Dependability analysis of critical infrastructures

Robin E Bloomfield

City University London

CSR
Centre for Software Reliability

IRRIIS - FP6-2005–IST-4

Sixth Framework Programme

Espoo, Finland

IRRIIS Mission

To enhance substantially the dependability of
Large Complex Critical Infrastructures
by introducing appropriate
Middleware Improved Technology
components within the next three years.
12M Euro, 3 yrs

IRRIIS Partners

Technology Provider

- Alcatel-Lucent, France
- Siemens AG, Germany
- Advanced Industrial Systems Ltd., Malta

Consultant & Service Provider

- Industrieanlagen-Betriebsgesellschaft mbH, Germany
- Aplicaciones en Informática Avanzada, Spain
- Fraunhofer Institute Intelligent Analysis and Information Systems, Germany
- Fraunhofer Institute Secure Information Technology, Germany
- Technical Research Centre of Finland

LCCI Stakeholder

- Gruppo Telecom Italia
- Red Eléctrica de España, Spain
- ACEA, Italy

Research Partners

- Italian National Agency for New Technology, Energy and the Environment
- École Nationale Supérieure des Télécommunications, France
- Centre for Software Reliability at City University London, Great Britain
- Technical University Dresden, Germany
- Netherlands Organisation for Applied Scientific Research

Overview

Enhanced Understanding of interdependent LCCIs

Analysis & Research

- Survey of existing tools and models
- Analysis of the state of the art (research gaps)
- Requirements for SYNTEX and MIT
- Scenario and Risk Analysis
- Topology Analysis
- Interdependency Analysis
- Analysis of Next Generation Networks

SimCIP Development

- Agent-based simulation of LCCIs' interdependencies
- Multi-layer simulation (technical, cyber, management)
- Integration of existing tools & models
- Test-bed for MIT components

SimCIP environment

MIT Development

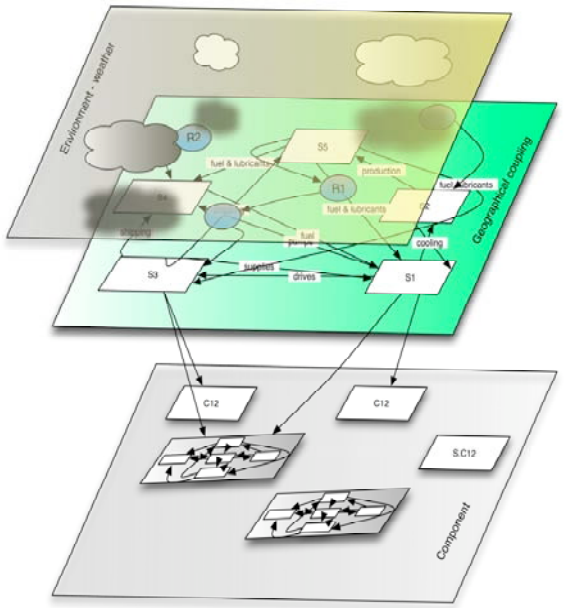
- Evaluation of MIT concepts
- MIT communication components to improve communication between different infrastructures
- "Intelligent" MIT add-on components for surveillance and mitigation of cascading effects
- Interfaces for easy integration into existing systems

MIT components

Diagnosis - Therapy

Role of models

- Understanding Interdependencies
  - Service level
  - Failure impact and common mode effects
  - Escalation and cascade
  - Coupling between infrastructures
  - at design, attack, effect and recovery phases
- Designing and validating MIT – and supporting procedures and services



Range of models

1. Structuring and scoping – build the right model
   - PIA, (services, timebands) ISE, Gamma
2. Network – physics
   - ENEA and TUD, ISE
3. Reliability and performability
   - SANS, (ISE)
4. High fidelity simulation of behaviour of LCCI systems
   - Scoped and structured with 1
   - Dependency models from 2 and 3
   - Flow and load models (e.g. of power grid)

Model basis

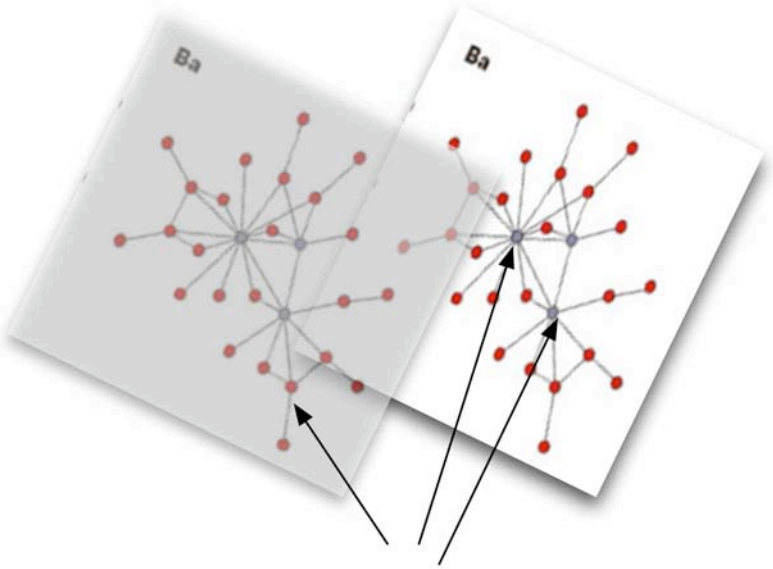
- Leontief, inoperability, SAN, CMF

$$x_i = \sum_k x_{ik} + c_i = \sum_k a_{ik} x_k + c_i \text{ for } i = 1,2,...n$$

where c_i is the external demand for service i.

$$\frac{dx_i}{dt} = -\frac{x_i}{\tau_i} + \Theta\left(\sum_{i \neq j} \frac{M_{ij} x_{ij}(t - t_{ij})}{f(O_j)} e^{\beta t_{ij}}\right)$$

$$\Theta(y) = \frac{1 - e^{-\alpha y}}{1 + e^{-\alpha(y - \theta_i)}};$$

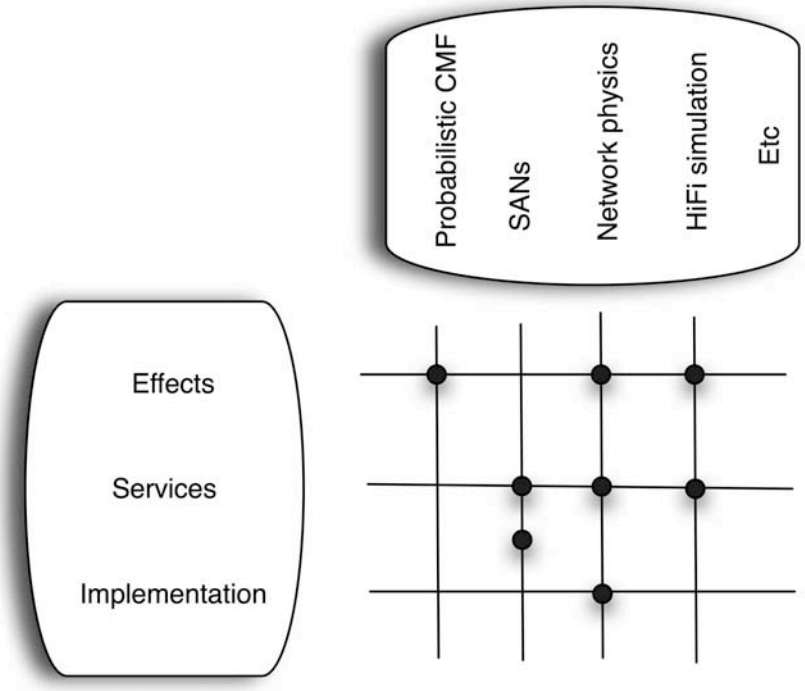


$$\lambda_i = \lambda_i^0 + \Theta\left(\sum_{i \neq j}^{i \in local} M_{ij} x_{ij}\right) + \Theta\left(\sum_{i \neq j}^{i \in neighbouringclique} K_{ij} x_{ij}\right)$$

$$P(i, j \mid w_i, w_j) = P(i \mid w_i) P(j \mid w_j)$$

$$\lambda(t)_i = f(w_i(t))$$

ISE and other models

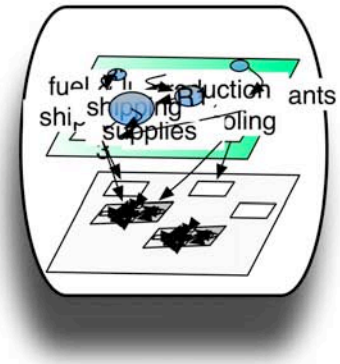


- Interdependency failures, or surprises, in critical infrastructures
  - Subtle surprise?
  - Obvious with hindsight?
- Research trends:
  - High fidelity simulation - extent and depth
  - Massive models, no stopping rules, difficult for stakeholders
  - Still draw boxes and arrows for analysis
- Systematic approach to preliminary interdependency analysis

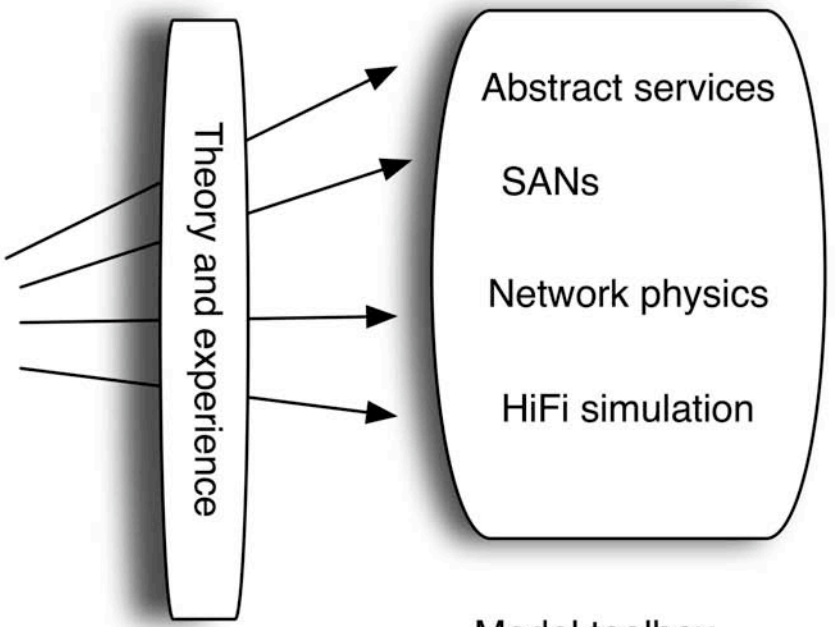
What is a system?

- Build model of system
  - What is the system?
  - What analyses do we want to do?
    - dependability of a service?

Interdependency theories and models



PIA to scope and define problems including threat assumption



Model toolbox

Preliminary Interdependency Analysis (PIA)

City University London

CSR
Centre for Software Reliability

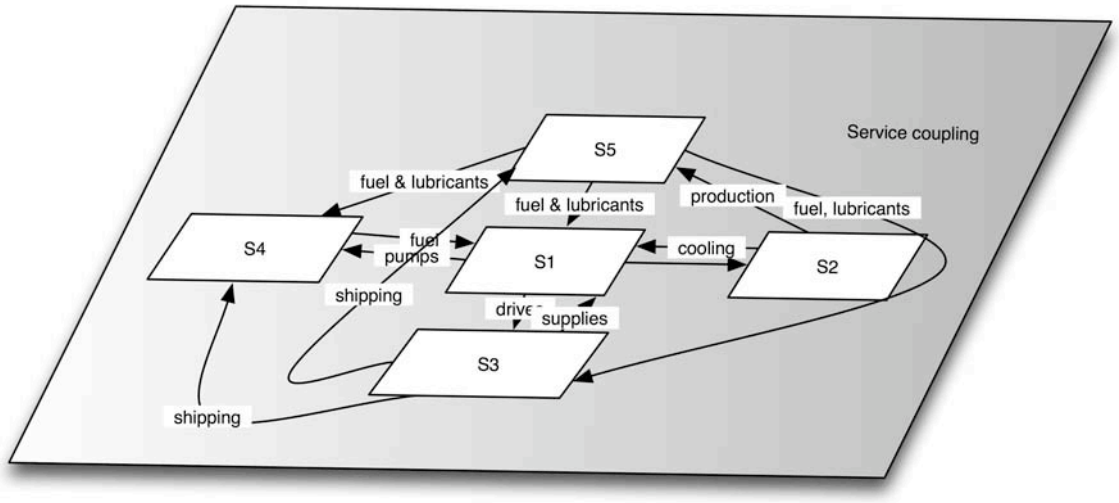
IRRIIS - FP6-2005–IST-4

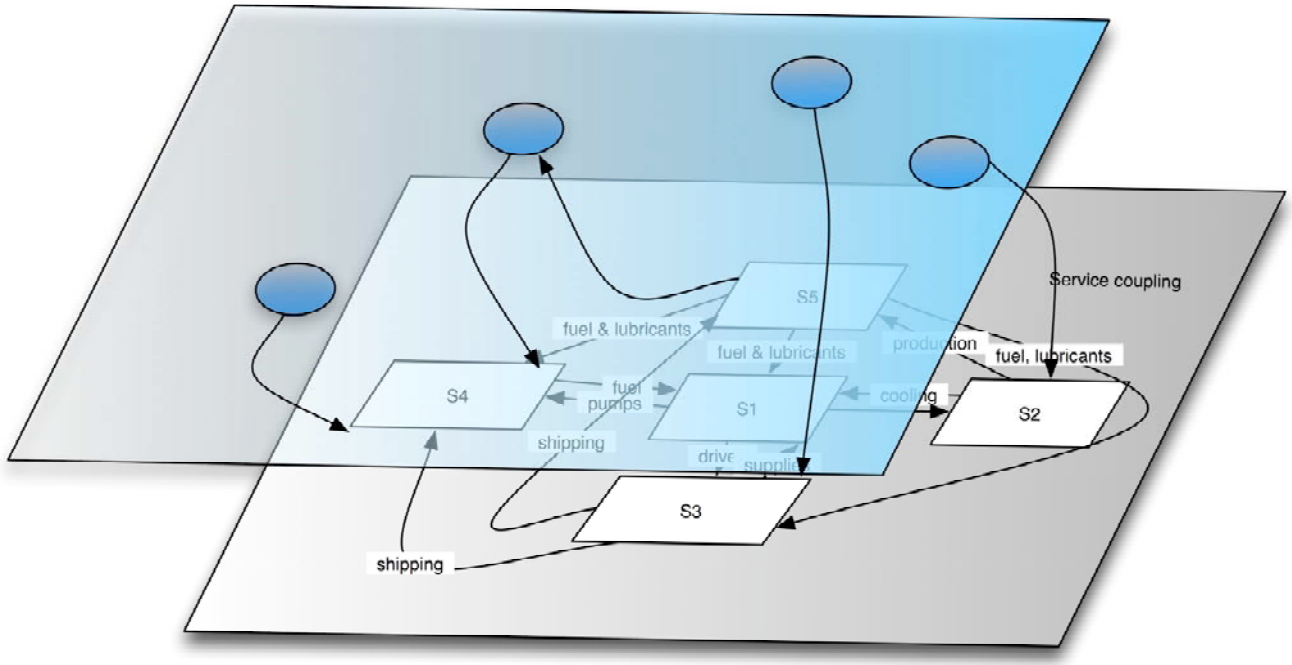
Sixth Framework Programme

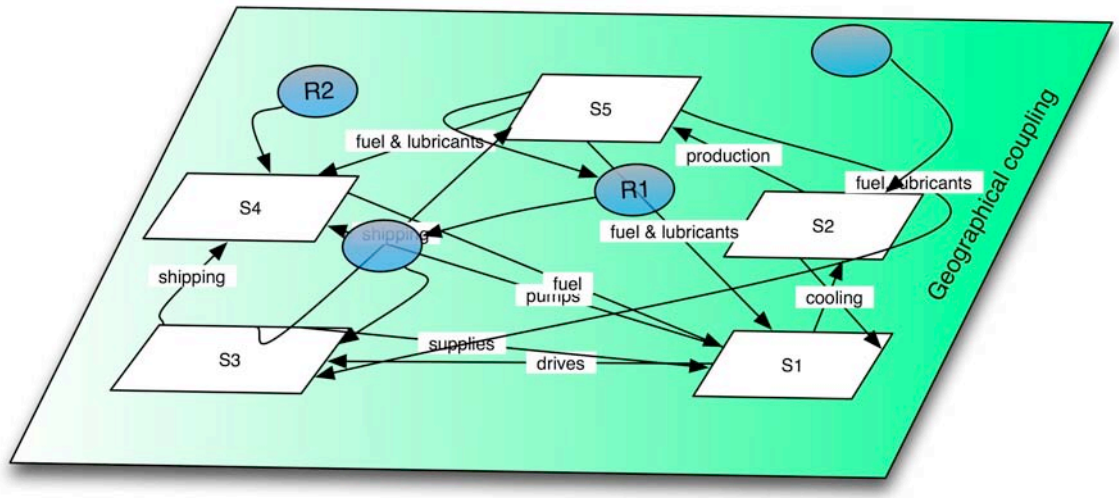
Espoo, Finland

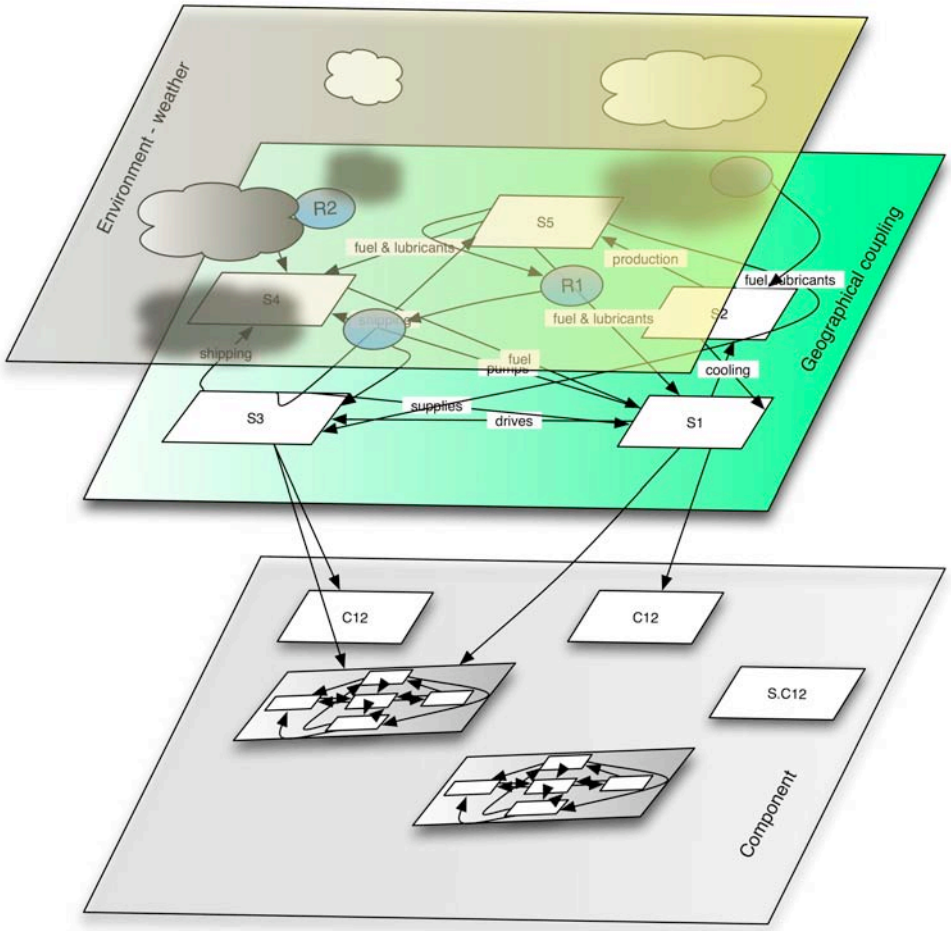
Elements of approach

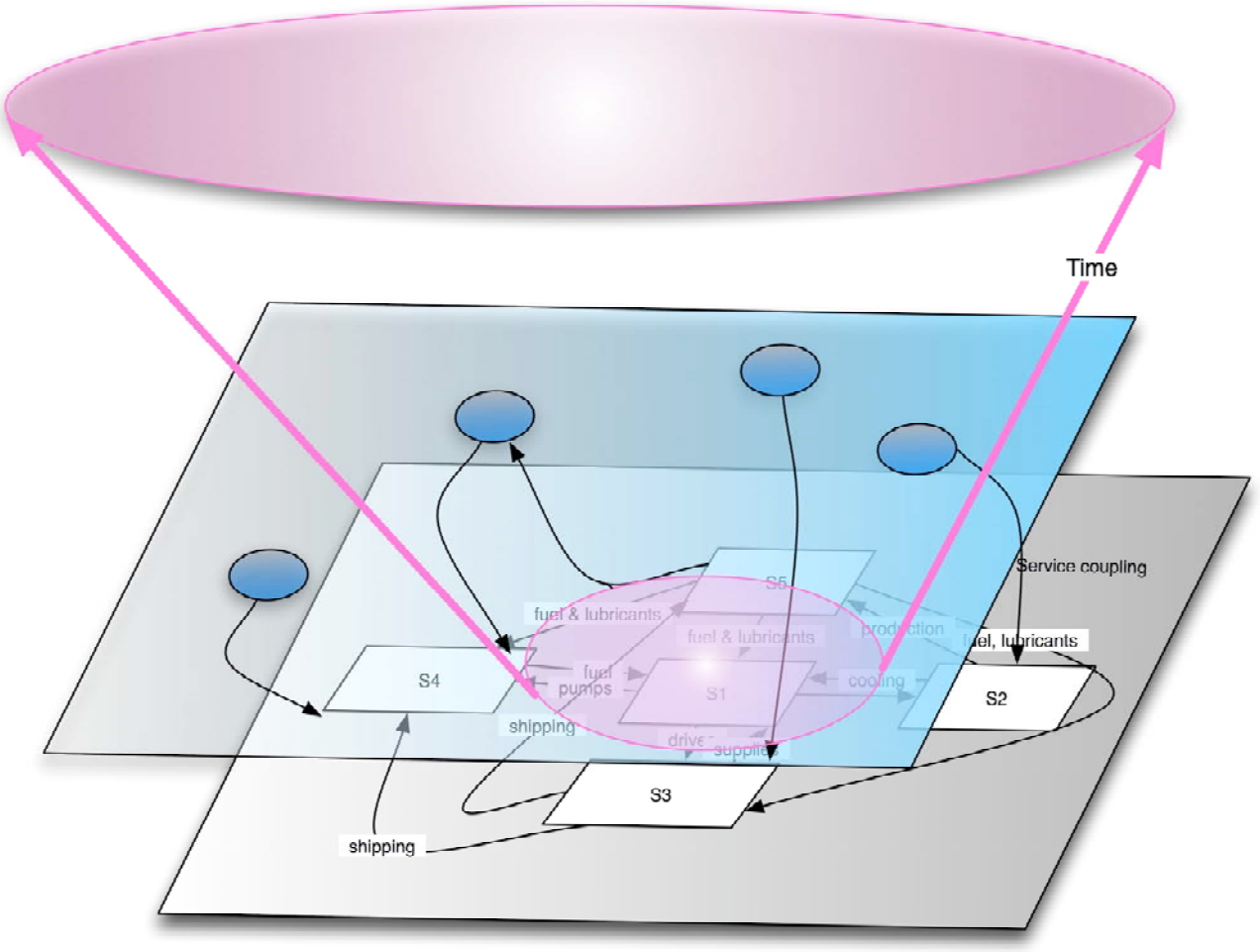
- Scenarios
- Service related model
- Resources
- Timebands
- Interdependency identification (systematic search for dependencies)
- Responsibility modelling
- Simulation at back end (Mobius)


Service coupling
S5
fuel & lubricants
fuel & lubricants
production
fuel, lubricants
S4
fuel
pumps
S1
cooling
S2
shipping
supplies
S3
shipping

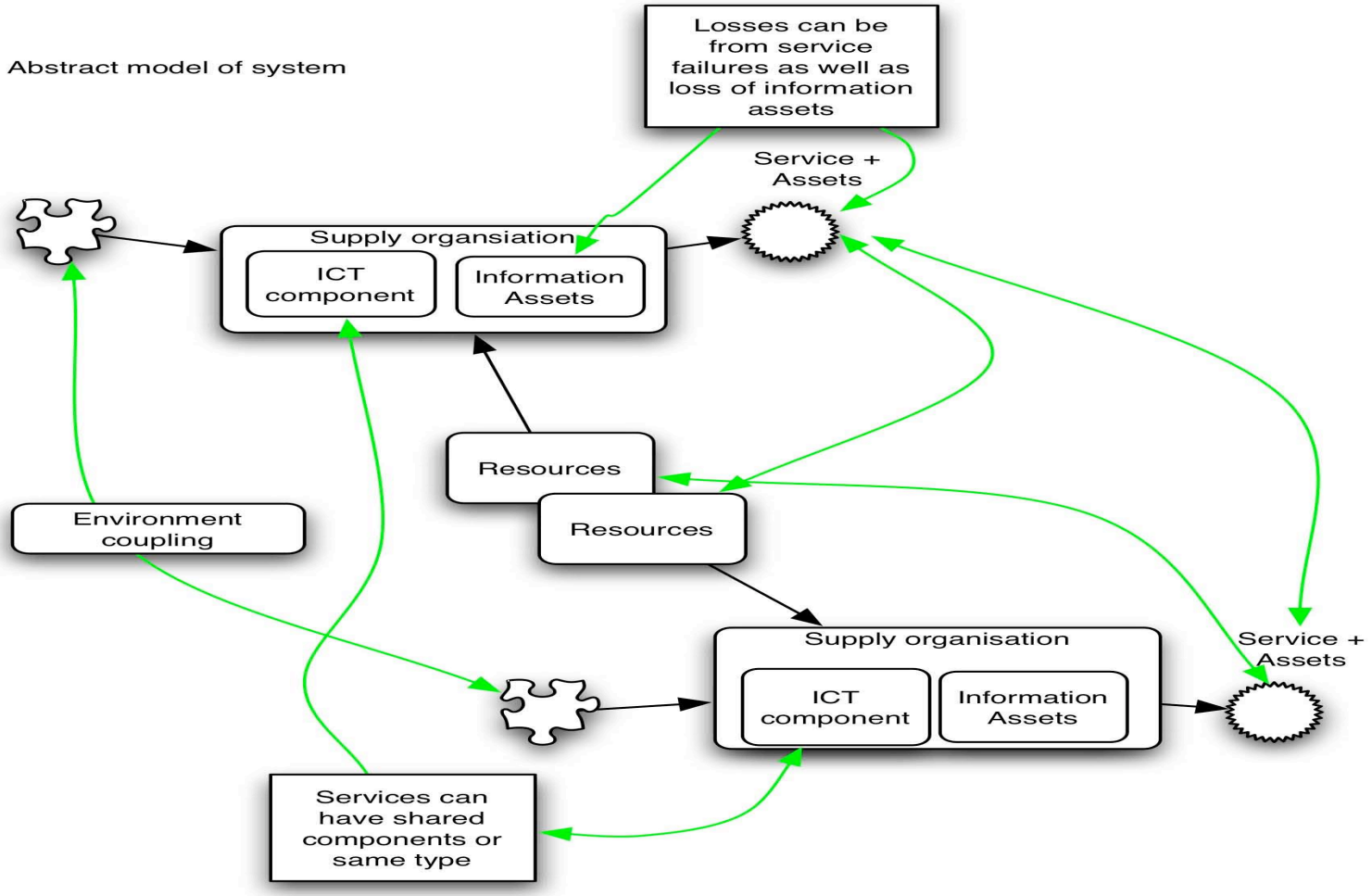

Service coupling
fuel & lubricants
fuel & lubricants
fuel, lubricants
S4
fuel
pumps
S1
S2
shipping
S3
shipping


R2
S5
fuel & lubricants
production
R1
S4
fuel & lubricants
S2
shipping
shipping
fuel
pumps
cooling
supplies
S3
drives
S1
Geographical coupling


Environment - weather
Geographical coupling
Component
R2
R1
S1
S2
S3
S4
S5
fuel & lubricants
production
shipping
fuel
pumps
cooling
supplies
drives
C12
C12
S.C12


Time
Service coupling
S5
fuel & lubricants
fuel & lubricants
production
fuel, lubricants
S4
fuel
pumps
S1
cooling
S2
shipping
drive
supplies
S3
shipping

PIA: Interdependencies identification



- Interconnectivity
  - Closure gives too large scope?
    - High degree of connectivity, small world problem
  - Probabilistic idea of depth?
    - And using correlation at boundaries (if no feedback, weather)
    - Probability and time
  - Need stopping rules
    - But without building all the high fidelity models
    - Sensitivity studies

But

Complex systems and complexity science

…. Slippery concepts

- "quote"
  - Emergence
    - Cascade failures, non-linear, fast, feedback
    - Stochastic properties
    - Rare events
    - …….
    - Is there anything special, do we need new analysis methods or new models to apply them too?

Status

- Work in progress
- PIA defined and being experimented with
  - Rome mini-blackout
- Scaling up simulations
  - Impact of complexity science
- What is a system in CIP?
  - Uncertainty in structure