Reaction Scenarios

Operational plannings

Deployment &
Hot reacation
Timescale: Minute-hour

Translator T31

Configuration rules

Decision module T33

Deployment & Reconfiguration T32

Self-healing
Timescale: seconds

Event monitoring T41

Serious incident detection T42

Self-healing T43

Managed mission critical system

The overall approach

- DESEREC propose a framework to improve the dependability of Information Systems:
  - Methods
  - Tools
- The approach is to minimize the cost of high resilience
  - By focusing on the dependability at business services level
    - Rather that at components level
  - With a proactive detection of incidents or intrusion
    - And immediate reaction, including containment of a part of the I.S.
  - By avoiding oversized redundancies and provisioning limited resources
    - To enable the usage of less critical resource to reconfigure high-priority business services in minutes
- The ultimate goal is to provide the I.S. manager with indicators
  - Showing, in real-time, the resilience margin of each business service
  - And a simulation tool to forecast the worst scenario for the next coming days
    - From the history of traffic and faults record track

Implementation Objectives

Rationale

- Target I.S. are mission critical information systems with multiple services
- The scalability is a challenging issue with real I.S.
  - With 1000s or more configuration items (computer, router, firewall, link, etc.)
- The immediate reaction to incident or intrusion by containment
  - Is realistic only with pre-existing methods to apply
    - Analyse of a large model under one second is not obvious and what about the reliability of the deployment?
    - In the contrary pre-defined methods could be evaluated (simulated)
- The component granularity is meaningless for reconfiguration
    - Especially when thinking about a set of methods attached to every atom
    - Some provisions such as software installation is a prerequisite
  - And unreliable for incident detection
    - Only a **set** of components could provide its proxy with its reliable own status

Service Fault management by Deserec

Objective of Deserec (in red)

n service fault prevention: prevent the occurrence or introduction of faults,

n service fault tolerance: deliver correct service in the presence of faults,

n service fault removal: reduce the number or severity of faults,

n service fault forecasting: estimate the present number, the future incidence, and the likely consequences of faults,

n service fault treatment: in order to prevent faults from happening several times

Service Fault definition (in Deserec context)

Cause of a service disturbance that affects its dependability attributes. Service fault origin could be of various nature from hardware/software fault or malicious attack.

Deserec monitoring

Deserec objective:

Monitor information system components (hardware, software, network) in order to detect incidents affecting services and make decision for fast reaction or later reconfiguration. The monitoring function shall collect information in order to inform about the status of the relevant service attributes and in particular the dependability margin.

Deserec means to reach objective:

Use of existing event monitoring techniques to collect events (SNMP, syslog, IDS), normalize collected data (to be defined) and process them to detect incidents (T4.2 / T3.3).

In addition to predefined reaction scenarios, Deserec will try to bring a self learning loop to improve reactions or assist operator to define new ones.

Deserec reconfiguration

Deserec objective:

Optimise allocation of resources to maintain critical services. None critical services can be interrupted.

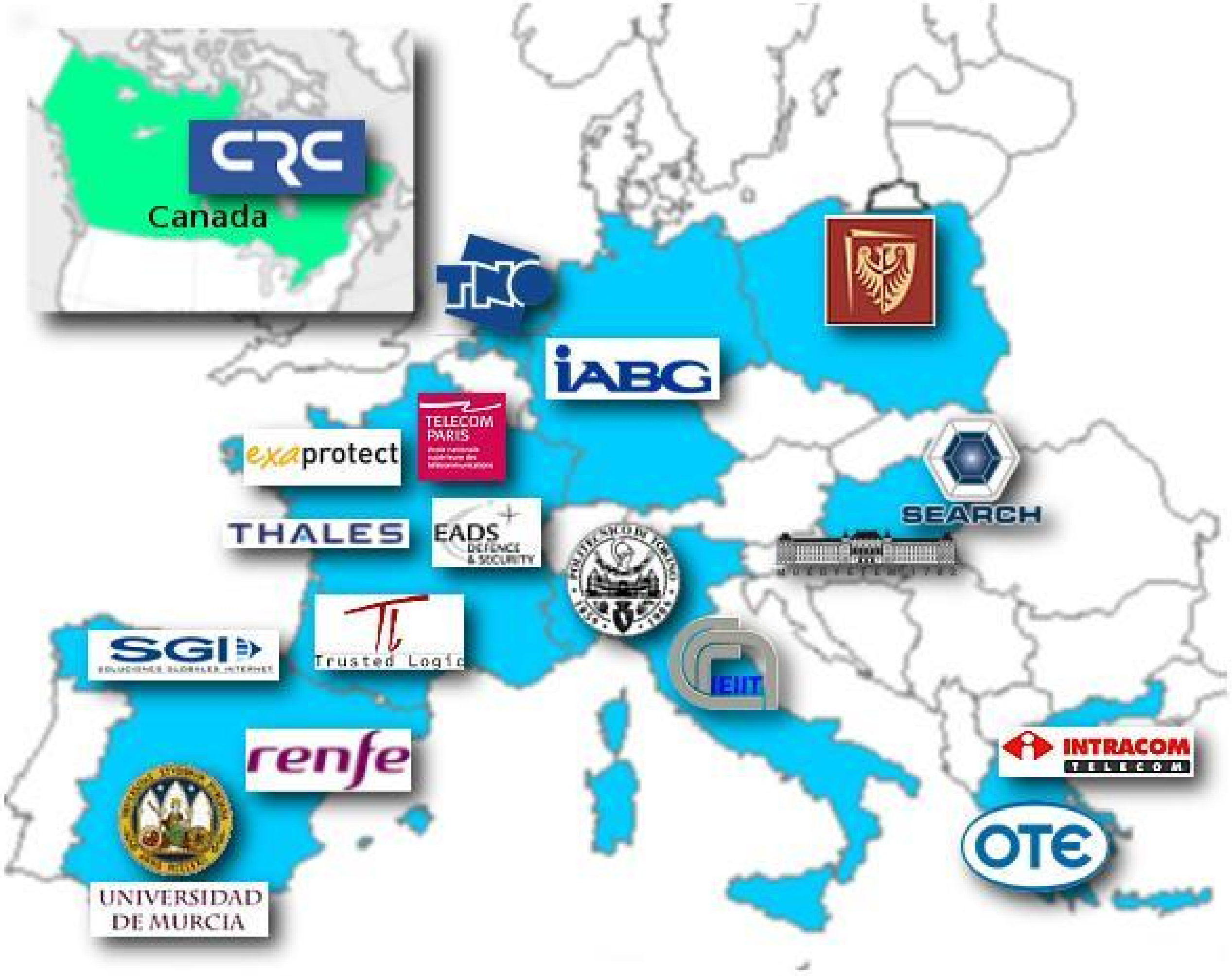
Deserec means to reach objective:

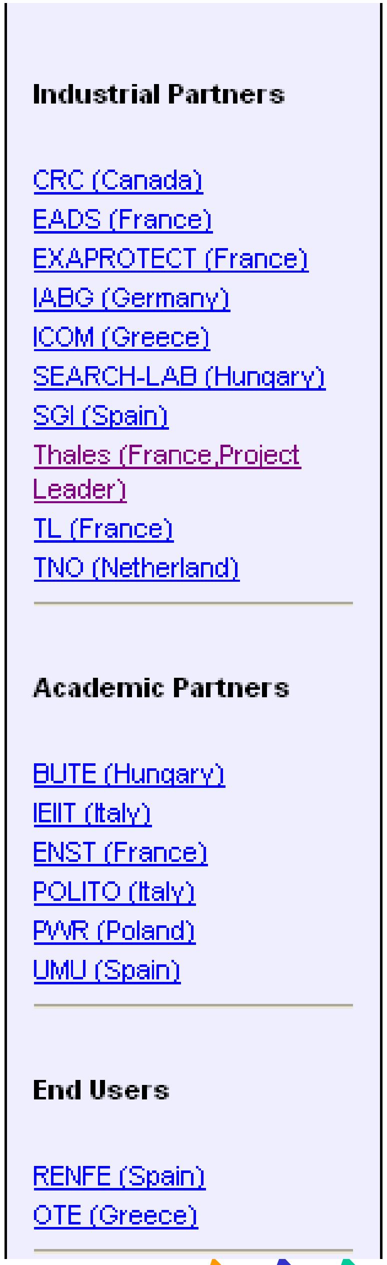
Deploy policies and other countermeasures via Deserec agents distributed over the Information System infrastructure.

Deserec will make use of existing Information System reaction means not requiring redesign or additional development of the IS itself.

Project organization

- THALES (leader); EADS (technical lead); POLITO (scientific lead)





Industrial Partners

CRC (Canada)
EADS (France)
EXAPROTECT (France)
IABG (Germany)
ICOM (Greece)
SEARCH-LAB (Hungary)
SGI (Spain)
Thales (France,Project Leader)
TL (France)
TNO (Netherland)

Academic Partners

BUTE (Hungary)
IEIIT (Italy)
ENST (France)
POLITO (Italy)
PWR (Poland)
UMU (Spain)

End Users

RENFE (Spain)
OTE (Greece)

Project Schedule

3-year project from Jan 2006 to Dec 2008

- Planned milestones and reviews
  - M9: Requirements and States of the art
  - M15: Architecture and specifications
  - M18: Intermediate Demo
  - M21: Modelling, validation, configuration & management tools
  - M24: Fast cicatrisation, self learning
  - M30: Simulation, formal verification & planning
  - M36: Full Demo

Project organization and schedule

Main Public Events

- Training workshops
  - Organised by PWR at Wroclaw, “Architecture, Modelling and Tools for Increasing Dependability and Security of Information Systems” (Sept-2006)
  - Organised by ICOM, “The Mechanisms used for Increasing dependability through enhanced reconfiguration” (2007)
  - Organised by UMU, “The results and Applications for DESEREC” (2008)

- Participation to international conferences on Dependability

Achievements and progress

End-user scenario

- Renfe
  - The national railway operator of Spain, providing the public service of train transportation for both passengers and trade goods.
  - The RENFE scenario includes the Web information, ticket selling and timetable information. RENFE Web Portal is available on www.renfe.es, offering services such as:
    - Web Information
    - Ticket Selling (called TIKNET)
    - Timetable Information

Achievements and progress

End-user scenario

- OTE
  - OTE is the major Greek telecom operator providing a wide range of telecom services in Greece and in the Balkan area
  - The end-user scenario is a combination of Fast Internet and IPTV services (both Video on Demand and Video Broadcasting). The end-user accesses these services through a network infrastructure that is composed of access and metro network elements.
  - Services:
    - Fast Internet,
    - IPTV
      - Video on demand
      - Video broadcasting

Achievements and progress

End-user scenarios and User requirements

- Available in D1.1 document

- User requirements will be refined and completed within D1.3 document (due at M12)

Achievements and progress

WP3, WP4 State Of The Art and Requirements

- WP3 requirements available in D3.1 document
  - In addition SOTA documents have been produced for each task

- WP4 requirements available in D4.1 document
  - In addition SOTA documents have been produced for each task

Introducing one possible approach

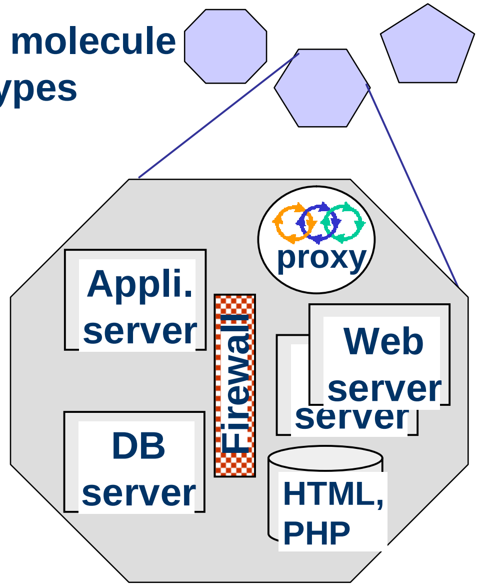
- Hereafter is introduced some concepts that are still under study
  - Objective is trying to reduce complexity for reconfiguration purpose
    - Introducing molecule concept
    - Introducing cell concept
  - These ideas are not yet finalised and may evolve

Introducing molecule concept

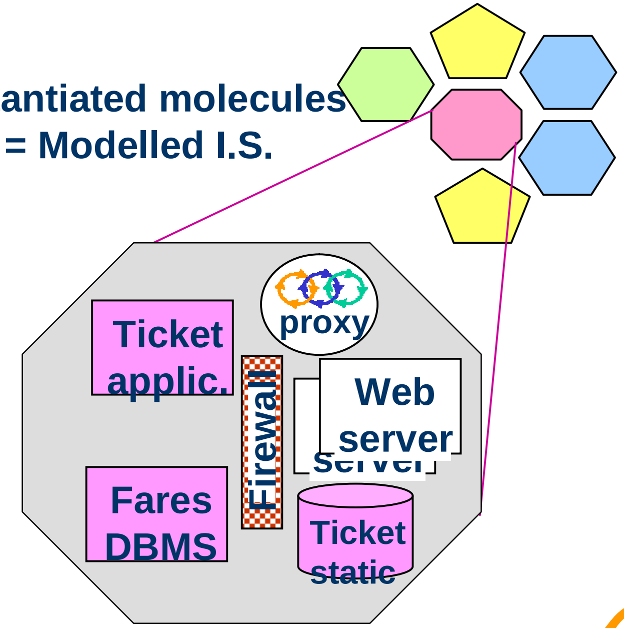
Design (reorganise) the I.S. in “molecules” or technical services

- A limited set of “prototypes” of such molecule
  - Each gathering several capabilities, with its own low-level resilience (redundancy, …)
  - Are instantiated with pre-installed software applications enabling a set of possible configurations
  - At a given time, it runs a specific application, data, parameters = current configuration

Dependable molecule prototypes

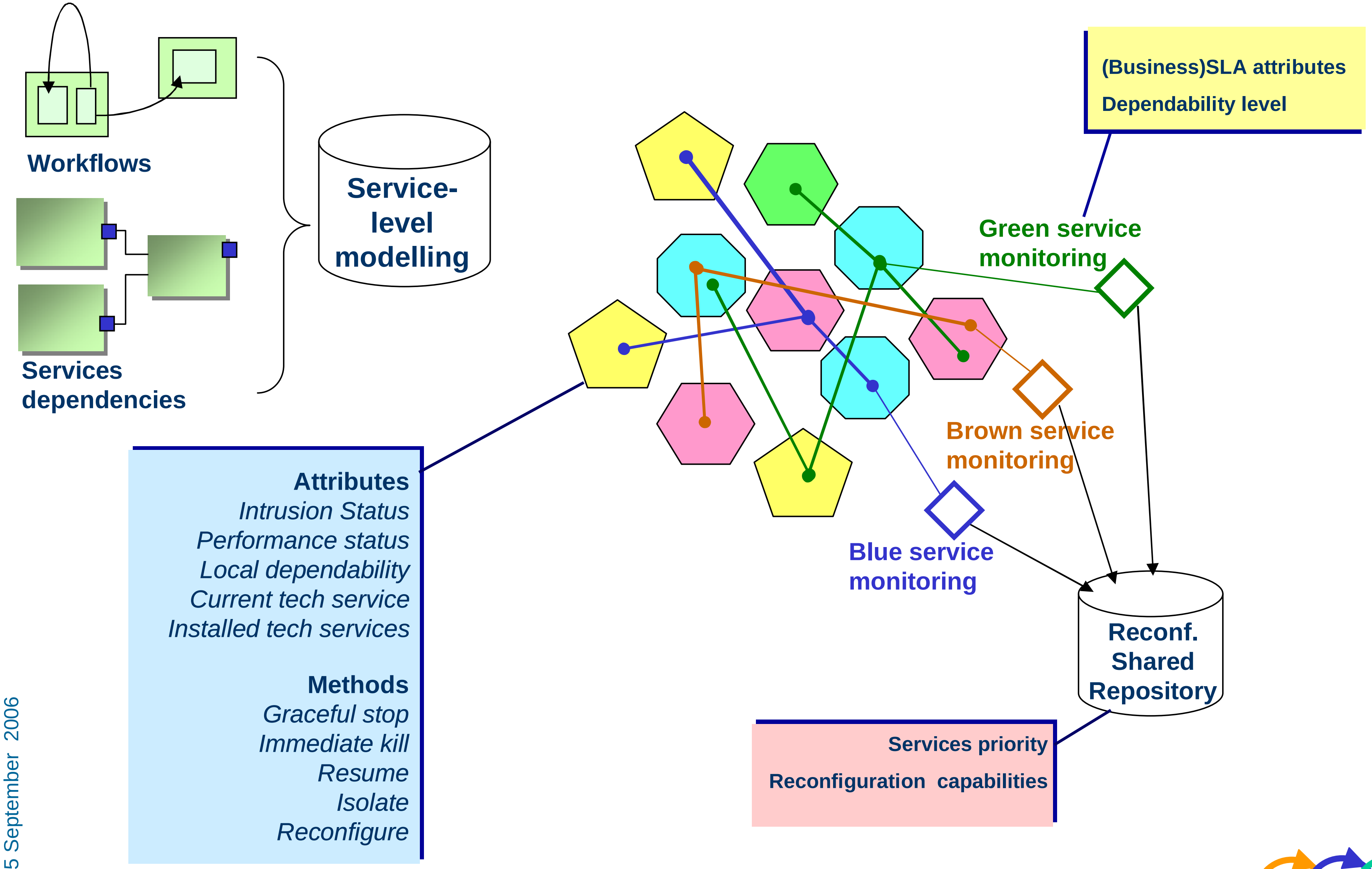


Instantiated molecules = Modelled I.S.



The business service level

- A business service is a combination of such technical services



(Business)SLA attributes

Dependability level

Attributes
Intrusion Status
Performance status
Local dependability
Current tech service
Installed tech services

Methods
Graceful stop
Immediate kill
Resume
Isolate
Reconfigure

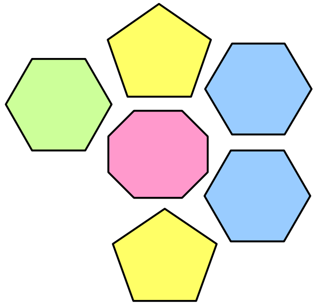
Services priority

Reconfiguration capabilities

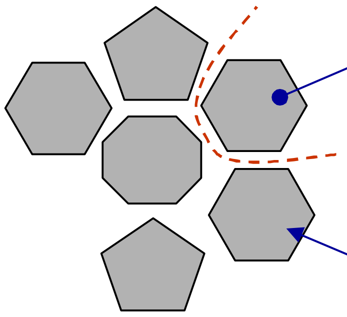
25 September 2006

The different functions

Instantiated molecules = Modelled I.S.



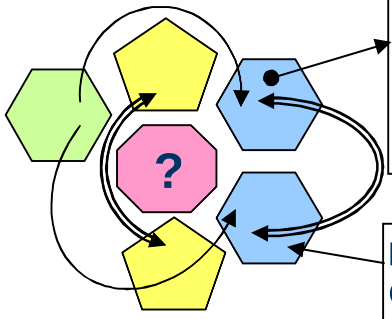
Monitoring & Self-healing



Attributes:
Intrusion status
Performance level
Local dependability

Self-healing methods
Immediate kill
Isolate

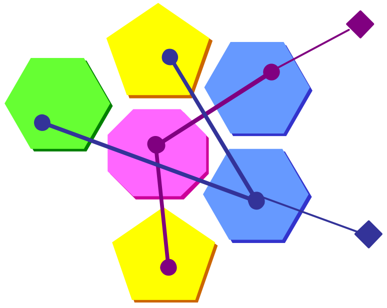
Reconfiguration



Attributes:.
Current configuration
Alternate configuration

Reconfiguration methods
Graceful stop
Reconfigure
Resume

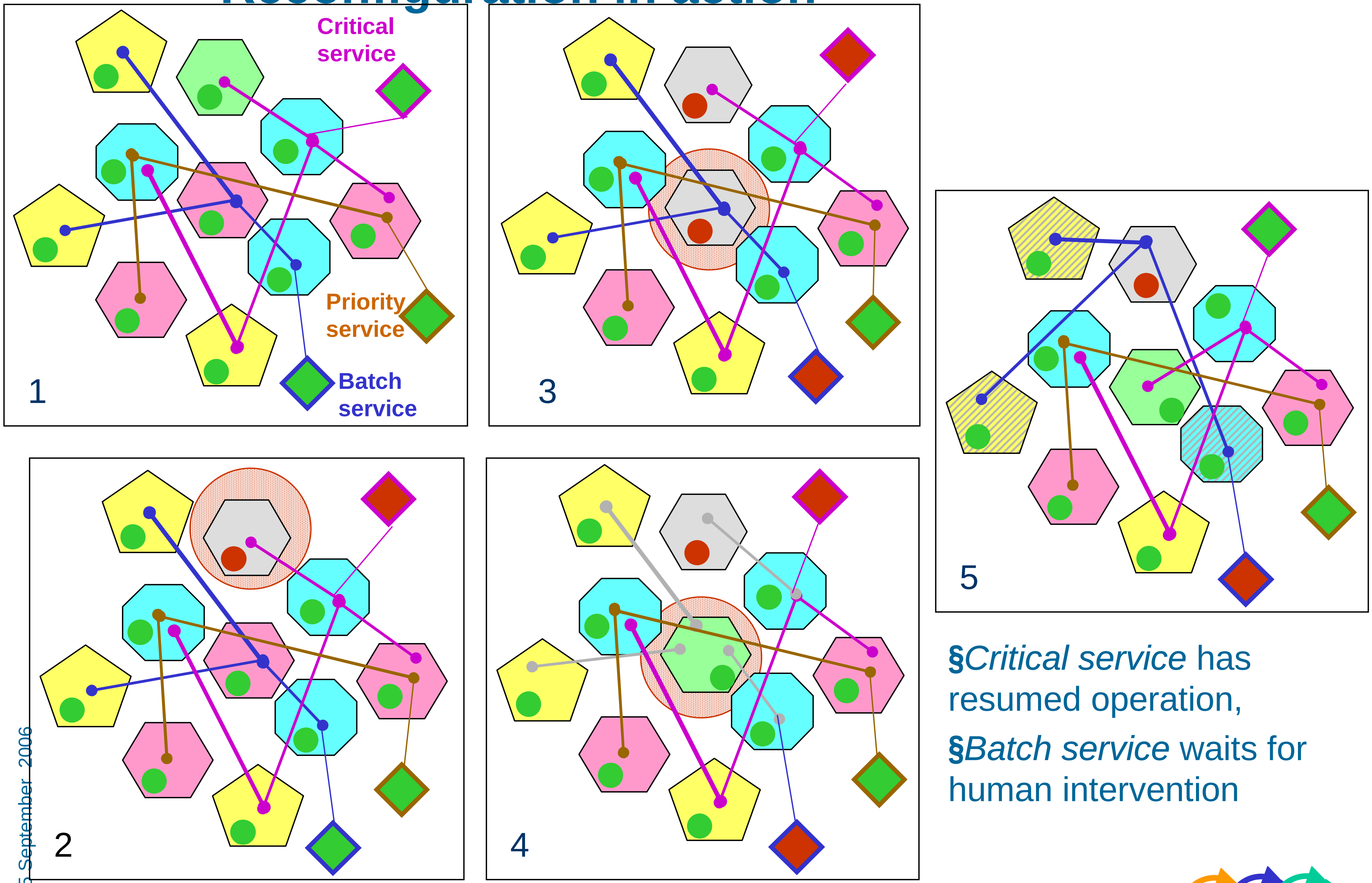
Business services composition



Attributes at B.S. level:.
SLAs & priority
Current status
Dependability level

Attributes at global level:.
Reconfiguration resources
Dependability margins

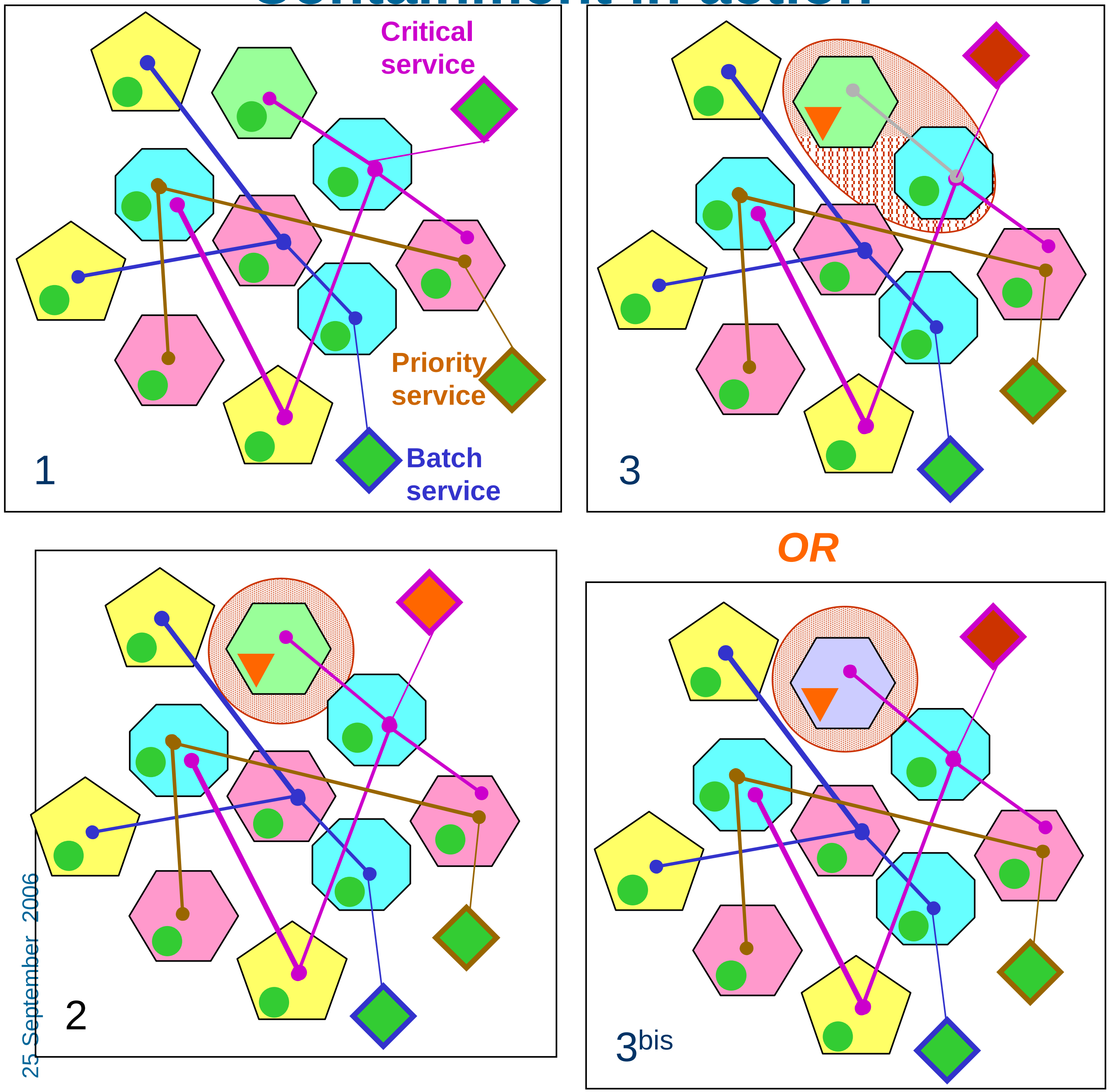
Reconfiguration in action



§*Critical service* has resumed operation,

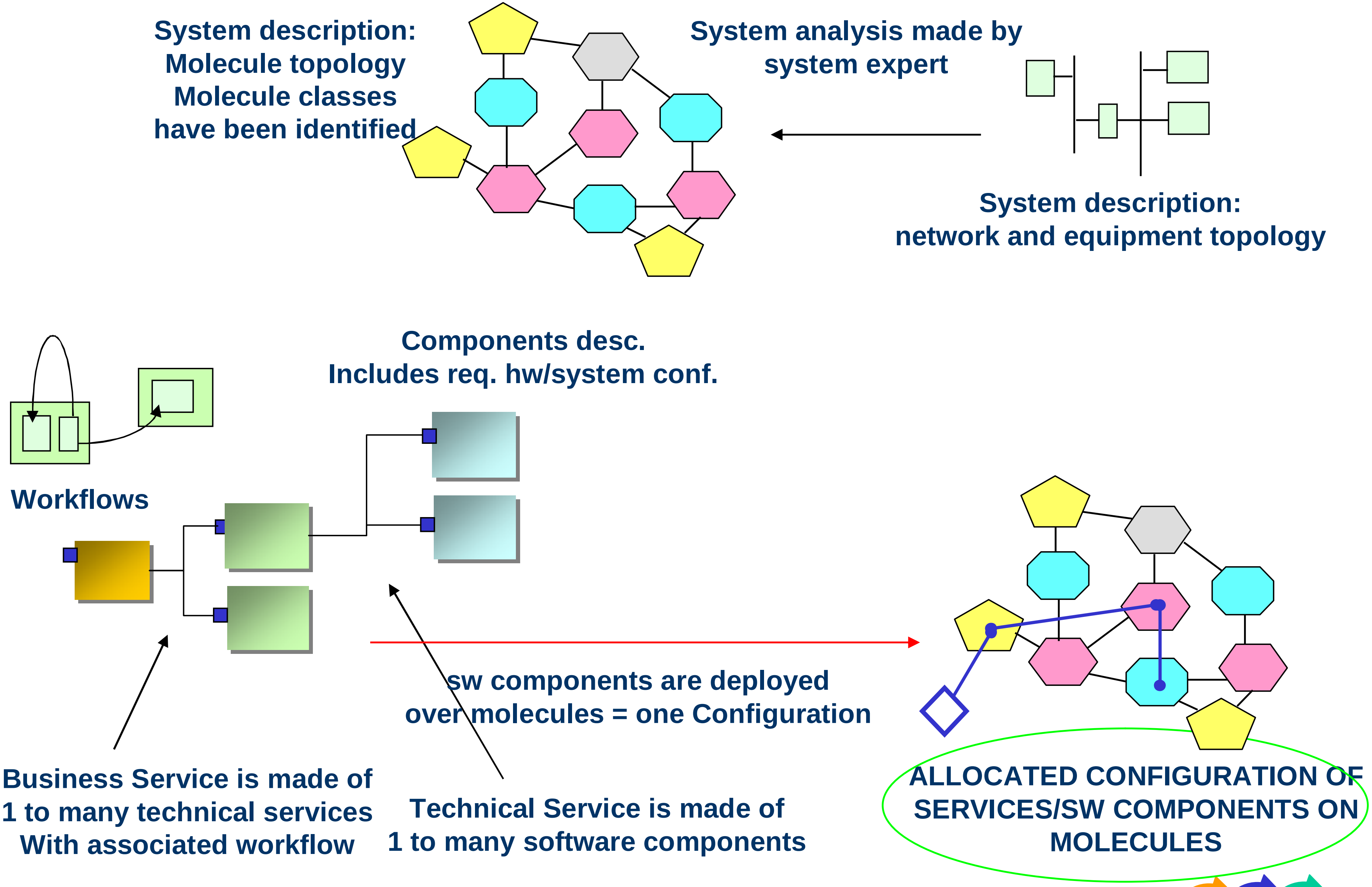
§*Batch service* waits for human intervention

Containment in action



- *Faulty molecule* is either stopped or isolated
- *Reconfiguration* of impacted business service could now take place

High level configuration



System description:
Molecule topology
Molecule classes
have been identified

System analysis made by
system expert

System description:
network and equipment topology

Components desc.
Includes req. hw/system conf.

Workflows

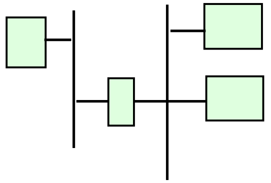
sw components are deployed
over molecules = one Configuration

Business Service is made of
1 to many technical services
With associated workflow

Technical Service is made of
1 to many software components

ALLOCATED CONFIGURATION OF
SERVICES/SW COMPONENTS ON
MOLECULES

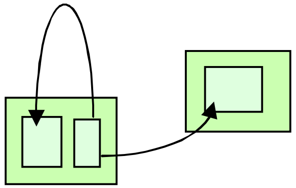
Molecules and Monitoring



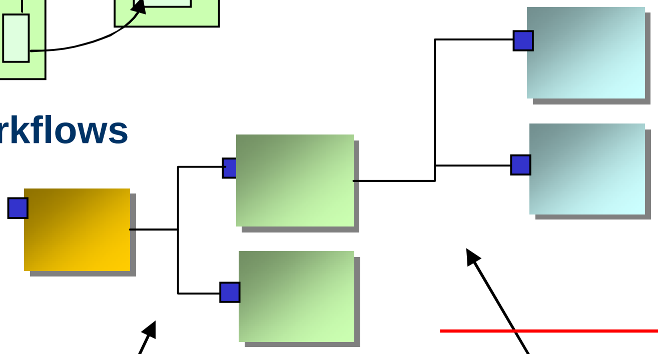
System description:
network and equipment topology

Monitoring tools are not under DESEREC control:
Already deployed and configured for all configs

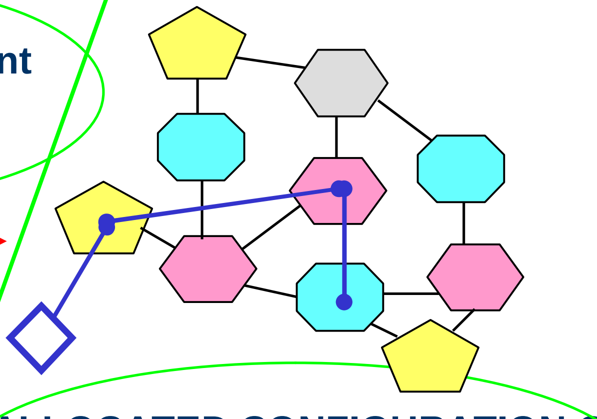
infrastructure monitoring tools
(snmp, syslog, IDS…)



Workflows



Software component
monitoring tools
(snmp, syslog…)



sw components are deployed
over molecules = one Configuration

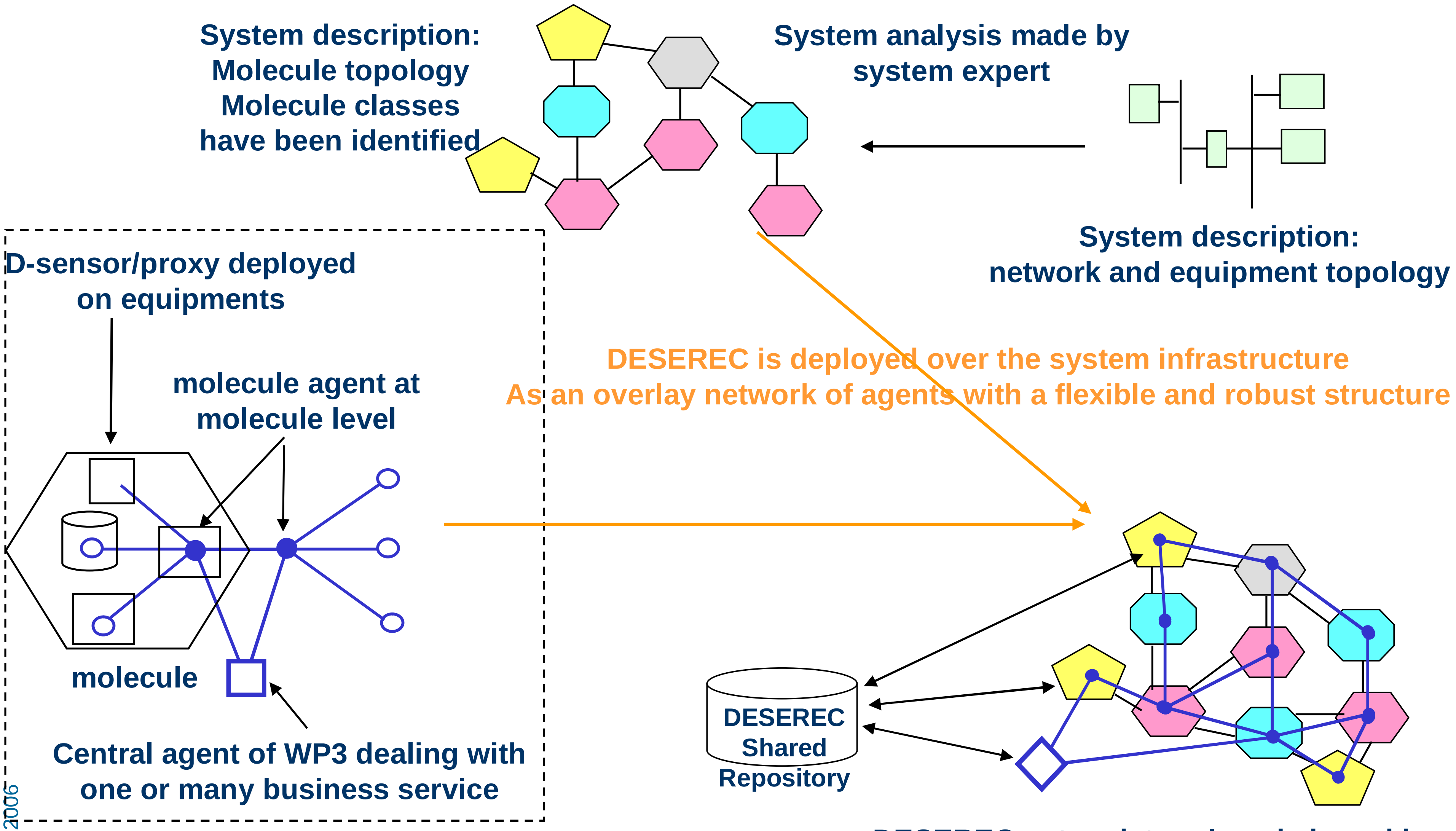
Business Service is made of
1 to many technical services
With associated workflow

Technical Service is made of
1 to many software components

ALLOCATED CONFIGURATION OF
SERVICES/SW COMPONENTS ON
MOLECULES

ALLOWS MONITORING OF
SYSTEM+COMPONENTS -> TECH. SERVICES -> BUSINESS SERVICES

DESEREC framework management



System description:
Molecule topology
Molecule classes
have been identified

System analysis made by
system expert

System description:
network and equipment topology

D-sensor/proxy deployed
on equipments

molecule agent at
molecule level

molecule

Central agent of WP3 dealing with
one or many business service

DESEREC is deployed over the system infrastructure
As an overlay network of agents with a flexible and robust structure

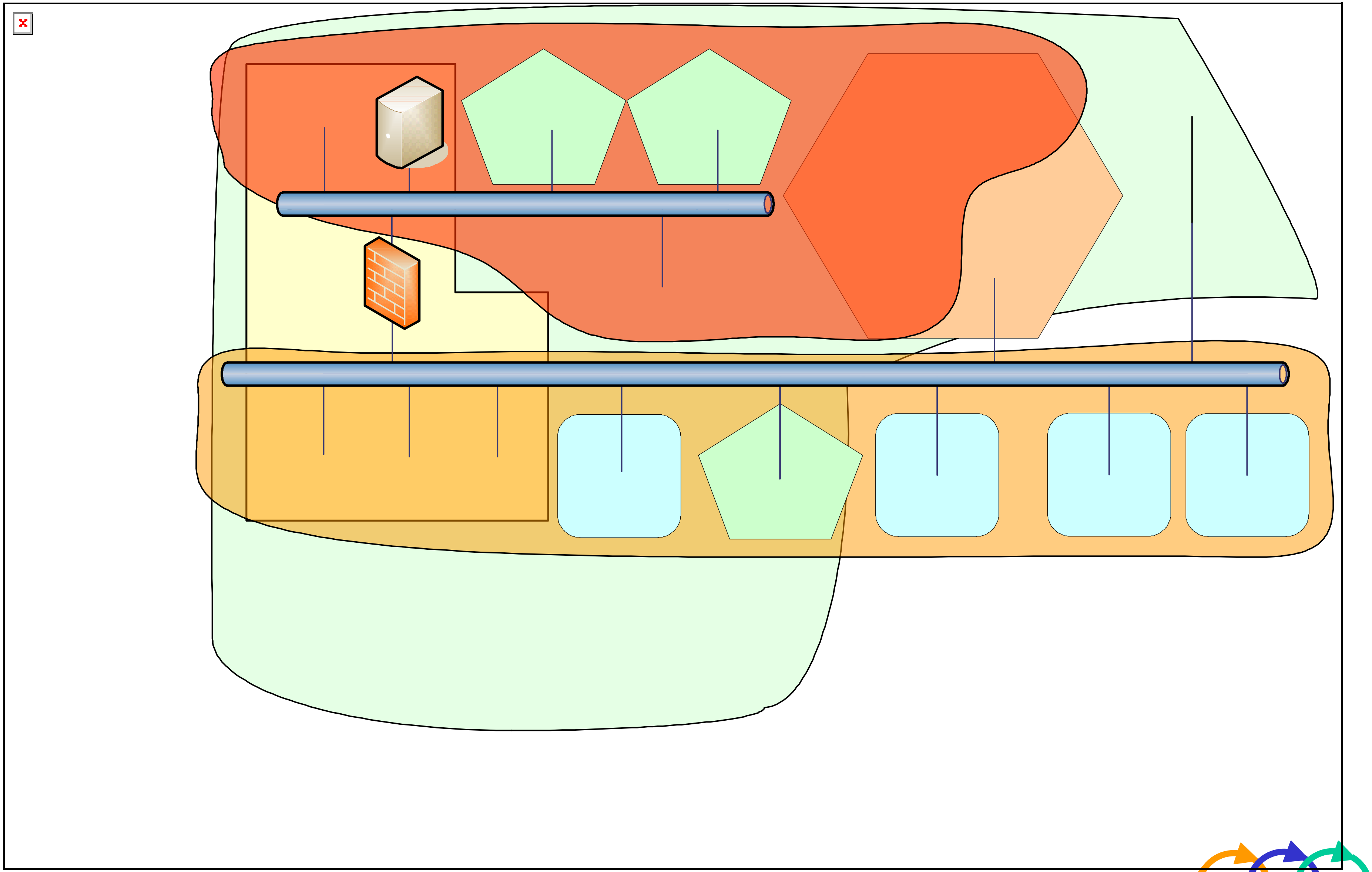
DESEREC Shared Repository

Preliminary DESEREC Architecture

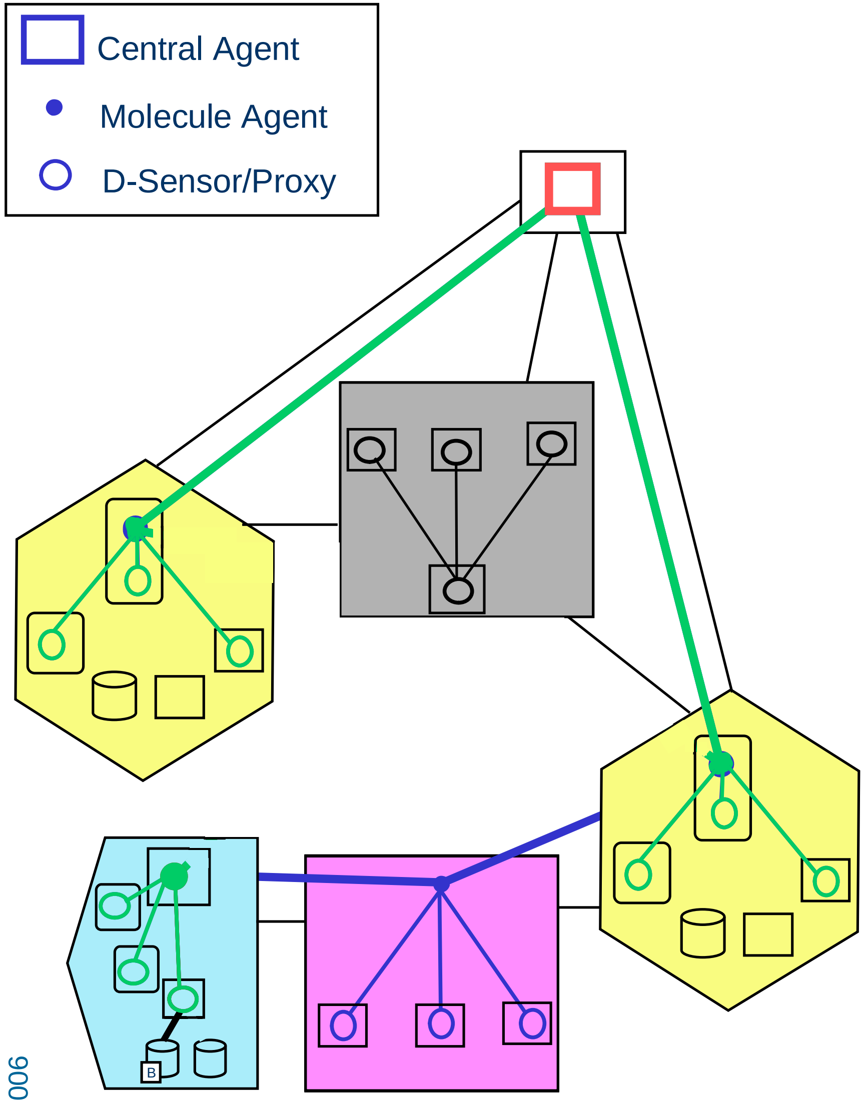
DESEREC network topology is based here
on the real network topology

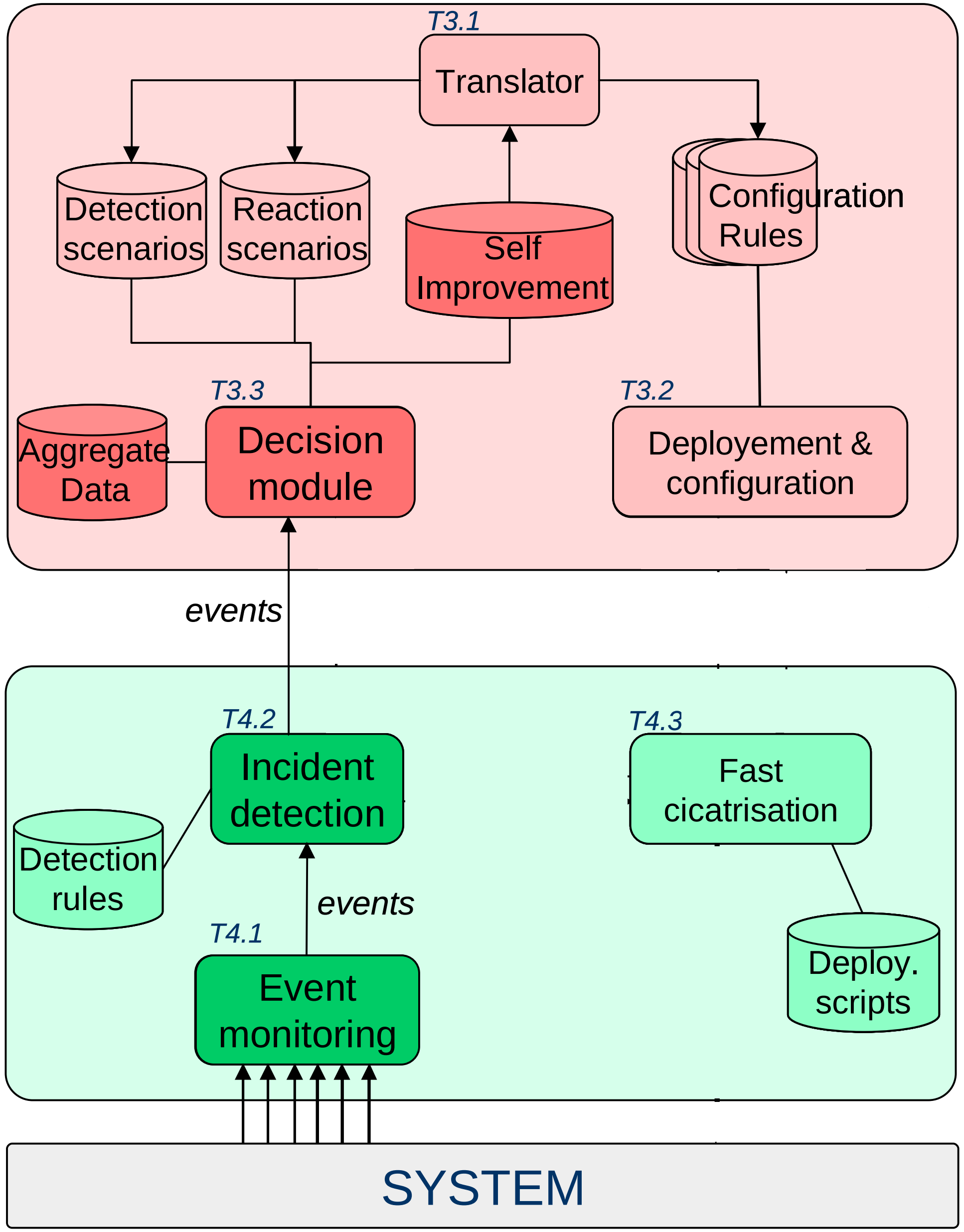
At any time, the whole DESEREC framework must be aware of the currently deployed configuration: each DESEREC agent must know what to monitor and control

DESEREC: introducing cell concept



Reconfiguration process WP3/WP4 level





12 – Self Improvement data is updated for WP2 needs

Achievements and progress

D1.2 Security and dependability model report

- The deliverable consists of a security and dependability model together with the first results of a risk assessment on one end-user's use-case (OTE)
- The first part of the document presents the risk-assessment methodology. Following a classical process, the methodology consists in the following steps:
    - 1. Identify assets and target system, assess the assets' values with a rationale
    - 2. Enumerating the threats, specify their potentiality and impact
    - 3. Deriving risk

Next Steps

Deliverables

- Initial system architecture and final requirements (D1.3, M12),
- Policy and system models (D2.1, M15)
- Modelling tools, 1st prototype (D2.2, M15)
- Product architecture and specification for WP3 (D3.2, M15)
- Product architecture and specification for WP4 (D4.2, M15)
- Security analysis report (D1.4, M18)
- Validation tools, 1st prototype (D2.3, M18)
- Configuration tools, 1st prototype (D2.4, M18)

At M18, Intermediate Demonstration

Training Workshop Objective

What is the objective of the workshop?

- The workshop provides participants with:
  - An overview of DESEREC project objectives and progress
  - A detailed presentation of end-user scenarios and preliminary user requirements
  - A preliminary view on DESEREC architecture and its associated main issues
  - An insight view on modelling techniques envisaged
  - An insight view on validation and simulation techniques envisaged

- In addition, presentation of some partner tools that might be part of DESEREC framework

DESEREC Contact points

Web site: www.deserec.eu

Coordinator: Andre Cotton (THC)

Project Manager: Benoit Bruyere (THC)

Technical Manager: Patrick Radja (EADS)

Scientific Manager: Antonio Lioy (POLITO)

Thank You for listening,

Any questions?