FP7 Grant Agreement N° 312450

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Project type: Network of Excellence (NoE)

Thematic Priority: FP7 Cooperation, Theme 10: Security

Start date of project: March 1, 2013 Duration: 48 months

D9.82 - Courses inside the Homeland Security Master (edition 2)

Due date of deliverable: 31/07/2015
Actual submission date v1: 28/07/2015

Revision: Version 2

Università Campus Bio-Medico di Roma (UCBM)

Project co-funded by the European Commission within the Seventh Framework Programme (2007–2013)		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Author(s)	Roberto Setola (UCBM) Maria Carla De Maggio (UCBM) Marco Tesei (UCBM) Francesca De Simio (UCBM)
Contributor(s)	

Security Assessment	**E. Rome (Fraunhofer)**
Approval Date	28/07/2015
Remarks	No security issues found

The project CIPRNet has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450.

The contents of this publication do not reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the authors.

TABLE OF CONTENTS

1 Introduction

Internal and external training activities represent a mandatory cornerstone for the creation of a European community able to support the realization of EISAC (European Infrastructures Simulation & Analysis Centre) and to exploit its functionalities. CIPRNet will arrange specific training activities aiming to provide basic and advanced knowledge about Critical Infrastructure MS&A (Modelling, Simulation and Analysis) targeted to a broad range of personnel related to CI (including, but not limited to, local administrations, utilities personnel, emergency operators and managers, security & safety operators and managers, CIP researchers, CIP policy makers, etc.).

The courses inside the Post Graduate Master in Homeland Security consist of three training editions scheduled for 2014, 2015, and 2016 in Rome. The courses consist of a generic part for each episode, dealing with basic knowledge in MS&A (repeated at each episode), followed by a more advanced part specified as following:

- ✓ Edition 2014: Federated Simulation and Open MI platform
- ✓ Edition 2015: Decision Support System (DSS)
- ✓ Edition 2016: What-if Analysis (WIA)

During the course, the attendees also have the opportunity to practice with the tools developed within the CIPRNet project (i.e. federated simulation, decision support systems and 'what if' analysis, within the three editions). This approach will certainly foster the new generation of risk assessment/management tools, which will enable an easier and more effective management of crises.

The first edition, conducted in 2014, is documented in CIPRNet deliverable D9.81. This deliverable D9.82 describes in details the second edition of the course inside the Post Graduate Master in Homeland Security in terms of training materials, scheduling and attendees' feedback monitoring. The structure of this document is composed of two sections: the first section presents the course in terms of venue, programme and attendees. The annexes collect the material prepared for the course and/or collected during the course.

1.1 Acronyms

Acronym	Explanation
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CIPMA	Critical Infrastructure Protection Modelling and Analysis
CIPRNet	Critical Infrastructure Preparedness and Resilience Research Network
CISIA	Critical Infrastructure Simulation by Interdependent Agents
DB	Database
DIESIS	Design of an Interoperable European Federated Simulation Network for CI
DSS	Decision Support System
EISAC	European Infrastructures Simulation & Analysis Centre
EU	European Union
FP	Framework Programme
FR	Functional Requirement
GIS	Geographic Information System
GPS	Global Positioning System
I2SIM	Infrastructure Interdependencies Simulator
IIM	Input Output Inoperability Model
MS&A	Modelling, Simulation and Analysis
NFR	Not Functional Requirement
NISAC	National Infrastructure Simulation and Analysis Center
OpenMI	Open Modelling Interface
PA	Public Authority
PSF	Participant Satisfaction Form
QoS	Quality of Service
RAFI	Risk Assessment Forecast Interval
S&A	Simulation and Analysis
VCCC	Virtual Centre of Competence and expertise in CIP
V&V	Verification and Validation

2 Course inside the Post Graduate Master in Homeland Security

The course on Modelling, Simulation and Analysis of Critical Infrastructures has confirmed the importance to pursue training activities within the project.

The present deliverable aims to illustrate the second edition of the course held inside the Post Graduate Master in Homeland Security with a considerable focus on the audience's feedback.

The second edition of this two-day event offered the opportunity to the attendees to familiarise with the modelling, simulation and analysis tools developed within the CIPRNet project. The program of the course is based on the design of the general training course, consolidated during the first edition of the Course and of the Master Class, and taking into account the results of the participant satisfaction forms. The program of the second day is particularly focused on the DSS tool developed within the CIPRNet project. To this end, new lessons were introduced. The new material has been tested and updated in accordance with the results of an internal rehearsal performed on 30th June 2015.

The Course provides a challenging learning environment where research endeavours are applied to real-world challenges associated with man-made and natural emergencies and critical incidents on the local, national, and global levels. Teachers bring their diverse professional, disciplinary, and cultural backgrounds into the learning processes.

Similar to the previous training event, the scheduling of this event has been slightly modified in order to meet speakers' needs and attendees' feedback to adopt a similar logical sequence of the lectures. This second edition of the course has been characterised by a stronger cooperation between lecturers and attendees, compared to its first edition.

2.1 Venue

The Course on Modelling, Simulation and Analysis of Critical Infrastructures has been held in the Aula Magna of the University Campus Bio-Medico of Rome (Italy) on 9th - 10th July 2015. The event has been organized by UCBM within the lessons of the Post Graduate Master in Homeland Security.

Figure 1: Venue of the course, UCBM

2.2 Program

Security is one of the fastest growing challenge in the world today, with applicability in a wide set of different industries and fields, such as services, infrastructures, government and business. The competences provided in the Post Graduate Master give the chance to the students to branch out into other areas, and develop skill sets that are unique.

Because the course of Modelling, Simulation and Analysis of Critical Infrastructures covers a broad area of topics, the Post Graduate Master in Homeland Security tends to focus on the dynamics of technological innovation and the need of adaptive behavior of businesses and markets. Within these dynamics it is possible to narrow the focus even further and learn the skills necessary to work in one of several emerging or well-established industries.

The program of the course is based on the design of the general training course, as described in D9.1 CIPRNet training Plan (Chapter 2.2) [1] and taking into account the results of the participant satisfaction forms collected during the previous internal CIPRNet Course (Delft, 3-4 February, 2014) [2], the Edition 1 of the Master Class (Paris, 24-25 April, 2014) [3] and the Edition 1 of the Course inside the Master in Homeland Security (Rome, 10-11 July, 2014) [4].

A rehearsal has been held the 30th of June 2015 with the participation of ENEA, UTP and UCBM lecturers, in order to better arrange the new lectures foreseen for this second edition, in particular the lecture on Cyber Threats for CI, presented by UTP, and the presentations regarding both introductory and detailed presentations of the CIPRNet DSS, held by UCBM and ENEA. The outcome of the rehearsal day introduced modification in the training material and in the arrangement of the course program (Annexes B and A, respectively).

2.3 Attendees

The course inside the Homeland Security Post Graduate Master was attended by 20 students of the master and 3 external participants, for a total of 23 attendees, excluding the lecturers. The external participants are former students of the Master, professionals coming from the partner companies of the Master and from companies belonging to the International Advisory Board of CIPRNet. The audience constituted by the students of the Master in Homeland Security is particularly appropriate for the aim of the course, as it is designed for young security managers, public authorities' representatives, young security or CIP researchers, and law enforcement officers.

Similar to the Master Class, the aim of this course is to prepare next generation security managers and experts to the use of services, methods and tools as those provided by CIPRNet and by the VCCC. Moreover, this event contributes to acquire feedback on the training materials and on the VCCC services for heterogeneous end-users: public authorities who can take advantage of the skills acquired on the job as well as representatives of private companies who can use the arguments within the company.

The need for qualified professionals is expanding at national and regional levels, as well as internationally, so a homeland security education portfolio suits the needs of many individuals working in this field and fosters national as well as international careers.

In the case of this second edition which includes the new topic of the CIPRNet DSS, the feedback received by the attendees will be used to improve the Master Class open to an external audience, that will be held in Rome the 11th – 13th November 2015 at ENEA premises.

The list of all the attendees is reported in Annex C. All the attendees received a "Certificate of Attendance" whose template is reported in Annex D.

Figures 2, 3, 4: Classroom

2.4 Feedback

The effectiveness and the quality of the training have been evaluated on the basis of the feedback received from the attendees. To this end, a specific Participant Satisfaction Form (PSF) has been elaborated and submitted to all the attendees.

On the basis of 15 collected PSFs the result was that the expectations of the attendees have been fully covered, and the overall satisfaction is very high.

The feedback of this course confirmed the results of the first editions of the training events, regarding the valuable opportunity to interact with experts and to acquire expertise regarding CIPRNet software tools.

Thanks to the active interest of the participants, several suggestions and contributions to the lectures quality were given also during the course itself, allowing for the improvement of the lectures' clarity with respect to their academic and technological aspects for future editions.

Comments from PSFs, all regarding general aspects, are reported in Annex E.

Finally the PSFs highlighted that the course has covered the expectation of the audience for almost all participants in terms of time scheduling, logistic facilities, contents and utility for their professional life. Figure 5 reports the results of the PSFs for the general aspects of the course, evaluated in a scale from 0 to 5.

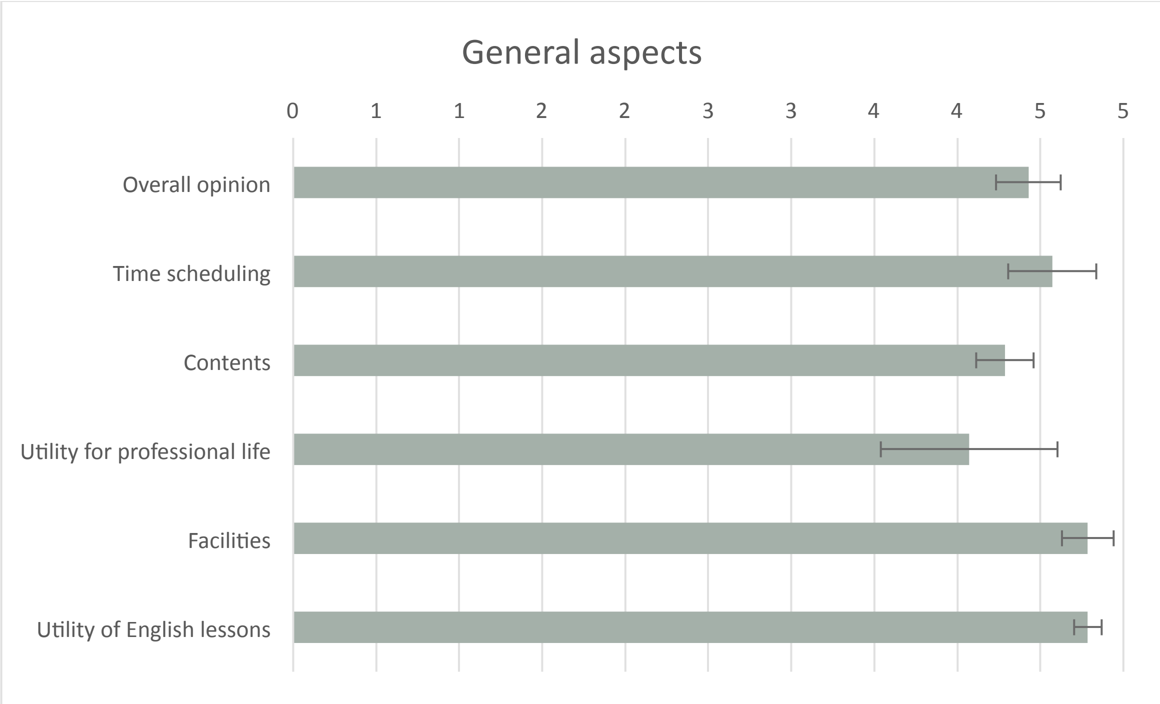


Figure 5: Data collected from Participant Satisfaction Forms on general aspects.

The PSFs also collected opinions regarding any specific lecture. The Figures 6 and 7 show the average values of the scores obtained by each lecture of the course of day 1 and day 2 respectively. Note that evaluations are positive for all speakers and scores range from a minimum value of 3.86 to a maximum value of 4.80.

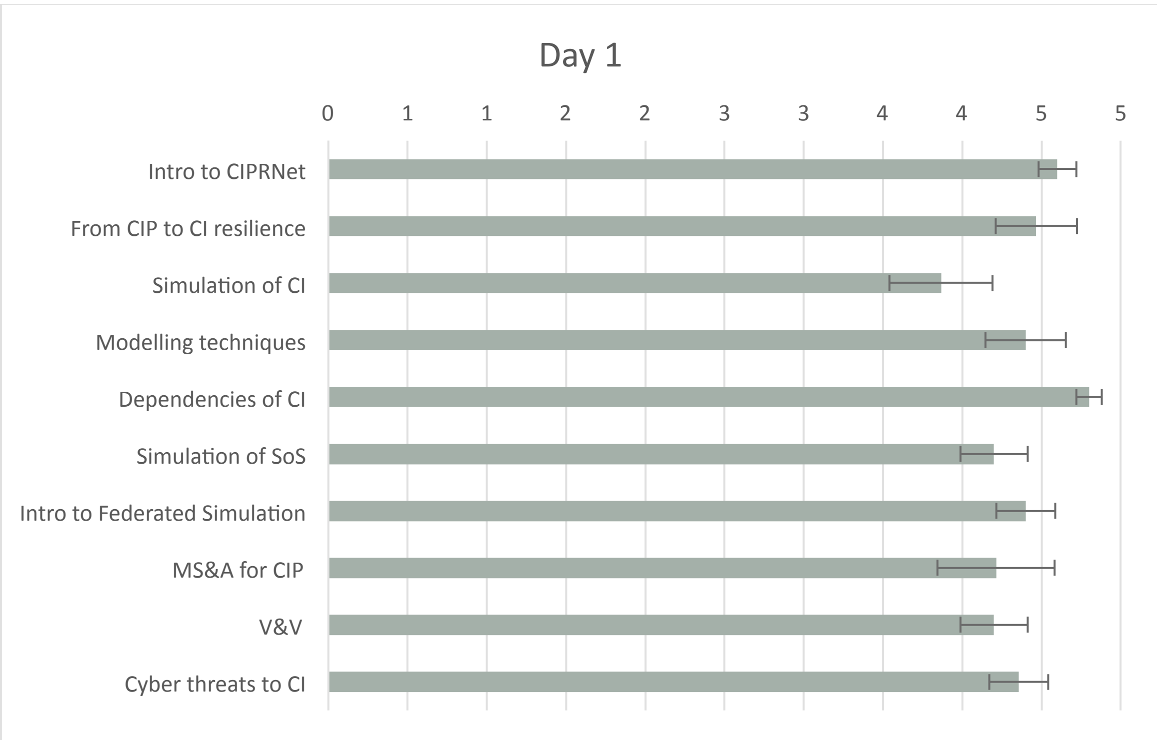


Figure 6: Data collected from Participant Satisfaction Forms on day 1 lessons.

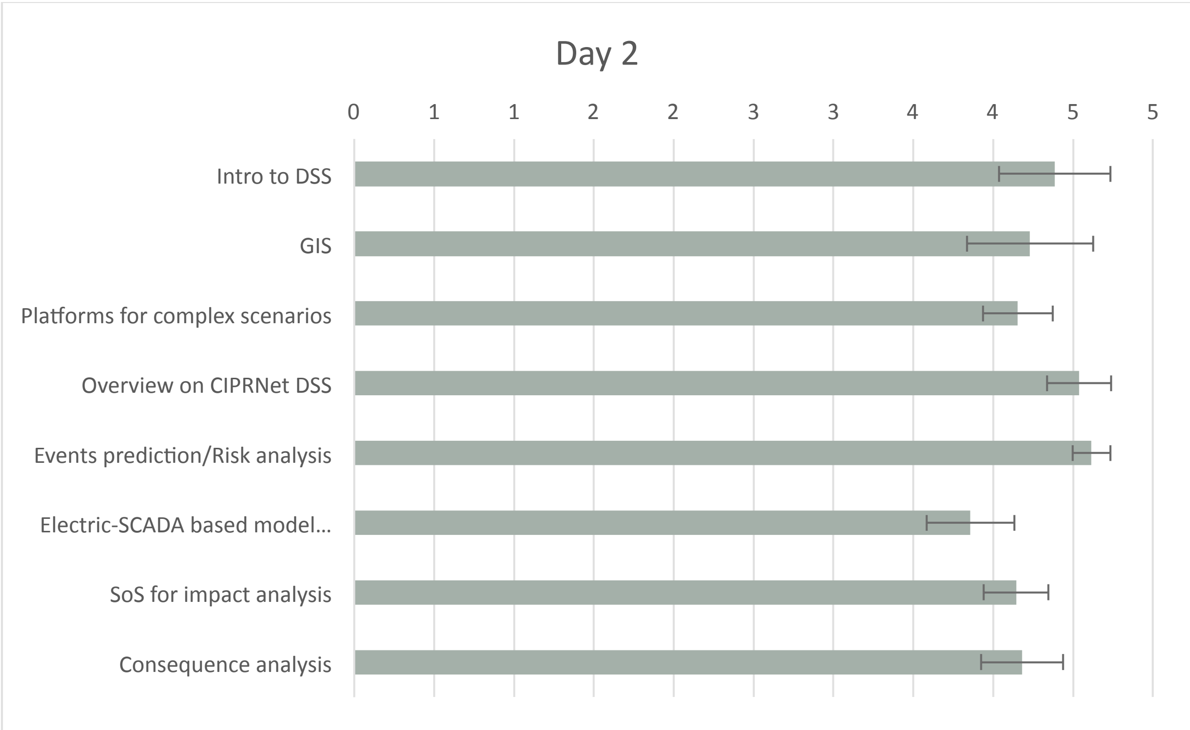


Figure 7: Data collected from Participant Satisfaction Forms on day 2 lessons.

This valuable information will be used, similarly to the past training events, to improve the training material, scheduling, organization, and focus for the next editions. Detailed general comments provided by attendees have been collected and reported in Annex E.

2.5 Comments

In conclusion, the second edition of the Course on Modelling, Simulation and Analysis of Critical Infrastructures inside the Post Graduate Master in Homeland Security has been successfully carried out, explaining and clarifying the project's approach challenging the critical infrastructures protection context. In the course, as occurred during the past training events, there was a great interaction between attendees and teachers, exchanging valuable and constructive ideas. Based on what detailed in this deliverable, the objectives set by the course have been achieved.

2.6 How data collected from Participant Satisfaction Forms have improved the course

The first editions of the Master Class and of the Course inside the Homeland Security Master with all feedbacks received by PSFs have represented an extensive source of suggestions for improving the quality level of the course. To care of feedback from attendees is extremely important in order to improve the level of training activities for the next events. Hence, from the analysis of the several PSFs collected after the Edition 1 of the training events some recommendations were very useful for improving the second edition of the course inside the Post Graduate Master in Homeland Security.

While the general part of the Course (day 1) was almost consolidate as highlighted by the PSFs of the first edition of the course, the part related to the CIPRNet DSS has been structured taking into account the general comments coming from the previous training events.

Some other changes in the program have been applied due to teachers' availability matching time scheduling. The high quality reached by the previous training events has been confirmed by the feedback received within this course, satisfactorily meeting the expectations of the attendees.

3 References

[1] UCBM: EU FP7 CIPRNet, Deliverable D9.1 – Training plan

[2] UCBM: EU FP7 CIPRNet, Deliverable D9.51 – Periodic training event internal

[3] UCBM: EU FP7 CIPRNet, Deliverable D9.61 – Periodic training event and Training review report (edition 1)

[4] UCBM: EU FP7 CIPRNet, Deliverable D9.81 – Course inside the Homeland Security Master (edition 1)

Annex A – Programme

CIPRNet Course inside the Master in Homeland Security
Edition 2

9-10 July 2015

University Campus Bio-Medico of Rome
Aula Magna, Trapezio Building

Agenda

Day 1 – 9th July 2015

Teacher	TOPIC	TIME
	Taking seats	*9.30 – 10.00*
Roberto Setola (UCBM)	Welcome	10.00 – 10.10
Roberto Setola (UCBM)	Introduction to CIPRNet	10.10 – 10.50
Marianthi Theocharidou (JRC)	From Critical Infrastructure (CI) Protection to CI Resilience	10.50 – 11.30
Eric Luiijf (TNO)	Simulation of CI: relevant applications	11:30 – 12.10
	Coffee break	*12.10 – 12.30*
Mohamed Eid (CEA)	Principal modelling techniques: applications and limitations	12.30 – 13.10
Roberto Setola (UCBM)	Modelling and investigating dependencies of CI	13.10 – 14.00
	Lunch	*14.00 – 15.00*
Alberto Tofani (ENEA)	Simulation approaches of System of Systems	15.00 – 15.40
Edwin van Veldhoven (TNO)	Introduction to Federated Simulation	15.40 – 16.20
	Coffee break	*16.20 – 16.40*
Marco Tesei (UCBM)	Modelling, simulation and analysis techniques for CIP	16.40 – 17.20
Edwin van Veldhoven (TNO)	Verification and validation techniques	17.20 – 18.00
Rafal Kozik (UTP)	Cyber threats to CI	18.00 – 18.40

Day 2 – 10th July 2015

Teacher	TOPIC	TIME
	Taking seats	*9.00 – 9.30*
Maria Carla De Maggio (UCBM)	Introduction to Decision Support Systems	9.30 – 10.10
Maurizio Pollino (ENEA)	Geographical information systems for visualisation and analysis	10.10 – 10.50
Alberto Tofani (ENEA)	Platforms for Large & Complex Scenarios	10.50 – 11.10
Vittorio Rosato (ENEA)	An overview on CIPRNet DSS design	11.10 – 11.30
	Coffee break	*11.30 – 12.00*
Maurizio Pollino (ENEA)	Events prediction and environmental sensing Risk analysis tools for events and damages simulations	12.00 – 13.20
	Lunch	*13.20 – 14.20*
Antonio Di Pietro (ENEA)	An Electric-SCADA based model to implement reconfiguration procedures in Electric Distribution grids	14.20 – 15.00
Alberto Tofani (ENEA)	Application of system of systems model for long term impacts analysis in large scenarios	15.00 – 15.20
Vittorio Rosato (ENEA)	Consequence Analysis and applications for supporting operator's decisions	15.20 – 15.40
ALL	Discussion	15:40 – 16:00

Annex B – Certificate of Attendance

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

CERTIFICATE OF ATTENDANCE

-Name and First name-

Hereby recognised for participation in

Course on Modelling, Simulation and Analysis of Critical Infrastructures (Edition 2)

Prof. Roberto Seto
(UCBM)

Organised by University Campus Bio-Medico of Rome

July 9th - 10th, 2015
Rome (Italy)

Annex C – Participant satisfaction feedback

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Course on Modelling, Simulation and Analysis of
Critical Infrastructures
Edition 2

PARTICIPANT SATISFACTION FORM

Organised by University Campus Bio-Medico of Rome

July 9th – 10th, 2015
UCBM, Rome (Italy)

1 Instructions

The aim of this questionnaire is to collect information about the CIPRNet Course with respect to each teacher and lesson. Please spend some time filling in the questionnaire, as **your feedback is paramount for our improvement**.

For some of the questions in the following form, please indicate a score from 1 to 5 (1 = very bad, 5 = excellent). Moreover, there are some open-ended questions for you to provide comments; please fill in these fields with as much detail as possible (using further space if needed).

The customer satisfaction form is filled out anonymously.

2 General Aspects

Question	*Score*
What is your overall opinion about this course?	
Is the time scheduling adequate?	
Did the course contents cover your expectations?	
Do you think that this course is useful for your professional activities?	
Were the facilities adequate?	
Was it interesting/useful having English lessons?	
What were the most positive aspects of this course?	
Which aspects should be improved in terms of topics, clarity, and time scheduling?	
Notes (please provide general comments and suggestions)	

2.1 Day 1 – 9th July 2015

Introduction to CIPRNet by Roberto Setola (UCBM) [10:10 – 10:50]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

From critical infrastructure protection to critical infrastructure resilience by Marianthi Theocharidou (JRC) [10:50 – 11:30]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

Simulation of Critical Infrastructures (CI): relevant applications by Eric Luiijf (TNO) [11:30 – 12:10]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

Principal modelling techniques: applications and limitations by Mohamed Eid (CEA) [12:30 – 13:10]

Question	*Score*
What is your overall opinion about this module?	

Notes (please provide general comments and suggestions regarding this module)

Modelling and investigating dependencies of CI by Roberto Setola (UCBM) [13:10 – 14:00]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

Simulation approaches of System of Systems by Alberto Tofani (ENEA) [15:00 – 15:40]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

Introduction to federated simulation by E. van Veldhoven (TNO) [15:40 – 16:20]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

Modelling, Simulation and Analysis Techniques for CIP by Marco Tesei (UCBM) [16:40 – 17:20]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

Verification and validation techniques by Edwin van Veldhoven (TNO) [17:20 – 18:00]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

Cyber threats to CI by Rafal Kozik (UTP) [18:00 – 18:40]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

2.2 Day 2 - 10th July 2015

Introduction to Decision Support Systems by Maria Carla De Maggio (UCBM) [9.30 – 10.10]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

Geographical Information Systems for visualization and analysis by Maurizio Pollino (ENEA) [10:10 – 10:50]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

Platforms for Large & Complex Scenarios by Alberto Tofani (ENEA) [10:50 – 11:10]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

An overview on CIPRNet DSS design by Vittorio Rosato (ENEA) [11:10 – 11:30]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

Events prediction and environmental sensing; Risk analysis tools for event and damages simulations by Maurizio Pollino (ENEA) [12.00 – 13.20]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

An Electric-SCADA based model to implement reconfiguration procedures in Electric Distribution grids by Antonio Di Pietro (ENEA) [14:20 – 15:00]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

Application of system of systems model for long term impacts analysis in large scenarios by Alberto Tofani (ENEA) [15:00 – 15:20]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

Consequence analysis and applications for supporting operator's decisions by Vittorio Rosato (ENEA) [15:20 – 15:40]

Question	*Score*
What is your overall opinion about this module?	
Notes (please provide general comments and suggestions regarding this module)	

Annex D – Training Material

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Introduction to CIPRNet

Roberto Setola
r.setola@unicampus.it

Modelling, Simulation and Analysis of Critical Infrastructures
CIPRNet Course

UCBM Headquarters – Rome (Italy) – 10-11 July 2014

Agenda

1. CIPRNet
2. “Critical” Infrastructures
3. CIPRNet: research context, activities, and new capabilities
4. Modelling, simulation and analysis of CI – setting the frame
5. Summary of CIPRNet introduction
6. CIPRNet’s training activities
7. Questions & Answers

1. CIPRNet – Facts

- Critical Infrastructures Preparedness and Resilience Research Network
- Co-funded by: EU FP7
- Instrument: Network of Excellence (NoE)
- Start date: March 1, 2013
- Duration: 48 months

1. CIPRNet – Consortium

1. Fraunhofer IAIS, DE (Coord.))
2. ENEA, IT
3. TNO, NL
4. UIC, FR
5. CEA, FR
6. Joint Research Centre, EU
7. Deltares, NL
8. University of Cyprus, CY
9. University of Technology and Life Sciences, PL
10. Università Campus Bio-Medico di Roma, IT
11. University of British Columbia, CA
12. ACRIS GmbH, CH

2. “Critical” Infrastructures

Definition of Critical Infrastructure according to ECI directive

- “A critical infrastructure (CI) consists of those assets and parts thereof which are essential for the maintenance of critical societal functions, including the supply chain, health, safety, security, economy or social well-being of people.” [EU2008]
- European CI (ECI) comprise CI of at least three Member States [EU2008]
- ECI sectors already identified [EU2008]: energy and transport CI
- National definitions vary, for example:
  - Germany: 9 CI sectors
  - The Netherlands: 12 CI sectors
  - France: 11 “activity sectors of vital importance”
- 2013: Review of ECI and EPCIP

[EU2008] European Commission:
***Council Directive 2008/114/EC** of 8 December 2008 on the identification and designation of European Critical Infrastructure and the assessment to improve their protection*

[EU2013] European Commission:
***CS Working Document** SWD(2013)318 of 28.8.2013 on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure*

2. “Critical” Infrastructures

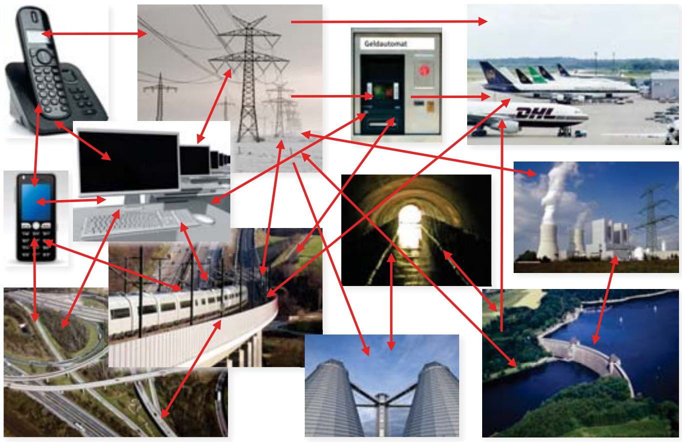
- Since the late 1990s, the CI topic gained importance with the advent of new threats
  - Year 2000 bug
  - WTC attacks on 11.9.2011
  - Climate change
- Follow-up activities
  - Identification of CI
  - Risk assessment of CI, following an **all hazards** approach
  - Measures for protection of CI
  - New research area: Critical Infrastructure Protection (CIP)
- The USA and Europe took different paths

2. “Critical” Infrastructures (CI)

CI

- are complex
- depend on other CI
- extend cross-border
- are continuously changing, adapting to changes in technology, economy, legislation, …

CI form a system of systems



2. “Critical” Infrastructures

Protection, resilience and preparedness

- A 100% safety and security of CI is impossible to achieve
- **In order to protect CI, to make them more resilient, and to maintain their vital societal functions, this super-system needs to be understood**
- Essential for any improvement in resilience or preparedness is a better understanding of CI
  - What CI are affected by a crisis or emergency?
  - What is the role of CI in emergency plans?
  - What CI are needed for supplying, evacuating, caring people affected by a crisis?

2. “Critical” Infrastructures

Insight on CI in crises, catastrophes, and emergencies

- **post mortem analyses** of real CI damages (like Kirchbach report on the Oder flood 2002)
- Real **exercises** (like LÜKEX)
- Computer-based **modelling, simulation and analysis (MS&A)** of crisis scenarios
- **Research results***

CI damage reports

*see presentation by E. Luiijf

3. CIPRNet research context

- USA: National Infrastructures Simulation and Analysis Center (NISAC)
- Canada: DR-NEP, i2Sim (University of British Columbia)
- EU:
  - Various nationally funded projects
  - Projects funded by Research Framework Programmes and successor
  - Projects funded by the European Programme for CIP (EPCIP) and successors

- Often used methods and tools: MS&A of complex scenarios involving CI and external threats
- Common challenges:
  - Transferring CIP related research results into practical application
  - Sustaining the support of CIP research experts to end users

3. CIPRNet joint activities

Capability forming

- Providing **new capabilities** to end users for better preparedness for CI-related emergencies:
  - Advanced decision support
  - ‘what if ’ analysis

Capacity building

- **Building capacities** by educating and training experts and researchers (reaching a critical mass)

Knowledge & technology

- **Providing knowledge and technology to end users** for improving their understanding of the role of CI in crises and emergencies

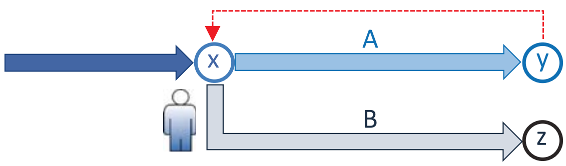
VCCC

- Provide **long-lasting support** by establishing a **Virtual Centre of Competence and Expertise in CIP (VCCC)**

3. CIPRNet’s new capabilities

CI MS&A modelling for exploring various possible courses of action

- **‘what if’ analysis:**
  The exploration of different courses of action and their different consequences



- Compare consequences of courses of action A, B (consequence analysis)
- Which action produces the least consequences? (e.g. duration of outages, number of affected people/businesses)
- Applications include:
  - Training of crisis managers
  - *post mortem* analyses

3. CIPRNet's new capabilities

Advanced Decision Support

- Decision Support System (DSS) for supporting Emergency Managers by providing a comprehensive assessment of the behaviour of CIs under severe perturbations
- DSS tasks:
  - Set-up the emergency scenario
  - Evaluate the impact of the disruption of CI elements causing a reduction in the Quality of the delivered Services
  - Provide end users with data and estimates helpful for making accurate scenarios assessment needed for undertaking the necessary decisions for optimal mitigation and healing strategies
- Applications include:
  - Warm and hot phase support of emergency managers and CI operators
  - Training

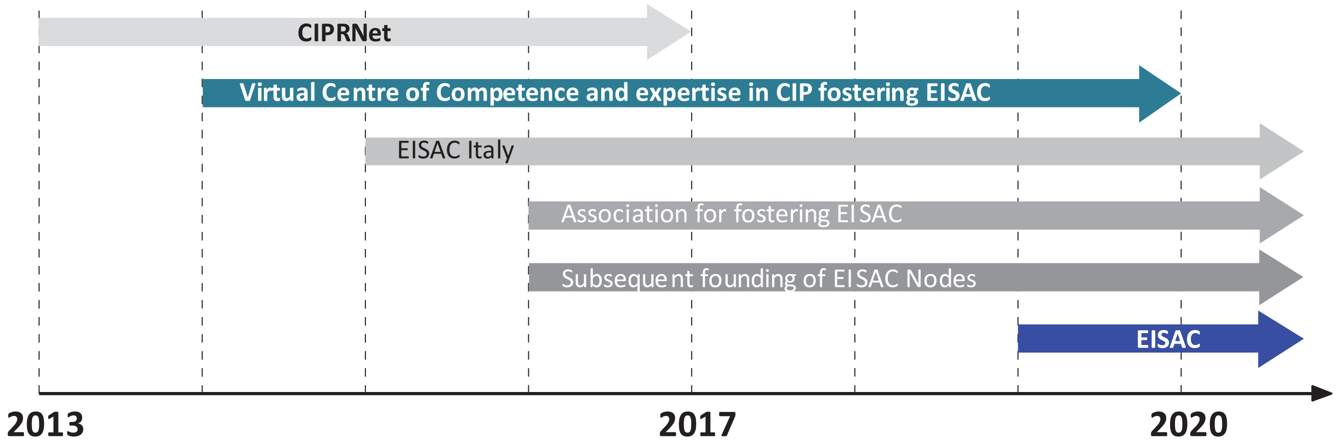
3. CIPRNet's new capabilities

Virtual Centre of Competence and Expertise in CIP (VCCC)

- How can CIP related research results be transferred into practical application?
- How can support of CIP research experts to end users be sustained?
- First step: VCCC – Role model is NISAC (USA)
- CIPRNet will create the tangible VCCC already during the project term
  - by implementing the CIPRNet agenda and
  - by combining and integrating the excellence in CIP knowledge, expertise, experiences and technology of the partners
- VCCC serves as foundation of the long-lasting European Infrastructures Simulation and Analysis Centre (EISAC)

4. Timelines

Timelines: CIPRNet, VCCC, and EISAC 2020



4. MS&A of CI – the frame

- Computer-based modelling, simulation and analysis of CI involves a complex setup of **multiple CI domains** and **external threats and events**
- There are many simulators, models, and analysis approaches around
- Challenges include:
  - Determination of what should and can be **investigated** using MS&A
  - Getting the required domain knowledge and **data**
  - Transforming this into valid and appropriate **computer models** at the adequate level of fidelity
  - Overcome technical difficulties (like **semantic interoperability**)
  - Performing the required **analyses**
  - Applying **verification and validation** approaches for maximising the validity of the results
  - Developing standardised **workflows for MS&A**

5. Summary of CIPRNet intro

- CIPRNet undertakes a next step towards realising EISAC by capability forming and capacity building
- CIPRNet will deploy new capabilities to its initial audiences
  - Advanced decision support
  - MS&A based 'what if' analyses with consequence analysis
- CIPRNet seeks collaboration with national projects and with end users
- A core element of CIPRNet technologies and of CI(P) related research in general is MS&A

6. CIPRNet's training activities

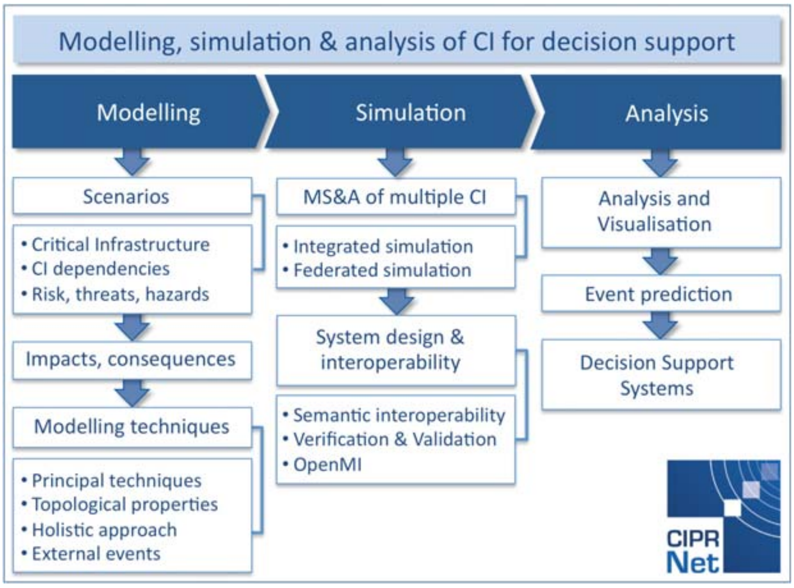
Elements of CIPRNet's training activities

- Internal training
  - Familiarising partners with each other's technology and know-how, fostering coherence
- CIPRNet lectures
  - Disseminating CIPRNet know-how to the CIP research community
- CIPRNet Master Classes
  - Familiarising CIPRNet's target audiences with CIPRNet's essential technologies
  - MC1, 2014: Modelling, Simulation & Analysis of CI
  - MC2, 2015: New CIPRNet capability: Decision Support System
  - MC3, 2016: New CIPRNet capability: MS&A-based 'what if' analysis
- CIPRNet courses in the Postgraduate Master in Homeland Security
  - Educating young researchers in the required multi-disciplinary mind-set

6. CIPRNet's training activities

- Audience
  - Students of the Postgraduate Master in Homeland Security
- Objectives of the CIPRNet Course in MHS
  - To perform training for the students of the MHS and familiarise them with MS&A of CI and its applications in analysis, decision support, and Crisis Management training
  - To prepare next generation security managers to the use of instruments as those provided by CIPRNet and by the VCCC
- Contents
  - basic concepts about MS&A of CI
  - advanced aspects related to federated simulation
  - introduction to DSS goals and functionalities
  - CIPRNet DSS
- Experts from the multi-disciplinary FP7 network CIPRNet will be presenting the lectures

7. Conceptual Map



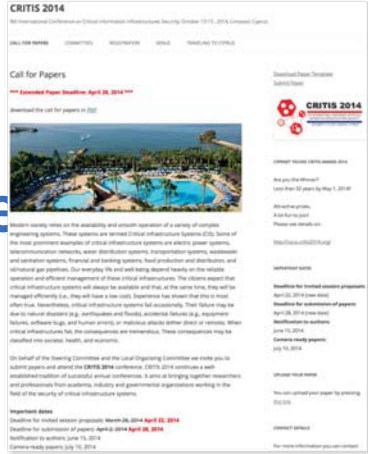
Locating the lectures

8. Questions & Answers

www.ciprnet.eu

European CIIP Newsletter

CRITIS 2014



CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

From critical infrastructure **protection** to critical infrastructure **resilience**?

Marianthi Theocharidou – European Commission, Joint Research Centre

marianthi.theocharidou@jrc.ec.europa.eu

Modelling, Simulation and Analysis of Critical Infrastructure
CIPRNet Course

UCBM – Rome (Italy) – 09-10 July 2015

Outline

- Protection or Resilience ?
- EU vs. US approach
- Definitions (CIPedia®)
- Resilience dimensions
- Resilience framework

Goal:
- Learn what resilience means from a critical infrastructure perspective.
- Understand why MS&A is needed.

Based on the report: C. Pursiainen & P. Gattinesi, "**Towards Testing Critical Infrastructure Resilience**", JRC Scientific and Technical Reports, European Commission, Joint Research Centre, 2014.

Definition of CIP

23.12.2008 EN Official Journal of the European Union L 345/75

COUNCIL DIRECTIVE 2008/114/EC

of 8 December 2008

on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

- ‘**Critical infrastructure**’ means an **asset**, **system** or **part** thereof located in Member States which is essential for the maintenance of **vital societal functions**, health, safety, security, economic or social well-being of people, and the **disruption** or **destruction** of which would have a **significant impact** in a Member State as a result of the failure to maintain those functions.

- ‘**Protection**’ means all activities aimed at ensuring the **functionality**, **continuity** and **integrity** of critical infrastructures in order to **deter, mitigate and neutralise** a threat, risk or vulnerability.

Protection vs. Resilience

Protection vs. Resilience

- The resilience discourse first started appearing in unofficial policy and scientific analyses in the **mid-2000s** in the context of **crisis** and **disaster management**.
- Focusing on resilience was justified with criticism of official government positions that complete **critical infrastructure protection can never be guaranteed**.
- Moreover, achieving the desired guaranteed level of protection is not **cost-effective** in relation to the actual threats. A small increment in the level of protection might introduce a large amount of additional costs, and therefore alternative approaches need to be considered.

“Resilience is the bridge beyond Protection….”

(R. David, IFIP CIP conference 2015).

Official EU vs. US approaches on Resilience

- CI Resilience in **USA**:
  - emerged first from **2006** onwards
  - primarily treated as a **subset** of protection (2006 NIPP)
  - based on **voluntary** public-private partnerships
- CI Resilience in **Europe**:
  - appears **around 2010-2012** in policy documents
  - somewhat stronger emphasis on (national) **regulation**
  - Is now considered **cross-sectoral**

- In both cases, the focus has mostly been in **organisational** and **community** resilience **measures**, although some **technological resilience** issues have more recently been brought forward, particularly in the US.

Definitions

www.cipedia.eu

Definitions

- USA: *"The term '**resilience**' means the ability to **prepare for** and **adapt** to changing conditions and **withstand** and **recover rapidly** from disruptions.*
  - *Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."*
- Europe: No official definition.
  - ***Resilience** (in the UK) is the ability of assets, networks and systems to **anticipate**, **absorb**, **adapt to** and / or **rapidly recover** from a disruptive event.*

CabinetOffice

Definitions

UNISDR:

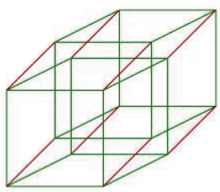
- The ability of a **system**, **community** or **society** exposed to **hazards** to **resist**, **absorb**, **accommodate to** and **recover** from the effects of a hazard in a **timely and efficient manner**, including through the preservation and restoration of its essential basic structures and functions.

The resilience of a community in respect to potential hazard events is determined by the degree to which the community has the necessary **resources** and is **capable of organizing** itself both **prior to** and **during** times of need.

UNISDR
The United Nations Office for Disaster Risk Reduction

Dimensions of resilience

- The exact boundaries of the 'resilience discourse' are still rather obscure.
- However, sub-discourses or research sub-fields and partially shared definitions have emerged and even become institutionalized.
- At least four different dimensions of critical infrastructure resilience:
  - **Societal resilience**
  - **Economic resilience**
  - **Organisational resilience**
  - **Technological resilience**



Other 'dimensions' found in the literature: 'functional resilience', 'personal resilience'; 'physical resilience'; 'planning resilience'; 'ecological resilience'; 'socio-ecological resilience'

Societal resilience

- '**Societal**', '**regional**' or '**community**' resilience - often used interchangeably
- Refers to empowering the whole society, including **local communities** and **businesses**, rather than only enhancing the authorities' crisis management capacities or control.
- Refers to the society's **survival** and **recovery** strategies, e.g. availability of shelters, time to restore lifeline services, etc.
- There is **no universally agreed definition** of societal resilience.
- While good practices of resilient communities exist, there are **no agreed methodologies or metrics** on how to test community resilience.

Economic resilience

- Focus on the **dynamics** of technological innovation and the need of adaptive behaviour of **businesses** and **markets**:
  - the extent of regional economic diversification
  - the ability to substitute and conserve necessary inputs
  - business and industry capacity to improvise
  - the time needed to regain capacity or lost revenues

- **Static economic resilience** is "the ability of an entity or system to maintain function (e.g., continue producing) when shocked".
- **Dynamic economic resilience** "is the speed at which an entity or system recovers from a severe shock to achieve a desired state."
- Metrics: **micro** (individual business, household), **meso** (single industry or market) and **macro** (combination)

Organisational resilience

- Concept applied to crisis management and civil protection systems.
- Organisational resilience also connects the resilience concept to the concept of **business continuity**.

Example: For electricity supply disruptions, operators need to:
- Make plans of how and when personnel should be called in, or put on stand-by
- Keep maps up to date
- Maintain information about how disruption affects operations
- Monitor weather forecasts
- Make arrangements with third parties for providing spare parts and additional equipment
- Prepare for cooperation with the emergency services,
- Find out vulnerabilities in telecommunication nodes, waterworks and sewage farms
- Prioritize support for vulnerable groups such as hospitals, nursing homes for older people, schools, day-care centres etc.

Organisational resilience

- The **ISO 28002:2011** standard for **resilience in the supply chain** (based on the US ANSI/ASIS organisational resilience standard): "[…] requirements for a resilience management system to enable an organization to develop and implement **policies**, **objectives**, and **programs** taking into account legal requirements and other requirements to which the organization subscribes, information about significant **risks**, **hazards** and **threats** that may have an **impact** on it (and its stakeholders'), and **protection** of critical assets (human, physical, intangible, and environmental."
- Focus on a proper risk management system embedded in the organization, including such elements as training, risk assessment, prevention, mitigation etc.

Technological resilience

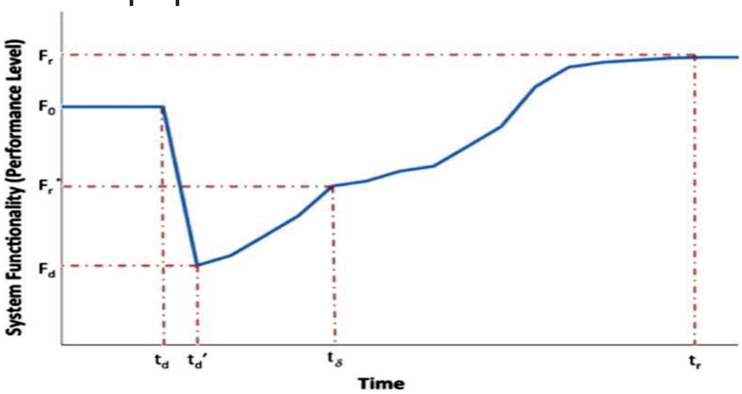
- Technological resilience is more **about the infrastructure** itself, rather than about the society around it, or the economic consequences of its disruption, or the organisation ensuring the functioning of the infrastructure

System Resilience

- Resilience at the system level is …"a measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables" (Holling, 1973)

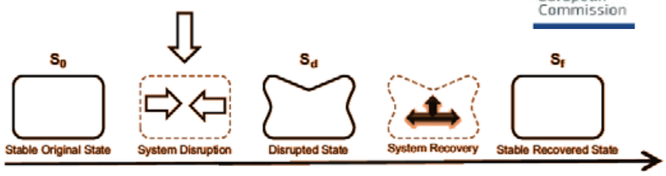
Infrastructure system resilience is generally regarded as the ability of the system to withstand a disturbance and recover back to its initial or a new state.

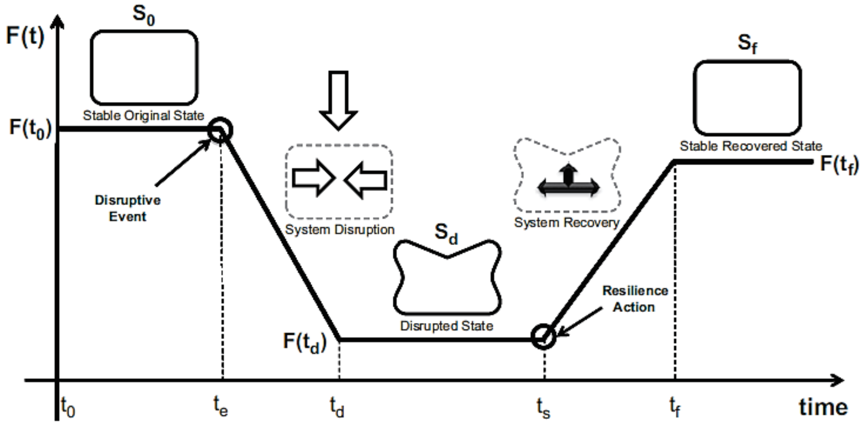
- Functional, Structural or Mixed



(Francis and Bekera, 2014)

Delivery Function Transition





Four Rs of Resilience

Robustness

- Strength, or ability of elements, systems, and other units of analysis to withstand a given level of stress or demand without suffering degradation or loss of function.

Redundancy

- Extent to which elements, systems, or other units of analysis exist that are substitutable, i.e., capable of satisfying functional requirements in the event of disruption, degradation, or loss of functionality.

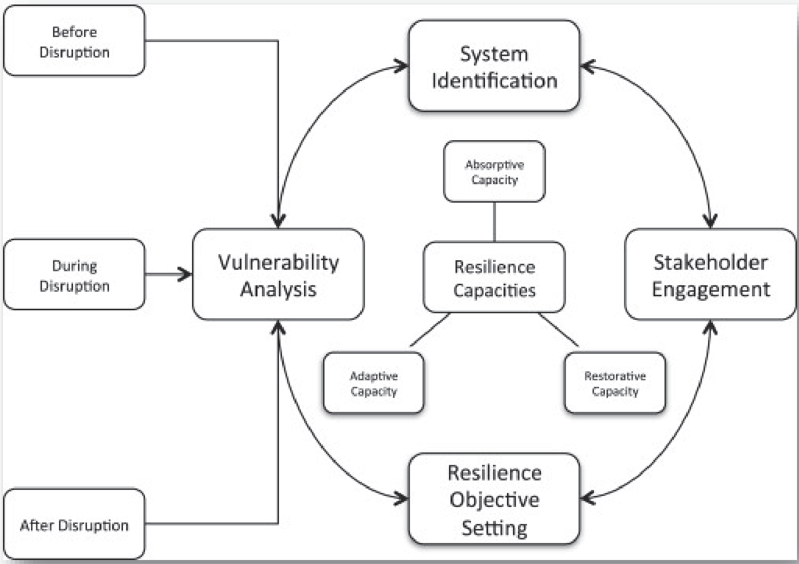
Resourcefulness

- Capacity to identify problems, establish priorities, and mobilize resources when conditions exist that threaten to disrupt some element, system, or other unit of analysis.

Rapidity

- Capacity to meet priorities and achieve goals in a timely manner in order to contain losses and avoid future disruption.

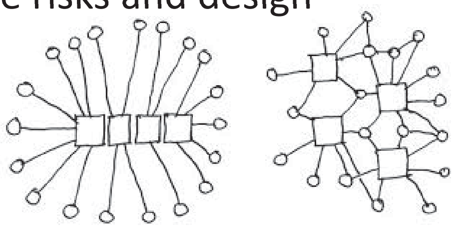
CI Resilience Framework



R. Francis , B.Bekera, A metric and frameworks for resilience analysis of engineered and infrastructure systems, *Reliability Engineering &System Safety*, Volume 121, 2014, 90 – 103)

Absorptive Capacity

- ‘**Resilient design**’, ‘**resilient engineering**’, ‘**reliability**’, ‘**robustness**’, or ‘**absorptive capacity**’ are largely overlapping terms.
- The safety and security factors should be built-in to the systems so that the **systems** would then be better capable of **absorbing** or **withstanding disturbances**, thereby minimising the consequences.
- It is however difficult in advance anticipate all the risks and design accordingly.



Adaptive Capacity

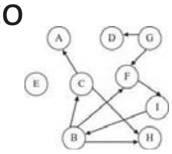
- ‘**Redundancy**’, ‘**interoperability**’, ‘**adaptive capacity**’ and ‘**resourcefulness**’… the *degree* that the function of a system temporarily disturbed can be replaced by other systems, substituted by other solutions, re-routed etc.
- **Duplication** or **triplication** of critical elements of a system with a **backup**, while avoiding common vulnerable points.
  - **Passive redundancy:** an element can fail while the main functions remain in tact though the performance decreases.
  - **Active redundancy:** monitor and detect, e.g. overload in one power line and circuit breakers should automatically disconnect this line and redistribute the power across the remaining lines.

Restoring capability

- ‘Restoring capability’ is basically the same concept as ‘**recovery**’ or ‘**rapidity**’ used in many occasions.
- Two basic ways to measure resilience:
  - Amount of time (or money/losses) it takes for an infrastructure or a function to recover fully to normal operations
  - Performance, that is, whether the system was put out of operation completely or not

Avoiding harmful dependencies

- A resilient critical infrastructure should not be such that, even if it would be robust itself, it would become easily dysfunctional due to dependencies between it and other related infrastructures or systems.



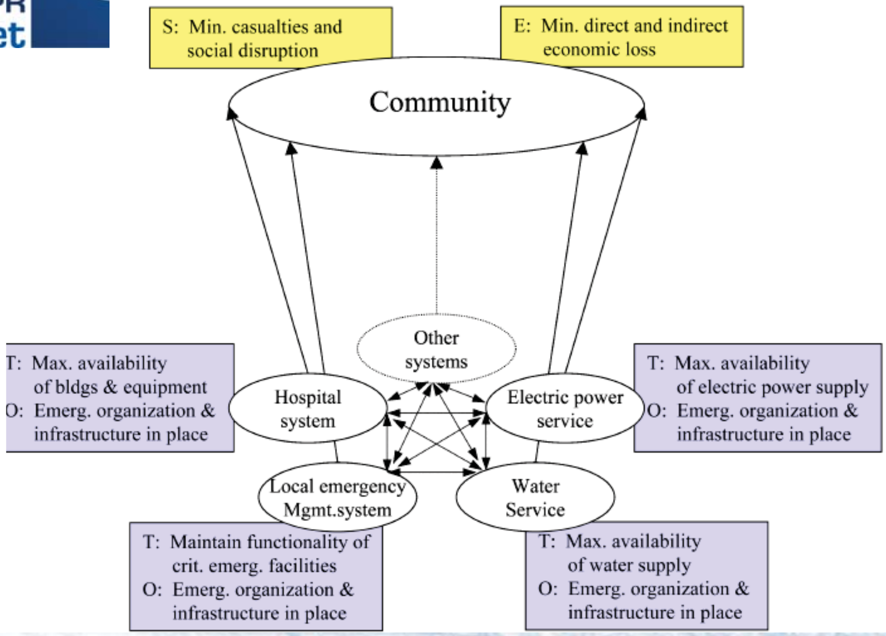
- It is difficult however to test these complicated dependencies in an operational environment (without causing too much harm).
- Therefore, in most cases the only feasible methodology to study and test dependencies, interdependencies and cascading effects is to focus on **modelling**, **simulation and analysis.**

Testing for resilience

- CI Technological resilience can be enhanced, measured and tested

What could be tested?	How should it be tested?
Absorptive capacity	e.g. tests of the resiliency of a component or a system based on real failure data
Adaptive capacity	e.g. passive and active redundancy testing
Restoring capability	e.g. calculating the amount of resources (times, money) the recovery takes, or measuring the ration of lost performance/total performance
(Inter)dependencies	e.g. computer-based modelling and simulation

Towards Community Resilience



- System and community resilience measures
  - T: Technical
  - O: Organisational
  - S: Societal
  - E: Economic

How to improve resilience with MS&A tools?

M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, Reliability Engineering and System Safety 121 (2014) 43–60

Absorptive capacity

- Identify key CIs or components which can cause cascading effects
- Learn and improve from previous accidents using accident models
- Design an observatory network to sense, monitor, and update system states in real time along with state visualizations based on emerging infrastructure modeling techniques to assess on-line risk for early warning
- Model consumer behaviors to keep the CIs load at a certain level to reduce the overload-induced hazards

Adaptive capacity

- Optimize and retrofit the topology of each CIs
- Design and prepare redundancy, backup and substitution to lower the interdependency impacts.
- Improve the absorptive capacities of some key CIs.
- Manage or directly control consumer behaviors to adjust the system load.

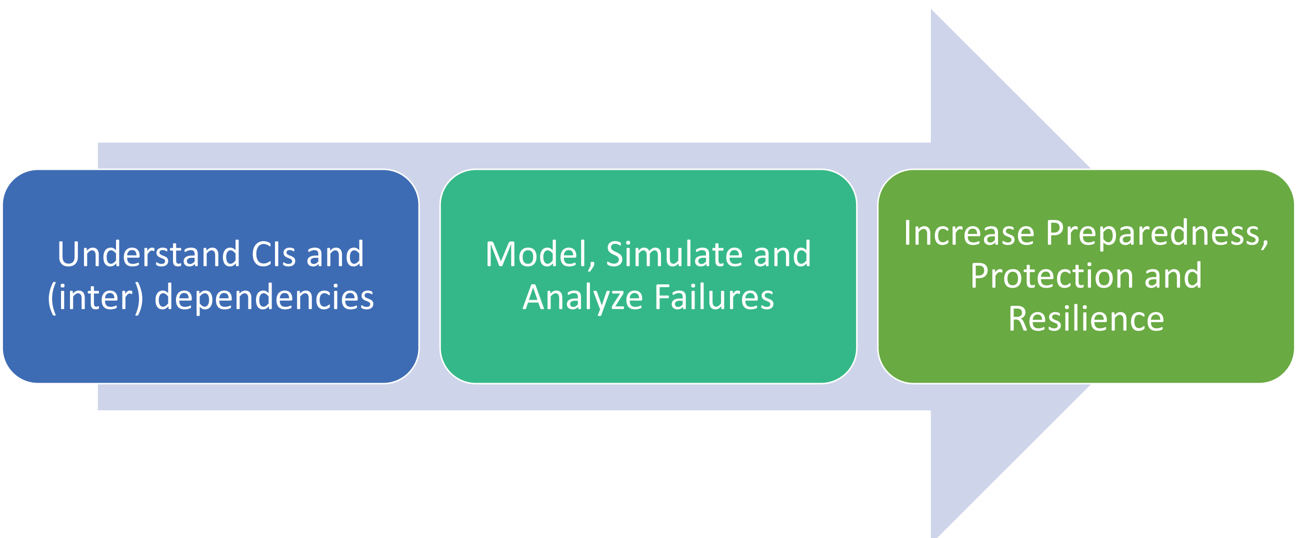
Restorative capacity

- Find restoration sequences and priorities or optimum resource allocation strategies.
- Improve the restorative capacities for key CIs or components.
- Increase the variety and robustness of communication channels.

Summary

- In short, resilience is a conceptual framework composed of multiple **dimensions**.
- **Absorptive**, **adaptive**, and **restorative** capacities are at the center of what a system needs to do and how it needs to respond to perceived or real shocks. We denote these as the resilience capacities.
- The objective of resilience is to **retain predetermined dimensions of system performance** and identity in view of **forecasted scenarios**.

Summary



Questions?

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Simulation of Critical Infrastructures (CI): Relevant Applications

Eric Luiijf, TNO
eric.luiijf@tno.nl

Modelling, Simulation and Analysis of Critical Infrastructures
CIPRNet Course

UCBM – Rome (Italy) – 9-10 July 2014

Agenda

- Application of Modelling, Simulation & Analysis in CIP/CIR
  - different areas of application
  - added value for stakeholders
- Existing activities
  - USA: NISAC / HITRAC
  - Australia: CIPMA
  - CIPRNet consortium: I2SIM, DIESIS toolset, CISIA, more …
- Looking forward
- Questions/discussion

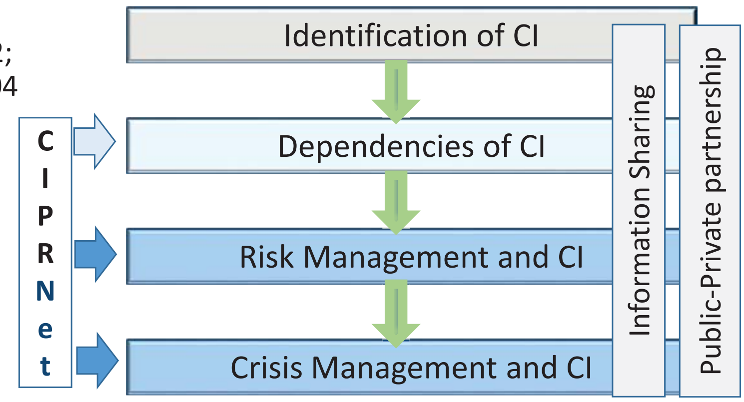
Objectives of this lesson

- Understand
  - the different application areas of CIP/CIR Modelling, Simulation & Analysis (MS&A)
  - the added value for stakeholders such as policy-makers, CI operators, and emergency management
    - exercises
    - what-if analysis
    - decision support

- Understand the current international activities in CIP MS&A and future directions

Main focus areas of Critical Infrastructure Protection (CIP)

- EU and its Member States
  - various Member States active since 2002; EU started with the CIP topic around 2004
  - some of the main action lines of the European Programme on CIP (EPCIP) may be supported by MS&A
  - Currently, a EU-wide drive for Critical Infrastructure Resilience (CIR)



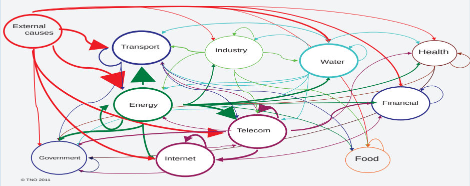
CI MS&A – What is it all about?

Threat simulator(s)

e.g.
- extreme weather
- flooding
- drought
- disrupted pipeline

- loss of sea lines

Federation of CI simulations



Effects & consequence simulator(s)/model(s)

e.g.
- casualty
- ecologically affected area
- damages
- economic impact (long term)

Visualisation & data exchange
(e.g. existing emergency systems)

STAKEHOLDERS

CI simulation – What is it all about?

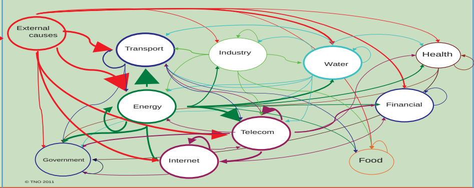
CIPRNet

Threat simulator(s)

e.g.
- extreme weather
- flood
- drought
- disrupted pipeline

- loss of sea lines

Federation of CI simulations



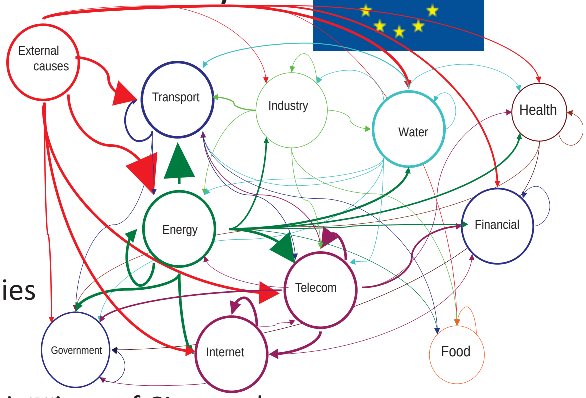
Effects & consequence simulator(s)/model(s)

e.g., casualty and other impact on people; affected area; economic impact and damages; impact on dependent CI

Visualisation & data exchange

STAKEHOLDERS

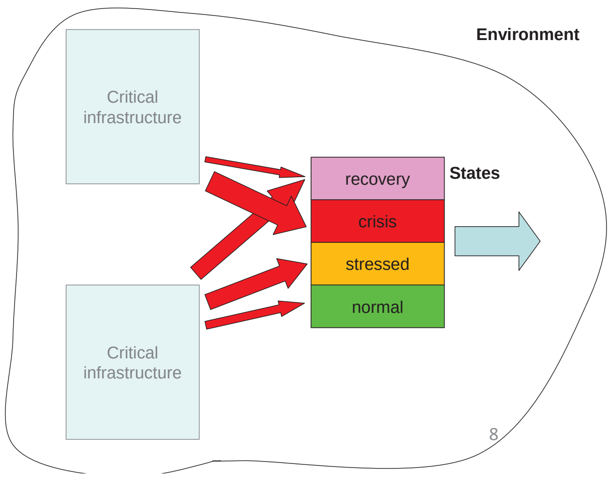
Application of MS&A in CIP/CIR – why?



- To analyse complex CI dependencies
  - different **modes of operation** of CI
    with other less known sets and strengths of dependencies
  - cascading effects with various
    disruption & recovery characteristics; QoS - SLAs
  - **common cause failure**: simultaneous disruptions & combinations of CI cascades

Application of MS&A in CIP/CIR – why?

- Set of critical dependencies may largely change with Mode of Operation
  - often a gap in risk analysis and the taking of mitigating measures
  - unplanned critical needs e.g. diesel, transport, ship, experts, …



Application of MS&A in CIP/CIR – why?

- Common cause failure
  - is not a dependency !
  - may create cascading effects

    even multiple dependency failures
    for a service

Threat affects

CI1 – e.g. telcom backbone → Mobile telcom, Internet access

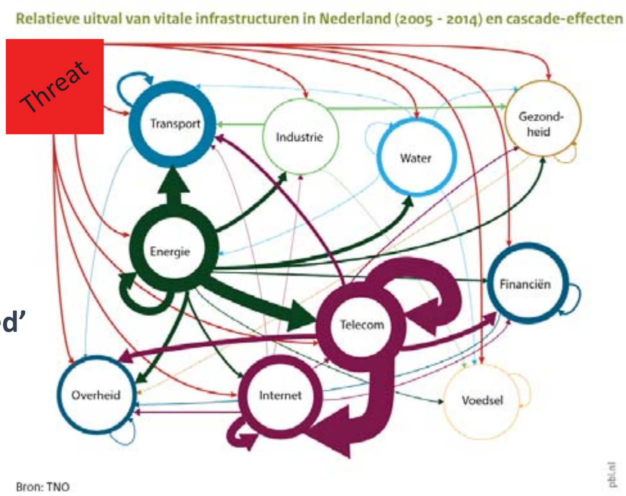
…

CI*n* – e.g. roads → Mobile telcom, Internet access, financial payments

→ financial payments

Application of MS&A in CIP/CIR – why?

- MS&A required for such analysis as
  - 1st order dependencies are simple:
    after x hours, y will happen
  - **more complex effects are hard for humans to assess**
    - N*M dependencies ➔ complex interactions
    - surprising outcomes other than the 'pre-programmed' outcomes we all already know
    - **mode of operation**
    - **service use patterns: time of the day; season; weather**



Application of CIP/CIR MS&A (2)

- CIP/CIR MS&A may support ***but has to prove its added value for stakeholders***
  - risk analysis and risk management (pro-action, prevention, preparation)
  - crisis management and response (prepare/exercises, response, recovery, aftercare)
  - CI resilience (CI design, what-if analysis, exercises)
  - resilient design of Next Generation Infrastructure

Risk analysis and CI

- Risk analysis (pro-action, prevention, preparation)
  - identifying risk scenarios and their impact on CI
  - all hazards, e.g. flooding, earthquakes, extreme weather, cyber attacks & failures, …
- CIP/CIR MS&A may help to assess the impact of different "what-if" scenarios and the effectiveness of countermeasures

Crisis Management and Response & CI Operators

- Crisis management and response (prepare, response, recovery, aftercare) of crisis response organisations & CI operators
  - identify which CI may be affected (next)
  - assess the impact of possible (sequences of) events

- MS&A may help to
  - assess effects of hazards on CI
  - assess effectiveness of countermeasures
  - perform a QUICK (coarse) first order assessment
  - prepare decisions
    - but, what level of detail is required?

  - identify lessons / better decisions by what-if ‘replay’

Agenda

- Application of Modelling, Simulation & Analysis in CIP
  - different areas of application
  - added value for stakeholders

- Existing activities
  - USA: NISAC / HITRAC
  - Australia: CIPMA
  - CIPRNet consortium

- Looking forward

- Questions/discussion

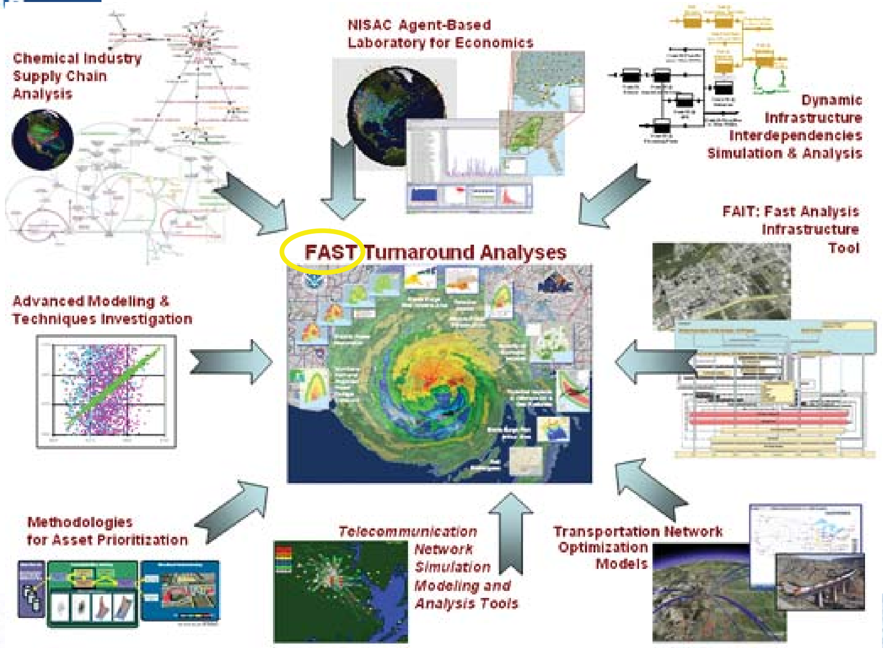
Activities: USA NISAC / HITRAC (1)

- US National Infrastructure Simulation and Analysis Center (NISAC)
  - Department of Homeland Security (DHS) as partner & sponsor
  - Sandia National Laboratories (SNL)
  - Los Alamos National Laboratory (LANL)
- Mandate and tasks
  - Congress mandated that NISAC serves as
    "*source of national expertise to address critical infrastructure protection*" research and analysis
  - NISAC prepares and shares analyses of CI including their dependencies, vulnerabilities, consequences, and other complexities
- Budget: 20 M$/year

Activities: USA NISAC / HITRAC (2)

- NISAC has developed large-scale CI models and data sets to support decision-making **before and during** emergencies
  - assist in emergency management at various levels of authority (county, state, federal)
  - analyse the impact of possible scenarios
  - assess the effectiveness of possible mitigating measures
  - support of (national) crisis management in **hot phase** (HITRAC)
- Models supported HITRAC during major emergencies
  - Katrina and Rita hurricanes (2005)
  - Superstorm Sandy (2012)

Activities: Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)



DHS
- Office for Infrastructure Protection
- Office of Intelligence and Analysis (OIA)

with NISAC

ALL HAZARDS

. prevention planning
. hot hazard analysis
. response planning
. base camp planning
. staging area

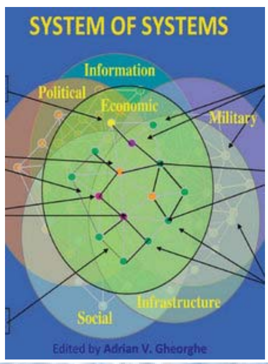
Source: DHS/HITRAC

Activities: USA Hampton Roads

(Prof. Adrian Gheorghe, Old Dominion Univ.)

- Detailed modelling of transport, shipping, … (major container port; main naval port)
  - in support of (all hazard) emergencies, hurricane lane is one of them
  - planning evacuation routes
  - support crisis management

  - much is detailed operational & crisis management information (thus classified)



Activities: Australia CIPMA (1)

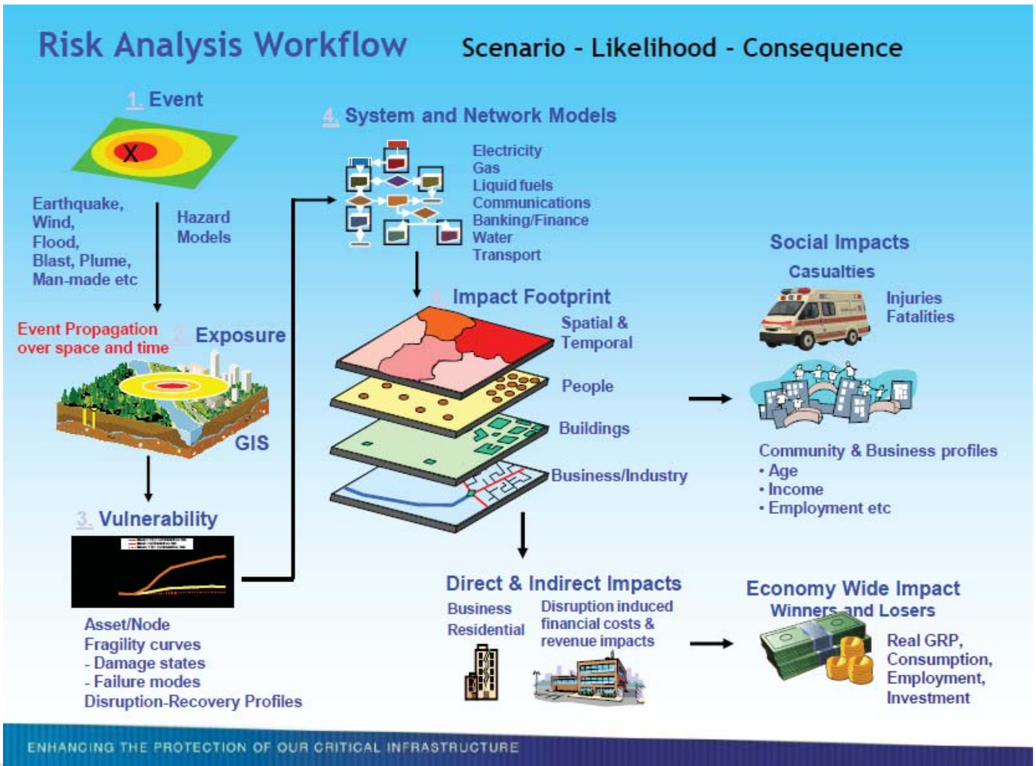
- AUS GOV Critical Infrastructure Program for Modelling and Analysis (CIPMA)
  - *governmental facilitation* of cross-sector analysis of the AUS CI sectors in a *joint public-private* approach *to increase CI sector resilience*
  - (single) sector by sector but stimulates inter-sector resilience studies

- Modelling capability is used to support CI sectors
  - strategic studies, fast turn-around analysis
  - *only* at request of a critical sector

- Budget: 23.4 M$ (16 M€) for 4 years plus *in kind investements* by sector(s)

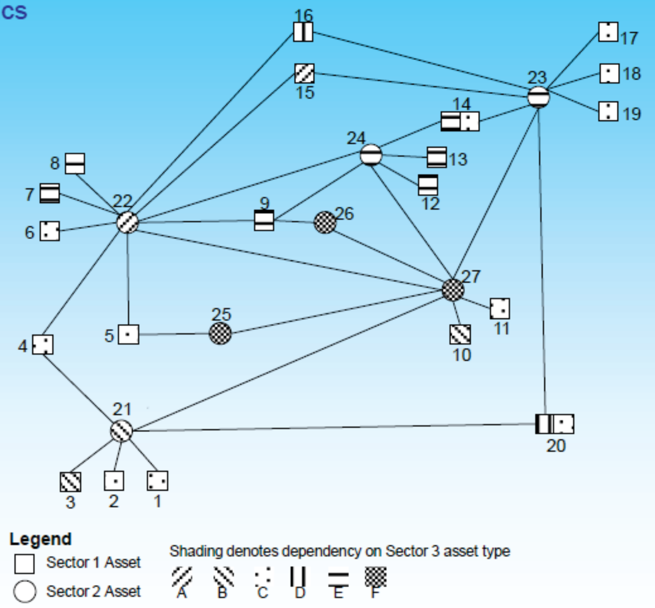
CIPMA

- CIPMA MS&A
  - reusability
  - consistency over time



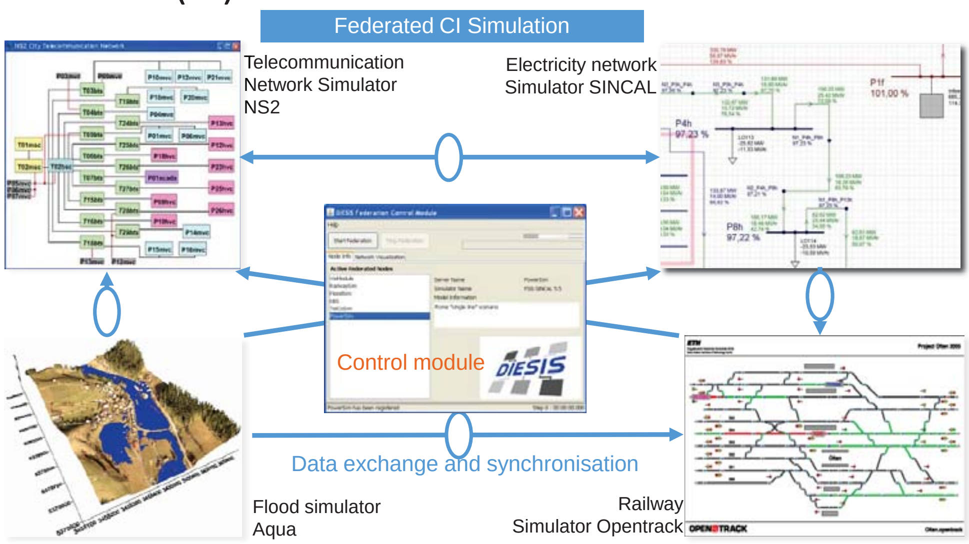
Network Analysis Example

- Cross sector dependencies
- Schematics



ENHANCING THE PROTECTION OF OUR CRITICAL INFRASTRUCTURE

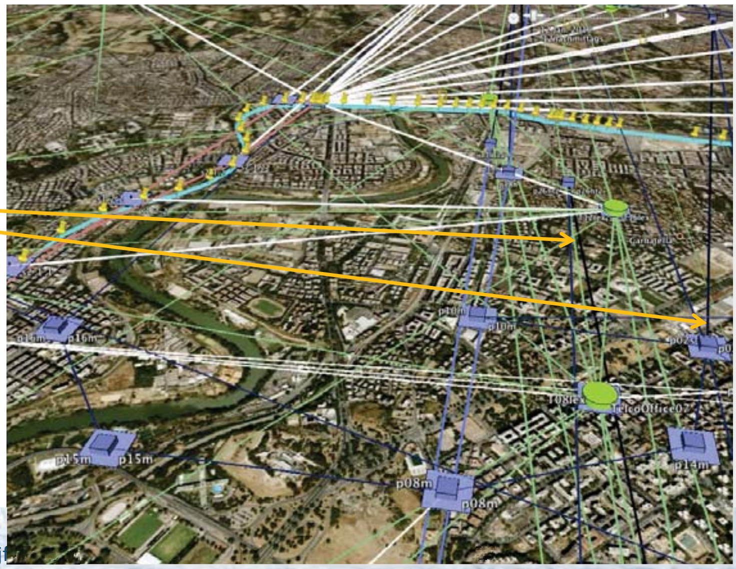
Activities of EU CIPRNet consortium: DIESIS (1)



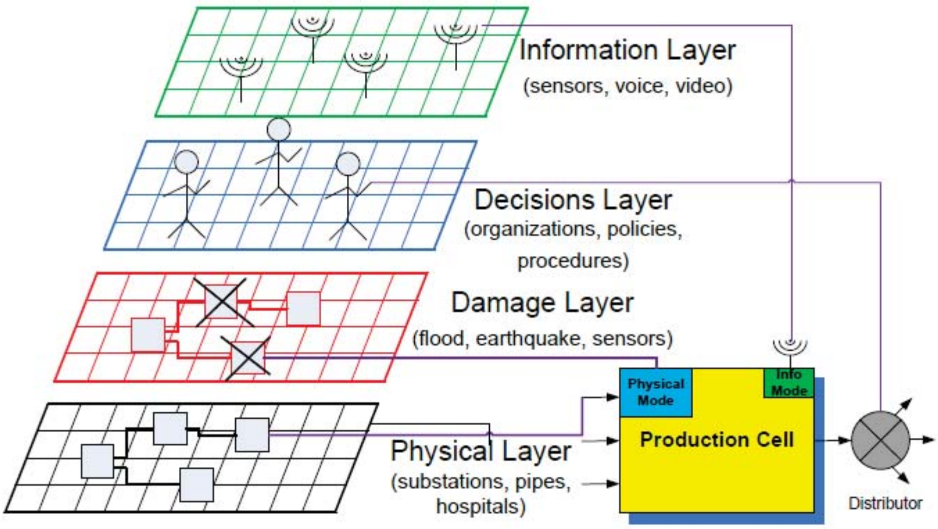
- details: see afternoon presentation by Fraunhofer

Activities EU CIPRNet consortium: DIESIS (2)

- Example of analyses
  - visualisation of cascading effects
  - black lines indicate disrupted parts of the CI networks



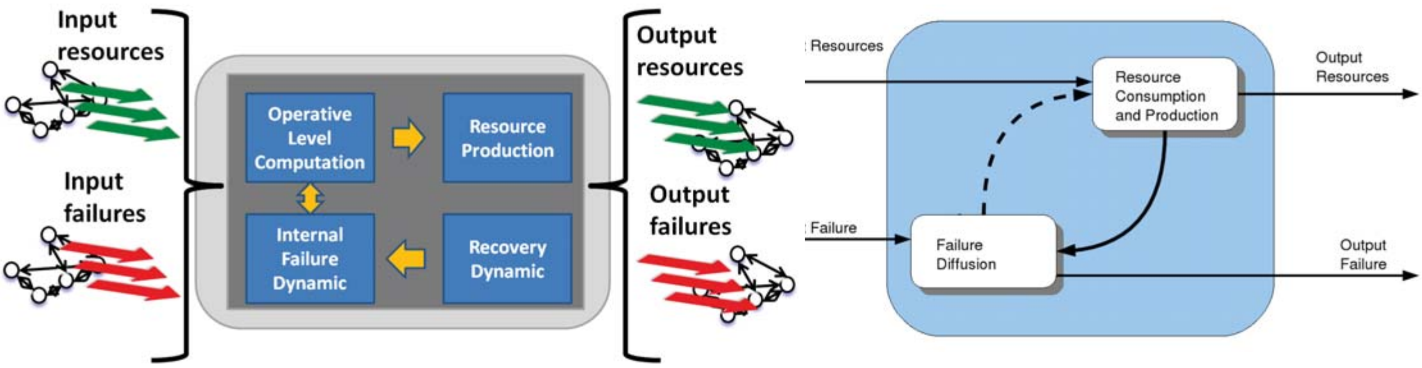
Activities EU CIPRNet consortium: I2SIM – agent-based simulation



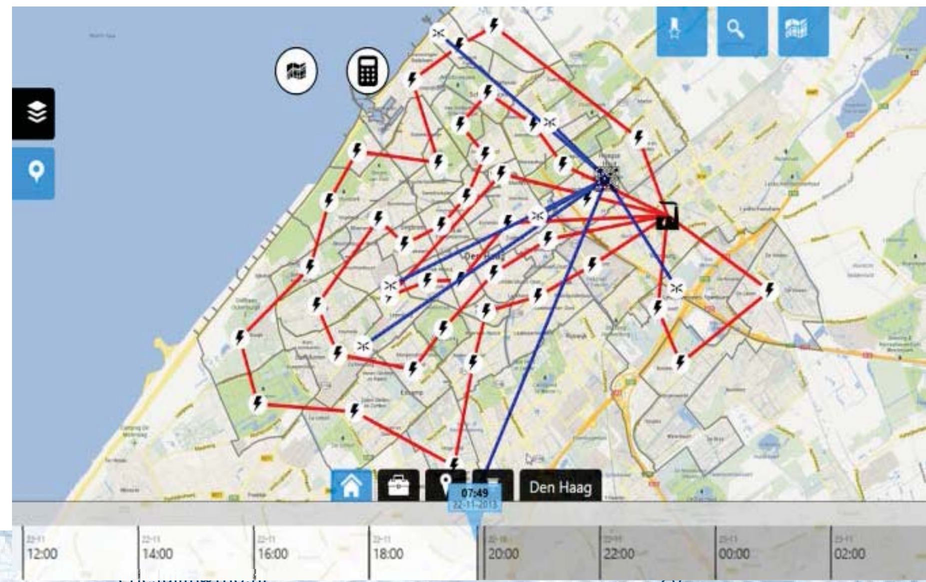
Activities EU CIPRNet consortium: CISIA

Critical Infrastructure Simulation By interdependent Agents (CISIA)

see Roberto Setola's lesson



Activities EU CIPRNet consortium – some other toolsets



Successful MS&A requires more than building a model …

- DATA, DATA, DATA
    - collecting data requires a large effort
    - issues: how to collect CIP information
      how to protect this (often sensitive) information
      artificial data === realistic data ==== real data

- Acquiring sensitive CI operator data requires trust-building, but
    - some information is in the public domain
    - some models do not require fine grained data
    - governments may stimulate data availability

Successful MS&A requires more than building a model … (2)

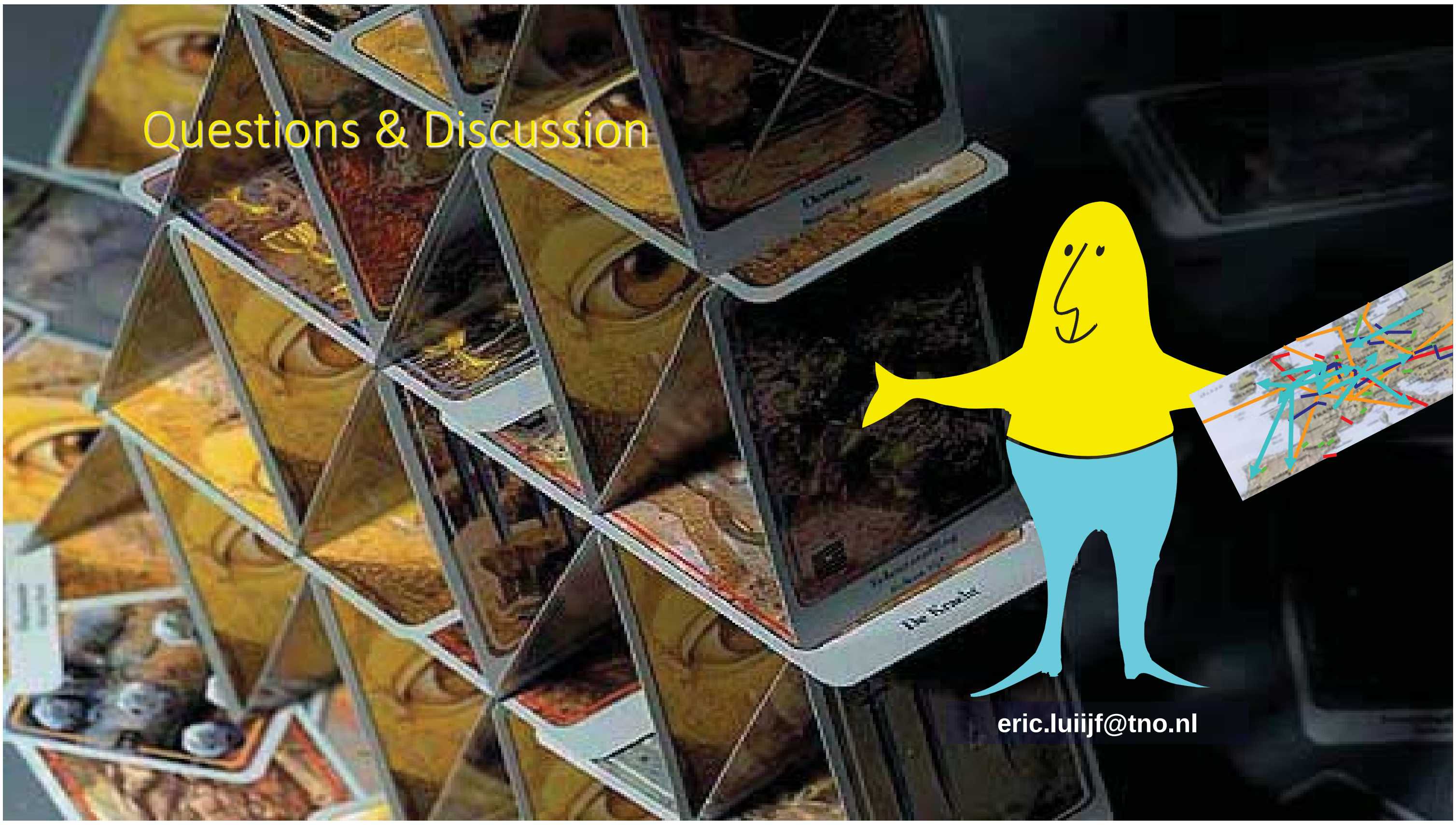
- What is the question?
    - academically precise results three weeks after the crisis..
      or *actionable* decision support four hours before the crisis with coarse figures?

- Public-private partnerships
    - collaboration between emergency management and CI operators is necessary
      “do not exchange a business card during an emergency”
    - added value of (longer-term) MS&A (investment) shall be clear for stakeholders
    - trust in each other and security arrangements to share valuable information

Looking forward

- CIPRNet's long-term vision is working towards a EU common MS&A toolset & (demo) data sets
  - based on good practices of e.g. NISAC
- CIP MS&A to assess the robust design of NGI, e.g. smart grids
- Coupling cause models with consequence/effects analysis models via CI models
- Metrics
  - economic impact (non-produce, damages)
  - how many people where in the impacted area? ➔ impact on evacuation, housing, psychological impact & behaviour of people, …
  - how many animals where in the impacted area? ➔ impact

➔ requires standard interfaces between components & GIS-based visualisation



Introduction to Modelling Techniques: Applications & Limitations

Mohamed Eid – CEA/DANS/DM2S

mohamed.eid@cea.fr

Modelling, Simulation and Analysis of Critical Infrastructures Master Class (Edition2)

Università Campus Bio-Medico di Roma, Rome (Italy) – 9 July 2015

What is the issue?

Understanding the behaviour of critical infrastructures, their dependences and their interdependences.

Developing advanced modeling and simulation methodologies & technologies

Enhancing the CIs' resilience against threats

Dependence & (Inter)dependence

- Physical/Structural
- Functional
- Procedure

Conceptual Models (1)

▪ Fluid Mechanics	:	**Navier-Stockes Equation**
▪ Heat Transfer	:	**Newton Equation**
▪ Electro-magnetic propagation	:	**Maxwell Equations**
▪ Electrical Circuits	:	**Kirchhoff's Law**
▪ Structure Dynamic	:	**Equations of motion / (Lagrange's Equation, …)**
▪ Neutron transports	:	**Boltzmann Equation**
▪ ……..		

Empirical & Statistical Models (2)

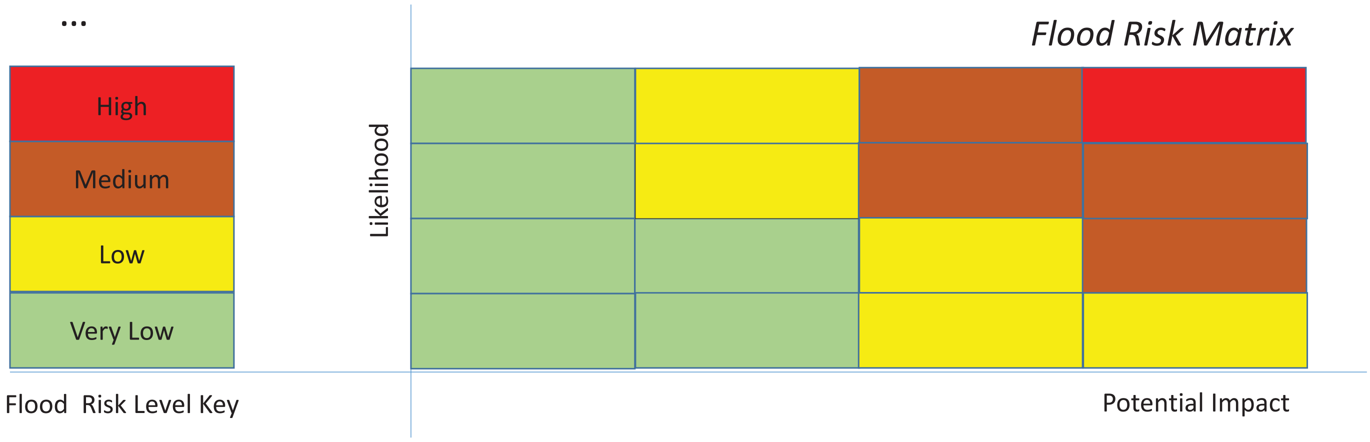
- Rains Flow & Distribution
- Wind Velocity & Direction Distribution
- Loss of Pressure in Pipes (in case of turbulent flow)
- Radiative Heat Transfer (Stefan's Law)
- Traffic & Road Accidents
- Components & Systems Failures
- Detection & Monitoring Failures
- ………………

Logical/Relational Models (3)

- Boolean models: minimal cut-sets, critical paths and disjoint cut-sets, conditional gates
- Sequential logical models: Event "E" occurs if Events "A" AND "B" AND "C" occur in that order: sequence analyses
- Fault Trees/Dynamic Fault Trees
- Event trees
- Decision Trees
- Reliability Block Diagrams
- Graphs (networks, states & transitions)
- ………………..

Qualitative & Descriptive Models

- Systems' behaviour, state, transition or reactivity are described using qualitative metrics: high/low, much/less, strong/weak, probable/rare …



Simulation

- ***The easy job :*** is to describe the behavior (in space and time) of any system whose functioning involves any of the previous models
- ***The hard job :*** is to describe the behavior (in space and time) of any system whose functioning involves many of the previous models (multi-scale, multi-physics, varying relational)
- ***The hardest :*** is to describe the behavior (in space and time) of any system whose functioning involves many of the previous models, mixing logical, deterministic and probabilistic models

System Complexity

Simulation of Complex Systems

- Needs for Integration Tools
- Integration at different levels of models: Data level, application interface level, method level, and the user interface level
- Stochastic Integration Tools: Monte-Carlo Simulation, Petri-Net & Stochastic Petri-Net, Genetic Algorithms, …
- Smart Agents: active, proactive and social

Recall the Issue

Understanding the behaviour of critical infrastructures, their dependences and their interdependences.

Developing advanced modeling and simulation methodologies & technologies

Enhance CIs' resilience against threats

Robustness & Resilience

In his report, Sir Michael Pitt, defined resilience "Resilience is the ability of a system or organisation to withstand and recover from adversity."

- Quantitative Modelling? [to be developed!!!]
  - Robustness $\propto \Delta 1$
  - Resilience $\propto 1/\Delta 2$

- Qualitative Modelling? [Sir Michael Pitt, "A comprehensive review of the lessons to be learned from the summer floods of 2007". Final report, June 2008.]

CIP vs Risk Management?

- The 3RG Focal Report, [*], argues that there are three main conceptualizations of the risk-resilience relationship in the theoretical literature and in CIP-policy documents: resilience as the goal of risk management, resilience as part of risk management and resilience as alternative to risk management.

* *3RG Report Focal Report 7 SKI, "Focal Report 7: CIP Resilience and Risk Management in Critical Infrastructure Protection Policy: Exploring the Relationship and Comparing its Use." Risk and Resilience Research Group Center for Security Studies (CSS), ETH ZürichZurich, Commissioned by the Federal Office for Civil Protection (FOCP), December 2011*

CIP vs Risk Management: resilience as the goal of risk management (1)

<u>Resilience Oriented Risk Management</u>

Resilience would be described as the overarching goal of protection policies and risk management as the method to achieve this goal. *Resilience replaces or complements the concept of protection,* which was previously defined as the goal of risk management activities.

CIP vs Risk Management: resilience as the goal of risk management (2)

<u>Comprehensive Resilience Risk Management</u>

Resilience is understood as a part of risk management. Activities to strengthen resilience are needed in order to deal with the so-called “remaining risks”, i.e. risks that have not been identified or underestimated and are thus not covered by appropriate protection (preventive) measures.

But a systematic resilience approach is still to be developed and it seems as if it can’t be deterministic, probabilistic, ..

CIP vs Risk Management: Replacing Risk Management (3)

Alternative to Risk Management

Challenges the traditional methods of risk management and promotes resilience as a new way of dealing *with* risks in a complex environment. It is argued that a probabilistic risk analysis is not an adequate approach for socio-economic systems that are confronted with non-linear and dynamic risks and are themselves characterized by a high degree of complexity. Instead of preventing risks and protecting the status quo, such systems should enhance their resilience by increasing their adaptive capacities.

But again! What is Resilience?

Since resilience is defined as the ability to resist, absorb, recover or adapt to adversity of changes in conditions, it is obvious that the concept is related to risk management – as the concepts "adversity" and "changes in conditions" can be described as risks.*

* *UK Cabinet Office, "Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards". Publication date: March 2010.*

Remind Our Ultime Goal

The main goal is

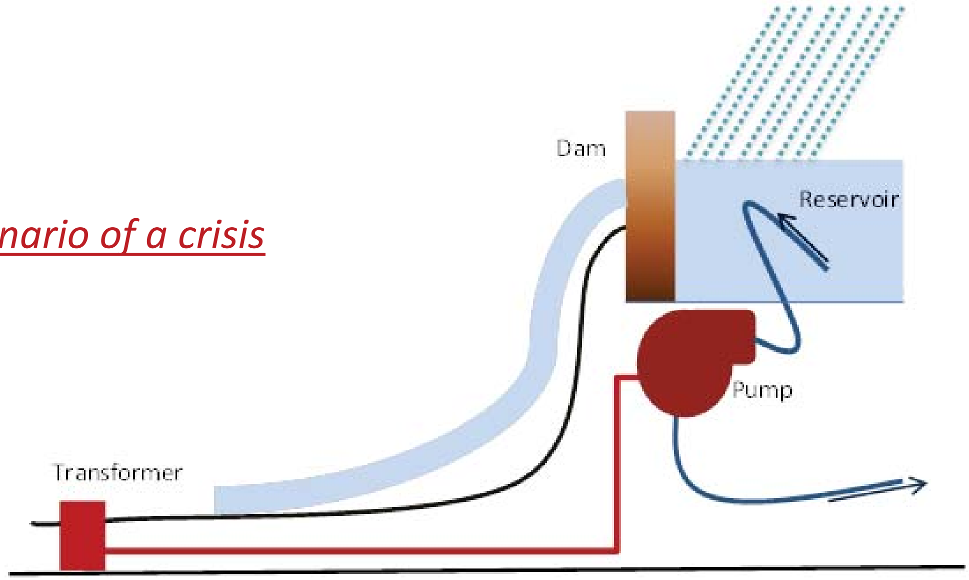
- to identify and assess risks associated to a well-defined threat

And to develop a range of options to;

- eliminate,
- reduce,
- transfer,
- accept or
- share those risks.

Practically Speaking: A hypothetical Case

A hypothetical scenario of a crisis ➔



The threat & involved events

- E1 : Heavy rains (the quantity and the duration). *Probabilistic Model*
- E2 : Static head growth rate. *Deterministic Model*
- E3 : Aged structure (mechanical degradation). *Semi-Deterministic Model*
- E4 : Emergency Pumping Station (EPS) failure. *Probabilistic Model*
- E4 : EPS feedback control loop system. *Probabilistic Model*
- E5 : Power Supply Line (PSL), from the valley. *Deterministic+Probabilistic Model*

How to Simulate this crisis in view of a Decision Making action?

The issue now is:

- To integrate all the models describing; threat, systems' behaviour, sensors, control systems and the potential (inter)dependence.
- To simulate the evolution of the crisis in the time (dynamic)
- To iterate the simulation in order to better identify the worst paths the crisis evolution may take (what if?)
- To assess the ultimate consequences of each possible path.
- To assess the decisions to be made in order to: intercept the threat, reduce, mitigate, accept or share the corresponding Risks

Thanks for attention

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Modelling and investigating dependencies of CI

Roberto Setola (UCBM)
r.setola@unicampus.it

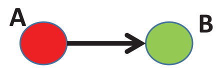
Modelling, Simulation and Analysis of Critical Infrastructures
CIPRNet Course

UCBM Headquarters – Rome (Italy) – 9 -10 July 2015

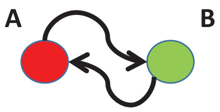
Objectives of this lesson

- What is the relevance of (inter-)dependencies?
- How to model these phenomena?
- Which are consequences if we neglect to capture them?

Dependency vs. interdependency



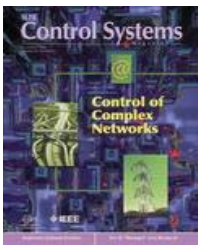
Dependency: is the capability of an infrastructure to influence the state of an other infrastructure. It is a *unidirectional* relationship.



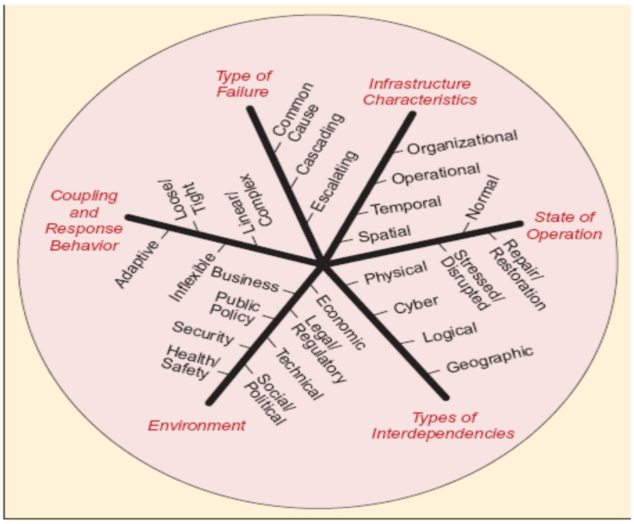
Interdependency: is a *bidirectional* relationship between two infrastructures through which the state of each infrastructure is influenced or is correlated to the state of the other.

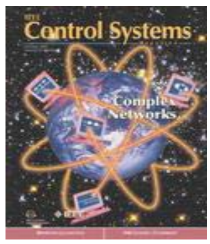
Notice that in literature, with an abuse of notation, the term "Interdependency" is used with a broad meaning absorbing in part the "dependency" meaning

Dimensions for describing infrastructure inter-dependencies



September 2011



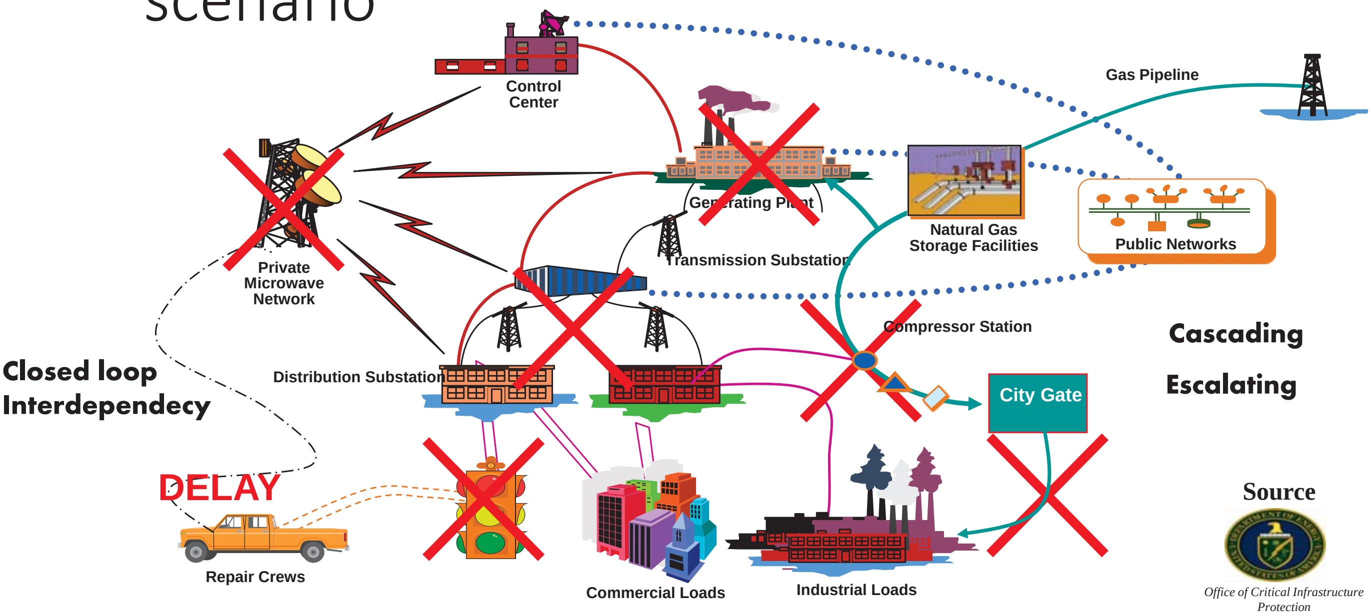


January 2012

S. Rinaldi, J. Peerenboom, and T. Kelly, "Identifying Understanding and Analyzing Critical Infrastructure Interdependencies," *IEEE Control System Magazine*, pp. 11–25, 2001.

M. Ouyang, "Review on modeling and simulation of interdependent critical infrastructure systems." *Reliability engineering & System safety* , pp. 43-60, 2014.

A failure inside an inter-dependent scenario



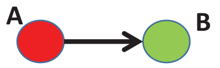
Italian black-out, September 28th, 2003

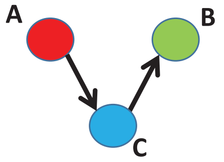
Due to a «problematic» configuration of the Italian grid, to a problem in Switzerland, to a misunderstanding between Italian and Switzerland TSO operators…

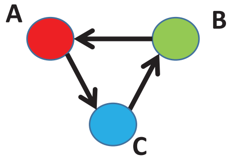
In a rapid sequence the two 400kV lines from France tripped and in 4s GRTN lost the control of the Italian grid

56 million people were affected for up to 9 hours

First and higher order dependency







- <u>First order</u> dependency **A -> B**

- <u>Second order</u> dependency **A -> C -> B**

The concept can be easily generalized to the **<u>n-th order dependency</u>**

When the sequence of influences creates a **<u>loop</u>**, **A** -> **C** -> **B** -> **A** then ALL the involved infrastructures are <u>inter-dependent</u>. Any event is **exacerbated.**

In the presence of loops, there is no more a **<u>tree</u>** structure (i.e. there is a root and the consequences go only downstairs to) but a **<u>graph</u>** structure (the consequences have no more a preferential direction)

Some events

1998 – Galaxy IV (USA)

Source

Failure in a communication satellite

Consequences

- 40 millions pagers out-of-services
- 20 United Airline flights delayed
- Many radio stations unable to operate
- Congestion at high-way gas stations: due to impossibility to process credit card

2000 – Maroochy Shire (Australia)

Source

An ex-employer used a wireless Internet connection to penetrate into SCADA of sewage treatment plant

Consequences

- 47 "abnormal" accidents in January-April 2000
- 1.200.000 liters of raw sewage dispersed in the environment
- Potable water compromised in the area

2004 – Italy

Source

an incident in the air conditioned system of an important telco nodes in Rome

Consequences

- Blackout in mobile and wired communication for about 6 h in Roma
- About 5.000 banks and 3.000 post offices off-line
- 70% check-in desks at Fiumicino airport off-line
- ACEA (local electrical distributor) lost the control on half of the network (near miss)

2006 - Europe

380kV lines across river Ems turned off at 21:30h to let the Norwegian Pearl through

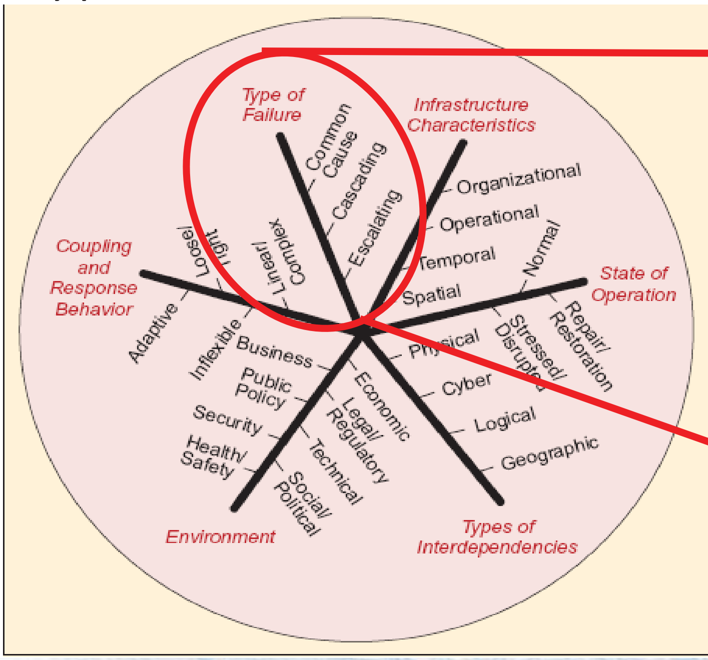
A large number of lines in Germany, Austria, Hungary and Croatia automatically tripped one after the other in a "domino" effect, as their automated protection systems detected load flows over the safety limit

15 million households affected in 11 countries

Power restored in 30 minutes in some places, 2 hours in Italy

TNO, CI disruption database containing over 4350 reported CI disruption events including over 1260 dependencies (2009)

Types of failure

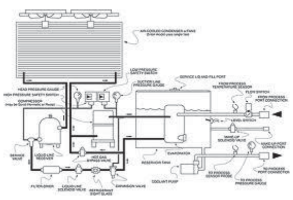


Common cause: the same event produces failure in two or more infrastructures.

Cascading: the failure into one infrastructure induces a domino effect on other infrastructures.

Escalating: the failure of one infrastructure exacerbates the consequences of failure induced by some other causes.

Planned vs. Induced dependency



- **Planned:** the dependency has been introduced at design stage (it is "functional" to the prescribed goal) and it is well known and well documented

- **Induced:** the dependency "*emerges*" due to modification of the environment (generally it is not present/evident in normal operation condition). It is generally not well documented, not perceived by the operators or even unknown

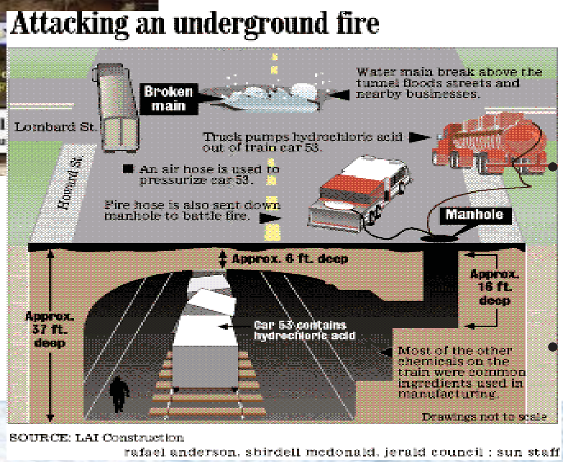
R. Setola, "How to Measure the Degree of Interdependencies among Critical Infrastructures", *Int. J. of System of Systems Engineering, (IJSSE),* pp. 38 -59, 2010.

CSX Tunnel Fire

Lessons identified – Baltimore, July 2001

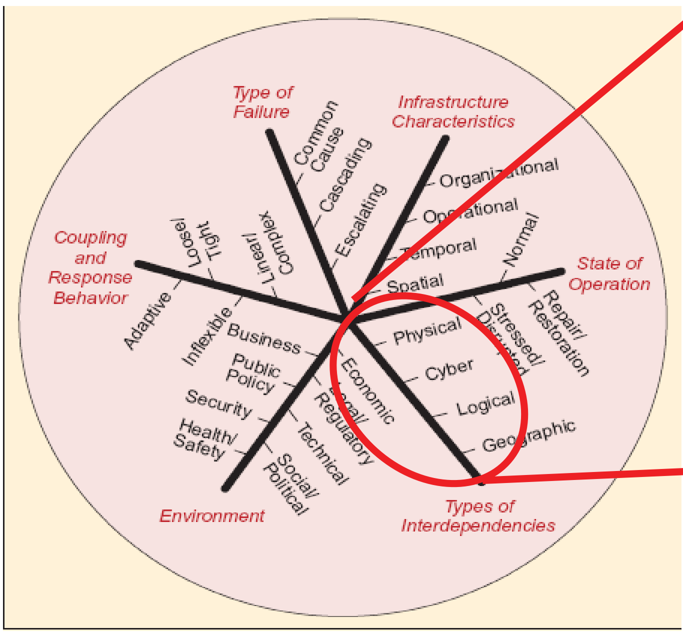
"unknown" geographical co-location of multiple CI

- Chloride-acid train derailment in tunnel; subsequently went on fire



- 70 million gallons of water flooded downtown streets and houses -> fire fighters lost their water supply.
- Glass fibers melted and caused problem to telephony (local) and Internet (world-wide).
- 1200 buildings lost power

Dimensions for describing infrastructure dependencies



***Physical** Interd.:* if the operations of one infrastructure depend on the physical output(s) of the other.

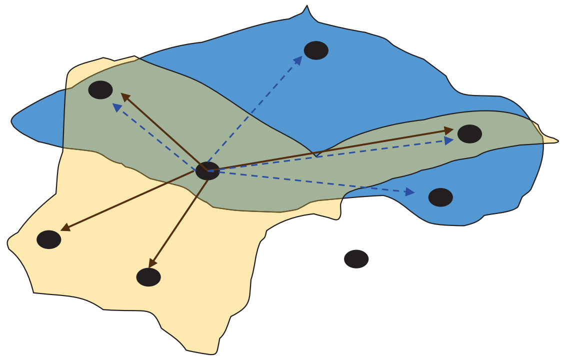
***Cyber** Interd.:* if its state depends on information transmitted via cyberspace.

***Geographical** Interd.:* when elements are in close spatial proximity.

***Logical** Interd.*: any other causes (e.g. regulatory).

***Sociologic** Interd.*: when coupling effects are mediated by (irrational) human behaviors

Several “concepts” of proximity



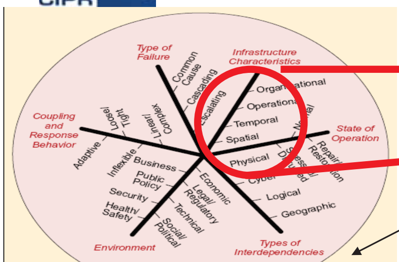
Geographic proximity.
Cyber proximity.

An entity has different sets of neighbors identified on the base of the dependency mechanism.

Hence a given phenomena/failure propagates along common/different pathways.

Consequently specific actions may contrast the propagation of some phenomena (but be ineffective for others).

Infrastructure Characteristics



Spatial	Temporal	Operational	Organizational

- Part
- Unit
- Subsystem
- System
- Infrastructure
- Interd. Infrastr.

Interdependency is more relevant as scope increase

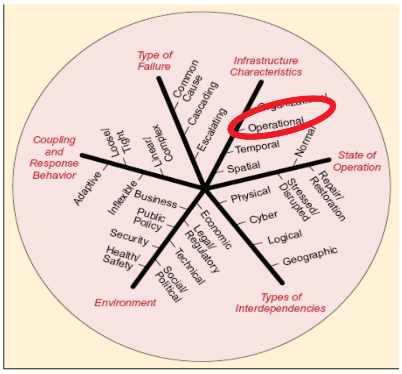
Relevant time scales vary from milliseconds to hours to years

The importance of each type of interdependency changes w.r.t. time horizon

Operational conditions

The dependency degree is influenced largely by the operational conditions:

- **Normal**
- **Stressed**
  - Maintenance
- **Crisis**
- **Recovery**



E. Luiijf, and M. Klaver. "Insufficient situational awareness about critical infrastructures by emergency management." TNO Defence, Security and Safety (2011).

2004 – Italy

Source

an incident in the air conditioned system of an important telco nodes in Rome

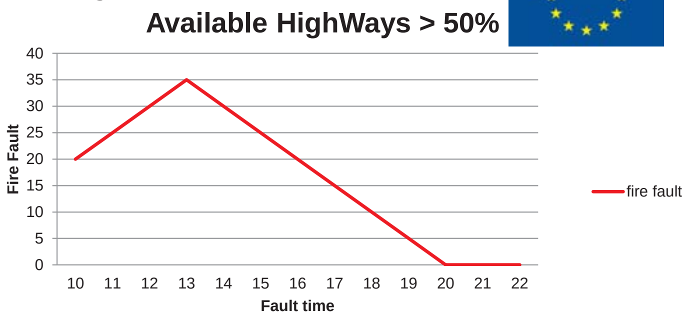
Consequences

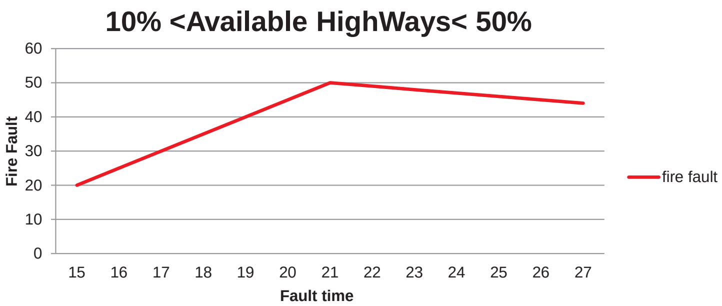
- Blackout in mobile and wired communication for about 6 h in Roma
- About 5.000 banks and 3.000 post offices off-line
- 70% check-in desks at Fiumicino airport off-line
- ACEA (local electrical distributor) lost the control on half of the network (near miss)

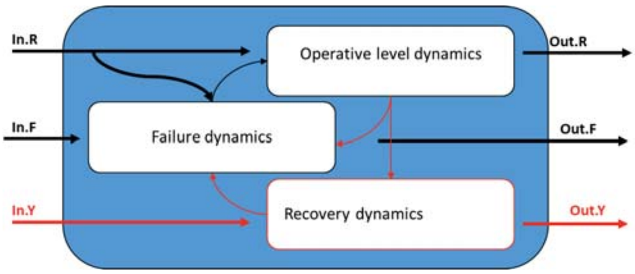
Recovery at an oil tank farm

Fire fault mitigation

Fire dousing at 13 minutes after the fire start. Every minute, its value will be reduced of 5%.







Fire dousing at 21 minutes after the fire start. Every minute, its value will be reduced of 1%.

What: Resources and/or Faults

Absence or degraded resource

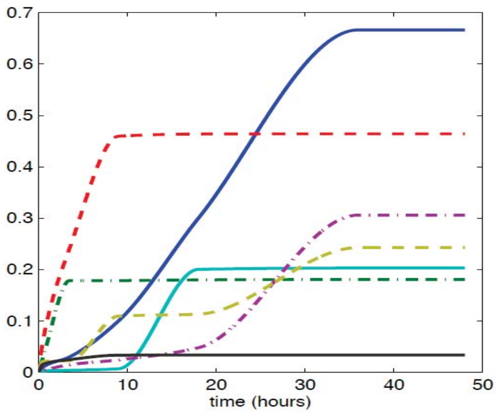
The supplier infrastructure is unable to provide adequate level of resources to the dependent infrastructure.
This later can use its own reserve (e.g. buffer or back-up elements) to reduce the **level of coupling** for a while.
Generally, when the level of resources is restored, the operativeness is rapidly restored.

Fault

The fault (e.g. break, fire, blame, fulmination, etc.) in an infrastructure is transmitted to the dependent infrastructure, where other types of fault can be generated.
The consequences can be mitigated (or nullified) due to the presence and quality of "**barriers**" which effectiveness depends on the amplitude and duration of the fault.
Removing the cause does not imply the restoration of the operativeness.

S. Panzieri and R. Setola, "Failures Propagation in Critical Interdependent Infrastructures", *Int. J. Modelling, Identification and Control* (IJMIC), pp. 69 – 78, 2008.

Time Varying coupling coefficients



Constant: it does not change with outage period, i.e. direct link (no buffer or back up)

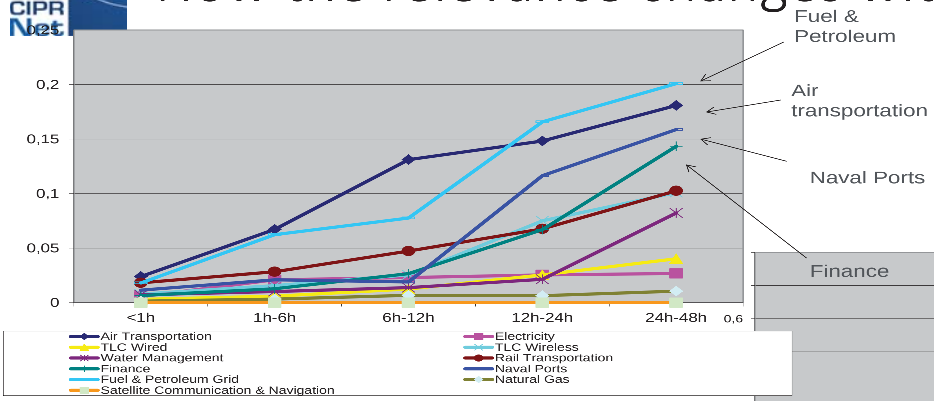
Linear + constant: buffer absorbs partially the inoperability until it expires

S-Shape: buffer absorbs quite completely inoperability for a while but when it expires there is a rapid degradation (no graceful degradation)

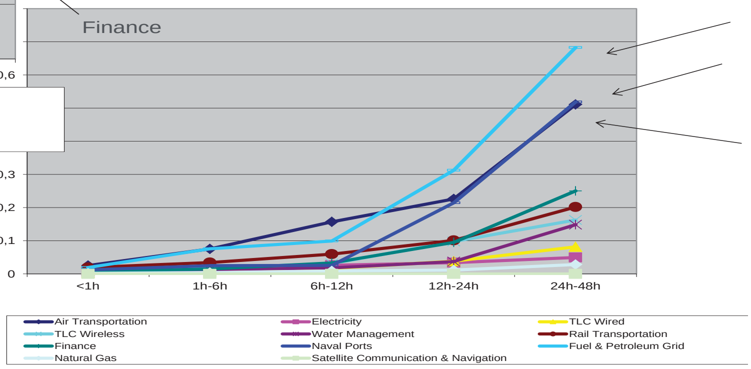
Double S-Shape: there are two types of buffers which are designed to support general and priority aspects

F. Conte, G. Oliva and R. Setola, "Time-Varying Input-output Inoperability Model", *Journal of Infrastructure Systems*, ASCE, 47–57 2013.

How the relevance changes with outage time



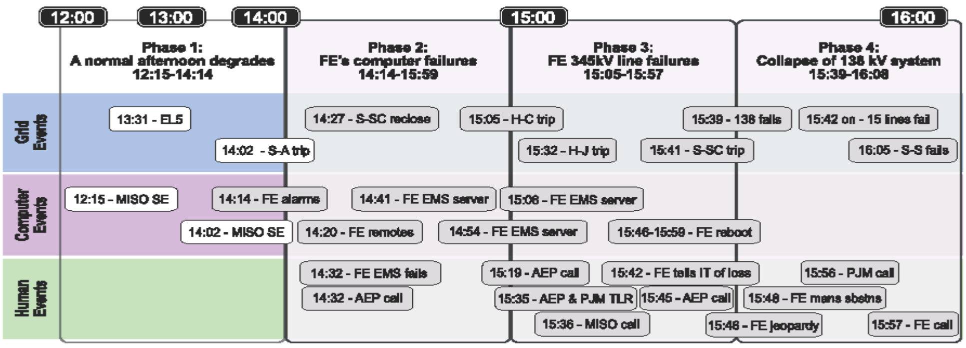
The curves cross each others, i.e. their relevance/fragility varies with the outage time



This phenomenon should be considered when emergency plans are designed

R. Setola, S. De Porcellinis, and M. Sforna "Critical Infrastructure Dependency Assessment Using Input-output Inoperability Model", *Int. J. Critical Infrastructure Protection (IJCIP)*, pp. 170 - 178, 2009.

2003 – US & Canada blackout



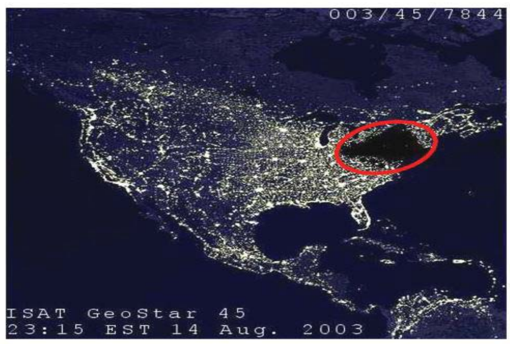
August 14th, 2003

Loss of 61,800 MW of electric load

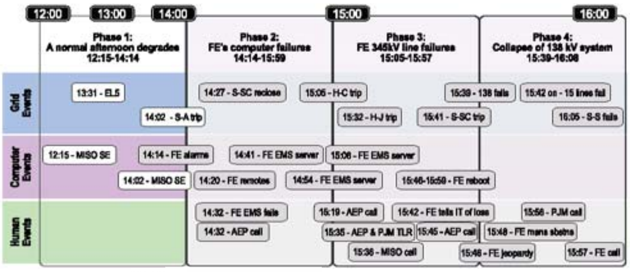
50 million people affected

Estimated cost: 4,5 B$ - 8.2 B$

https://reports.energy.gov/



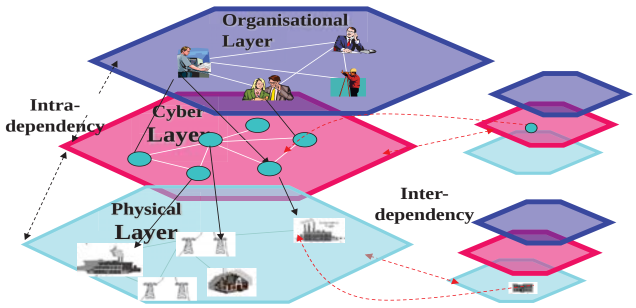
Physical, Logical & Organizational dependencies



- Physical
- Logical
- Organizational

Each layer is characterized by its own components, resources, faults and links

To correctly capture the complexity of the phenomena, it is mandatory to have an holistic vision able to aggregate the different visions.



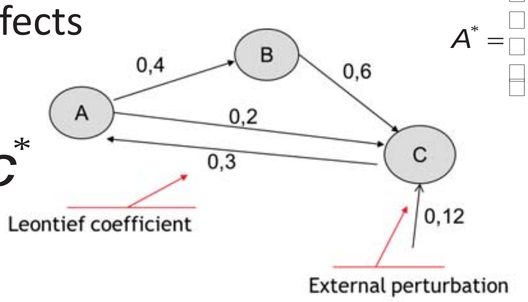
S. De Porcellinis, S. Panzieri and R. Setola, “Model Critical Infrastructure via a Mixed Holistic-Reductionistic Approach”, *Int. J. Critical Infrastructures* (IJCIs), vol. 5, pp. 86 -99, 2009.

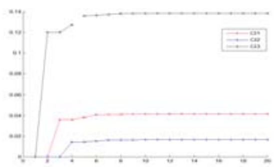
Input-Output Inoperability Model

- Based on the economic equilibrium theory of W. Leontief
- Each infrastructure has an **inoperability** q (% of malfunctioning)
- The model considers constant external perturbations and analyzes the domino effects

$$A^* = \begin{bmatrix} 0 & 0 & 0.3 \\ 0.4 & 0 & 0 \\ 0.2 & 0.6 & 0 \end{bmatrix}; c^* = \begin{bmatrix} 0 \\ 0 \\ 0.12 \end{bmatrix}$$

$$q(k+1) = A^* q(k) + c^*$$





W. Leontief, Input-Output Economics, Oxford University Press, 1966.

Y. Haimes et al., Inoperability input-output model for *interdependent* infrastructure sectors I: Theory and methodology, Journal of Infrastructure Systems, vol. 11(2), pp. 67-79, 2005.

Dependency index & Influnce gain

$$\mathbf{A} = \begin{pmatrix} 0 & * & * & * \\ * & 0 & * & * \\ * & * & 0 & * \\ * & * & * & 0 \end{pmatrix}$$

$$\rho_j = \sum_i a_{ij}$$

influence gain

Is a measurement of the influence that a specific infrastructure has on the global system

dependency index

$$\delta_i = \sum_j a_{ij}$$

Is a measurement of the robustness with respect to the transmitted inoperability

Steady-state solution

$$\overline{\mathbf{x}} = (\mathbf{I} - \mathbf{A})^{-1} \mathbf{c} = \mathbf{S}\,\mathbf{c}$$

If A is positive and stable, then

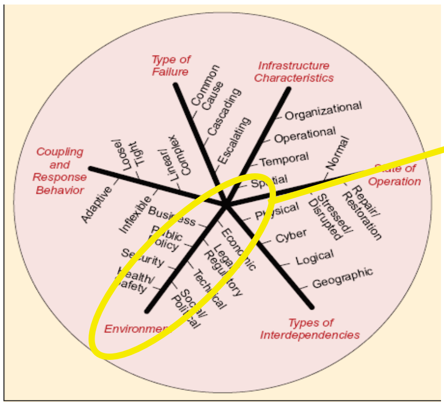
$$\mathbf{S} = [\mathbf{I} - \mathbf{A}]^{-1} = \mathbf{I} + \mathbf{A} + \mathbf{A}^2 + \mathbf{A}^3 + \cdots$$

Overall dependency index and influence gain

$$\overline{\rho}_j = \frac{1}{n-1} \sum_{i \neq j} s_{ij} \qquad \overline{\delta}_i = \frac{1}{n-1} \sum_{j \neq i} s_{ij}$$

R. Setola and S. De Porcellinis, "A Methodology to Estimate Input-output Inoperability Model Parameters", *Critical Information Infrastructures Security 2007,* Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp. 149 – 160, 2008.

IIM Operational vs. Economic



Economic (business) links represent just one of the dimension of dependency

Fukushima Nuclear plant

To capture (other) depedencies we have to consider also operational dimension

IIM from Technicians point of view

Identify IIM parameters on the base of operative technicians' expertise (operators' perceptions).

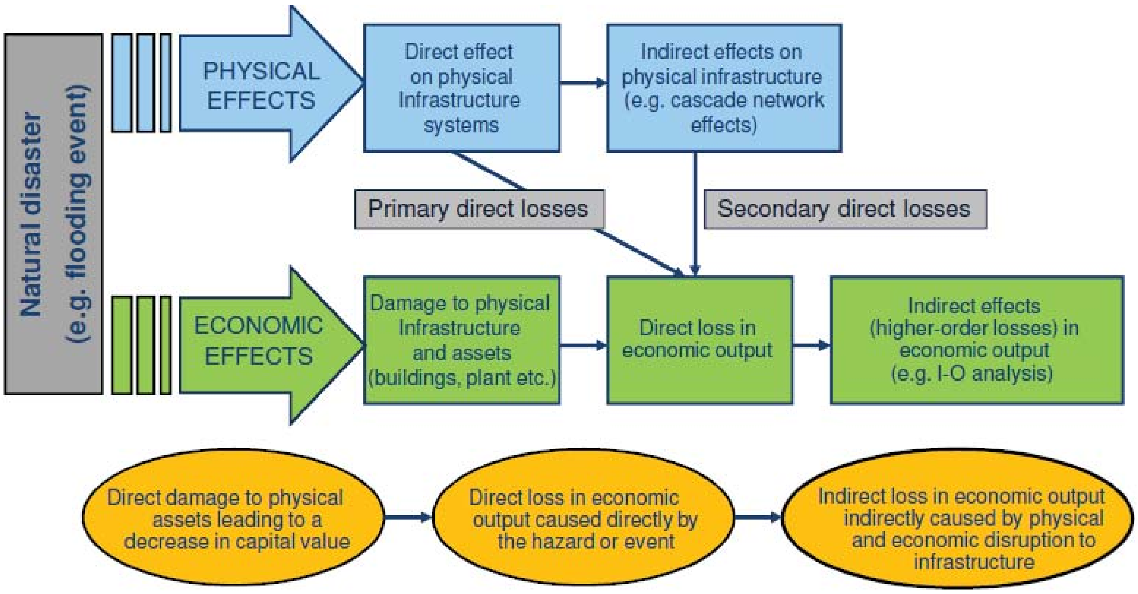
Ask to experts the follow question

Which is the impact of the complete absence of services provided by *yyy* infrastructure for a time period of *zzz* on *your* infrastructure?

In this way we try to acquire directly from their expertise an estimation about the dependency parameters to set-up a technical oriented IIM

R. Setola, S. De Porcellinis, and M. Sforna "Critical Infrastructure Dependency Assessment Using Input-output Inoperability Model", *Int. J. Critical Infrastructure Protection (IJCIP),* pp. 170 - 178, 2009.

Consequences



S. Kelly, «The cost of cascading failure risk and resilience within UK infrastructure networks", 2014

Recap

- In actual socio-technical scenario all infrastructures are tightly linked each other ➔ negative consequences may increase due to cascading effects and exacerbate in presence of interdependencies
- The mechanisms at the base of dependencies are multiple ➔ this induces several concepts of proximity
- Such phenomena may be more evident in the case of crisis ➔ take into account the effects of dependencies on emergency services

r.setola@unicampus.it

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Hybrid Engineering/Phenomenological Approach to Simulate System of Systems

José R. Marti[1]– The University of British Columbia, Vancouver, Canada / Alberto Tofani[2] – ENEA, Rome, Italy

[1] jrms@ece.ubc.ca, [2] alberto.tofani@enea.it

Modelling, Simulation and Analysis of Critical Infrastructures
CIPRNet Course

UCBM Headquarters – Rome (Italy) – 9-10 July 2014

Presentation

1. World Models
2. Divide et Impera
3. i2Sim Multi-system Engineering/Phenomenological Modelling
4. DR-NEP Federated Simulation
5. Appendix: Sample Scenarios

World Models | Divide et Impera | i2Sim | DR-NEP

World Models

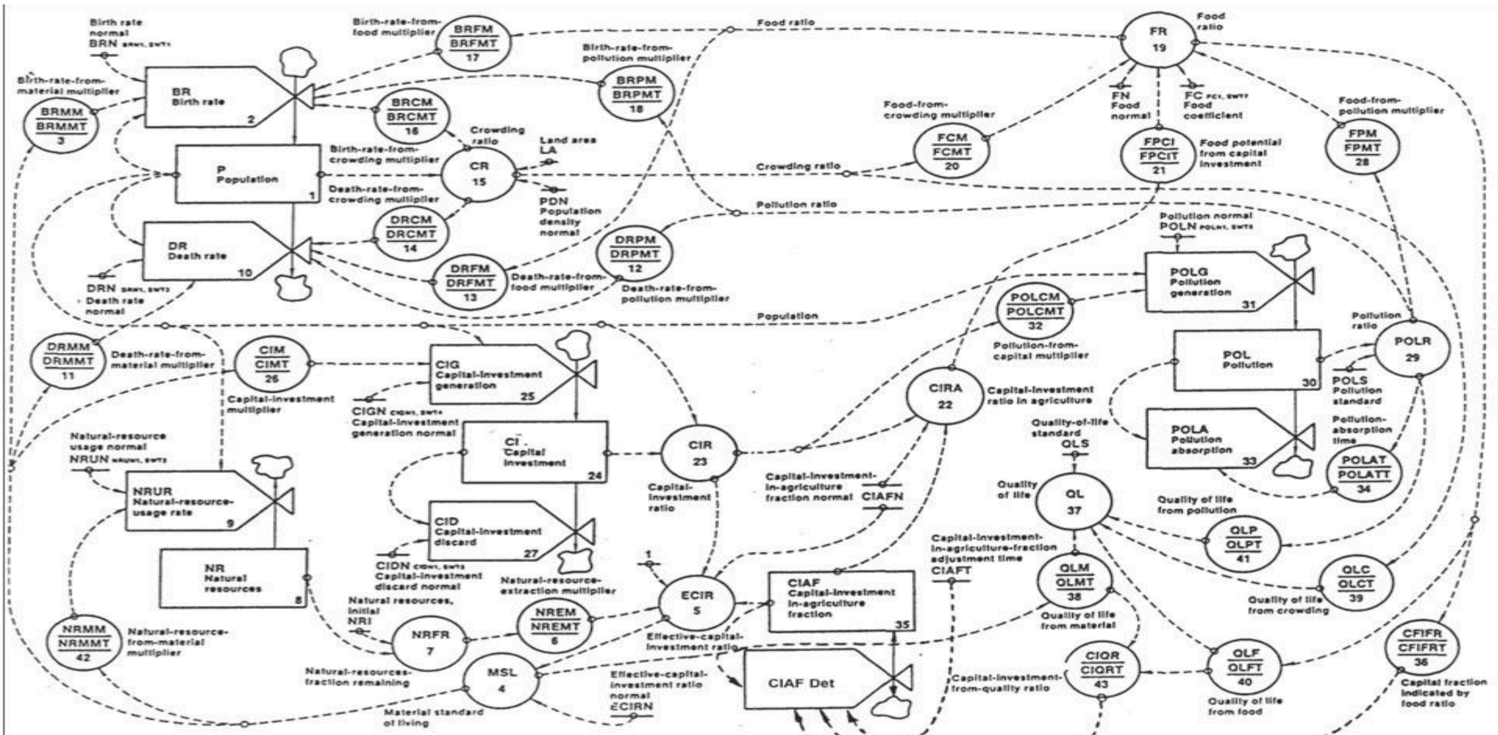
Represent processes to produce goods and services to support human well-being

- **Forrester System Dynamics World Model (1961)**
  - Prof. Jay Wright Forrester, b. Nebraska, Electrical Engineering degree, MIT, Professor Management, MIT.
- **Leontief Input/Output Production Model (1951)**
  - Prof. Wassily Leontief, b. Munich, Economics degree, Leningrad, Professor Economics, Harvard, New York, Nobel Prize Economics (1973).
- **i2Sim Interdependencies World Model (2004)**
  - Complex Systems Integration (CSI) Laboratory, UBC, Canada.
- **Other Models[1]**

[1] Jamshidi, Mo, Editor (2009) System of Systems Engineering, Innovations for the 21st Century, Wiley

Forrester's World Model (1961)

- Based on control systems theory. Includes positive and negative feedback loops to relate production and consumption variables at a macroscopic level.
- It is a flat world model where all processes occur in the same layer.
  - The food system
  - The industrial system
  - The population system
  - The non-renewable resources system
  - The pollution system

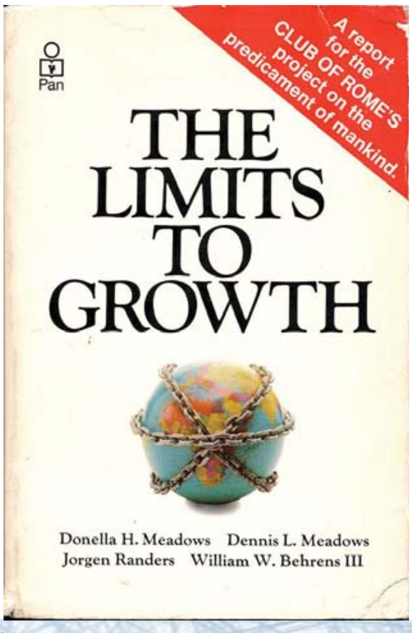


Forresters World2-Modell

Forrester, J.W. (1971). World Dynamics, 2nd Ed. Wright-Allen Press, Massachusetts. 1

The Limits to Growth (1972)[1]

- Based on Forrester's World 2 model.
- It predicts that the limits to growth on this planet will be reached within the next one hundred years.
- Reviewed (2004): We are on track with the predictions!



[1] Donella H. Meadows, Dennis L. Meadows, Jørgen Randers, and William W. Behrens III (1972). Universe Books

Leontief's World Model[1] (1951) (Nobel Prize 1973)

- Uses input-output tables to relate the amount of input resources needed for a given amount of finished product.
- To manufacture 10 cars we need ten engines, 40 tires, etc. If we only have 5 engines, we can only build 5 cars. The engines, tires, etc. are inputs to the factory. The tires are the output of some other factory that requires rubber as an input, etc.
- It is a flat model that assumes a linear relationship between parts and units produced.

[1] Leontief, Wassily (1986) Input-Output Economics, 2nd ed., Oxford University Press

Leontief's World Model

		agriculture and fisheries	food and kindred products	textile mill products	apparel	lumber and wood products	furniture and fixtures	paper and allied products	printing and publishing	
		1	2	3	4	5	6	7	8	… 42
agriculture and fisheries	1	10.86	15.70	2.16	0.02	0.19		0.01		
food and kindred products	2	2.38	5.75	0.06	0.01	•	•	0.03	•	
textile mill products	3	0.06	•	1.30	3.88	•	0.29	0.04	0.03	
apparel	4	0.04	0.20		1.96		0.01	0.02		
lumber and wood products	5	0.15	0.10	0.02	•	1.09	0.39	0.27	•	
furniture and fixtures	6			0.01			0.01	0.01		
paper and allied products	7	•	0.52	0.08	0.02	•	0.02	2.60	1.08	
printing and publishing	8		0.04	•					0.77	
chemicals	9	0.83	1.48	0.80	0.14	0.03	0.06	0.18	0.10	
products of petroleum and coal	10	0.46	0.06	0.03	•	0.07	•	0.06	•	
rubber products	11	0.12	0.01	0.01	0.02	0.01	0.01	0.01	•	
leather and leather products	12			•	0.05	•	0.01		•	
stone, clay, and glass products	13	0.06	0.25	•	•	0.01	0.03	0.03		
primary metals	14	0.01	•		•	0.01	0.11		0.01	
fabricated metal products	15	0.08	0.61	•	0.01	0.04	0.14	0.02	•	
machinery (except electric)	16	0.06								
electrical machinery	17									
motor vehicles	18	0.11								
other transportation equipment	19	0.01								

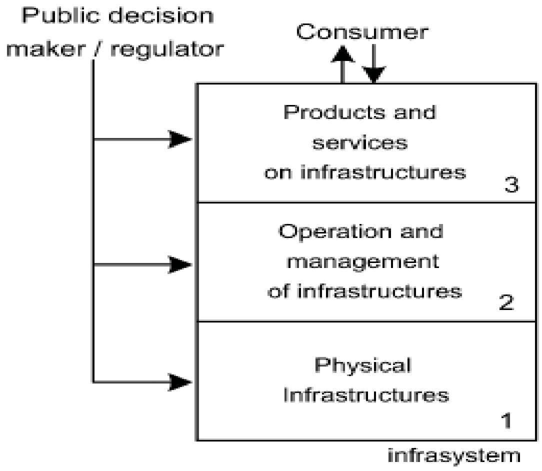
… 42

$$\mathbf{x} = \mathbf{A}\mathbf{x} + \mathbf{c} \Leftrightarrow \left\{ x_i = \sum_j a_{ij} x_j + c_j \right\} \forall\, i$$

Forrester Jay W. (1971) World Dynamics 2nd Ed. Wright-Allen Press, Massachusetts.

Hierarchical Models

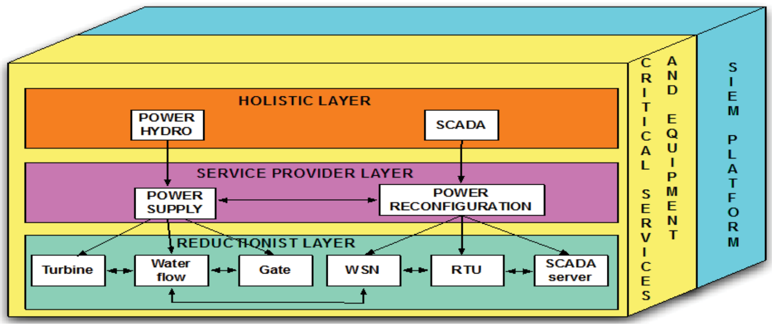
- Thissen and Herder (2009)[1] propose that a system of systems can be described using hierarchical layers:
  - Physical Layer
  - Operations and Management Layer
  - Products and Services Layer
  - Consumer Layer
  - Public Decisions Layer



[1] Thissen, Wil A.H., Herder, Paulien M. (2009). In: System of Systems Perspectives on Infrastructures, Chapter 11 in System of Systems Engineering, Innovations for the 21st Century, Jamshidi, Mo, Editor, Wiley.

Mixed Holistic Reductionist Layers1

- De Porcellinis, Panzieri, and Setola have applied MHR in risk analysis to identify equipment and services as related to Critical Infrastructures.



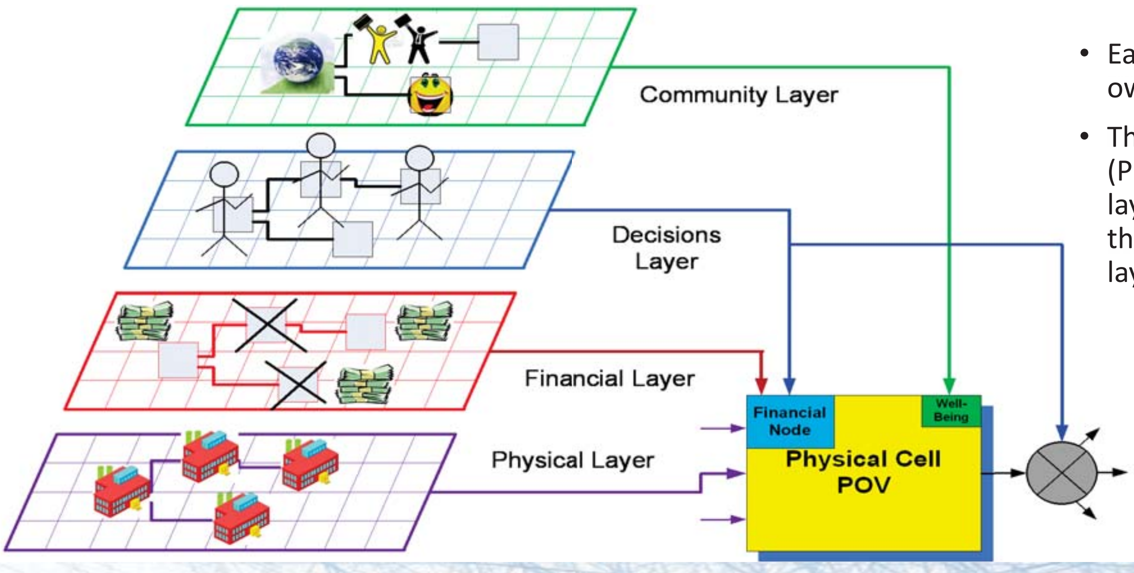
[1] S. De Porcellinis, S. Panzieri, and R. Setola, Modeling critical infrastructure via a mixed holistic reductionist approach, International Journal of Critical Infrastructures, vol. 5(1/2), pp. 86-99, 2009

i2Sim World Model[1] (UBC, 2004)

- Extends Leontief's production model by including nonlinear factors and phenomenological factors into the production process.
- In addition to engines, tires, etc. to produce cars, we need workers, electricity, equipment, building, money to buy the parts, etc. These "components" cannot be factored out linearly into the final product. Building, lights, and workers are needed in times of high production or low production.
- Human factors like tiredness, enthusiasm, cannot be factored out into Leontief's production functions but can be included in i2Sim.

[1] Marti JR (2014) Multisystem Simulation: Analysis of Critical Infrastructures for Disaster Response. In: D'Agostino G, Scala A (eds) Networks of Networks: The Last Frontier of Complexity, Springer, Heidelberg, p 255-277.

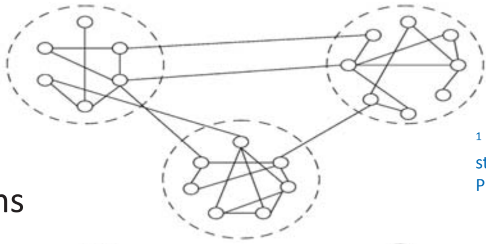
Stack of Infralayers



- Each infralayer has its own production cells.
- The Point of View (POV) of a cell in a layer interconnects this layer to the other layers.

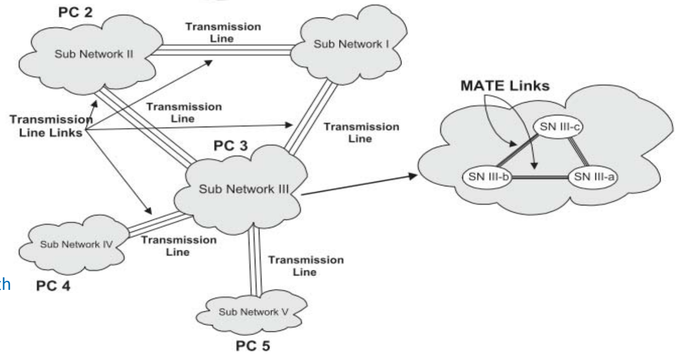
Divide et Impera

- “Divide et impera” (divide and conquer) (Julius Caesar, 100 BC)
- Establish self-sufficient subsystems with “help” through links when needed.



Community Structure Theory[1]

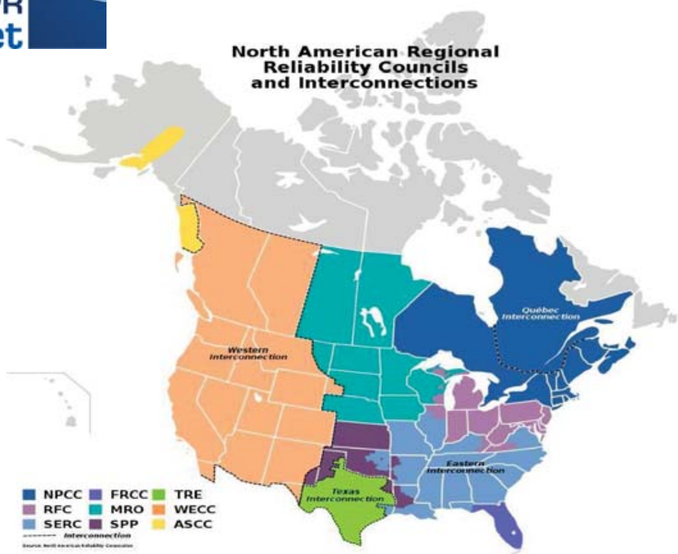
[1] Girvan M, Newman MEJ (2002) Community structure in social and biological networks. In: Proceedings of the National Academic of Sciences



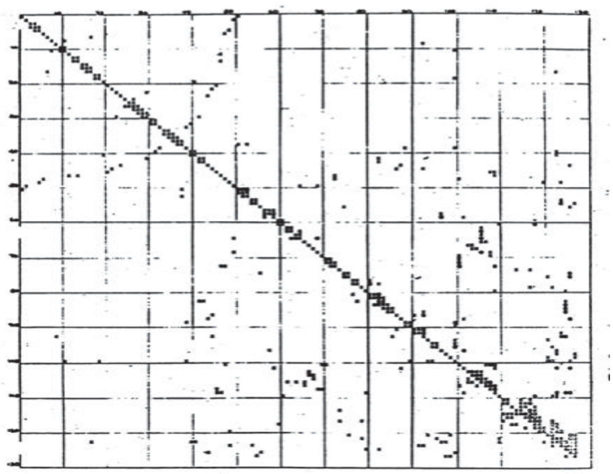
Multi-Area Thévenins (MATE)[2]

[2] Martí JR et al (2002) OVNI: Integrated Software/Hardware Solution for Real-Time Simulation of Large Power Systems. In: Proc. 14th PSCC, Seville, Spain, June 24th – 28th, 2002

North American Power Grid



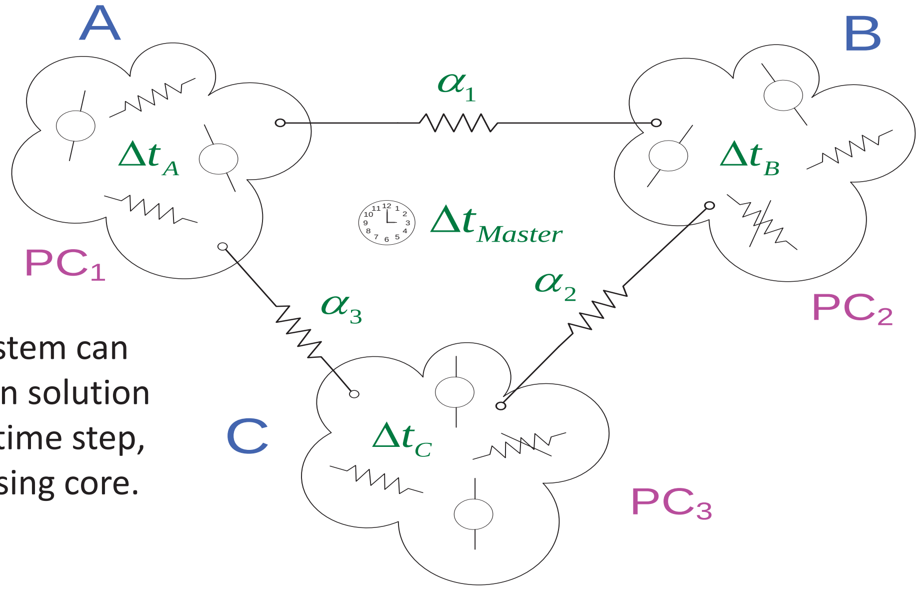
(Easter System, Western System, Quebec System, and Texas System)



WECC System [Y] matrix (14,327 busses, 16,607 branches)

(Notice Sparsity)

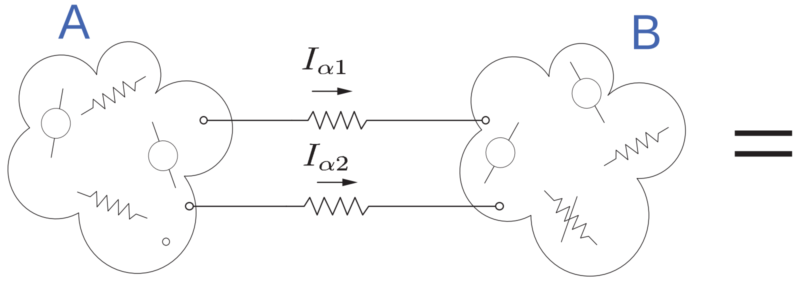
MATE Subsystems and Links

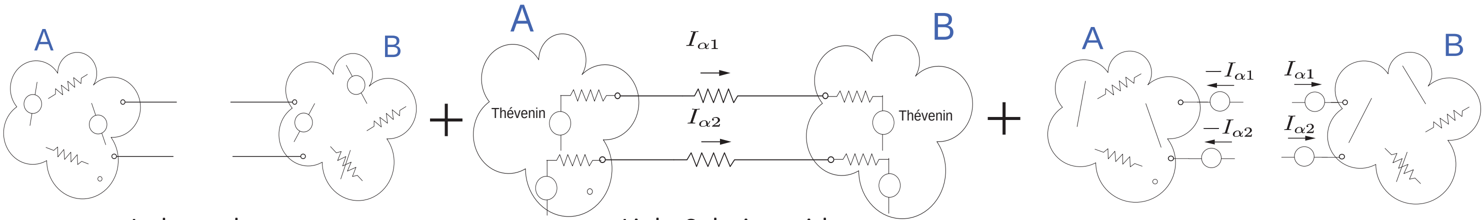


Each subsystem can have its own solution algorithm, time step, and processing core.

Total Solution = Internal + Links + Update

Complete System Partitioned into Subsystems





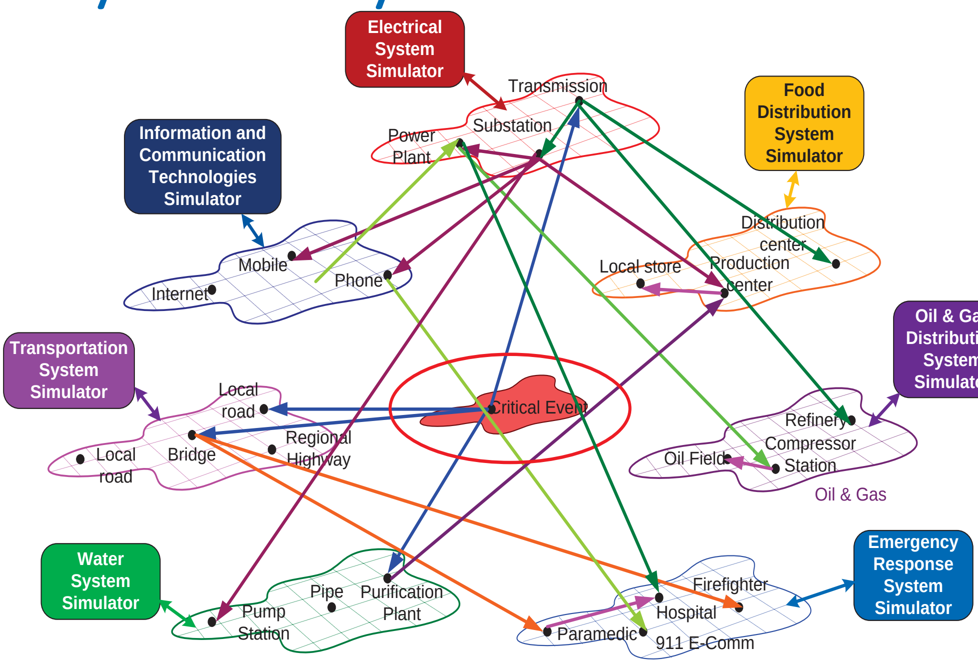
Independent Detailed Solutions

Links Solution with Equivalent Subsystems

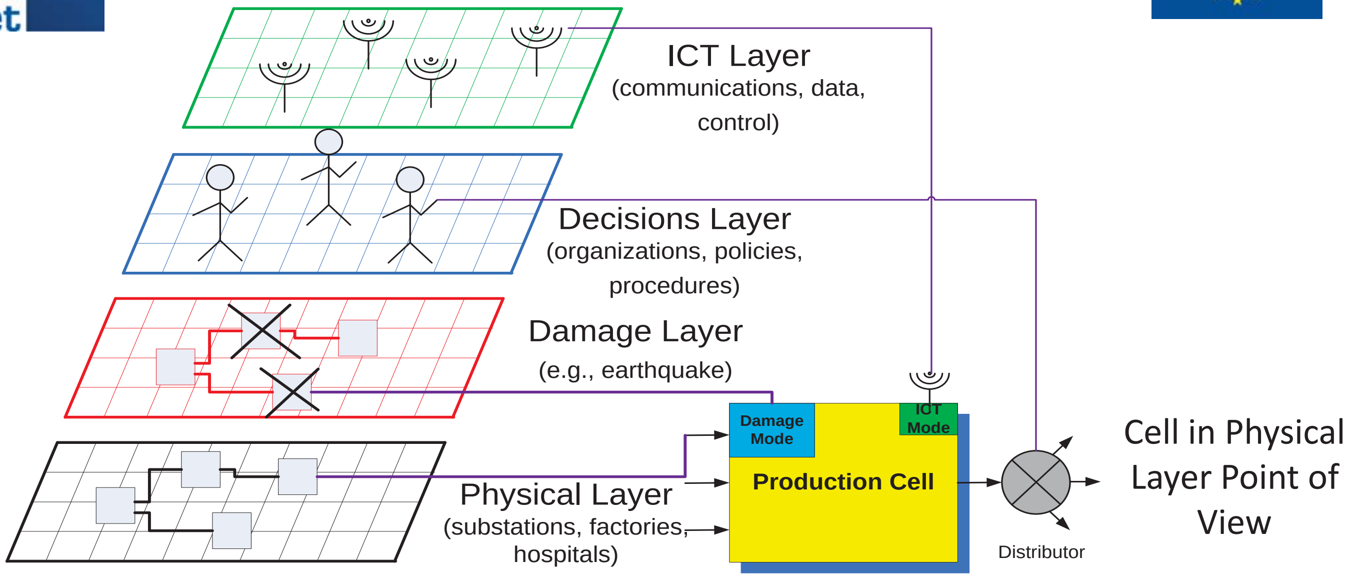
Subsystems Update

I2SIM REAL TIME FEDERATED SIMULATOR

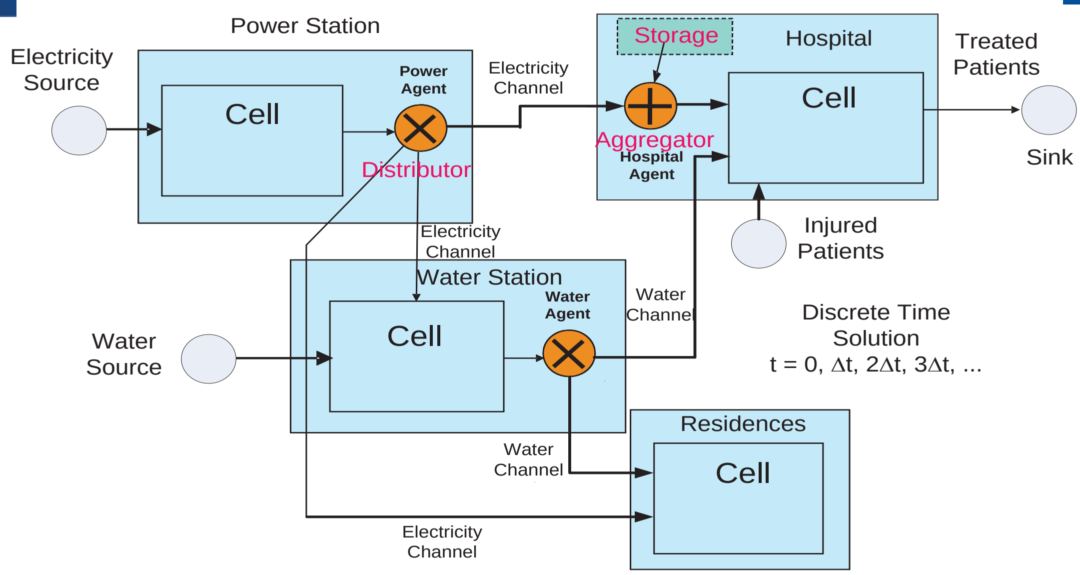
System of Systems of CI



Each CI has Multiple Layers



i2Sim Ontology

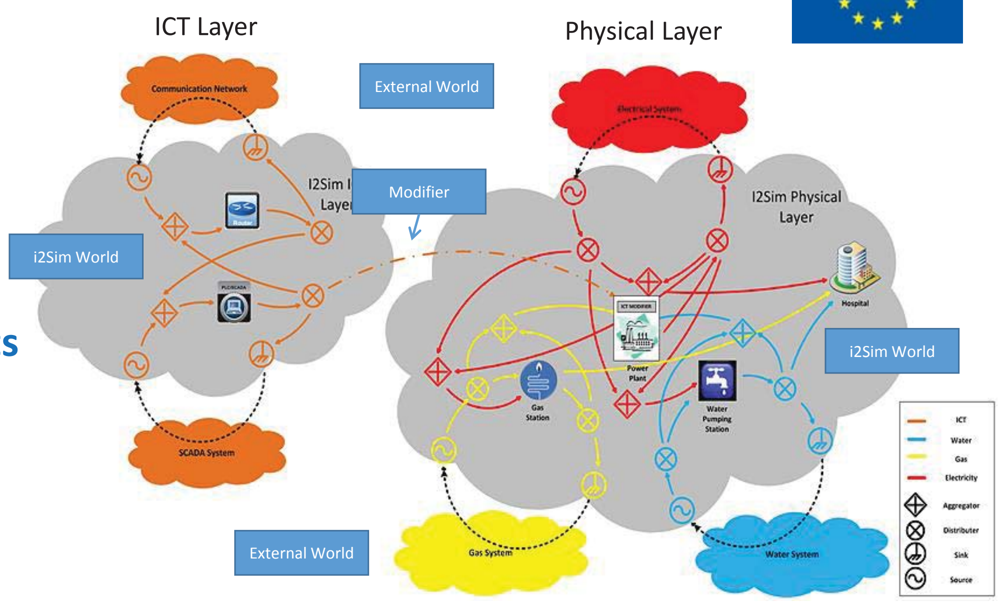


Basic Objects

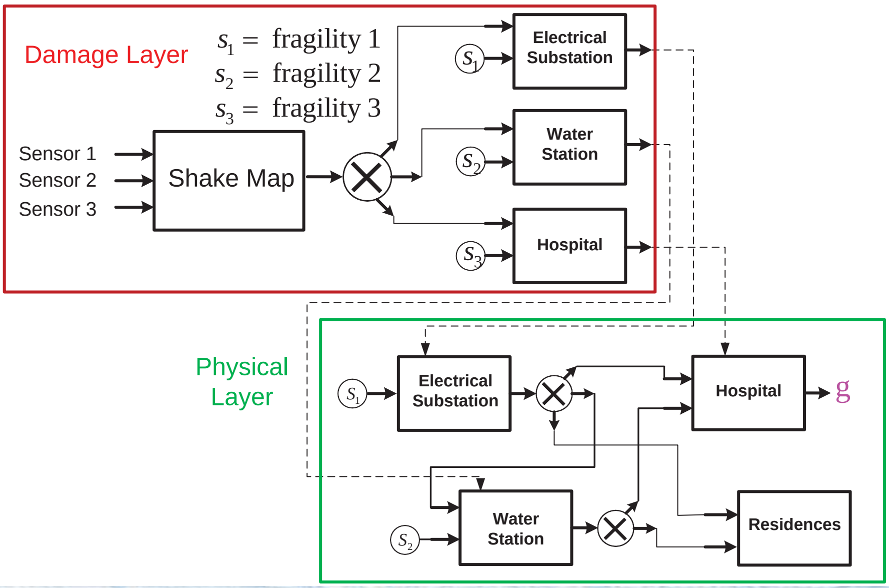
- **Tokens:** What "flows" in the system. Countable (e.g., ambulances) or Rates (e.g., liters/hr, KW, patients/hr).
- **Cells:** The production units. They take input tokens (e.g., electricity, engines, patients) and produce one output token (e.g., cars, treated patients).
- **Channels:** The conduits that carry the tokens (e.g., electrical cables, water pipes, roads).
- **HRT:** The Human Readable Table gives the functional relationship between the input tokens and the output token.

Other Objects

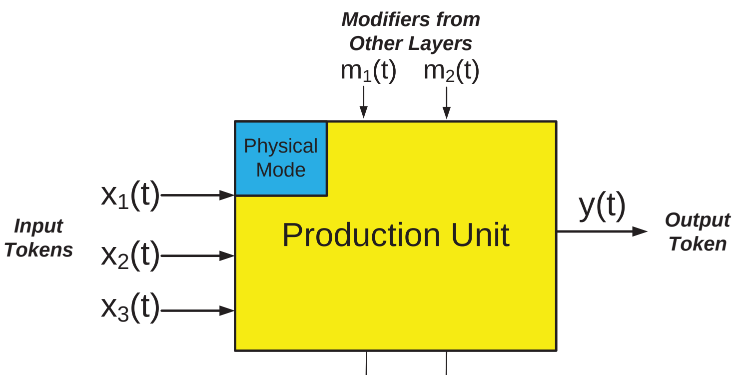
- **Controls**
  - Distributors
  - Aggregators
  - Storage
- **Exchange Objects**
  - Sources
  - Sinks
  - Modifiers



Example: Damage Layer with Physical Layer



i2Sim Production Cell

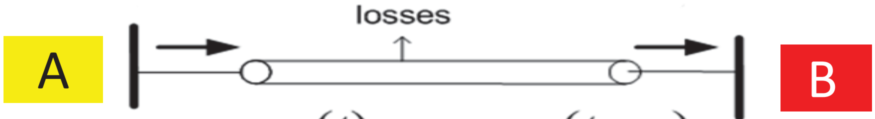


Output y(t) is determined by inputs x(t) in the same layer and by modifiers m(t) from the other layers.

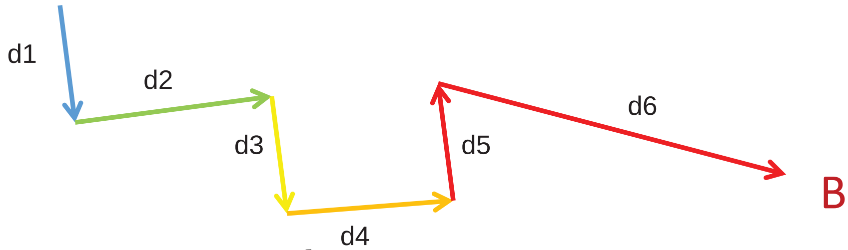
Colour	State
Green	100%
Blue	75%
Yellow	50%
Orange	25%
Red	0%

Cell symbol is colour coded. Upper left colour is the physical damage. Cell body colour is the output level.

Channel Abstraction



$$x_{arrive}(t) = \alpha x_{send}(t-\tau)$$

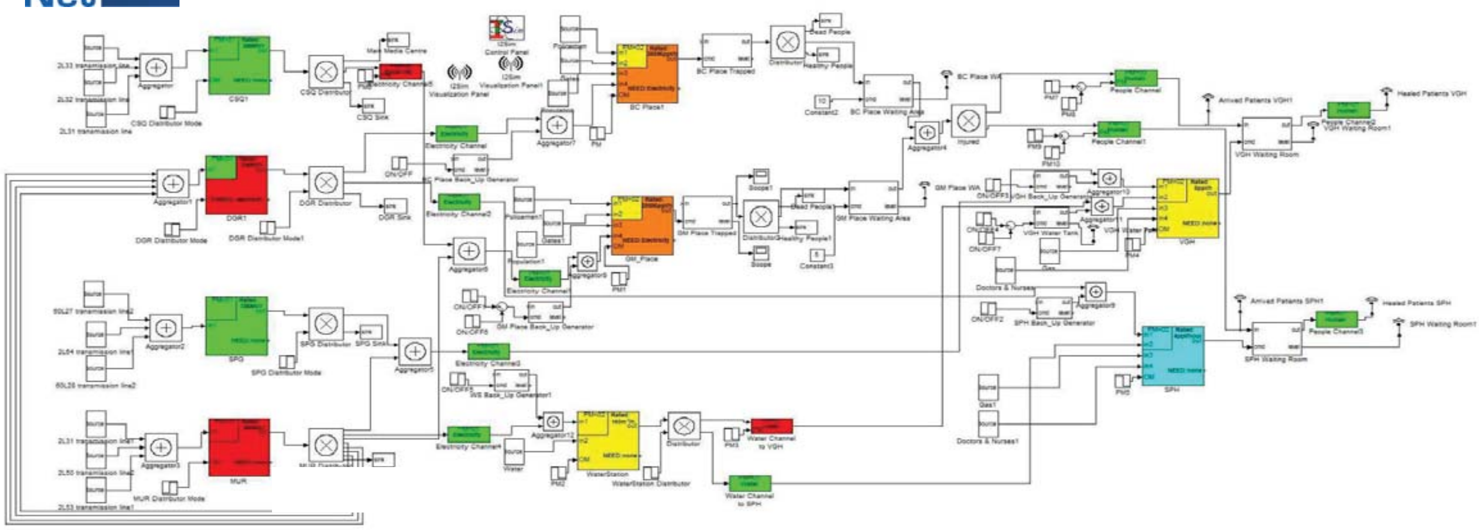


Multiple pipes are combined into a single equivalent channel

$$loss = \sum_{i=1}^{6} damage_i \times V_i$$

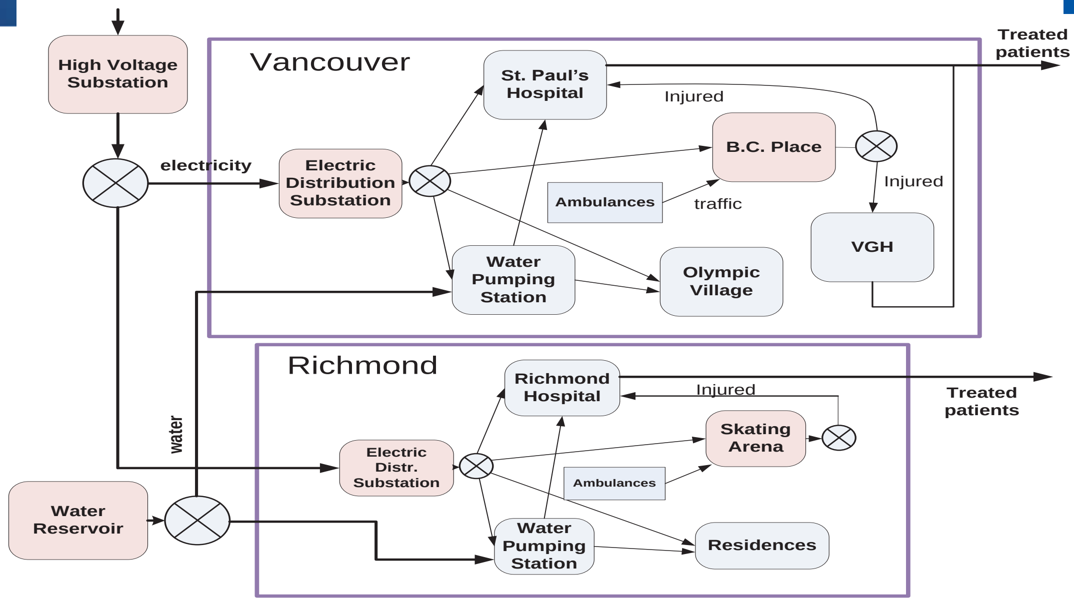
$$\alpha = 1 - loss$$

MATLAB/Simulink Implementation

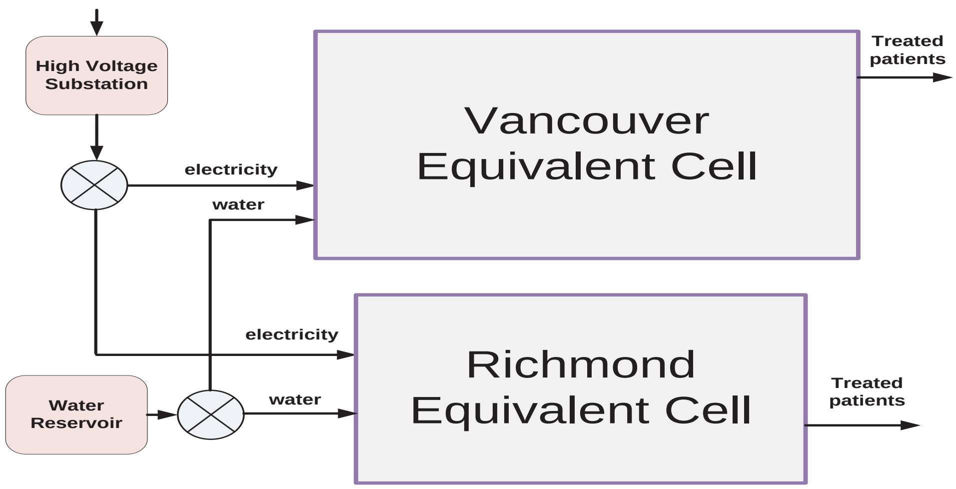


Vancouver 2010 Winter Olympics Simulink Model

Equivalencing for Coarser Resolution



High Level View



HUMAN READABLE TABLE (HRT) INTEGRATES ENGINEERING AND HUMAN EXPERIENCE

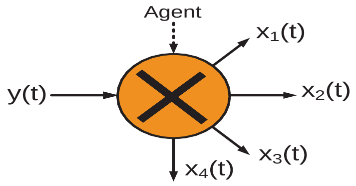
Electrical Substation

Cell HRT

Operability	y(t)	x(t)	Condition
	Low Voltage Power (MW)	High Voltage Power (MW)	Transformers Working
Green	200	200	2
Yellow	100	100	1
Red	0	0	0

Distributor Decision

Agent Decision: Choose 2 out of 4 feeders to supply
Implementation: Action on Breakers B1, B2, S1, S2, S3, S4



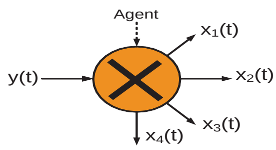
Water Pumping Station

Cell HRT

	High Pressure Water (kL/h)	Low Pressure Water (kL/h)	Electricity (kW)	Pumps Working
	y(t)	$x_1(t)$	$x_2(t)$	
Green	500	500	50	10
Blue	350	350	35	7-8
Yellow	250	250	25	5
Orange	200	200	20	2-3
Red	0	0	0	0

- If the upstream water mains only provides 250 kL/h then, assuming electricity is available, regardless of whether 5 or more pumps are working, the output will be 250 kL/h.

Distributor Decision



- Since only four pipes are going out, assuming 125 kL/h on each, if 5 pumps are working, then the distributor will have to choose the two most important delivery pipes.

HRT Hospital with Damage

	management	engineering	engineering	management	management	engineering
	y(t)	**$x_1(t)$**	**$x_2(t)$**	**$x_3(t)$**	**$x_4(t)$**	**$m_1(t)$**
Operability	Patients per hour	Electricity (kW)	Water (L/h)	Doctors	Nurses	Physical Integrity
100%	20	100	1,000	4	8	100%
75%	15	50	500	3	6	80%
50%	10	30	300	2	4	50%
25%	7	20	200	2	3	20%
0%	0	0	0	0	0	0%

- Notice that the columns in an HRT must be monotonically increasing from bottom to top. For this reason, “Physical Integrity” is used instead of physical damage for the input damage modifier.
- Operability is determined by the least available resource. In the example water is the limiting factor.
- Since only 30 kW of electricity, etc. are needed, we can reallocate electricity, doctors, etc. to other hospitals or other cells, internal or external.

i2Sim

HRT Hospital with Tired Doctors

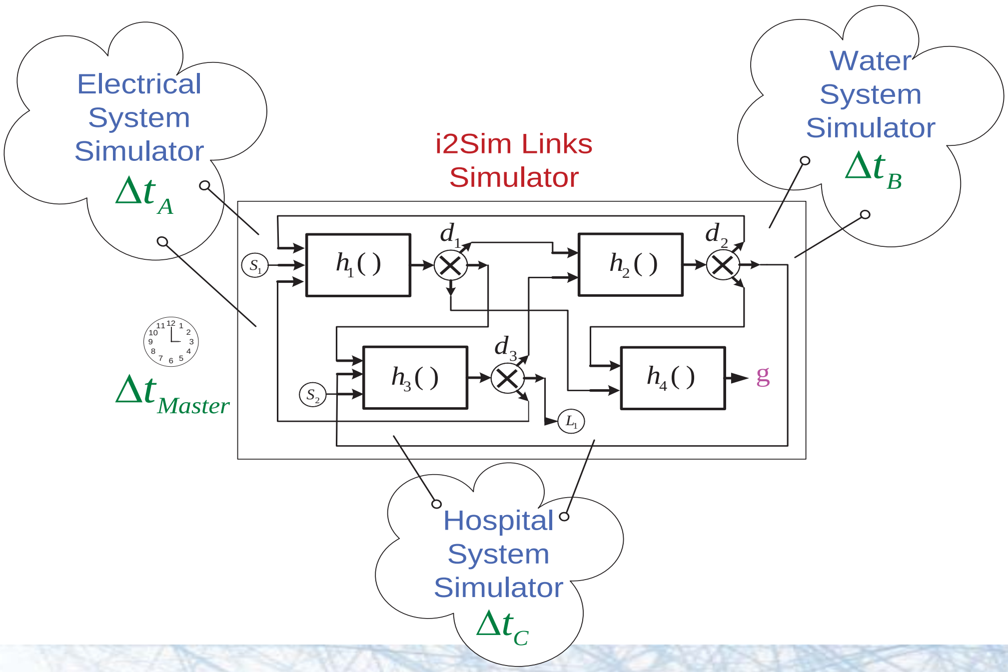
psychology

(*)	y(t)	x_1(t)	x_2(t)	m_1(t)	m_2(t)	(*)
Operability	Patients per hour	Doctors	Nurses	Physical Integrity	Doctors Shift Factor	Doctors Shift Hours
100%	20	4	8	100%	100%	10
75%	15	3	6	80%	75%	15
50%	10	2	4	50%	50%	20
25%	7	2	3	20%	25%	35
0%	0	0	0	0%	0%	> 48

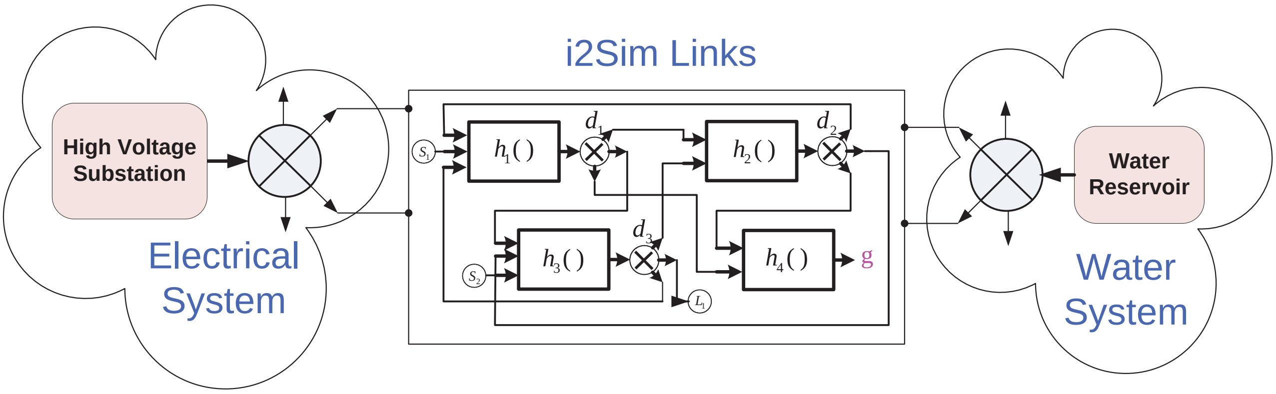
- In this example we suppose that electricity and water are not lacking, but doctors' shifts are very long. A modifier column can be added to account for this condition. The example assumes that the Nurses' shifts are optimum.

(*) Only the y(t), x(t), and m(t) columns are needed for the model. The other columns are descriptive comments.

i2Sim "Links" the CI Simulators



Privacy of Information

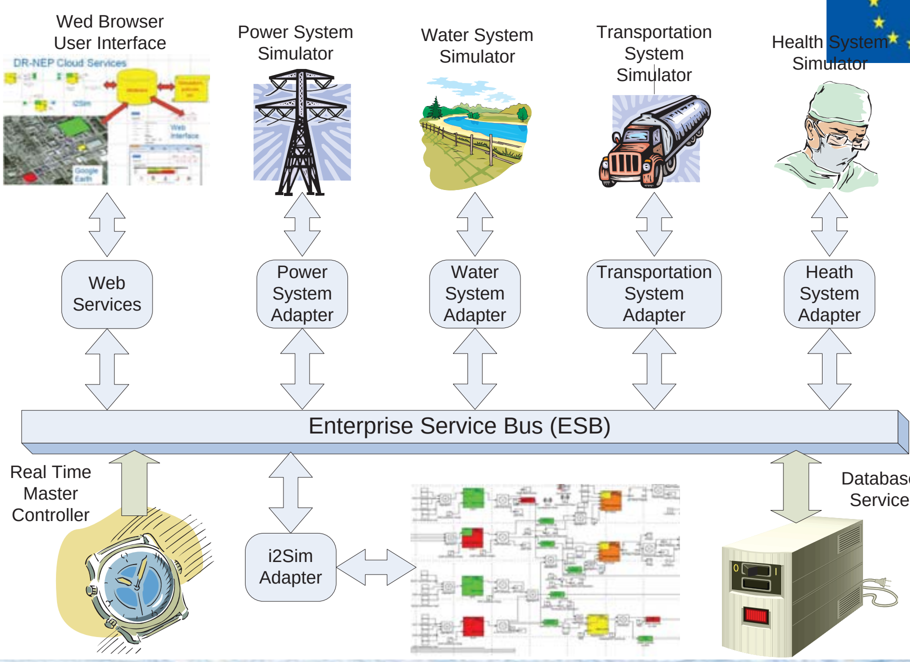


CI owners only need to provide point-of-entry information. They do not need to provide the internal physical details or the operational strategy of their system.

CI provide available point-of-entry resource (source) and a "Table of Choices" (distributor)

Federated Real-Time i2Sim Platform

- Off-the-shelf simulators (or the internal CI simulators) can be used for the CI.
- Input/output of the simulators are translated by the Software Adapters.
- Communication with all other simulators takes place in the common ESB language.
- Additional simulators can be easily added by writing software adapter.



Conclusions

- It is possible to model engineering systems and human systems in the same mathematical framework.
- It is possible to model interdependencies among critical infrastructures at the interdependency links while hiding the internal details of the CI.
- Very fast solution speeds can be achieved for large and complex systems by partitioning the solution.
- The i2Sim federated framework applies and extends the capabilities of MATE to allow for real time solutions of large multi-CI System of Systems including hybrid engineering/human systems.

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Federated Simulations

Edwin van Veldhoven - TNO
edwin.vanveldhoven@tno.nl

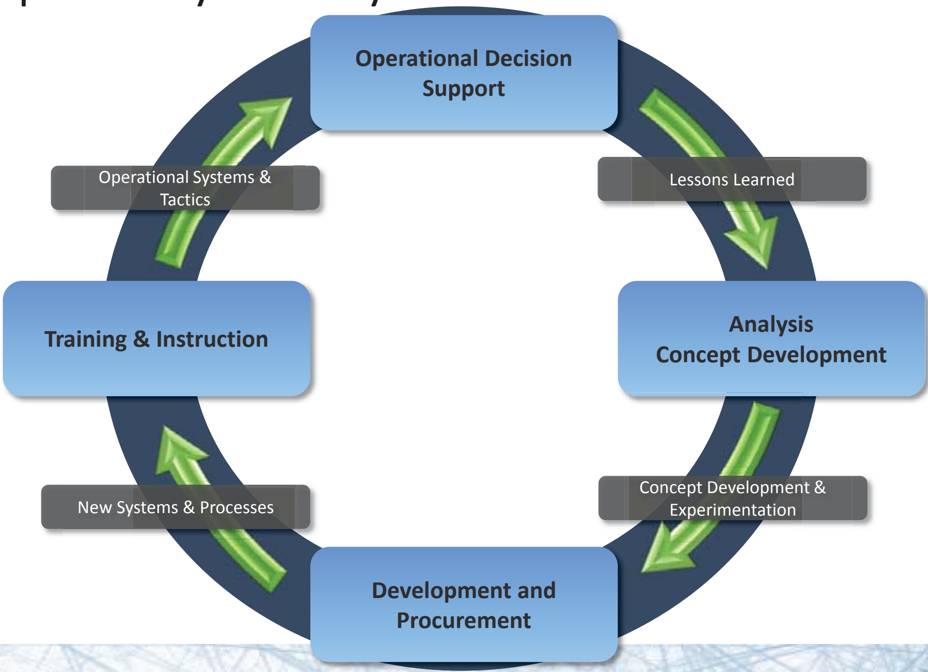
Modelling, Simulation and Analysis of Critical Infrastructures
CIPRNet Course

UCBM – Rome (Italy) – 9-10 July 2015

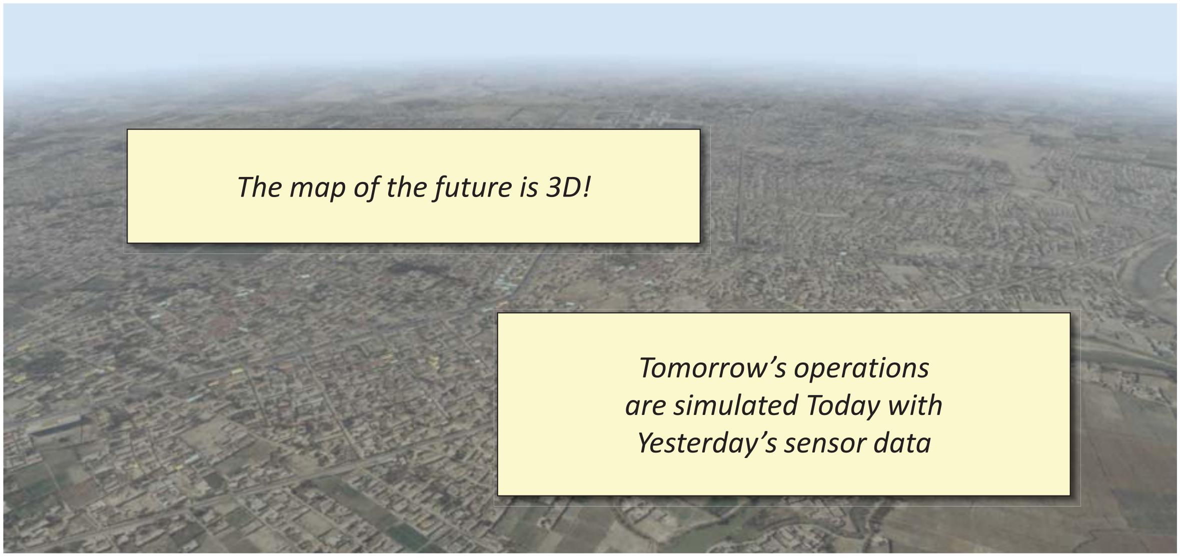
Contents

- Why federated simulation?
- Federated simulations
- Interoperability standards
- High Level Architecture (HLA)
- Distributed Simulation Engineering and Execution Process (DSEEP)

Capability life cycle

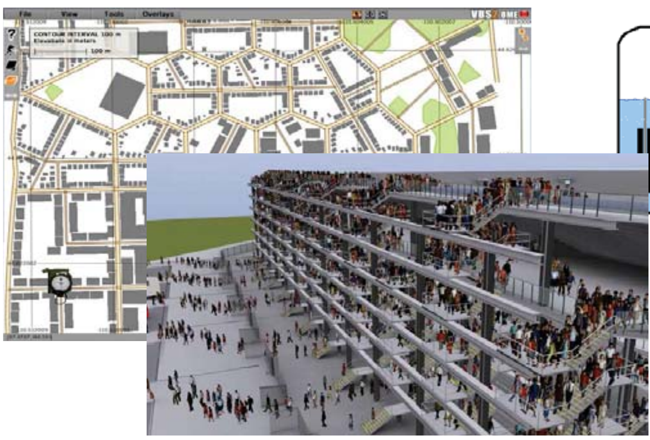


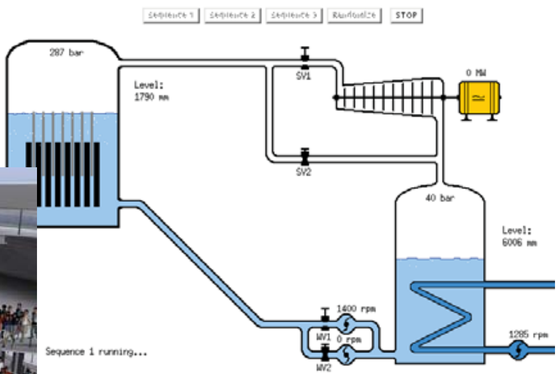
Synthetic environment modelling



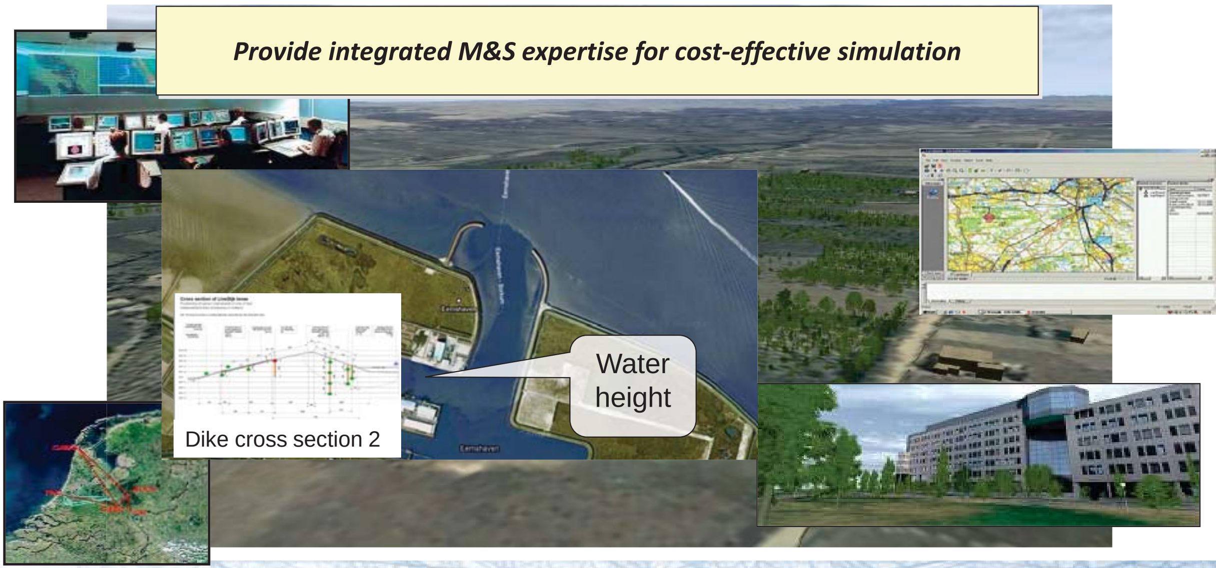
Synthetic environment modelling

System and behaviour modelling





Simulation systems engineering



Why federated simulation?

- No single simulation can solve all your problems
- Monolithic simulations are hard to re-use:
  size does matter, smaller is better
- Interoperable components of suitable granularity provide maximum flexibility

Federated simulation: terminology

- **Federation**: a set of simulations, a common federation object model, that are used together to form a larger model or simulation

- **Federate**: a member of a federation; one simulation
  - Could represent one platform, like a cockpit simulator
  - Could represent an aggregate, like an entire national simulation of air traffic flow

- **Federation Execution**: a session of a federation executing together

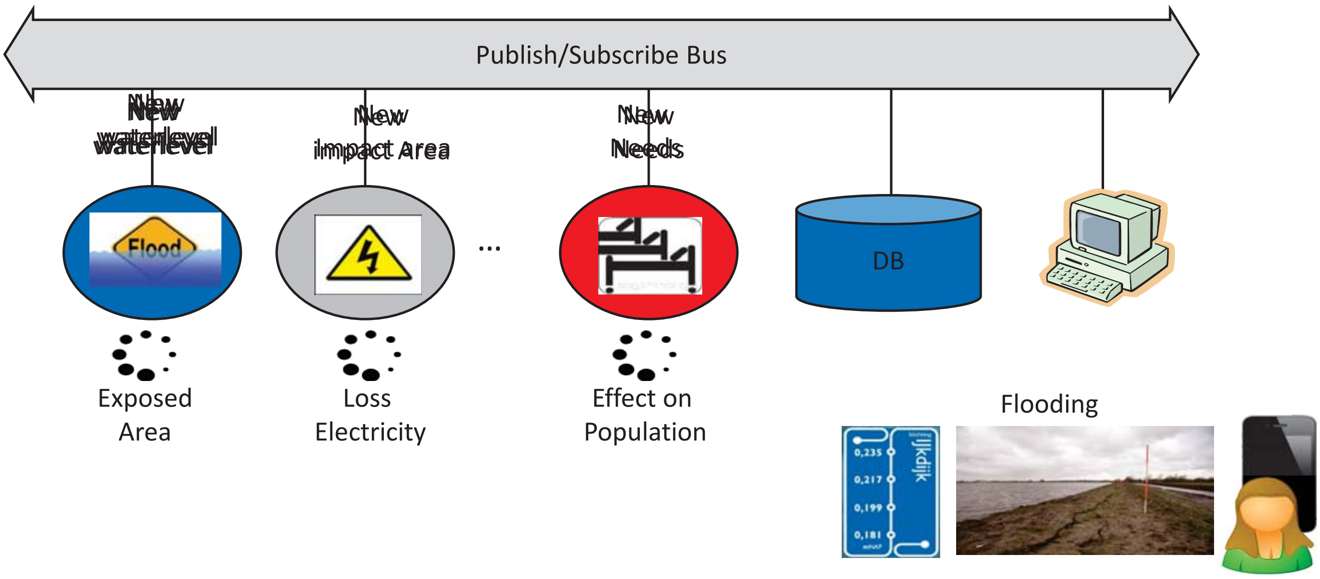
Federated simulation components

- **Man-in-the-loop simulators**
  - Aircraft, vehicles
  - Human players
  - Systems, Command & Control (C2) stations
- **Computer generated entities**
  - Vehicles, individuals, systems
  - Environmental effects (e.g. weather)
- **Exercise management facilities**
  - Scenario development tools
  - Briefing/debriefing tools
- **Analysis and assessment tools**
  - Loggers
  - 3D viewers
- **Network infrastructure**
  - Local
  - Wide area
  - Security/encryption

CIP federation example (1)

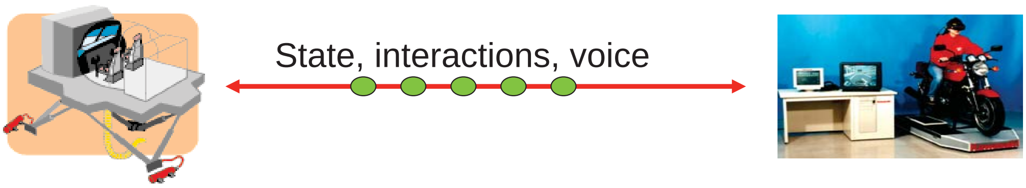
- Flooding impact

CIP federation example (2)

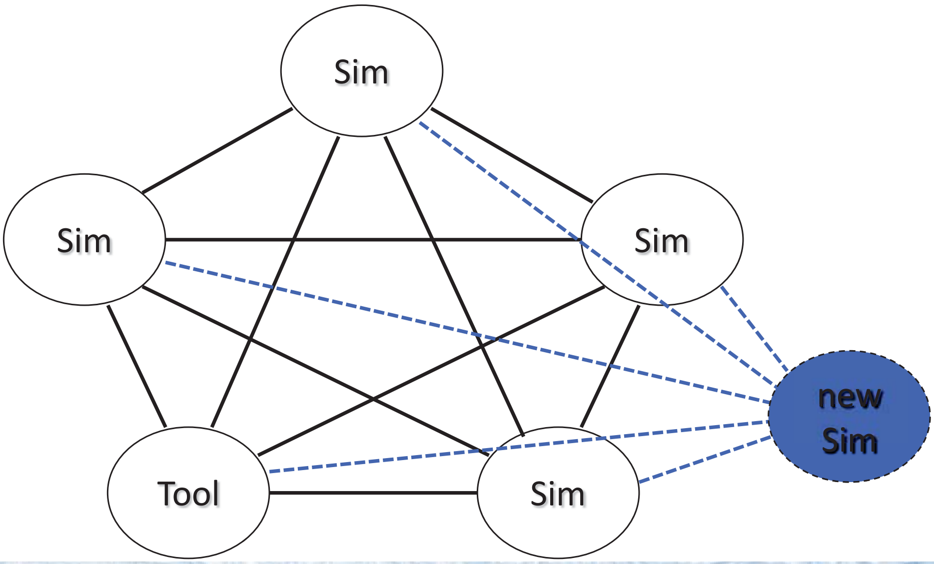


Interoperability

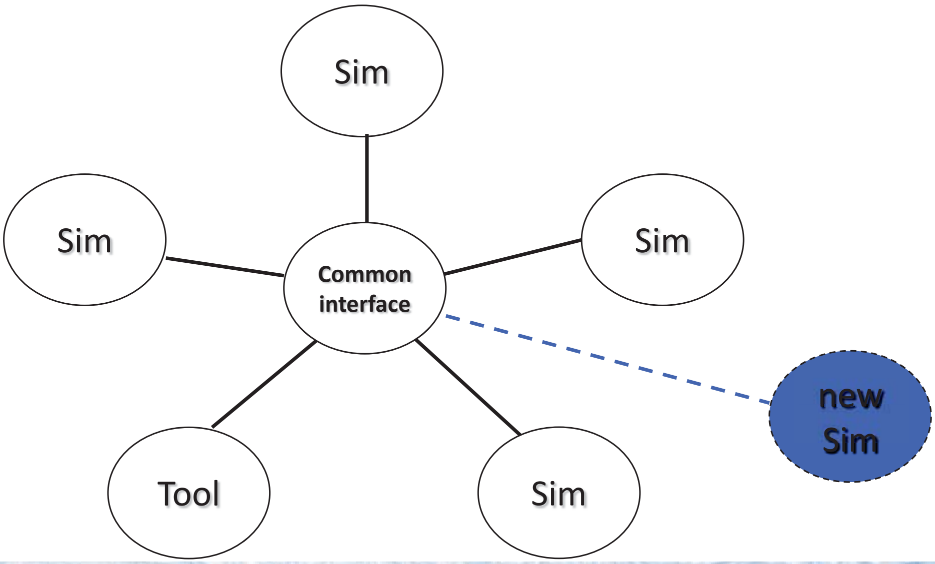
- Definition: the ability of simulations to provide services to and accept services from each other



Interoperability of simulation assets



Interoperability of simulation assets



The interoperability challenge

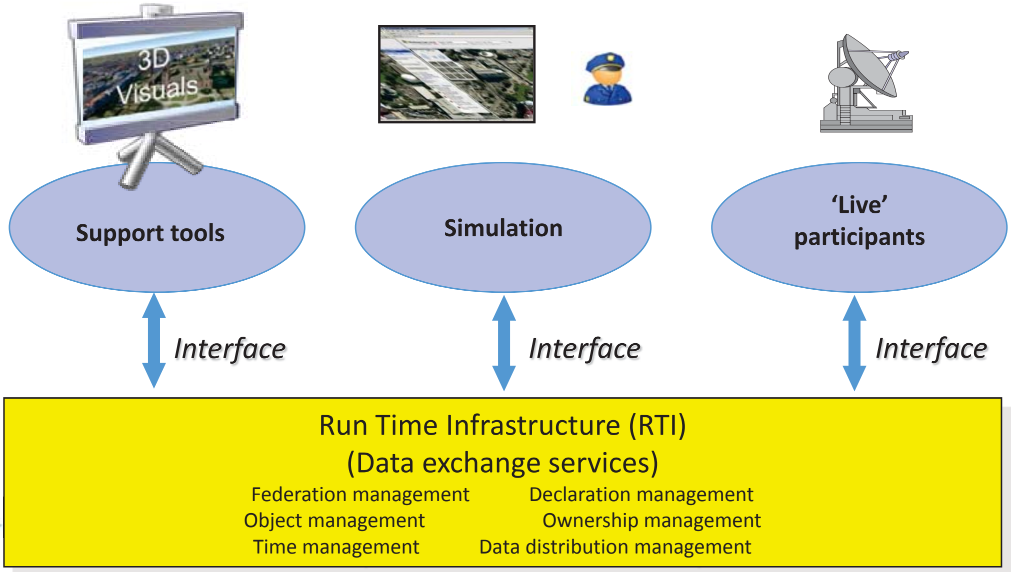
- Bits & bytes vs. meaning:
  - ’23’: 23 what? ft. altitude, bottles of beer?
  - ‘You are dead’: ‘No way, You’ve missed me’
  - ‘You are 50% dead’: ‘So what, I can still fight’
  - ‘I can see you, but you can’t see me’
- Challenges:
  - Standards and versions (HLA, DIS, …)
  - Vendor implementations & compliancy

Modelling & simulation standards

- Advantages:
  - Economy of scale
  - Comply with legislation
  - Promote interoperability
  - Promote common understanding
  - Introduce innovations, transfer research results
  - Encourage competition
  - Facilitate trade
- Challenges:
  - Consensus
  - ‘Not Invented Here’ syndrome
  - Openness / vendor lock-in
  - Maintenance

Modelling & simulation standards

High Level Architecture (HLA)



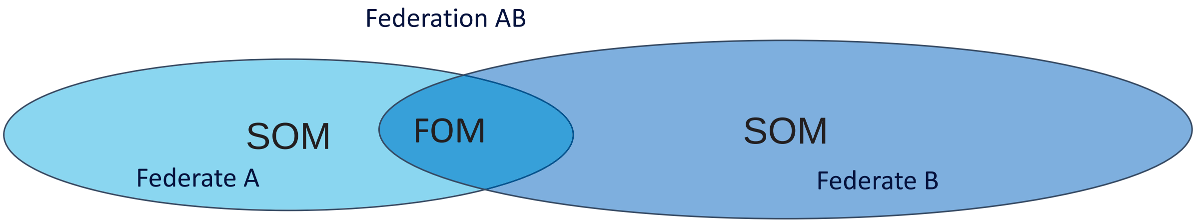
IEEE 1516-2010

High Level Architecture (HLA)

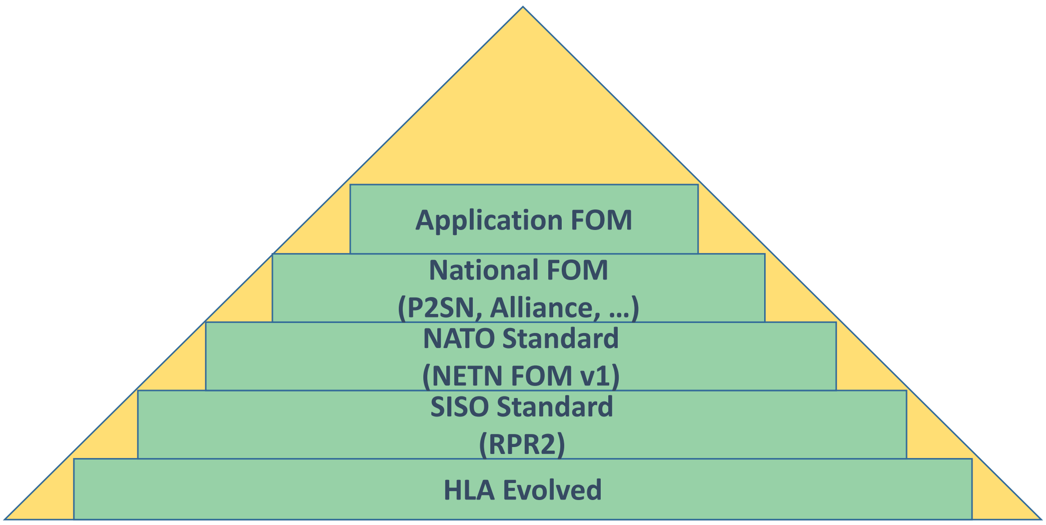
- HLA rules:
  - Must be observed by federates
  - 5 requirements for federations
  - 5 requirements for particular federates
- Runtime Interface (RTI):
  - Defines functional interfaces (service) between federates and the RTI
  - RTI is software, it is not a part of specification
- Object Model Template (OMT):
  - Specification of all objects and interactions
  - Federation Object Model (FOM)
  - Simulation Object model (SOM)
  - Management Object model (MOM)

Object models

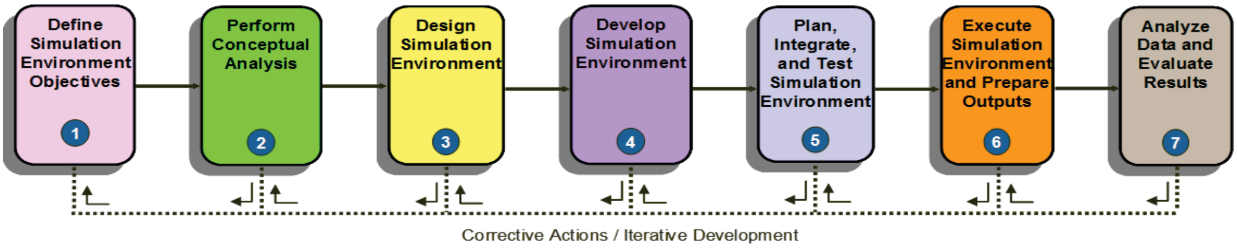
- Federation Object Model (FOM):
  - A description of all shared information (objects, attributes, and interactions) essential to a particular federation
- Simulation Object Model (SOM):
  - Describes objects, attributes and interactions in a particular simulation which *can* be used externally in a federation



FOM: technical baseline



Distributed Simulation Engineering and Execution Process (DSEEP)



- IEEE 1730-2010: a seven step **engineering process model** for the development and execution of a distributed simulation environment
- Each step is broken down in activities and tasks, with activity inputs and potential outcomes
- Generally applicable, evolving further by input from the user community

1. Define simulation environment objectives

*Define and document a set of **needs** to be addressed through the development and execution of a simulation environment and transform these needs into **objectives** for that environment.*

Activities include:

- Identify needs
  - Program goals, constraints, mission area, …
- Develop objectives
  - Determine feasibility, risks, objectives
  - Determine Measures of Effectiveness/Performance (MOEs/MOPs)

2. Perform conceptual analysis

*Develop **representation of the real-world domain** that applies to the defined problem space, develop the **scenario**, and transform objectives for simulation environment to **requirements**.*

3. Design simulation environment

*Produce the design of the simulation environment. This involves identifying **member applications**, creating new member applications, allocating **required functionality** to member applications, and developing **planning documents**.*

Activities include:

- Member application selection and trade-off analysis
- Allocation of responsibility to represent entities and actions in the conceptual model to member applications

4. Develop simulation environment

*Define the **information that will be exchanged** at runtime during the execution of the simulation environment, **modify member applications** if necessary, and prepare the simulation environment for integration and test.*

Activities include:

- Develop simulation data exchange model
- Establish simulation environment agreements:
  - initialization, synchronization, termination, progression of time, events, life cycle of entities, update rates, time and space units, dead reckoning, entity ownership, …

5. Integrate and test simulation environment

***Plan execution** of simulation, **establish all required interconnectivity** between member applications, and **test** simulation environment prior to execution.*

Activities include:

- Incremental integration and test, according to test and integration plan

6. Execute simulation

Execute the integrated set of member applications (i.e., the 'simulation') and preprocess the resulting output data.

Activities include:

- Execute simulation
  - Collect data, document problems, monitor execution ….
- Prepare simulation environment outputs
  - Merge, reduce/transfer, review data

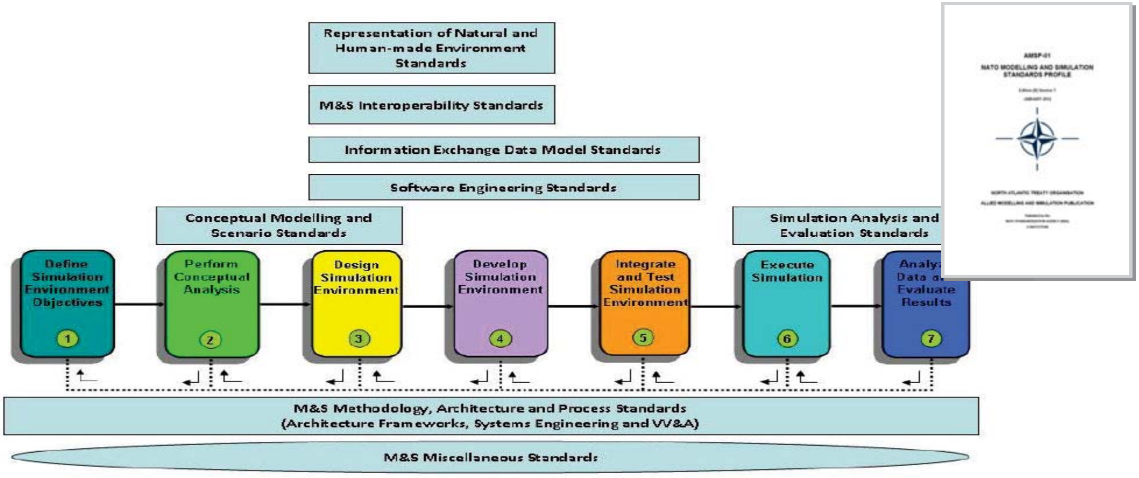
7. Analyse data and evaluate results

Analyse and evaluate data acquired during the execution of the simulation environment, and report the results back to the user/sponsor.

Activities include:

- Analyse data
  - Apply analysis methods and tools to data
  - Define appropriate presentation formats
  - Prepare data in chosen formats
- Evaluate and feedback results
  - Determine if all objectives have been met
  - Provide feedback and conclusions to user/sponsor

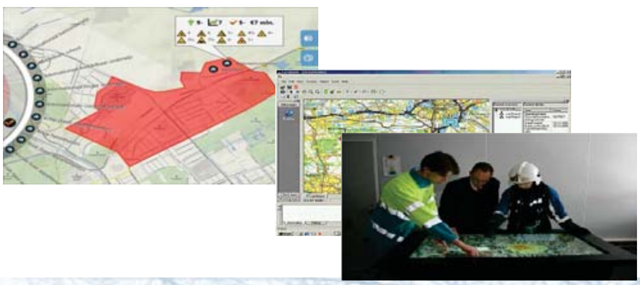
M&S standards categories



The 7-step DSEEP simulation engineering process and the standards categories

‘Take home’ messages

- Modelling and simulation are complimentary areas of **problem analysis** and **solution synthesis**, which are needed to support the full life cycle of a capability
- A set of **coherent principles** and **standards** is required to fully exploit the potential of modelling and simulation



More information

- Wim Huiskamp (wim.huiskamp@tno.nl)
- Tom van den Berg (tom.vandenberg@tno.nl)

- SISO website: http://www.sisostds.org
- NMSG website: http://www.cso.nato.int/panel.asp?panel=5

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Modelling and Simulation Techniques for Critical Infrastructure Protection

Roberto Setola
r.setola@unicampus.it

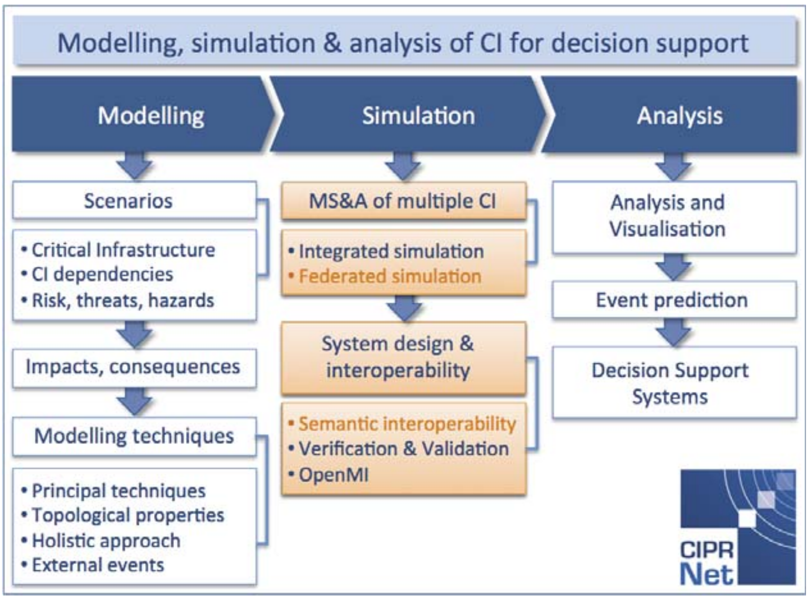
Modelling, Simulation and Analysis of Critical Infrastructures
CIPRNet Course

UCBM Headquarters – Rome (Italy) – 9 - 10 July 2014

Agenda

- **Simulation for CIP**
  - **Application areas**
  - **Challenges**
- **Integrated modelling and simulation**
  - **Basic modelling ideas**
  - **Example: CISIA framework**
  - **Advantages and disadvantages**
- **Federated modelling and simulation**
  - **Motivation**
  - **Challenges**
  - **Example: DIESIS architectural approach**

Locating the presentation topic



Simulation for CIP

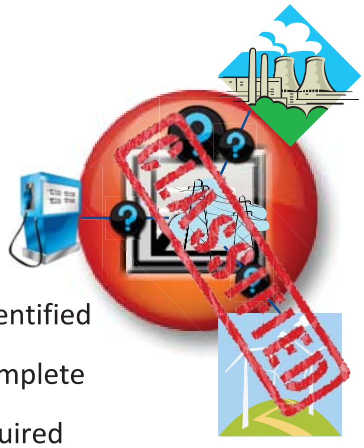
Some applications areas

- **General (offline) CI analysis**
  - Investigating (inter)dependencies between critical infrastructures
    - Implicit, indirect and hidden relations
    - Feedback loops and cascading effects
    - Stability analysis and risk estimation
  - Testing existing and benchmarking new CI control methods
- **Improving preparedness**
  - Soft exercises and real-time training
    - Confrontation with a wide spectrum of emergency situations
- **Operational support**
  - Decision support
    - Extended representation of current situation
    - What-if analysis

Simulation for CIP

Cross-sector simulation: modelling challenges

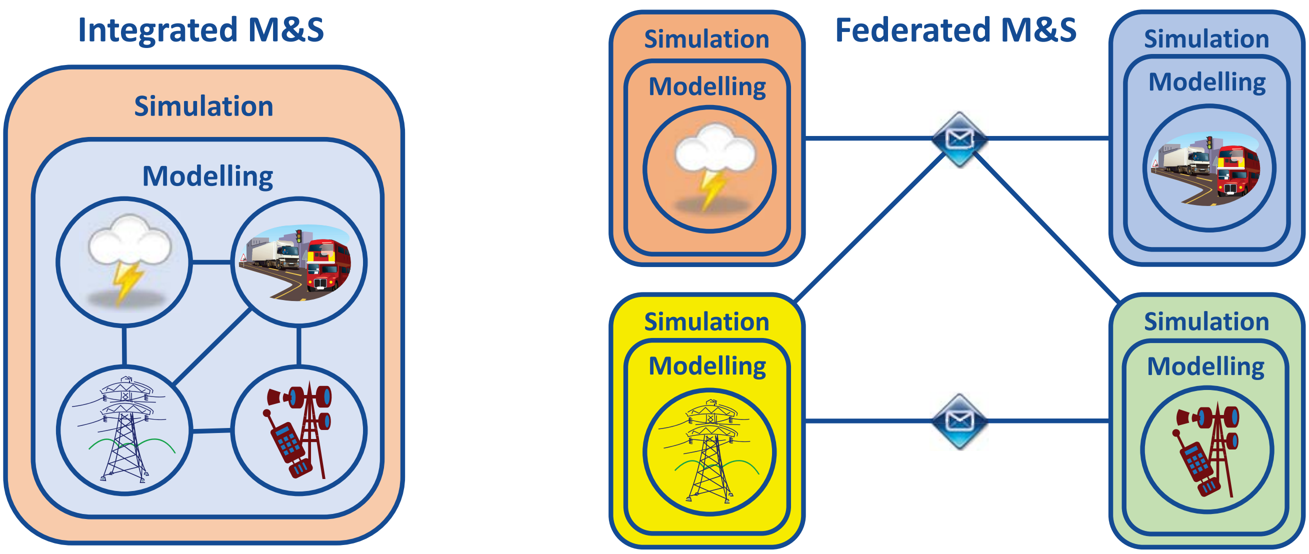
- **Heterogeneous CIs**
  - Different modelling functional principles
  - Different granularity required
  - Different time scales
  - Interdisciplinary expertise needed



- **Data acquisition**
  - Analysis goal has to be defined
  - Concrete CI dependencies have to be identified
  - Data may be sensitive, classified or incomplete
  - Close cooperation with CI operators required

Simulation for CIP

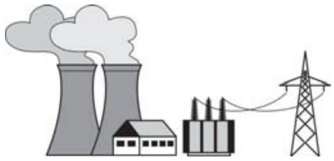
Integrated and federated M&S approaches



Integrated modelling and simulation

Basic modelling ideas

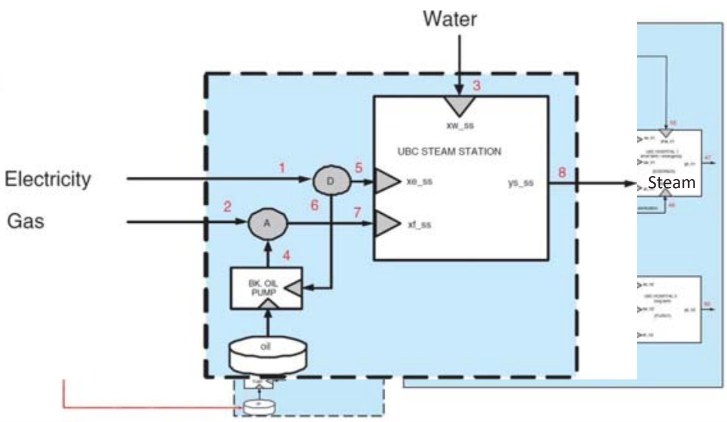
- Identify the analysis goal
- Find the suitable level of abstraction that:
  - Preserves realistic representation of all analytically relevant properties (qualitative or quantitative)
  - Allows system modelling by means of a generic formalism
- Identify the appropriate modelling formalism
- Create a large homogeneous holistic model
  - V&V: ensure completeness and correctness of the model
- Find existing or implement own simulation and analysis tool



- Simple model: power plant, transmission line, location, working / not working
- Detailed model: power plant, transmission line, transformer, distribution line, substation, location, capacity, nominal and real voltage, production and consumption fluctuations, etc.

Integrated modelling and simulation

I2Sim framework (early version from 2008)



- Formalism: cell-channel model
  - Basic structure: cells and channels
  - Components: controls and function blocks
- Elements: model of a steam station*
- Model: connect cells into one network *
- Solve: I2Sim simulator
- Current version of I2Sim supports federated simulation

*Picture from: Rahman, H. A., et al. I2Sim: a matrix-partition based framework for critical infrastructure interdependencies simulation. In: *Electric Power Conference, 2008. EPEC 2008. IEEE Canada*. IEEE, 2008. p. 1-8.

CISIA

CISIA → Native multidomain simulator

CISIA is a multidomain simulator which enables what-if analyses in the presence of etherogeneous interdependent systems.

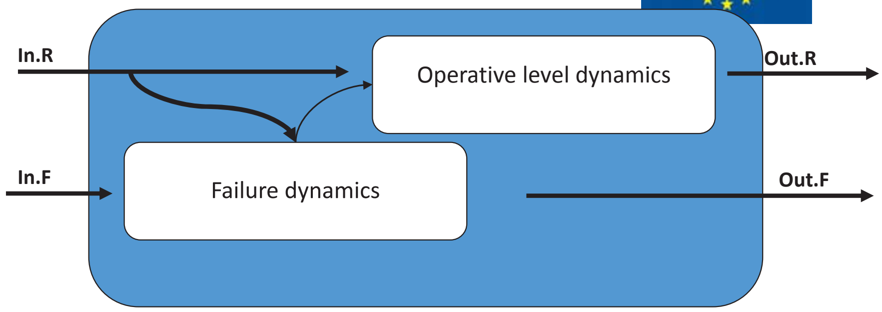
Through CISIA, infrastructures and their components are modeled describing the **internal dynamics** of each element and its **interdependencies** with the **environment** (in terms of input-to-state and state-to-output functions).

S. Panzieri, R. Setola, and G. Ulivi, "An Approach to Model Complex Interdependent Infrastructures", *16th IFAC world-congress 2005*, Praha, Czech Republic, 4-8 July, 2005.

S. De Porcellinis, S. Panzieri, R. Setola, and G. Ulivi, "Simulation of Heterogeneous and Interdependent Critical Infrastructures", *Int. J. Critical Infrastructures* (IJCIS), vol. 4, n. 1/2, pp. 110 – 128, 2008.

CISIA internal model

- Inputs
  - Resources
  - Faults
- Outputs
  - Resources
  - Faults



- Internal dynamics are characterized by operative level and failures
- External events or wrong operative conditions may induce faults (several classes of internal faults are considered)
- The lack of resources or the presence of internal faults may induce operative level degradation
- Internal failure levels can ONLY grow up

ENTITY DESCRIPTION USING QUESTIONNAIRES

Required Resources
- Current
- Impedance
- Recovery

Produced Resources
- Current
- Impedance

Received Failures
- Sabotage
- Mechanic
- Geographic

Internal failures
- Geographic
- Aging
- Misconfiguration

Code	001
Infrastructure code	ECI
Class name	SUBNET

Short description (max 60 words)

MV Power grid segment that connects ECI components. May contain several wires and manually operated switches. If faulted, it can be manually reconfigured by Repair crew.

Its functioning is similar to a wire.

Localization (geographical or top

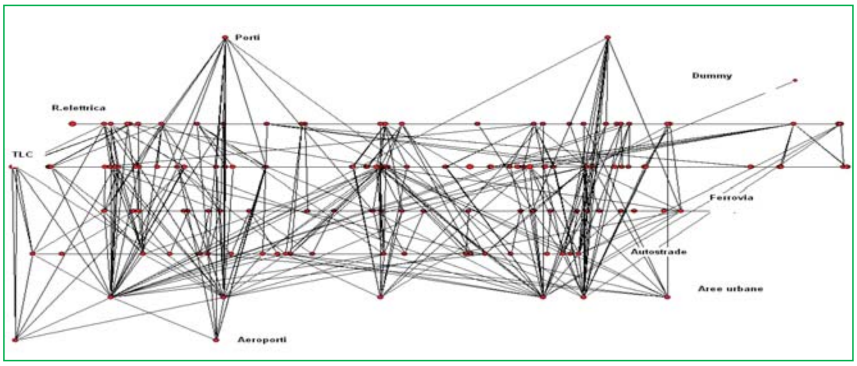
Subnets are inside MV power grid.

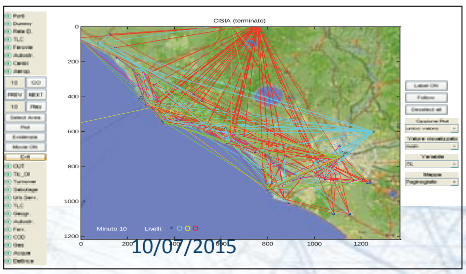
Its operation depends on the availability of resources from outside? **It has incoming resources that do not directly affect the operativeness?**	**Name**	**NfI**	**Name**	**NfI**
	Current	**RR-1**		**RR-6**
	Impedance	**RR-2**		**RR-7**
	Recovery	**RR-3**		**RR-8**
		RR-4		**RR-9**
				RR-10

Produces or provides resources ? **Transports or forwards resources ?**		**Name**	**NfI**	**Name**	**NfI**
		Current	**PR-1**		**PR-6**
		Impedance	**PR-2**		**PR-7**
			PR-3		**PR-8**
No	**Yes** (use the pattern to the right to specify)		**PR-4**		**PR-9**
			PR-5		**PR-10**

Case-study 2007

Infrastructure	**Macro-components**
Electric Grid	35
Urban areas	6
Air-ports	2
Sea-ports	2
Railway	27
Highways	23
TLC	141



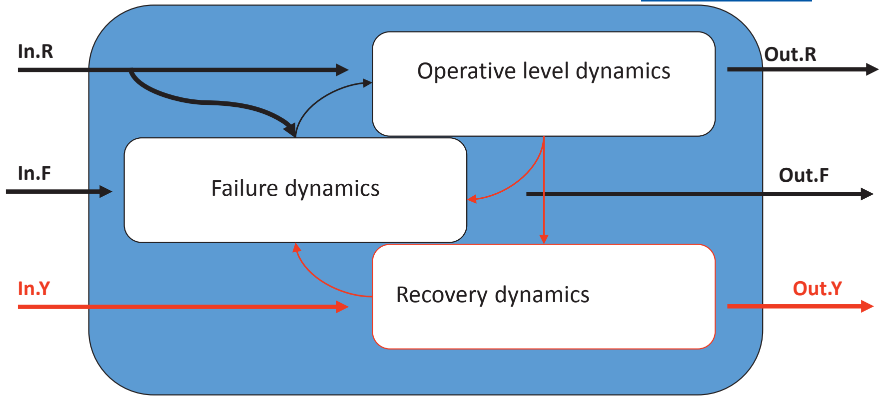


233 Entities
844 Link

SELEX Sistemi Integrati
Una Società Finmeccanica

CISIA model with recovery dynamics

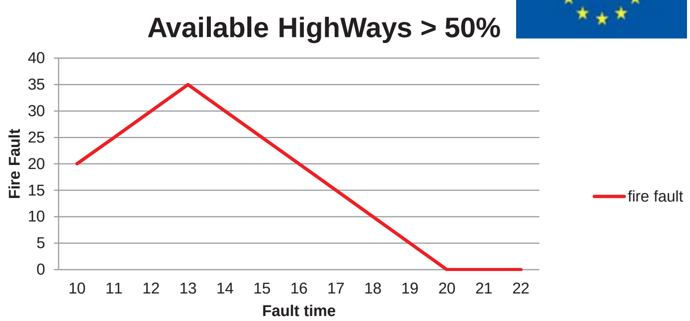
- Inputs
  - Resources
  - Faults
  - Recovery
- Outputs
  - Resources
  - Faults
  - Recovery



Failure dynamics may be damped or inverted through the influence of recovery dynamics. Recovery actions can have both endogenous or exogenous nature

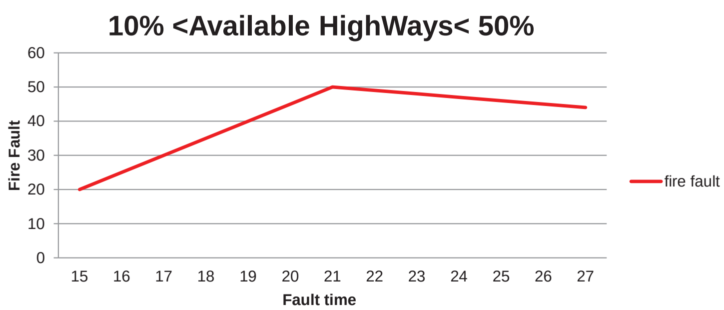
Recovery dynamics

Fire fault mitigation



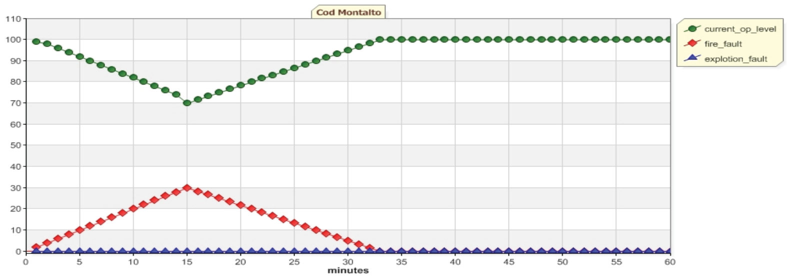
Recovery at oil tank farm

Fire dousing at 13 minutes after the fire start. Every minute, its value will be reduced of 5%.

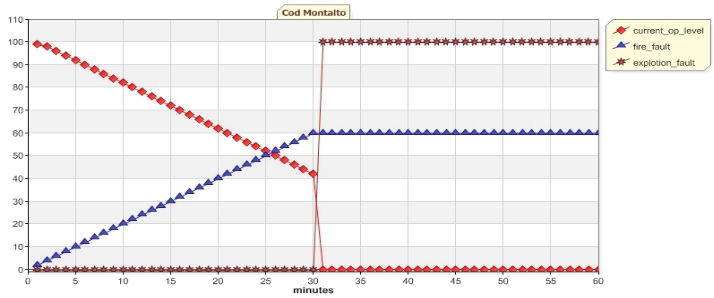


Fire dousing at 21 minutes after the fire start. Every minute, its value will be reduced of 1%.

Recovery Dynamics - results

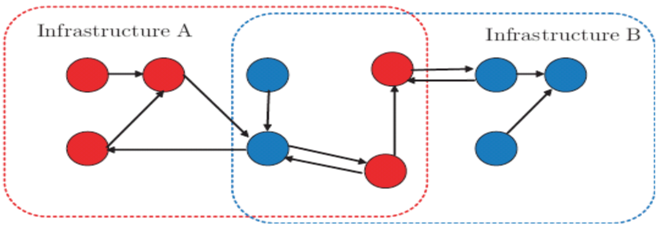


simulation of the operativeness of an oil stocking facility assuming the presence of "Highway Avail" resource

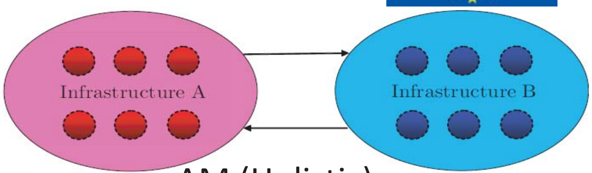


assuming the absence of enough of "Highway Avail" resource

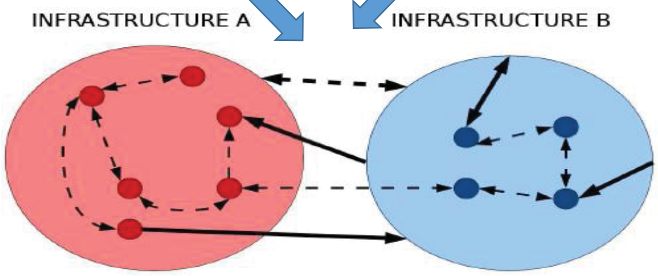
Hybrid Models



RM (Reductionistic)



AM (Holistic)



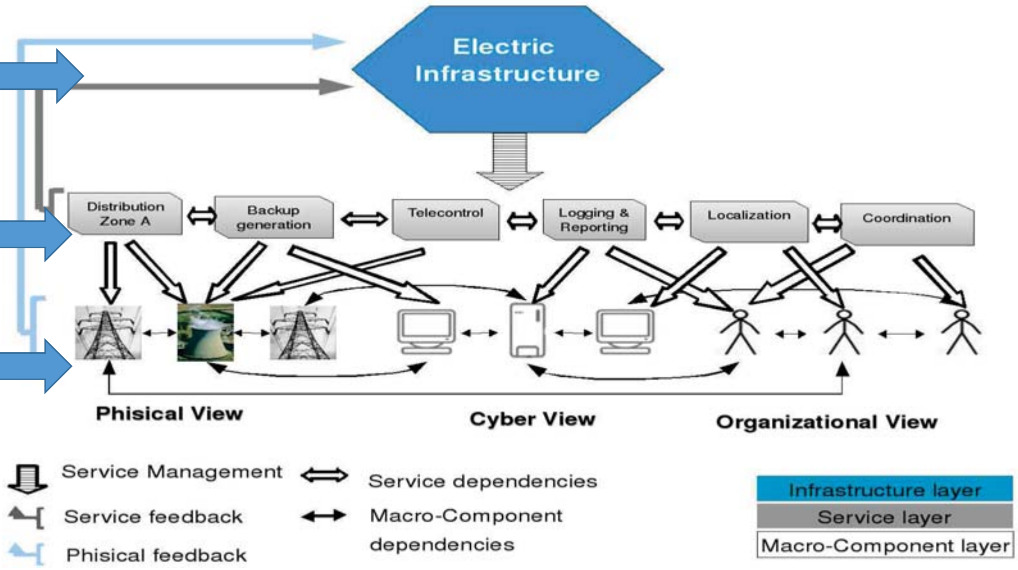
Mixed Holistic-Reductionistic

The HR model of an infrastructure

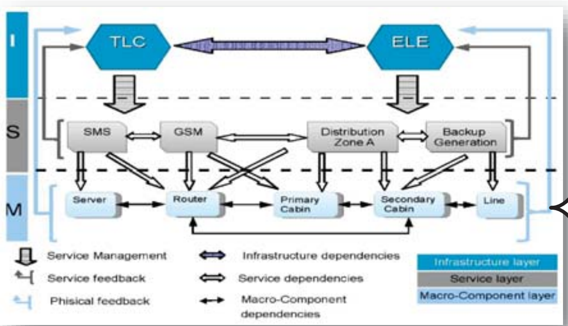
A business partner or a customer sees this…

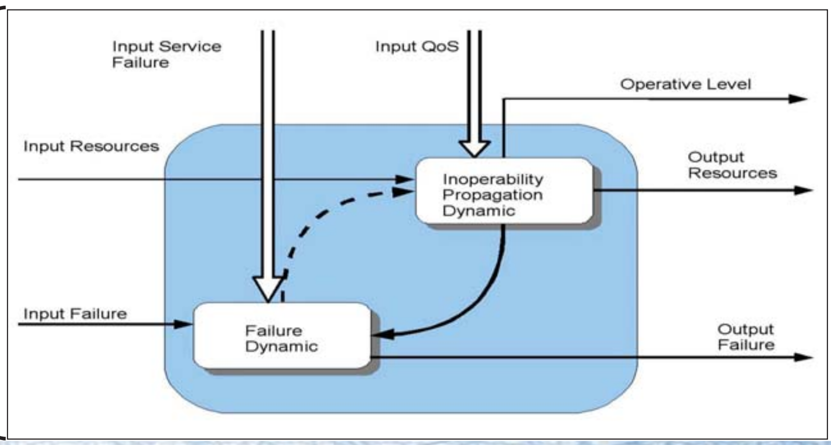
..which is controlled via these…

…based (also) on the existence of them

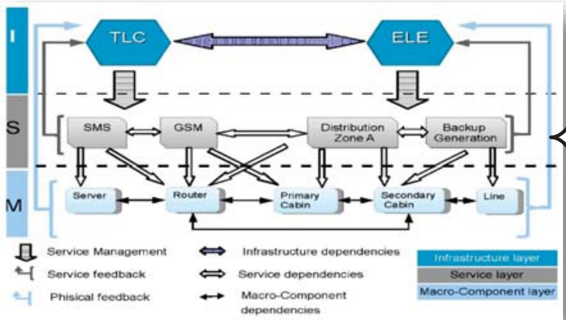


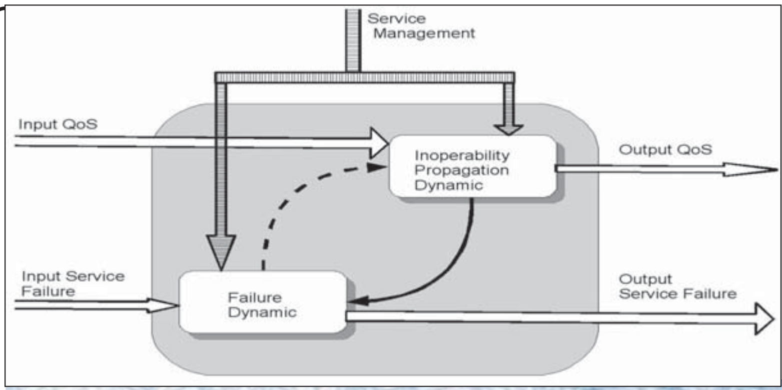
Components are representative of ‘small’ parts or elements of the infrastructure, with a recognizable functional, phisical or sociologic individuality.



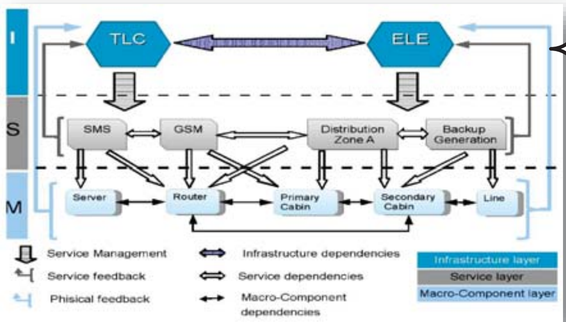


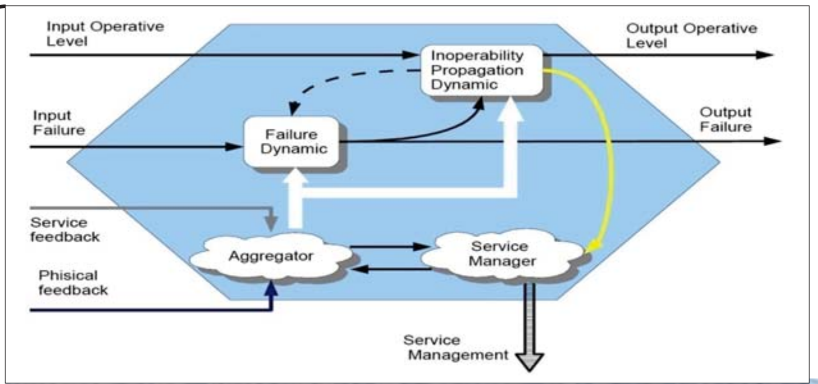
An element in the '**service**' (or functional) layer represent a (logical, organizative or real) element which provides an **aggregate** resource (like a VoIP service or telecontrol).



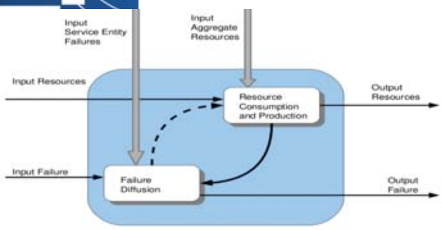


The upmost layer should represent the infrastrcture **as a whole** (or its general organizative divisions), in order to have a model which can take into account the **global dynamcs** of the infrastructure (and, possibly, the behaviours related to policies, strategies, etc.).



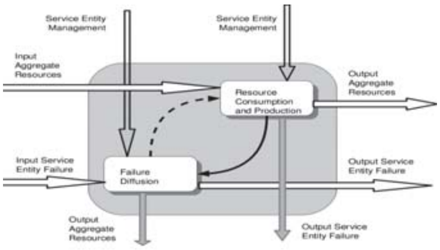


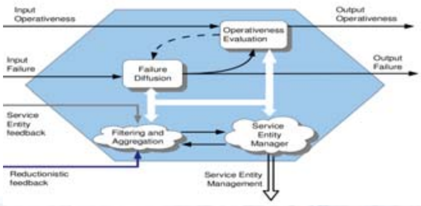
Failures Within MHR



Traditional failures (e.g. tornado, fire, disruptions, etc..)

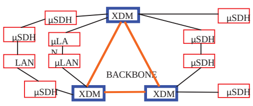
Complex and high-level failures (e.g. the effects of cyber attacks) that, instead, are very complex to model with a mere reductionist perspective.

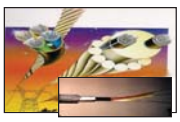


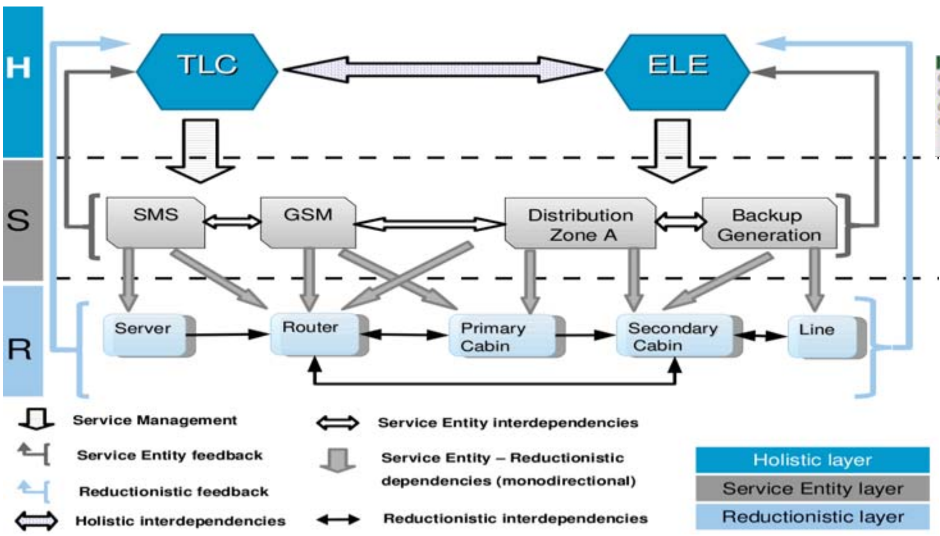


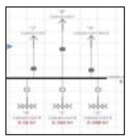
Sociological related events (e.g. strike, panic, malicious behaviours, etc..) that are very difficult to model at different level of detail.

MHR Approach Within MICIE Project

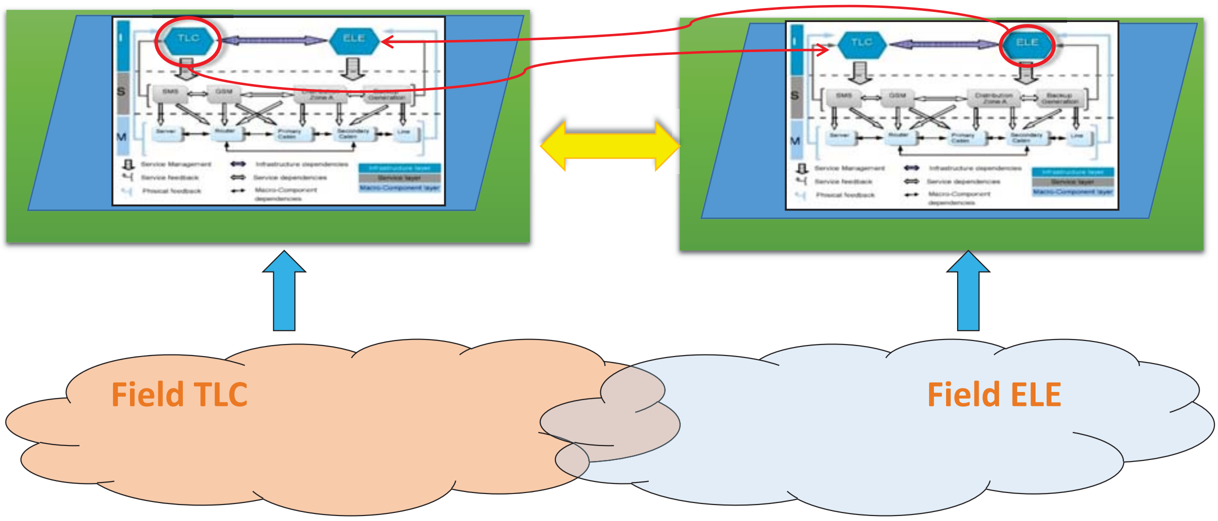








MHR and MICIE Online Riskr Pediction Tool



Integrated modelling and simulation

Advantages and disadvantages

- **Advantages**
  - Proper level of abstraction for a given analysis task
  - As much detail as required but not more than necessary
  - No redundant computations, good simulation performance
  - Does not reveal too much technical details
  - One single simulator can be employed
- **Disadvantages**
  - Models have to be created from scratch (e.g., CI element behaviours)
  - Modelling is very time and resource-consuming
  - Modification of analysis goal and/or scenario: re-modelling is often required
  - Modification of abstraction level for one model part is not possible

Federated simulation
Motivation

- We can save resources by reusing existing models and interconnect ready-made simulators
- For most domains and CIs, dedicated ready-made commercial and/or free high-fidelity simulators already exist
  - No need for implementation of new tools
- Most CI operators maintain either ready-made correct simulation models of their CIs or detailed inventories of CI elements.
  - Makes resource-consuming modelling and V&V unnecessary
- Requirement: create interaction models that describe interactions between domains and contain only relevant CI elements
- Several approaches exist (often emerged from the military area, e.g., HLA)

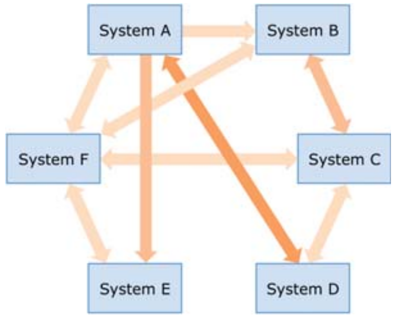
Federated simulation
Challenges

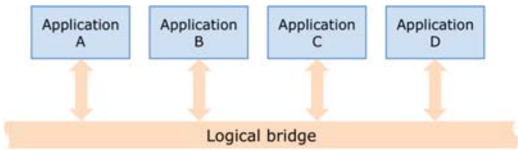
- **Semantics**
  - Data integration and conversion
  - Different time models: synchronisation (preservation of causality)
  - It may be necessary to create concepts or elements outside particular domains at federation level
- **Technology**
  - Heterogeneous software: interfacing simulators
  - Different levels of abstraction: avoid redundant computations
  - Orchestration of different execution concepts of federate simulators
  - Communication and event routing among federates

Federeted architectural approach

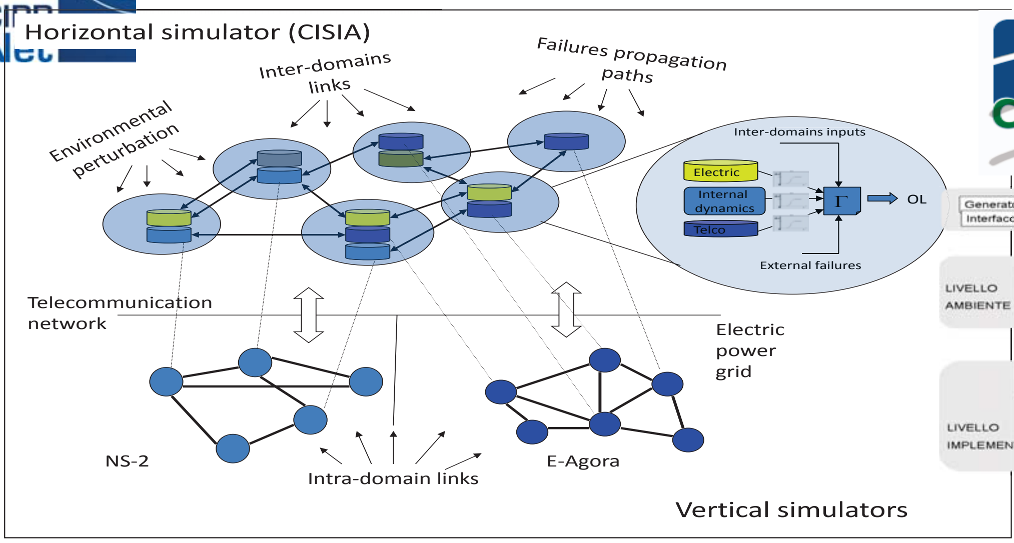
Interoperability middleware for federated MS&A

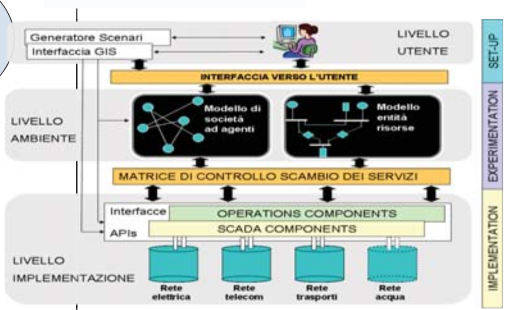
- Designed for heterogeneous interdependent federated CI simulations
  - Federates are not required to support common standards (e.g., HLA)
  - Federates have different time models and different time scales
  - Methodology for arbitrary scenarios, scenario-oriented federation design
  - Flexible modelling, extensibility of federations
  - Service-oriented scenario design
- interoperability middleware is based on two concepts
  - Separation of technical and semantic interoperability
  - Lateral (instead of central) coupling of federates





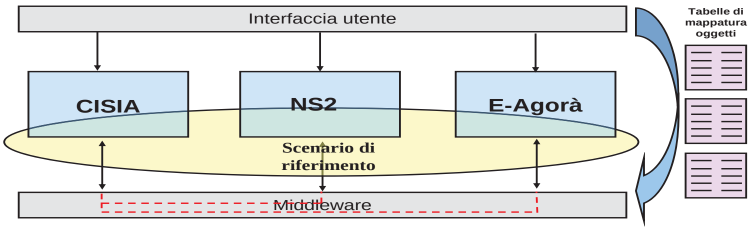
CRESCO project - Federation

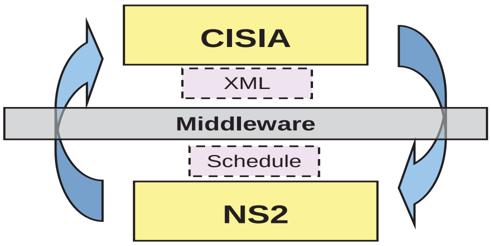


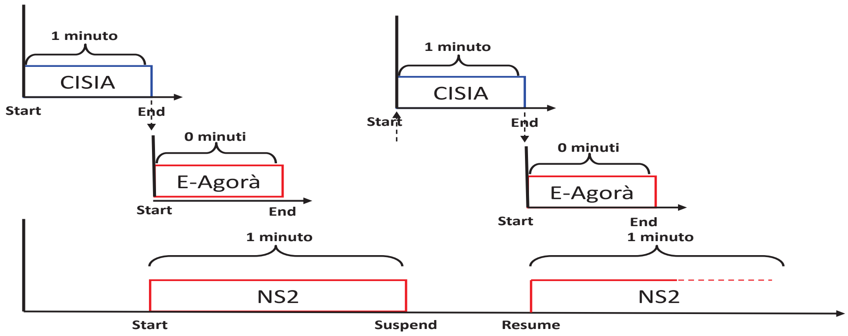


R. Setola, S. Bologna, E. Casalicchio and V. Masucci, "An Integrated Approach for Simulating Interdependencies" in *Critical Infrastructure Protection II,* M. Papa and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 221 – 231, 2008.

CRESCO Project - Federation







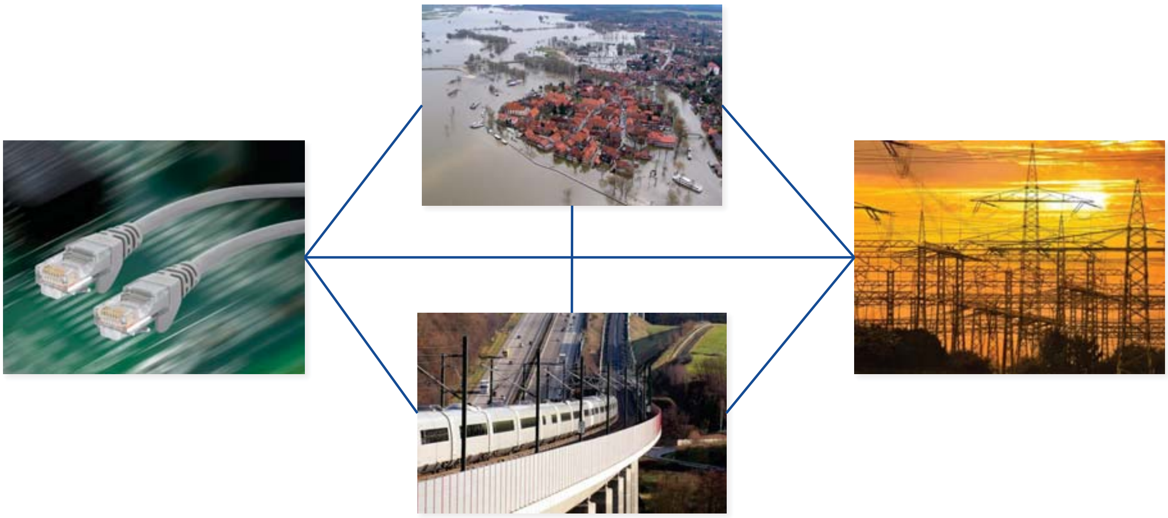
DIESIS architectural approach

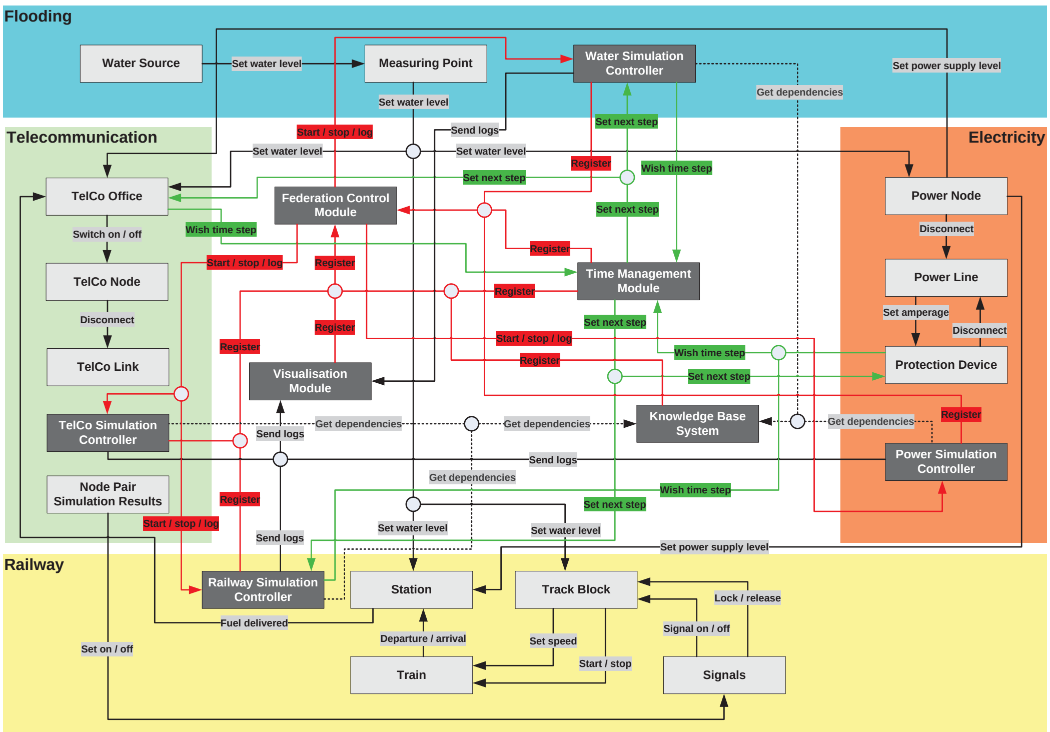
Interoperability layers

- **Semantic interoperability**
  - DIESIS Knowledge Base System: a general modelling framework
  - CI elements/properties that are involved in cross-domain interactions
  - Federation level concepts: static dependency representation (relations), dynamic dependency concepts (behaviour)
- **Technical interoperability**
  - Reusable simulator coupling links, dedicated types:
    - Time links: ensure correct event ordering
    - Data links: exchange state changes (events)
    - Function links: mutual function calls
    - Control links: manage runtime behaviour

DIESIS architectural approach

DIESIS demonstrator





DIESIS architectural approach

Scenario-oriented design: modelling phase

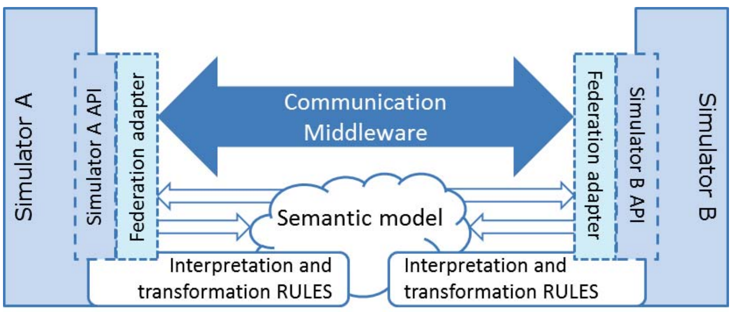
- Provide a formal, machine-readable representation of the informal model
  - Conceptual level: add all concepts for domain element types and their relations
  - Instance level: instantiate domain element types, add concrete elements and relations
  - Dynamic level: provide description of service behaviour

- A *power station* provides energy for a *TelCo building*.
- *TelCo building* **TB12** receives power from the *power stations* **P20m** and **P18m**.
- Any kind of equipment inside a *TelCo building* is **off** if none of the *power stations* linked to it has a property **VoltageLevel** over 80% and the own *backup power supply unit* is discharged.

DIESIS architectural approach

Scenario-oriented design: implementation phase

- Implement all technological components (see service network)
- Implement communication layer or add interfaces to existing RTIs
- Implement federation adapters for all simulators
- Remove bottlenecks, optimise performance
- Validate simulation results



DIESIS architectural approach

Features and advantages

- Structuring of modelling and development in order to facilitate the process and to minimise efforts
- Modelling at federation level concerns only those elements that are relevant for dependency definition
- No deep insight into structure and behaviour of all (scenario-relevant) domains is required for modelling
- Flexibility: depending on desired results, particular simulators and models can be added, removed or replaced
- Reusability: technical components, models and concepts and can be utilised for various scenarios

M&S methodologies for CIP

Conclusion

- Modelling and simulation are very useful for many applications related to CIP
- Analysis of multi-CI systems is challenging
- Integrated M&S approach
  - Uniform modelling: single simulator required
  - Good performance: important for real-time applications
  - Limited flexibility in relation to realisation of new scenarios
- Federated M&S approach:
  - Reuse existing simulators and models: reduce realisation costs
  - Best flexibility for changing scenarios and different analysis tasks
  - Interoperability: currently no established standards for CIP but several approaches exist

Thank you for your attention!

Any questions?

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Verification and Validation

Edwin van Veldhoven - TNO
edwin.vanveldhoven@tno.nl

Modelling, Simulation and Analysis of Critical Infrastructures
CIPRNet Course

UCBM – Rome (Italy) – 9-10 July 2015

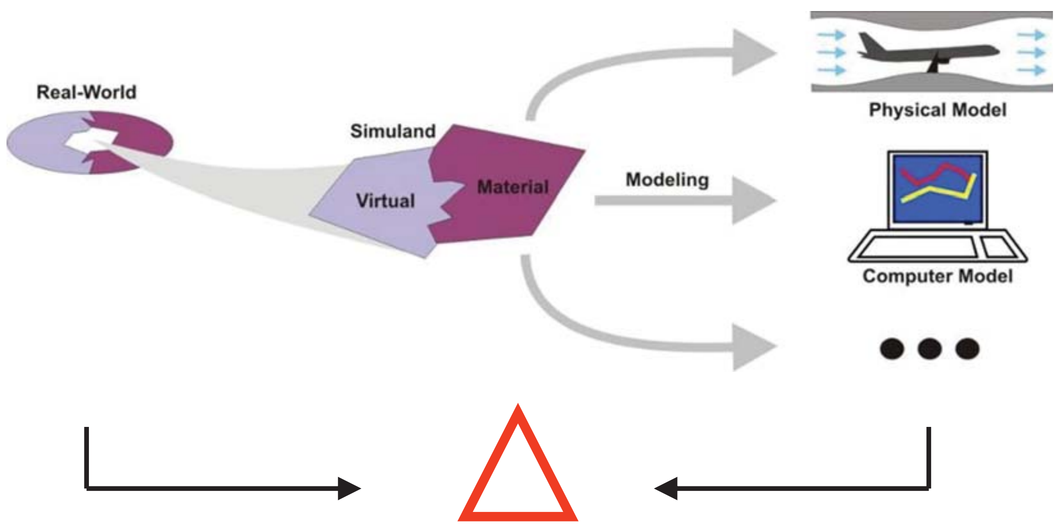
This lecture is about three things:

- You have to do V&V
  - because there is risk involved
- You have to do V&V in a structured way
  - if you want to do it more effective and more efficient
- You have to choose the right V&V technique
  - in order to balance the risk with the effectiveness and efficiency

Part 1

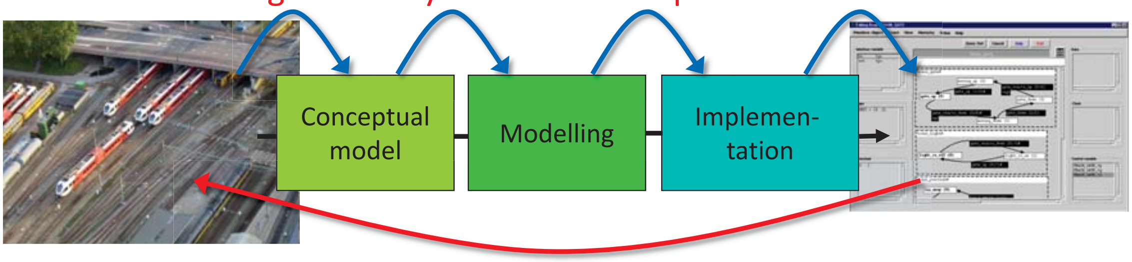
- You have to do V&V
  - because there is risk involved
- You have to do V&V in a structured way
  - if you want to do it more effective and more efficient
- You have to choose the right V&V technique
  - in order to balance the risk with the effectiveness and efficiency

What is 'Modelling and Simulation' (M&S)?



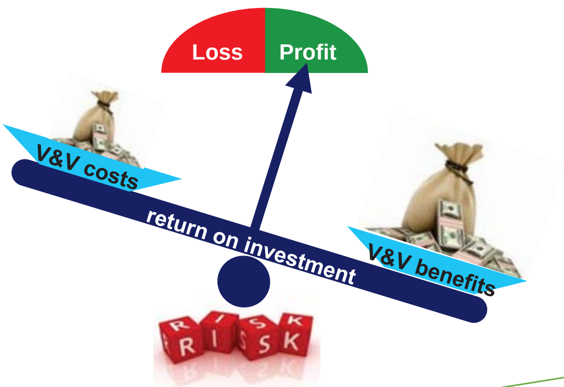
What is ‘Verification and Validation’ (V&V)?

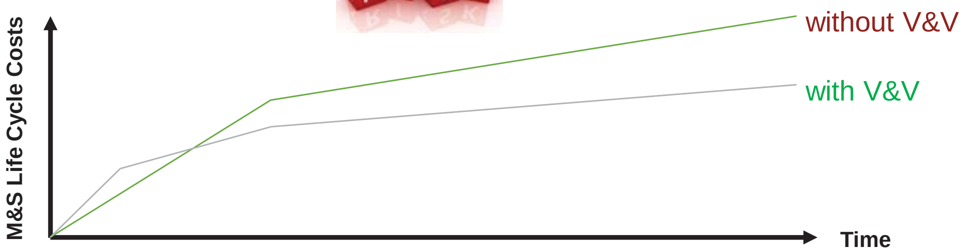
- Verification
  - assesses if the M&S system is built and used right
- Validation
  - assesses if the right M&S system is built or procured



Provides <u>insight</u> into and <u>advice</u> on the <u>quality</u> of the M&S system over its entire <u>life cycle</u>, and the associated <u>risks</u>

Should you always do V&V?





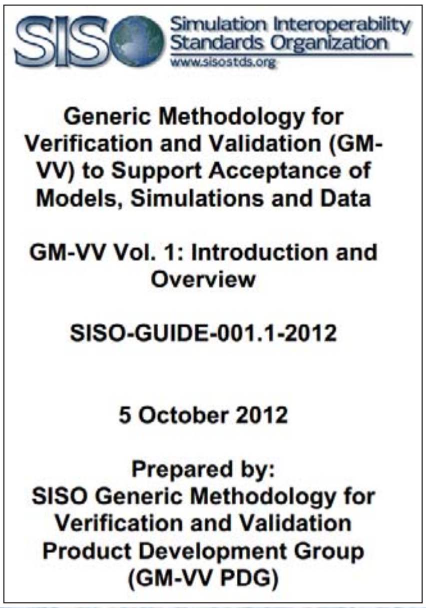
Part 2

- You have to do V&V
  - because there is risk involved

- You have to do V&V in a structured way
  - if you want to do it more effective and more efficient

- You have to choose the right V&V technique
  - in order to balance the risk with the effectiveness and efficiency

Structured approach to V&V



SISO Simulation Interoperability Standards Organization
www.sisostds.org

Generic Methodology for Verification and Validation (GM-VV) to Support Acceptance of Models, Simulations and Data

GM-VV Vol. 1: Introduction and Overview

SISO-GUIDE-001.1-2012

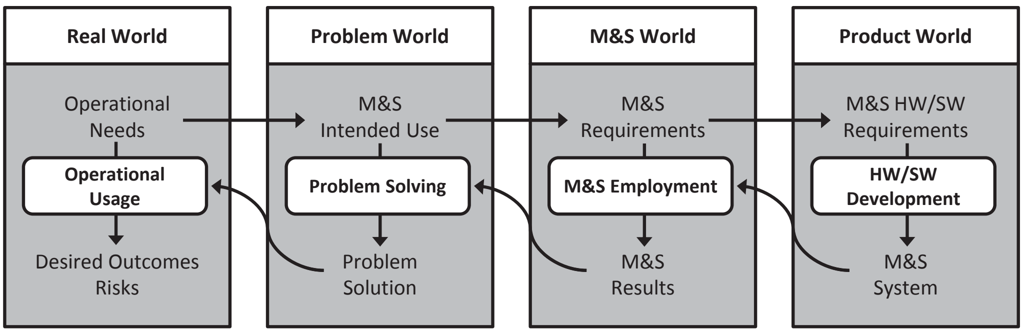
5 October 2012

Prepared by:
SISO Generic Methodology for Verification and Validation Product Development Group (GM-VV PDG)

Generic Methodology for V&V (GM-VV)

- Conceptual framework
  - basis of GM-VV
  - connection to other V&V methods
- Implementation framework
  - products, processes, roles
  - technical, project, enterprise
- Tailoring framework
  - adaption
  - optimization

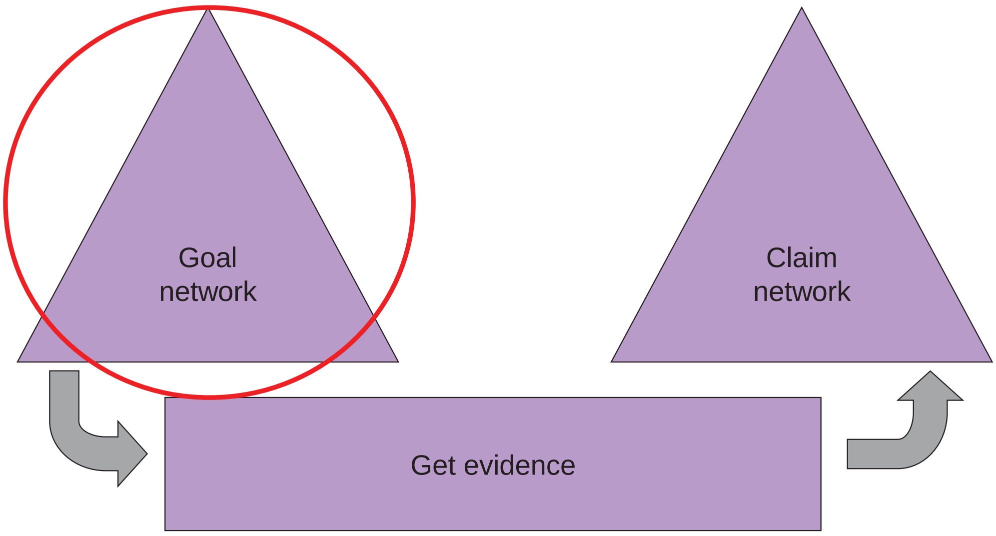
Four-worlds model



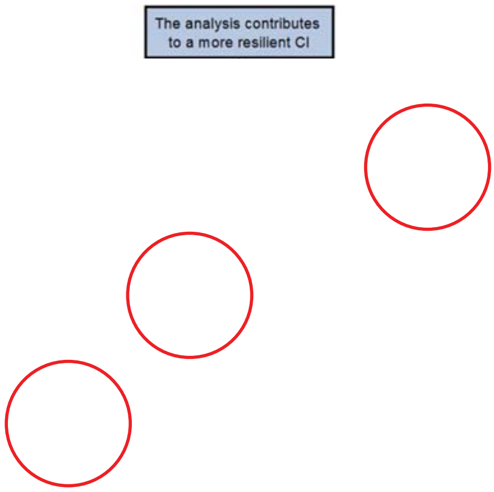
What needs to be V&V-ed for CIP?

- Simulators: power plants, banks, traffic generators, networks, ...
  - man-in-the-loop simulators
- Exercise management facilities
  - scenario development tools
  - briefing/debriefing tools
  - trainers
- Analysis and assessment tools
  - specialized analysis tooling
  - loggers
  - 3D viewers
  - generic didactic modules (scoring, computer assisted instruction)
- Network infrastructure
  - local
  - wide area
  - security/encryption
  - different architectures used

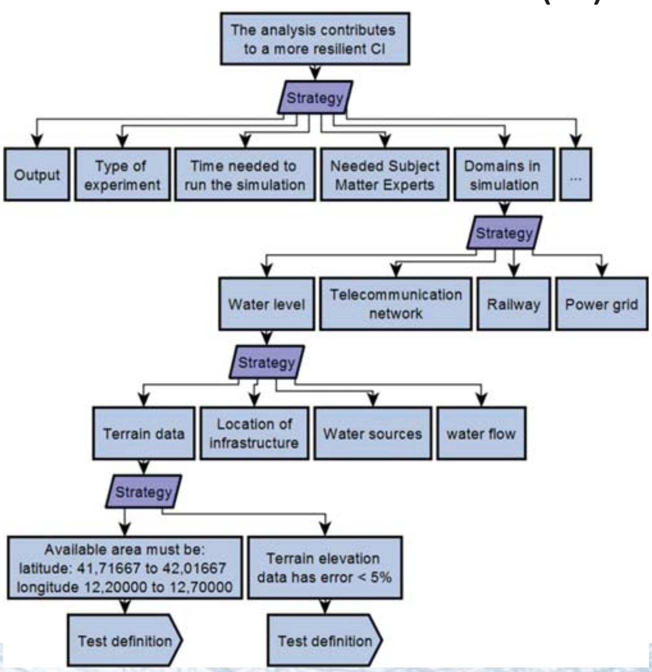
Argumentation network (1)



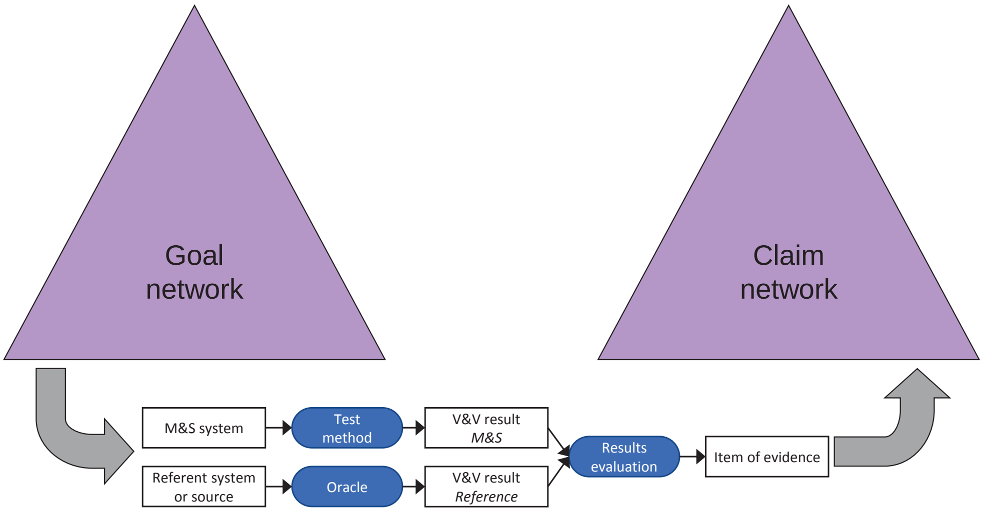
Argumentation network (2)



Argumentation network (2)

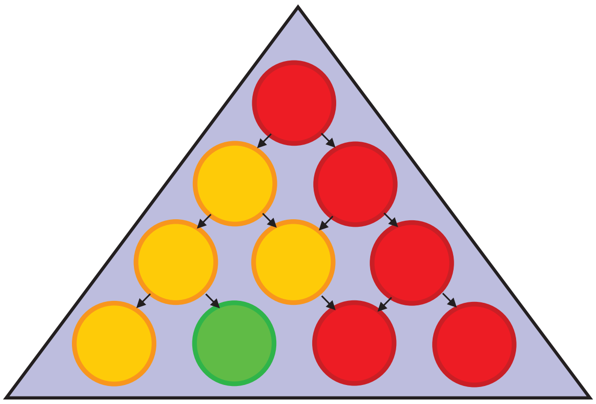


Argumentation network (3)

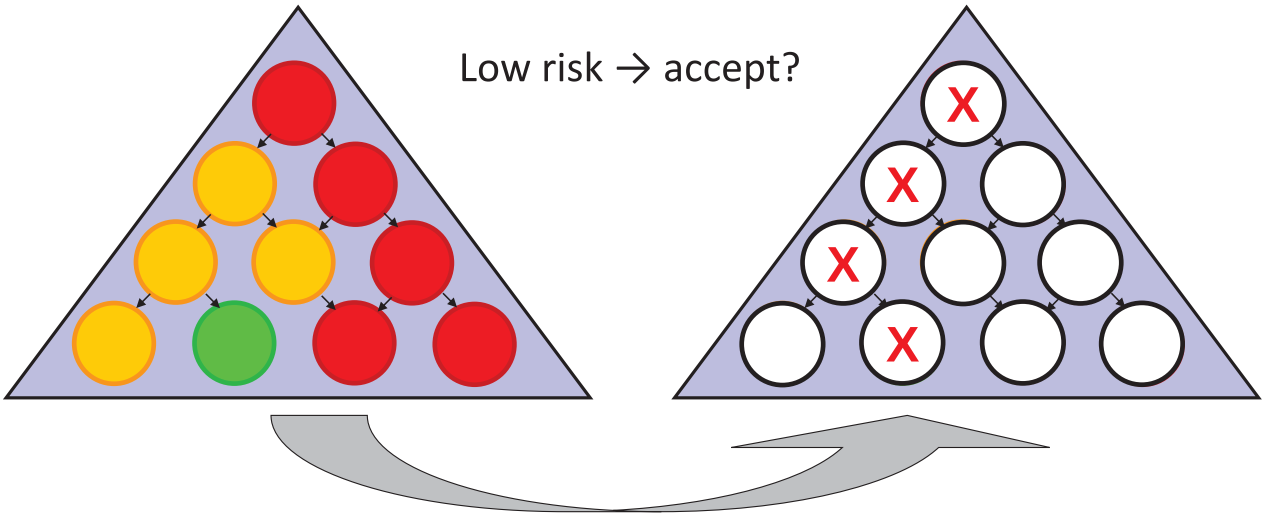


Risk decomposition

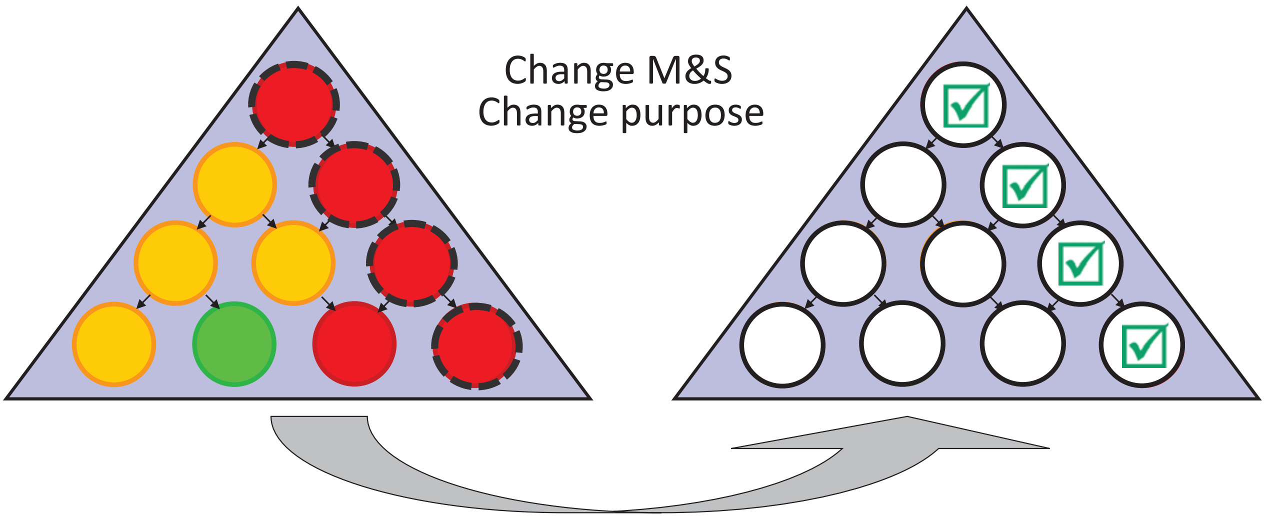
- Priorities
- Required certainty
- Specification of tests
  - resource distribution



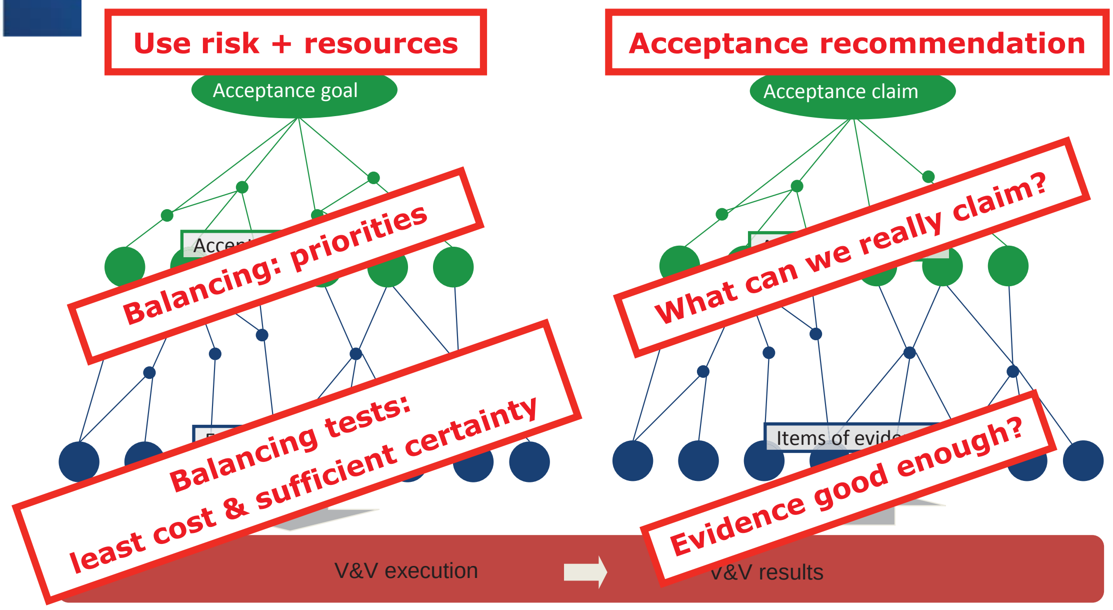
Not all criteria have been met! (1)



Not all criteria have been met! (2)



Project level



Enterprise level

- Execute and/or manage projects, provide training
- V&V expertise, tools, re-use, ...
- Q-tility is an implementation of the GM-VV enterprise level

Advantages of the structured approach (1)

- You start at the right point (effectiveness)
  - the risk of the user who applies the M&S results in the real world
- Re-usable domain knowledge (efficiency & effectiveness)
- Distribute the V&V work among all partners (efficiency)
  - V&V your own simulator (or you can assign it to another partner!)
- You can already do one branch of the Argumentation Network while waiting (efficiency)
  - you can already identify problems and fix them

Advantages of the structured approach (2)

- If a new M&S system replaces a current one, you know immediately which tests have to be performed (efficiency)
- You have a good idea of how complete your V&V work is (effectiveness)
  - at every disaggregation you have to show if it is complete or not
- You can assign priorities based on the risk (efficiency)
  - disaggregate the risk over the sub-nodes
- You can determine the required convincing force and assign resources such as budget, time, experts (efficiency)

Advantages of the structured approach (3)

- By standardizing the way the V&V work is documented, it is more easy to recall and re-use (efficiency)
  - re-use parts or the whole
  - no big problem if a key-person leaves your organization
- You can re-use the work over projects (efficiency)
  - if the M&S is re-used for a slightly different purpose, you can easily determine what additional tests have to be performed
  - add to what you already know → more and more complete → less chance you forget something (effectiveness)

Part 3

- You have to do V&V
  - because there is risk involved
- You have to do V&V in a structured way
  - if you want to do it more effective and more efficient
- You have to choose the right V&V technique
  - in order to balance the risk with the effectiveness and efficiency

How to choose the right V&V technique?

- Risk
  - the higher the risk, the more rigorous the technique
  - expected residual uncertainty
- Available means
  - budget, time, knowledge, testing facilities, ...
- Referent data
  - knowledge of the real world
- M&S system availability
  - access to development documents, M&S system internals

V&V techniques

- Balci [1998]
- Sargent [2010]
- M. Petty [2013]

Informal	Formal	Static	Dynamic
• Audit • Desk checking • Documentation Checking • Face validation • Inspections • Reviews • Turing test • Walkthroughs	• Induction • Inductive Assertions • Inference • Logical Deduction • Lambda Calculus • Predicate Calculus • Predicate Transformation • Proof of Correctness	• Cause-Effect Graphing • Control Analysis • Calling Structure Analysis • Concurrent Process Analysis • Control Flow Analysis • State Transition Analysis • Data Analysis • Data Dependency Analysis • Data Flow Analysis • Fault/Failure Analysis • Interface Analysis • Model Interface Analysis • User Interface Analysis • Semantic Analysis • Structural Analysis • Symbolic Evaluation • Syntax Analysis • Traceability Assessment	• Acceptance Testing • Alpha Testing • Assertion Checking • Beta Testing • Bottom-Up Testing • Comparison Testing • Compliance Testing • Authorization Testing • Performance Testing • Security Testing • Standards Testing • Debugging • Execution Testing • Execution Monitoring • Execution Profiling • Execution Tracing • Fault/Failure Insertion Testing • Field Testing • Functional (Black-Box)Testing • Graphical Comparisons • Interface Testing • Data Interface Testing • Model Interface Testing • User Interface Testing • Object-Flow Testing • Partition Testing • Predictive Validation • Product Testing • Regression Testing • Sensitivity Analysis • Special Input Testing • Boundary Value Testing • Equivalence Partitioning Testing • Extreme Input Testing • Invalid Input Testing • Real-Time Input Testing • Self-Driven Input Testing • Stress Testing • Trace-Driven Input Testing • Statistical Techniques • Structural (White-Box) Testing • Branch Testing • Condition Testing • Data Flow Testing • Loop Testing • Path Testing • Statement Testing • Submodel/Module Testing • Symbolic Debugging

4 basic categories of tests

- Informal
- Formal
- Static
- Dynamic

Informal tests

- Usually executed and interpreted by humans
- Typically few resources are required
- Convincing force depends on trust

- Techniques:
  - Audit, documentation checking, face validation, inspections, reviews, Turing test, walkthroughs

Formal tests

- Based on mathematical proofs of correctness
- Application often limited due to large resource costs
- Convincing force of the V&V results is very high

- Techniques:
  - Induction, inductive assertions, inference, logical deduction, lambda calculus, predicate calculus, predicate transformation, proof of correctness

Static tests

- Can be applied early in the development process
- Typically specialized tools are used
- Required resources are normally limited
- Access to documentation and half-products is required
- Convincing force depends on the rigor of the test

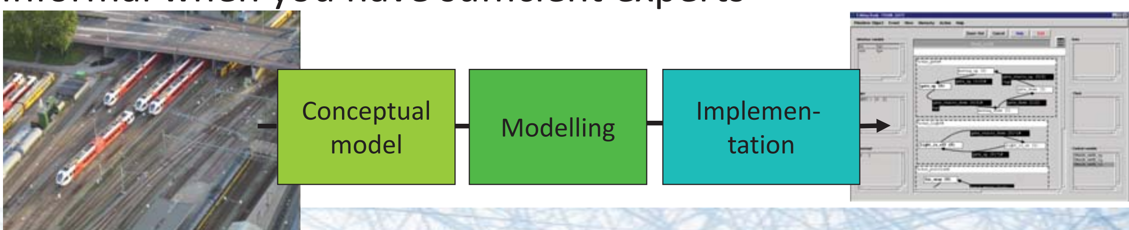
- Techniques:
  - Cause-effect graphing, control flow analysis, state transition analysis, data analysis, fault/failure analysis, interface analysis, semantic analysis, structural analysis, symbolic evaluation, syntax analysis

Dynamic tests

- Execution of (part of) M&S system is required
- Dynamic properties of the M&S system are studied
- Typically specialized tools are used
- Required resources are normally limited
- Access to internals of the M&S system may be required
- Convincing force depends on the rigor of the test
- Techniques:
  - Comparison testing, compliance testing, performance testing, security testing, standards testing, debugging, execution testing, fault/failure insertion testing

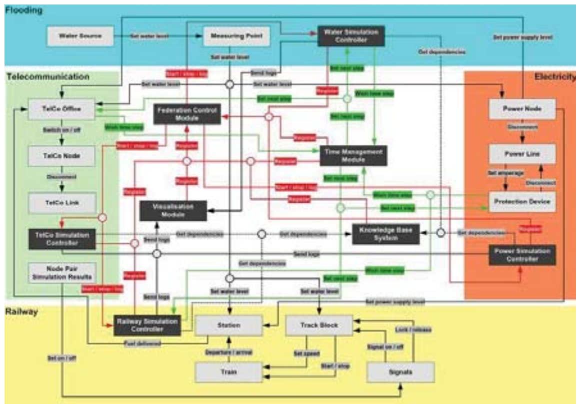
During development

- Static
  - models, design documents
- Dynamic when parts become available
  - (parts of) implementations
- Formal if you have sufficient resources
- Informal when you have sufficient experts



After development (but before use!)

- Dynamic
  - Components of the simulation, interoperability between components, emerging behaviour: cascading failures



- Informal
  - Face validation
  - Walkthroughs

'Take home' messages

- You have to do V&V
  - because there is risk involved
- You have to do V&V in a structured way
  - if you want to do it more effective and more efficient
- You have to choose the right V&V technique
  - in order to balance the risk with the effectiveness and efficiency

References

- SISO. GM-VV Vol. 1: introduction and overview, SISO-GUIDE-001.1–2012, October, 2012
- SISO. GM-VV Vol. 2: implementation guide, SISO-GUIDE-001.2-2013, June 2013
- SISO. GM-VV Vol. 3: reference manual, SISO-REF-039-2013, December 2013
- Q-tility, q-tility.nl
- O. Balci, "Verification, Validation, and Testing", in J. Banks (Editor), Handbook of Simulation: Principles, Advances, Applications, and Practice, John Wiley & Sons, New York NY, 1998, pp. 335-393
- Mikel D. Petty, "Model Verification and Validation Methods", I/ITSEC tutorial 2013
- Robert G. Sargent, "VERIFICATION AND VALIDATION OF SIMULATION MODELS", Proceedings of the 2010 Winter Simulation Conference, B. Johansson, S. Jain, J. Montoya-Torres, J. Hugan, and E. Yücesan, eds

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Cyber Threats to CI

Rafał Kozik – UTP University of Technology and Science in Bydgoszcz, Poland

rafal.kozik@utp.edu.pl

Modelling, Simulation and Analysis of Critical Infrastructures
CIPRNet Course

UCBM Headquarters – Rome (Italy) – 9-10 July 2015

Outline

- Introduction
  - importance of cyber security
  - increasing number of dependencies
- CI-related Cyber Incidents
  - case studies
  - current challenges
- How to model cyber aspects
  - cyber risk evaluation
  - system and attacker behaviour modelling
- Conclusions

Introduction

- Nowadays, there is a significant effort focused on **national critical infrastructure** evaluation, simulation and threat analysis
- EU is still lacking an infrastructure **simulation and analysis centre** that will allow for fast and adequate response to a complex emergencies affecting or originating from critical infrastructures
- Current study shows that **cyber-related** threats should be concerned as **significantly contributing** factors incorporated into strategic analysis of infrastructure disruptions, consequences evaluation, and assessment of systems dependencies

Increasing number of dependencies – ICS[1] vs. ICT[2]

- Information and communication technology
- Finance
- Manufacturing
- Food
- Health
- Energy
- Water
- …

- Information Management Systems
- Internet Technologies
- Communication systems
- GIS systems
- …

[1]ICS – Industrial Control System
[2]ICT – Information and Communication Technologies

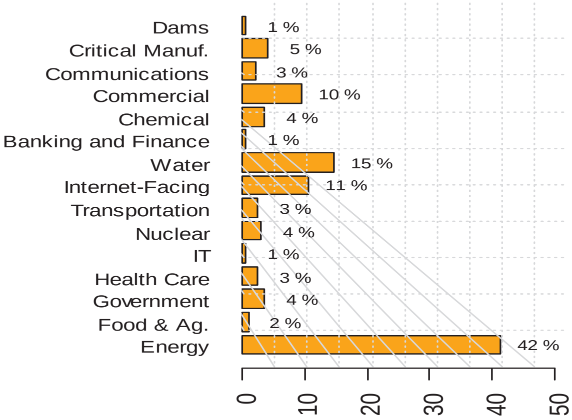
ICS cyber incidents - case studies

- Attacks on power grids and nuclear facilities
  - nuclear processing facilities had been infected with malicious software called Stuxnet, BlackEnergy, Havex
- Water sector
  - Australian SCADA system - hacker has released over 264,000 gallons of raw sewage
  - US water filtering plant - attacker uploaded malware that was able to affect the water treatment processes
  - Illinois water pump burn out – hacker attacked remotely SCADA system
- Healthcare
  - Chicago area hospital-all operations back to the paper age
  - Dutch Groene Hart Hospital - sensitive data of more than 100 000 patients were stolen
- Information and Financial Systems
  - DDoS attacks (part of military conflict) were targeted at servers of National Bank of Georgia in order to paralyze the Republic of Georgia and the society

ICS cyber incidents - case studies

- Attacks targeting Industrial Control System, causing malfunction/failure of ICT system without consequences to controlled industrial processes or/and CI
  - weakly connected with open network trough controlling system
  - only less relevant aspects of industrial process are controlled remotely
  - there is redundancy in infrastructure (e.g. stock exchange)
- Attacks targeting Industrial Control System, causing malfunction/failure of ICT system and having impact on CI and/or controlled industrial process
  - example: Stuxnet
- Attacks targeting Industrial Control System, that consequences have a cascading impact both on controlled industrial process and other depending systems
  - example: Port of Houston case - collateral damages from DDoS attack conducted on a communication infrastructure of the ISP

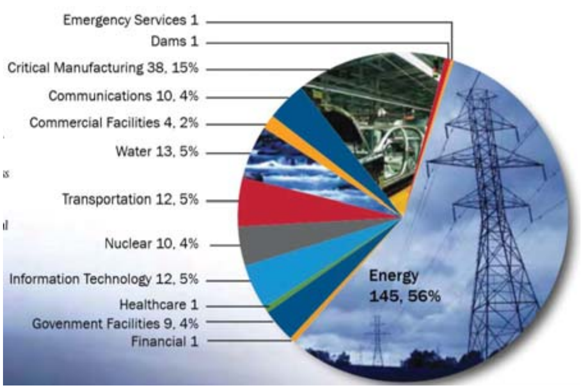
Statistics– 2012 (1/3)



https://ics-cert.us-cert.gov

- 198 incidents handled
- 42% related to Energy sector
- 15% related to Water sector

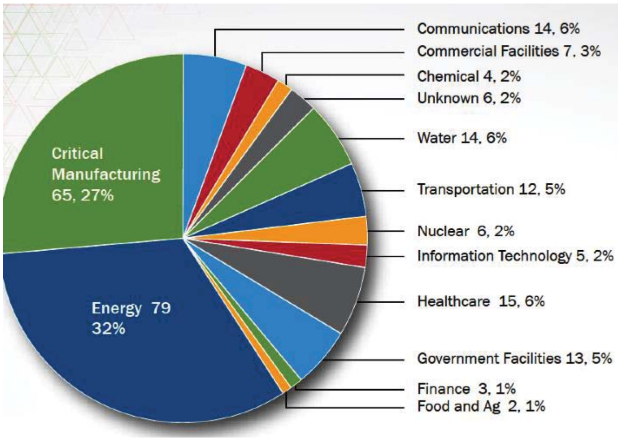
Statistics– 2013 (2/3)



https://ics-cert.us-cert.gov

- US ICS-CERT handled **235** incidents
- 56% related to Energy sector
- 13.5% related to water sector

Statistics– 2014 (3/3)



https://ics-cert.us-cert.gov

- US ICS-CERT handled 245 incidents
- 32% related to Energy sector
- 65% Critical Manufacturing
- 14.6% related to Water sector

Increasing volume of data

- PandaLabs neutralized 75 million new malware samples in 2014, twice as many as in 2013
- „Antivirus signatures exist, they're still important, just not the most important…”

  -- Eugene Kaspersky
- „… antivirus is dead …”

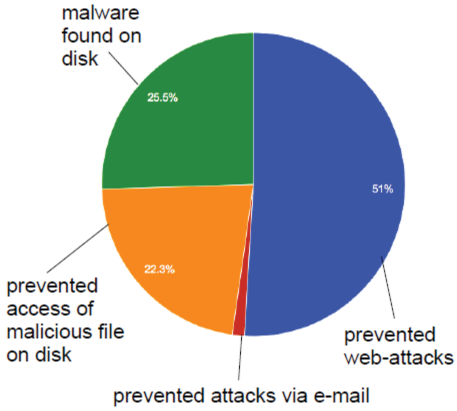
  -- Symantec's senior vice president Brian Dye, May, 2014

Common technologies everywhere

- Have access anytime and anywhere
- No compatibility issues
- No installation
- Fast and responsive
- A collaborative working environment

Cyber attacks – current trends

- Recently there is an **increasing** number of security incidents reported all over the world
- Among all attack targeted on **web-servers** the injection attacks still remains one of the most important network threat which is ranked as one of the top threats in the MITRE and OWASP list:
  1. Injection attacks
  2. Broken Authentication and Session Management
  3. Cross Site Scripting - XSS
  4. Insecure Direct Object References
  5. Security Misconfiguration
  6. Sensitive Data Exposure
  7. …



Source: Kaspersky Lab

SQL Injection

Server Code

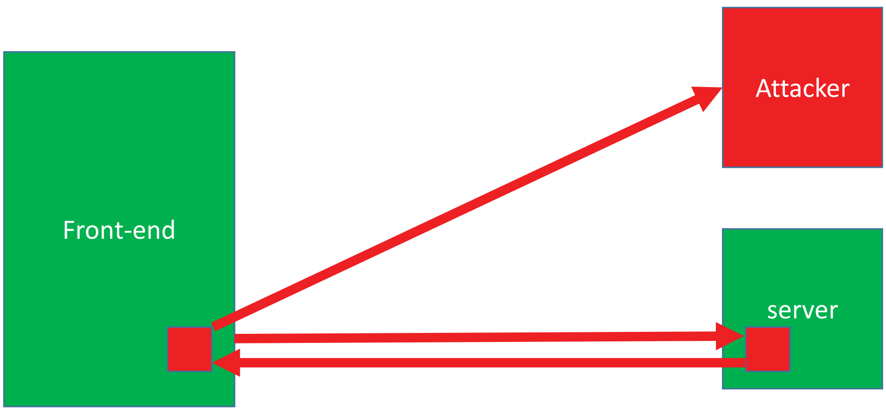
```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

Server Result

```
SELECT * FROM Users WHERE UserId = 105 or 1=1
```

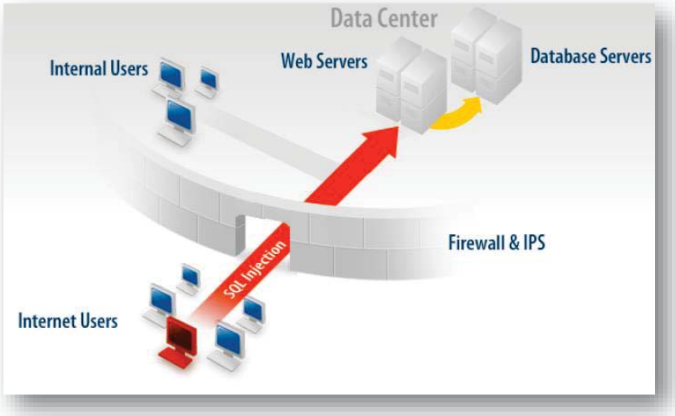
Privilege escalation

XSS – Cross Site Scripting



Application layer attacks

- IPS (Intrusion Prevention Systems) are infective solutions for application layer attacks detection



http://www.imperva.com/

Havex case

- *„..In 2014, attackers began distributing new versions of a remote access Trojan (RAT) program called Havex* ***by hacking into the websites of industrial control system*** *(ICS) manufacturers and poisoning their legitimate software downloads…"*

F-Secure

- 88 variants of the Havex RAT used to gain access to, and harvest data from, networks and machines of interest
- Trojanized installers planted on compromised vendor sites
  - attackers chose to compromise an intermediary target - the ICS vendor site - in order to gain access to the actual targets
  - attackers abuse vulnerabilities in the software used to run the websites to break in and replace legitimate software installers available for download to customers

Application layer attacks

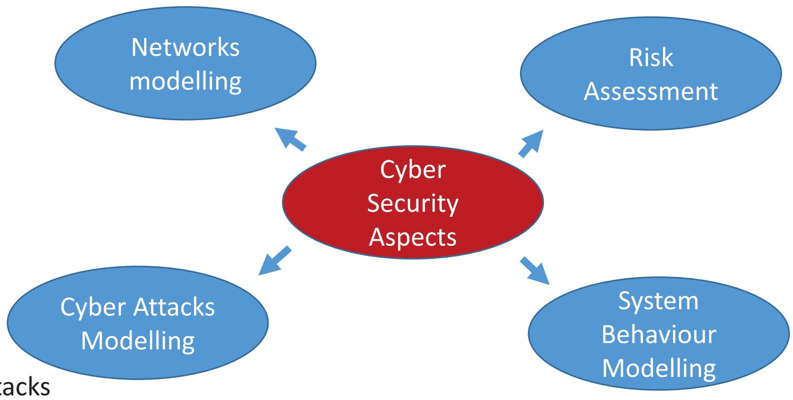
- IPS (Intrusion Prevention Systems) are infective solutions for application layer attacks detection
- There are many combination to obfuscate the injection (evasion techniques)
- It is easier to understand the protected application and model it normal behaviour

http://www.imperva.com/

What cyber security aspects can be modelled ?

Identify impact of attacks (DDoS, flooding) on connected assists

Assess probability that attack will be successfully conducted (What will happen if…)



Detect anomalies in system behaviour

Match symptoms of attacks with models to recognize them on time

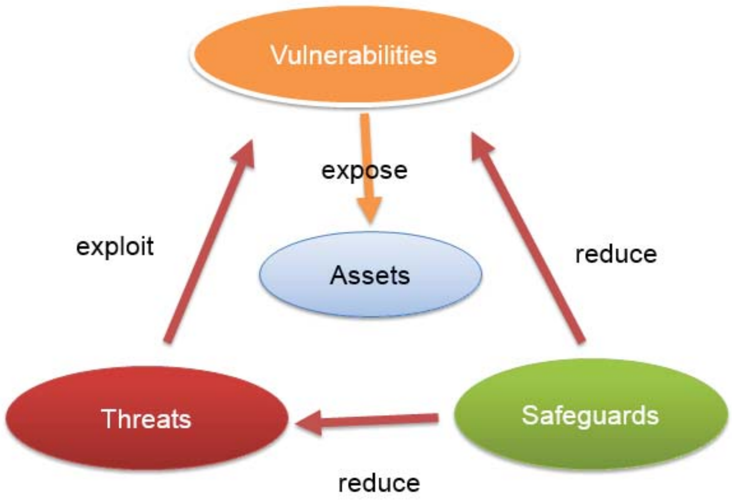
Network modelling

- The goal is to evaluate the influence of a given cyber incident on whole infrastructure of connected assets.
- Some tools allows for very detailed description of analysed system of systems (connections, bandwidth, applications types, routers, etc.).
- These can be used to identify the influence of bandwidth saturation (e.g. caused by DDoS attacks) on quality of provided services.
- However, these are difficult to analyse impact of web-layer attacks (e.g. SQLi, XSS, etc.)

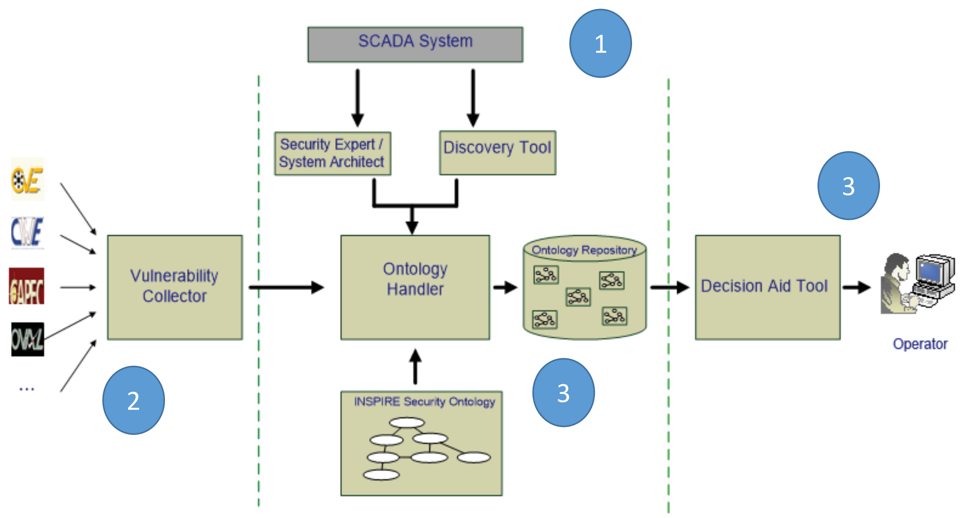
Risk assessment

- The goal is to evaluate the probability that an intelligent threat agent could successfully implement an attack (the probabilities can be used to calculate risk according to adapted methodology).
- It is assumed that in a given scenario the threat agent may implement a complex attack vector (including several steps) in order to achieve a goal.
- Analysed infrastructure can be modelled with varying granularity (as a black box system or detailed network of connected assets).
- The result of the analysis is a set of prioritised countermeasures.

Assets and vulnerabilities

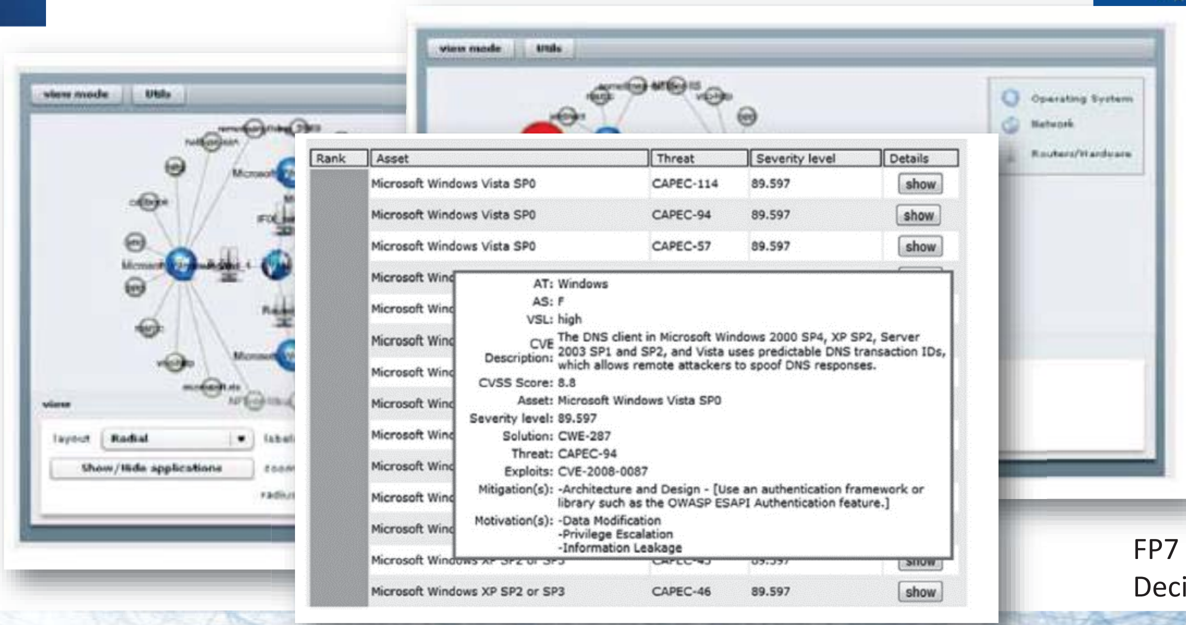


Example[1] of analysis workflow



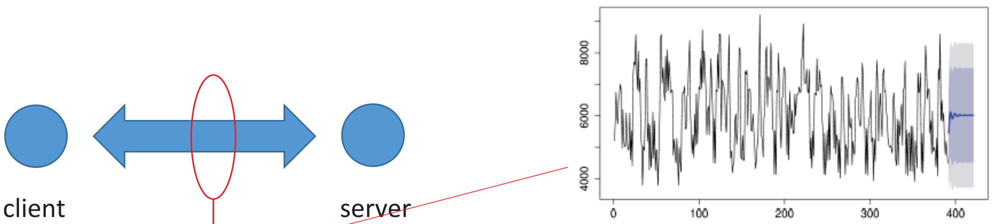
[1] Choras Michal, Kozik R., Flizikowski A. **FP7 INSPIRE Decision Aid Tool**: a Support for Risk Management and Cyber Protection of Critical Infrastructures , Telecommunications Review, vol. 8-9, p. 1215-1221, 2012.

Example of result analysis



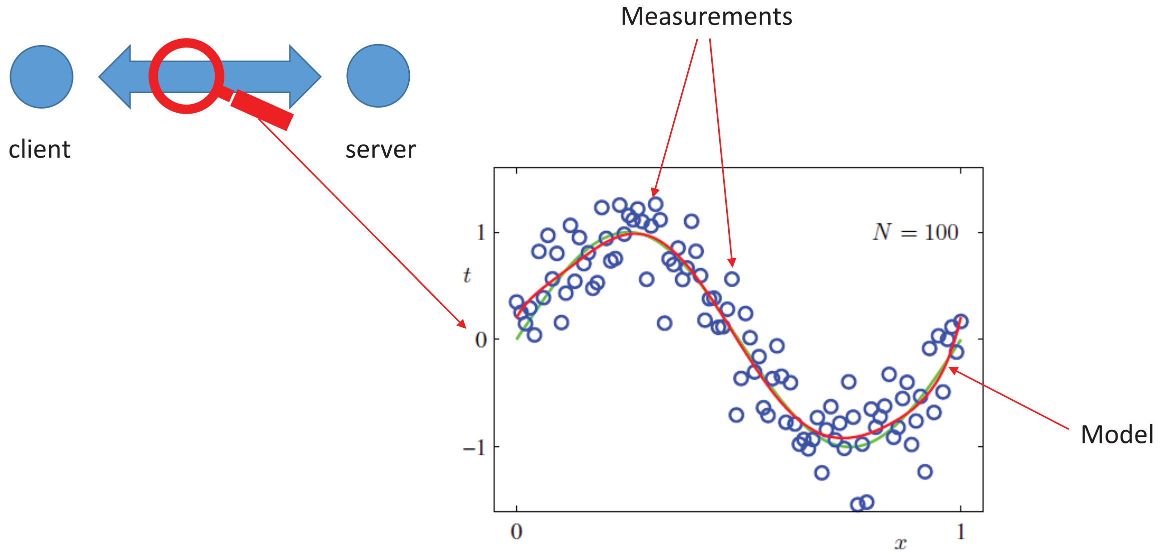
FP7 INSPIRE
Decision Aid Tool

System behaviour modelling

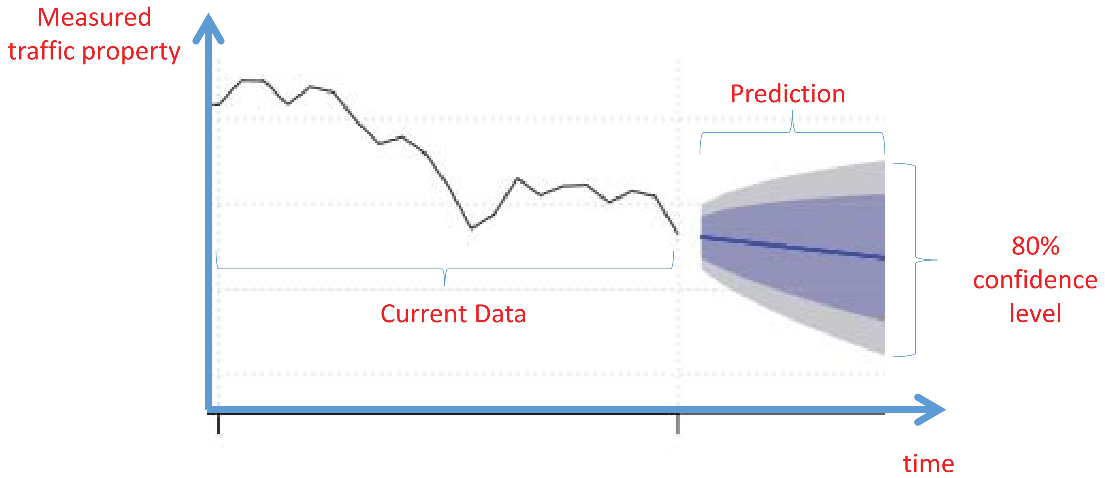


f1 - Duration: the length (number of seconds) of the connection,
f2 - Service: the connection's service type, e.g., http, telnet, etc.,
f3 - Source bytes: the number of data bytes sent by the source IP address,
f4 - Destination bytes: the number of data bytes sent by the destination IP address,
f5 - Count: the number of connections whose source IP address and destination IP address are the same to those of the current connection in the past two seconds,
f6 - Same srv rate: % of connections to the same service in Count feature,
f7 - Error rate: % of connections that have "SYN" errors in Count feature,
f8 - Srv error rate: % of connections that have "SYN" errors in Srv count(the number of connections whose service type is the same to that of the current connection in the past two seconds) feature,
f9 - Dst host count: among the past 100 connections whose destination IP address is the same to that of the current connection, the number of connections whose source IP address is also the same to that of the current connection,
f10 - Dst host srv count: among the past 100 connections whose destination IP address is the same to that of the current connection, the number of connections whose service type is also the same to that of the current connection,

System behaviour modelling – example



System behaviour modelling – predicting



Example of formal model

ARFIMA(p,d,q)
Autoregressive Fractional Integrated Moving Average

the time series

moving average polynomial

white noise process with zero mean

$$\Phi(L)(1-L)^d y_t = \Theta(L)\varepsilon_t, \quad t = 1, 2, \ldots T,$$

$$\Phi(L) = 1 - \phi_1 L - \phi_2 L^2 - \ldots - \phi_p L^p$$

autoregressive polynomial

$$(1-L)^d = \sum_{k=0}^{\infty} \binom{d}{k} (-1)^k L^k$$

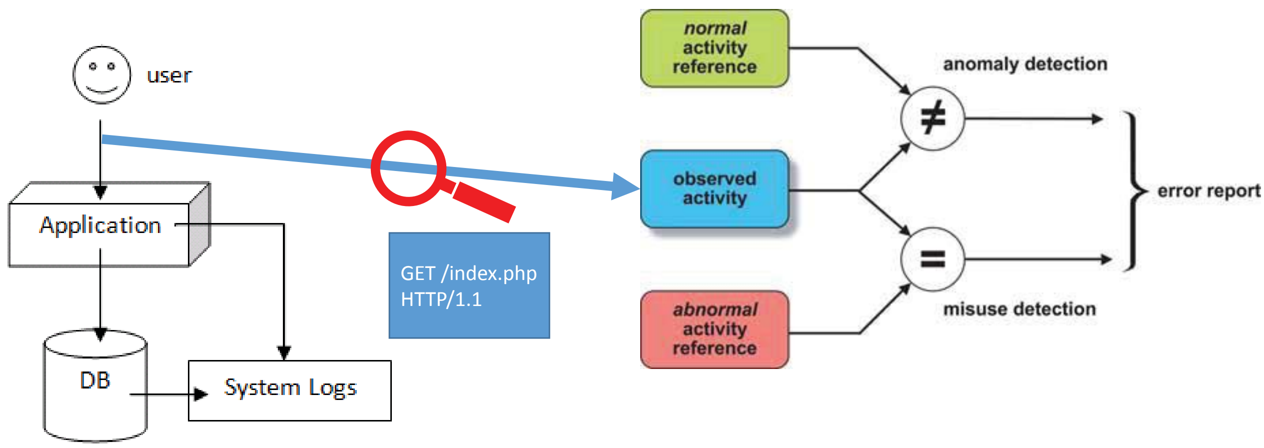
backward shift operator

fractional differencing operator

$$\hat{Y}(t) = \mu + \phi_1 Y(t-1)$$

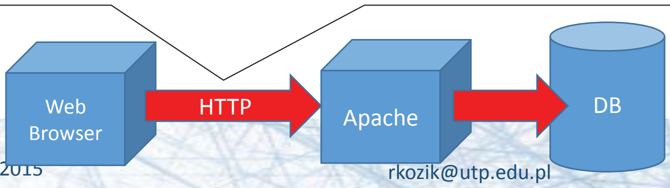
$$\hat{Y}(t) = \mu + Y(t-1) + \phi_1 (Y(t-1) - Y(t-2))$$

Looking inside the packet

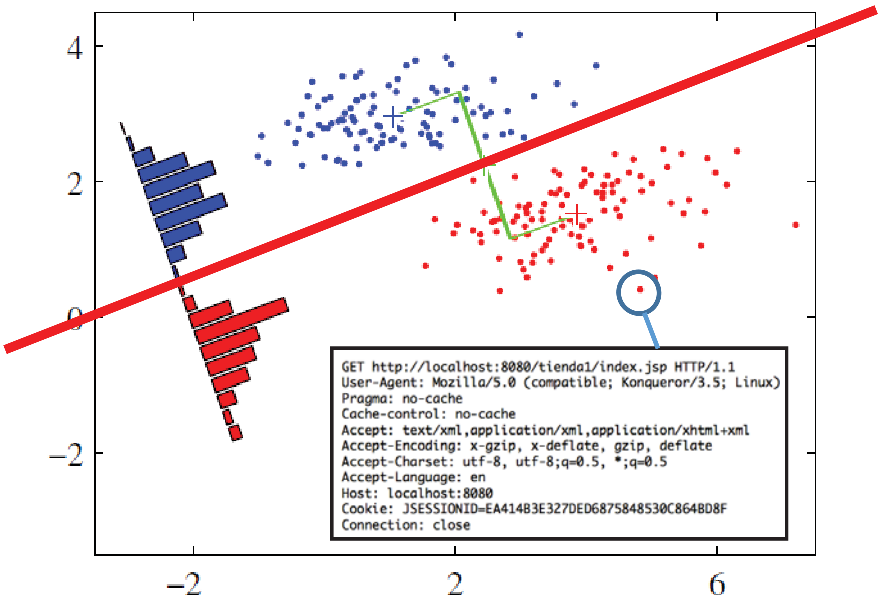


Looking inside the packet

```
GET http://localhost:8080/tienda1/index.jsp HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; Konqueror/3.5; Linux)
Pragma: no-cache
Cache-control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml
Accept-Encoding: x-gzip, x-deflate, gzip, deflate
Accept-Charset: utf-8, utf-8;q=0.5, *;q=0.5
Accept-Language: en
Host: localhost:8080
Cookie: JSESSIONID=EA414B3E327DED6875848530C864BD8F
Connection: close
```



Classification problem



Data encoding

Dictionary
1: i
2: id
3: id=
4: id=1
…

HTTP params

Id=1&method=add&sid=1&value=5&commit=true

ENCODE

Vector:
4
55
33
11
…

Calculate histogram

Vector of constant length

Data encoding

Dictionary
1: i
2: id

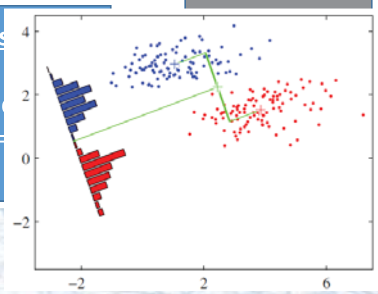
Classifier

Decision: Anomalous/Normal

What could it be ? SQLI, XSS, CRF, etc.

HTTP params

Id=1&metho
sid=1&value=
mit=true



Vector:
4
55
33
11
…

Calculate histogram

Vector of constant length

Structure modelling

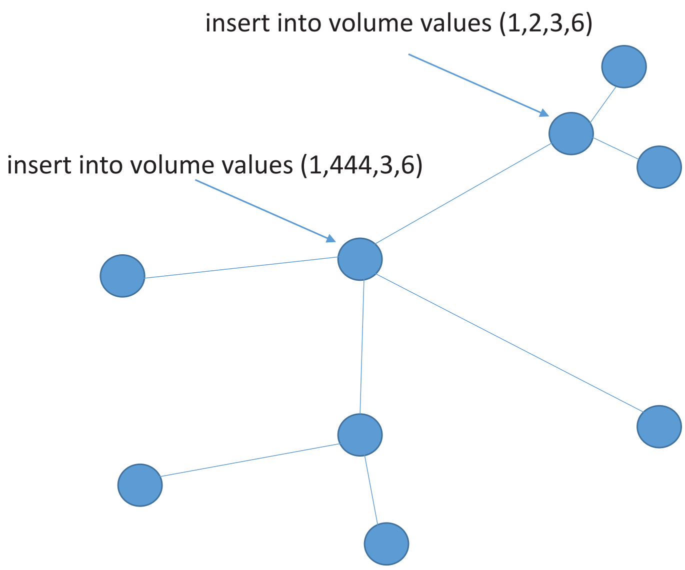
Inut data:

insert into volume values (1,2,3,6)
select * from volume where id=11
select id,name from volume where id=33
insert into volume values (1,2,dunno,6)
insert into volume values (1,2,dunno dunno dunno,6)
select id1,name from volume where id=abc
select * from volume where id=234

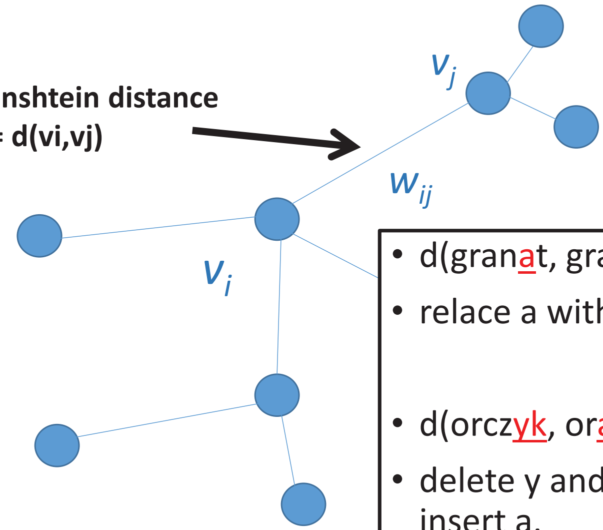
- Genetic algorithm
- Graph-based clustering
- Dynamic programing

Result:

rule-0: insert into volume values (1,2,[a-z0-9]+,6)
rule-1: select [a-z0-9*,]+ from volume where id=[a-z0-9]+

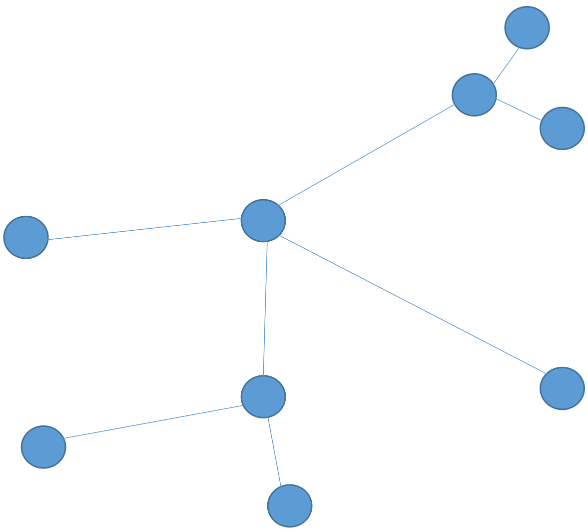


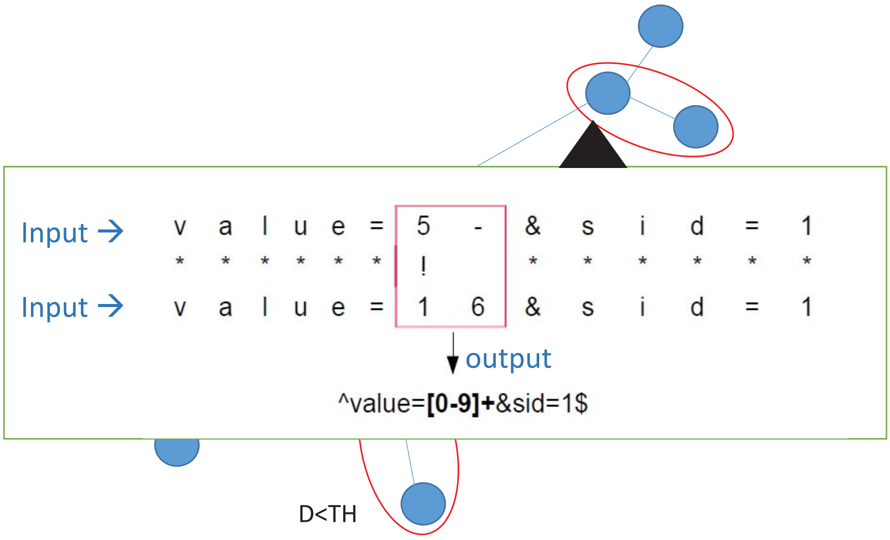
Levenshtein distance
wij = d(vi,vj)

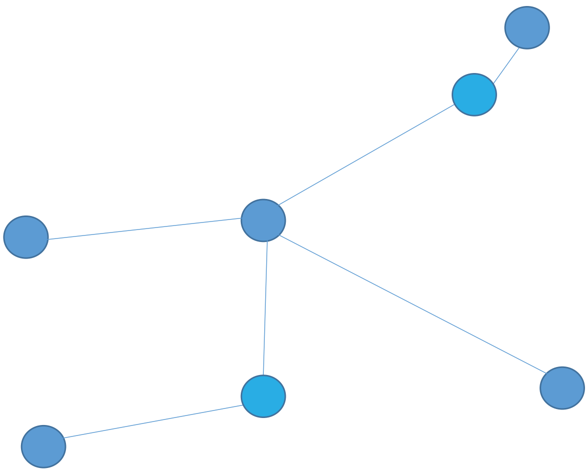


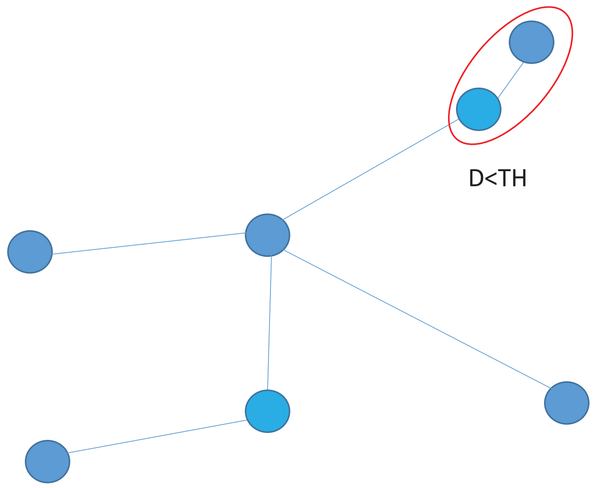
- d(granat, granit) = 1
- relace a with i

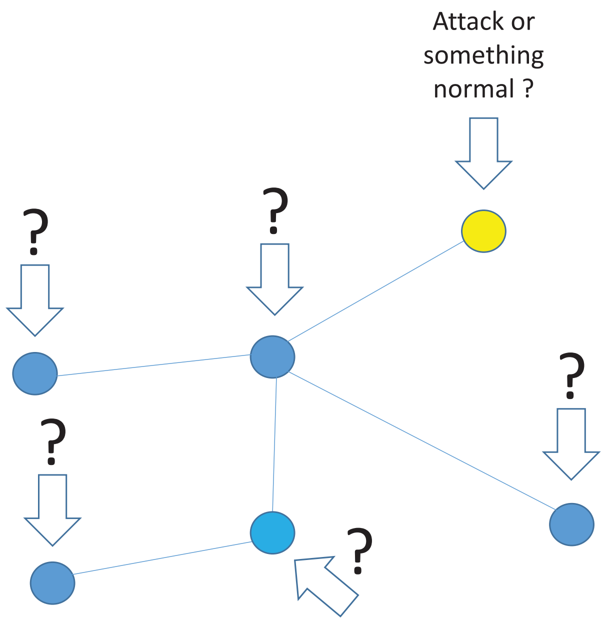
- d(orczyk, oracz) = 3
- delete y and k and insert a.



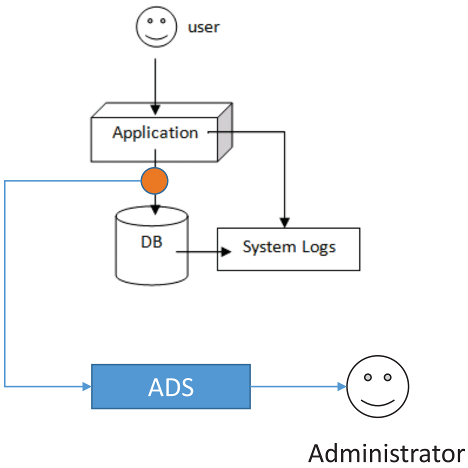

Input →
v a l u e = 5 - & s i d = 1
* * * * * * ! * * * * * *
Input →
v a l u e = 1 6 & s i d = 1
output
^value=**[0-9]+**&sid=1$
D<TH

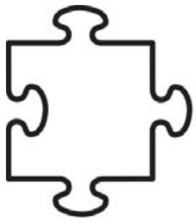



D<TH


Attack or
something
normal ?
?
?
?
?
?

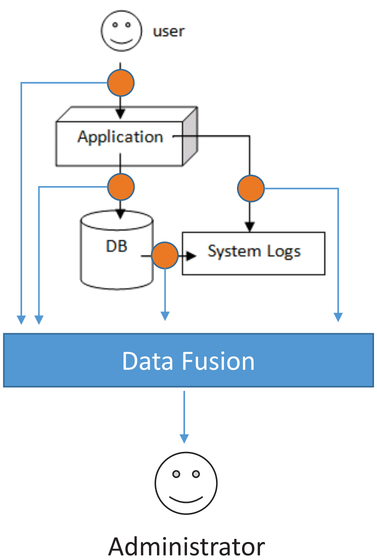
Data correlation – bigger operational picture

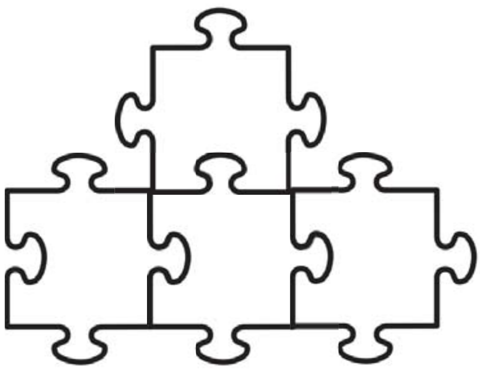




operational picture

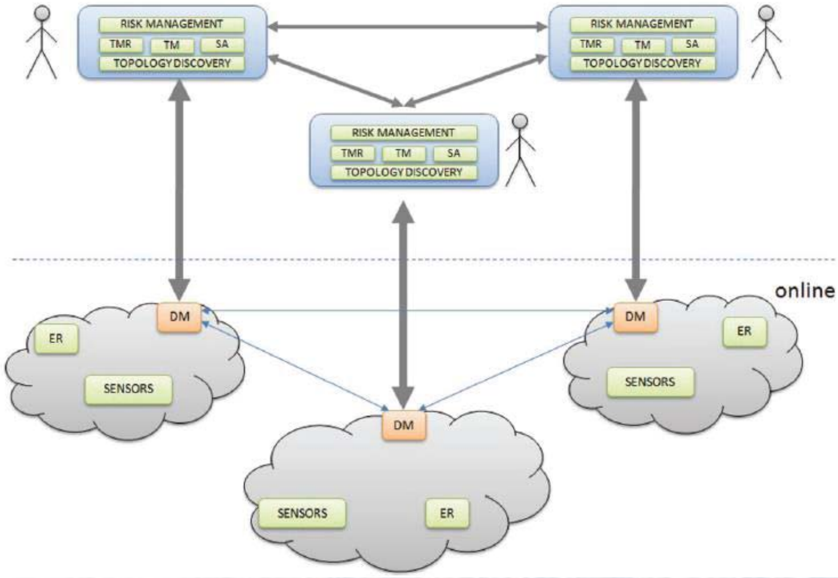
Data correlation

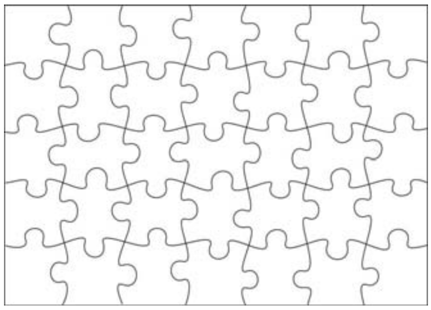




operational picture

Data correlation




operational picture

Conclusions

- I presented:
  - current trends and challenges (with respect to cyber security aspects) in critical infrastructures protection were presented
  - an overview of cyber incidents impacting critical infrastructures have been described
  - different approaches to cyber security aspects modelling have been presented
- there is no perfect method to address cyber security aspects:
  - risk analysis and security audits allows for evaluating cyber security posture, but they are missing real-time data
  - on-line/host-based cyber security allows for rapid threat detection, but theses are missing the big operational picture
- presented techniques are currently gaining in popularity since these allows achieving better results in contrast to classical signature-based approaches

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Introduction to Decision Support Systems

Maria Carla De Maggio (UCBM)
m.demaggio@unicampus.it

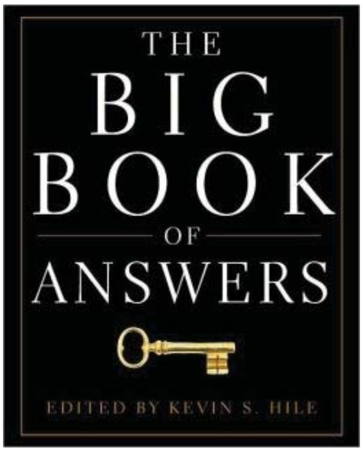
Modelling, Simulation and Analysis of Critical Infrastructure
Course inside the Master in Homeland Security (Edition 2)

Università Campus Bio-Medico di Roma (Italy) – 9-10 July 2015

Objectives of this lesson

- What is a Decision Support System
- Brief history of DSS
- Benefits and scope of a DSS
- Types and components of a DSS
- DSS for CI applications

What is a DSS

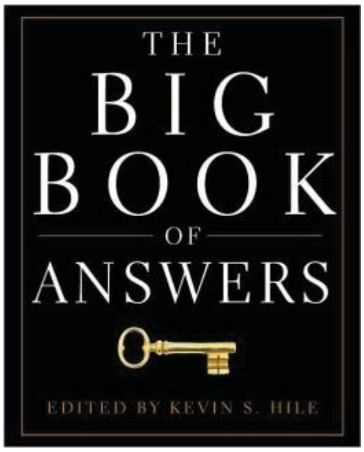


DSS definitions

1970	“Model-based set of procedures for **processing data and judgments** to assist a manager in his decision making (*sic*)” [Little]
1978	“Decision Support Systems **couple the intellectual resources of individuals with the capabilities of the computer to improve the quality of decisions**. It is a computer-based support system for management decision makers who deal with **semi-structured problems**” [Keen and Scott Morton]
1984	“A decision support system is an **interactive system** that provides the user with easy access to decision models and data in order to support semi-structured and **unstructured** decision-making tasks” [Mann and Watson]
1989	“a computer-based information **system consisting of hardware/software and the human element** designed to assist **any decision-maker at any level**. However, the emphasis is on semi-structured and unstructured tasks” [Bidgoli]
1996	Computer-based systems that help decision makers confront ill-structured problems through **direct interaction with data and analysis models** [Sprague and Watson]
1997	DSS are computer-based systems that **bring together information** from a variety of sources, assist in the organisation and **analysis of information** and **facilitate the evaluation** of assumptions underlying the use of **specific models** [Sauter]
2005	“A computer-based information system that **combines models and data** in an attempt **to solve semi-structured and some unstructured problems with extensive user involvement**” [Turban, Rainer, and Potter]

What is a DSS

A decision support system (DSS) is a computer program application that analyzes (business) data and presents it so that users can make (business) decisions more easily. It is an "*informational application*" (to distinguish it from an "operational application" that collects the data in the course of normal business operation).



What is a DSS

Decision

- Focus on decision-making in a problem situation rather than the subordinate activities of simple information retrieval, processing or reporting

Support

- Computer technologies help for decisions, but not substitute the decision maker

System

- Integrated nature of the overall approach, suggesting the wider context of machine, user and decision environment (data, methodologies…)

[U. R. Averweg]

Decision process

Intelligence
- Internal and external data collection

Design
- Understanding the problem, solutions analysis

Choice
- Evaluation and choice through a set of parameters and indices
- Comparisons and forecasting

Implementation
- Result verification
- Feedback

Brief history of DSS (1/2)

Before 1965

- **Management Information Systems** (MIS) in large companies (Davis, 1974). MIS focused on providing managers with **structured, periodic reports**. Much of the information was from accounting and transaction systems.

Late 1960'

- **Model-oriented DSS or management decision systems**. Two DSS pioneers, Peter Keen and Charles Stabell, claim the **concept of decision support** evolved from "the theoretical studies of organizational decision-making done at the Carnegie Institute of Technology during the late 1950s and early '60s and the technical work on interactive computer systems, mainly carried out at the Massachusetts Institute of Technology in the 1960s. (Keen and Scott Morton, 1978 preface)"

1971

- DSS for portfolio management: Sloan Management Review article titled "**The Design of Man-Machine Decision Systems: An Application to Portfolio Management**". His system was designed to support investment managers in their daily administration of a clients' stock portfolio. DSS for portfolio management have become very sophisticated since Gerrity began his research.

Brief history of DSS (2/2)

1974

- Gordon Davis defined a Management Information System as "an **integrated, man/machine system** for providing information to support the operations, management, and **decision-making functions** in an organization." Davis's work created the setting for the development of a broad foundation for DSS research and practice.

1980'

- 1980: First International Conference on Decision Support Systems was held in Atlanta, Georgia
- 1979: John Rockart published an article leading to the development of executive information systems (EISs) or executive support systems (ESS).
- Executive Information Systems (EIS) evolved from single user model-driven Decision Support systems and improved relational database products
- 1989: Howard Dresner introduced the concept of **Business Intelligence** referring to data-driven DSS

1990'

- Technology shift: introduction of desktop On-Line Analytical Processing tools, web-based and web-enabled DSS

[D. J. Power]

Peculiarities of a DSS

- Easy to use and flexible interface
- Interactive environment
- Support for unstructured and semi-structured problem solving
- Efficient models for the analysis of data
- System flexibility in order to be part of the decisional process

DSS types (1/5)

- **Communication-driven DSS**
  Most communications-driven DSSs are targeted at internal teams, including partners. Its purpose are to help conduct a meeting, or for users to collaborate. The most common technology used to deploy the DSS is a web or client server.

DSS types (2/5)

- **Data-driven DSS**
  Most data-driven DSSs are targeted at managers, staff and also product/service suppliers. It is used to query a database or data warehouse to seek specific answers for specific purposes. It is deployed via a main frame system, client/server link, or via the web.

DSS types (3/5)

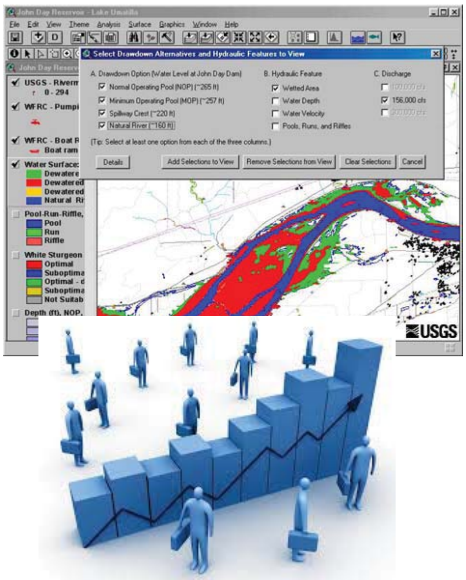
- **Document-driven DSS**
  Document-driven DSSs are more common, targeted at a broad base of user groups. The purpose of such a DSS is to search web pages and find documents on a specific set of keywords or search terms. The usual technology used to set up such DSSs are via the web or a client/server system.

DSS types (4/5)

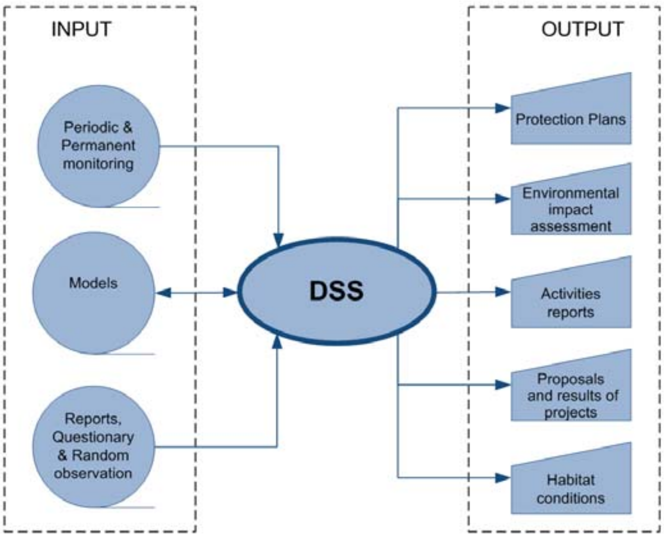
- **Knowledge-driven DSS:**
  Knowledge-driven DSSs or 'knowledgebase' is a catch-all category covering a broad range of systems. The "expertise" consists of knowledge about a particular problem domain, understanding of problems within that domain, and "skill" at solving one or some of these problems. The generic tasks include classification, configuration, diagnosis, interpretation, planning and prediction. The typical deployment technology used to set up such systems could be client/server systems, the web, or software running on stand-alone PCs.

DSS types (5/5)

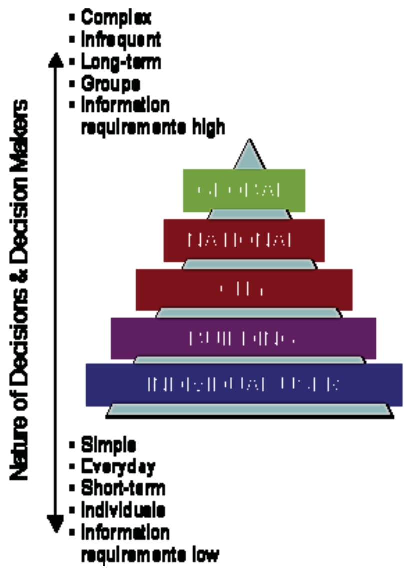
- **Model-driven DSS**
  Model-driven DSSs are complex systems that help analyse decisions or choose between different options. They emphasize access to and manipulation of a model, for example, statistical, financial, optimization and/or simulation models. These DSSs can be deployed via software/hardware in stand-alone PCs, client/server systems, or the web.



Components of a DSS



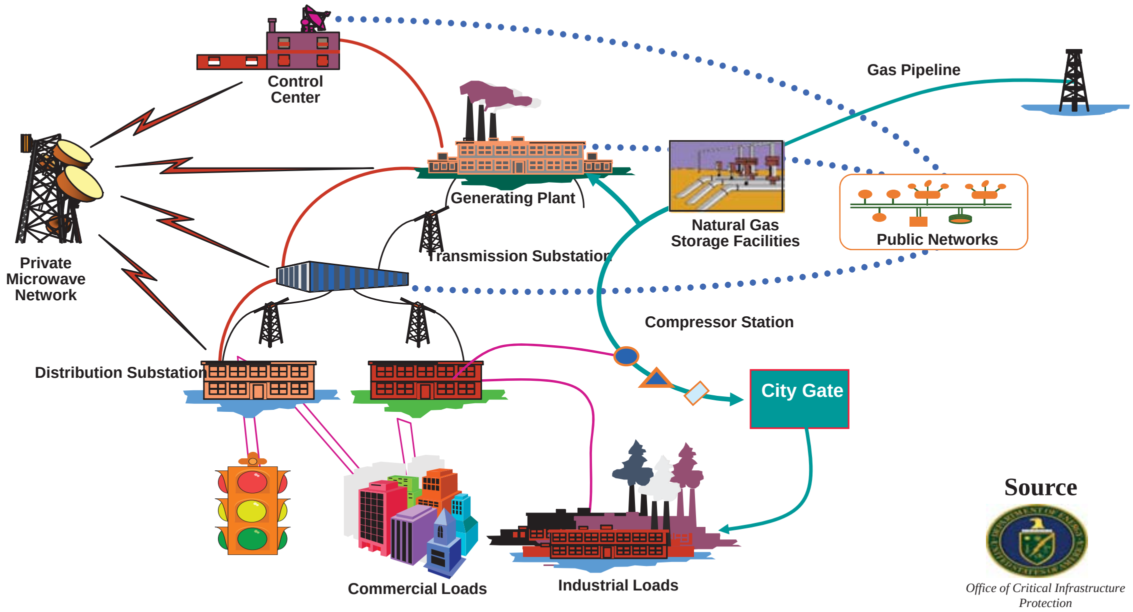
Benefits and scope of a DSS



DSS application domains

- Business and management applications
- Financial Planning System
- Clinical DSS
- CRITICAL INFRASTRUCTURES
- Marketing and strategy DSS
- Business Intelligence

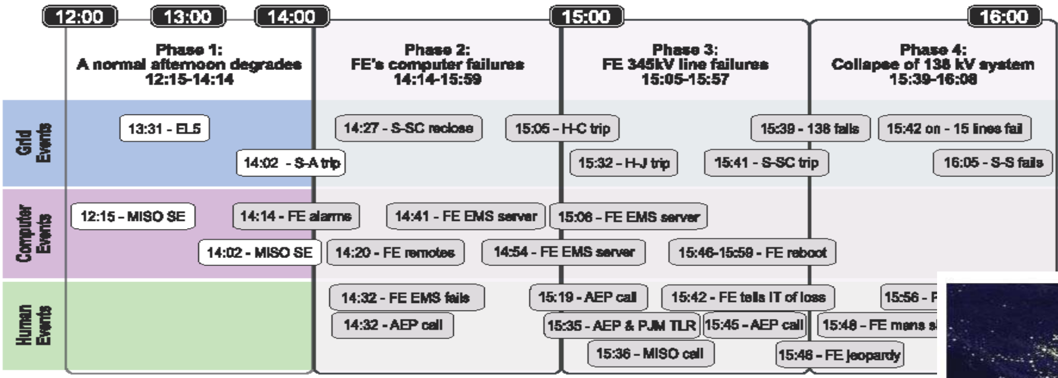
Why to use a DSS for CIs



Peculiarities of a DSS for CI

INPUT		DSS	OUTPUT
Open source data		Threat analysis	Damage scenario
CI's data	***Physical*** *Interd.* ***Cyber*** *Interd.* ***Geographical*** *Interd.* ***Logical*** *Interd.*	Vulnerability analysis	Impact scenario
External data	***Sociological*** *Interd.*	Forecasting	Consequence analysis
		Simulations	Supporting tools for crisis management

The human factor

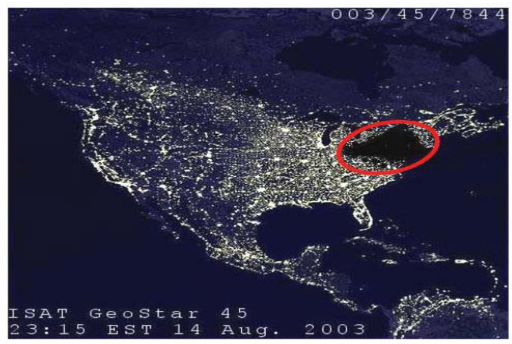


2003 North America blackout

50 million people affected

Estimated cost: 4,5 B$ - 8.2 B$

https://reports.energy.gov/



Summary

- A DSS is a system helping decisions, which practice is influenced by several disciplines: computer science, artificial intelligence, engineering, psychology, management theories…
- A DSS is a complex system integrating data and knowledge, that needs a continue update
- A DSS in any case substitutes the human decisions
- The theory of DSS is continuously evolving

Maria Carla De Maggio
Complex Systems & Security Lab
University Campus Bio-Medico of Rome
m.demaggio@unicampus.it

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Geographical Information Systems for visualisation and analysis

Maurizio Pollino - ENEA
maurizio.pollino@enea.it

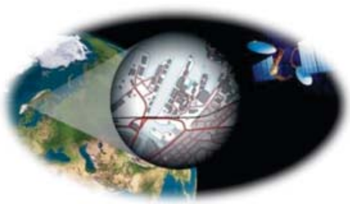
CIPRNet Course inside the Master in Homeland Security
Second Edition

University Campus Bio-Medico of Rome, 09-10July 2014

Geomatics

- The term ***Geomatics***[(*)] was created at Laval University in Canada in the early 1980s:
  - Geomatics is defined as a systemic, multidisciplinary, integrated approach to selecting the instruments and the appropriate techniques for collecting, storing, integrating, modeling, analyzing, retrieving at will, transforming, displaying, and distributing spatially georeferenced data from different sources with well-defined accuracy characteristics and continuity in a digital format.

Most relevant elements of Geomatics:
- Geographical information system (GIS)
- Decision support system (DSS)
- WebGIS



[(*)] *Mario A. Gomarasca, (2009), Basics of Geomatics, Springer Netherlands, DOI 10.1007/978-1-4020-9014-1*
http://link.springer.com/book/10.1007%2F978-1-4020-9014-1

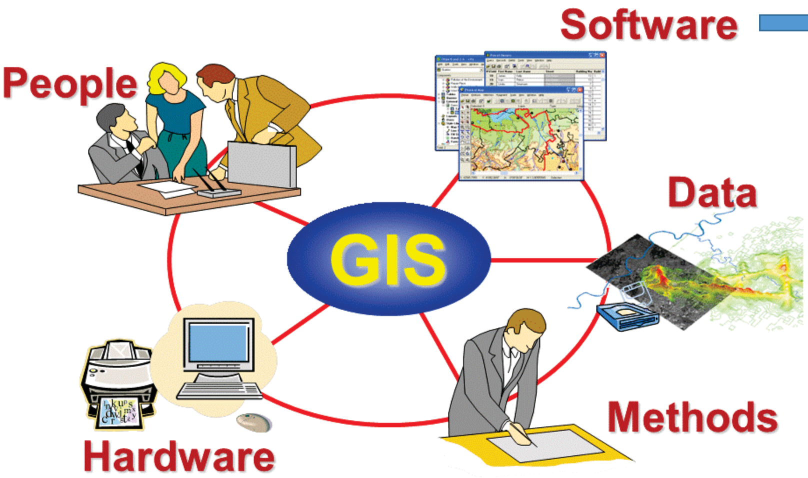
Geomatics

- **Geographical information system (GIS)**: to make use of a powerful combination of instruments capable of receiving, recording, recalling, transforming, representing, and processing georeferenced spatial data;
- **Decision support system (DSS)**: to implement complex geographical information systems meant to create possible scenarios by modeling the ground truth and to offer a set of solutions to the decision maker;
- **WebGIS**: to distribute geographic data remotely stored on dedicated machines for databases, according to complex network architectures.

Geographic Information System

- We define **GIS (Geographic Information System)** as a structure constituted by a powerful set of instruments and technologies committed to acquire, store, manage, transform, analyze and visualize georeferenced spatial data.
  - Georeferenced information: every document or event referred to a particular portion of Earth's surface is an example of georeferenced information
  - Geospatial information: every document or event that is also represented from a cartographic point of view or by maps or aerial/satellite images is an example of geospatial information
- Often the two terms (georeferenced and geospatial) are used as synonyms.

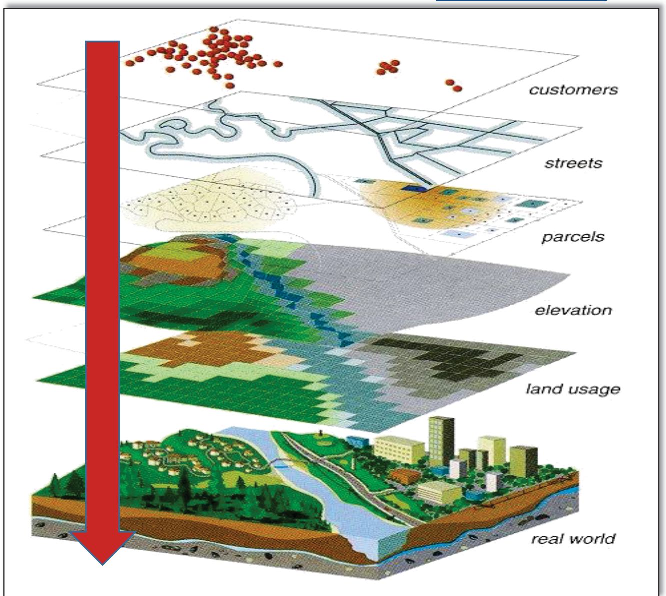
GIS elements and technology



- **Proprietary**
  - ✓ESRI ArcGIS
  - ✓Intergraph
  - ✓MapInfo
- **Free/Open Source (FOSS)**
  - QuantumGIS (QGIS) (http://qgis.org/)
  - GRASS GIS (http://grass.osgeo.org/)

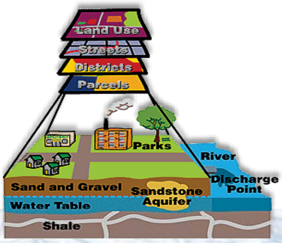
How GIS works

- ✓ In a GIS, different types of information are represented as separate map layers, coming from different sources or disciplines (multidisciplinary)
- ✓ Each layer is linked to descriptive information
- ✓ Layers are numerically combined to make a new map containing further information
- ✓ Data modeling in environmental GIS:
  - Basic functionalities
  - Specific functionalities

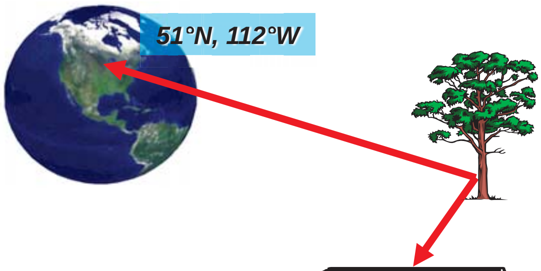


Geographic Information System

- **Spatial or geographic data represent REAL WORLD PHENOMENA and they are characterized by:**
  - their POSITION in space with respect to a reference and coordinate system;
  - NON-SPATIAL ATTRIBUTES (color, temperature, etc…);
  - mutual SPATIAL RELATIONS (topological, directional, distance relations).



- **We can describe any element of our world in two ways:**
  - **Location Information: Where is it?**



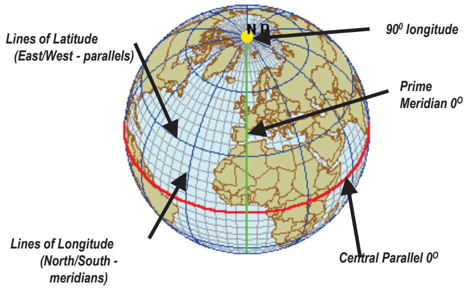
  - **Attribute Information: What is it?**

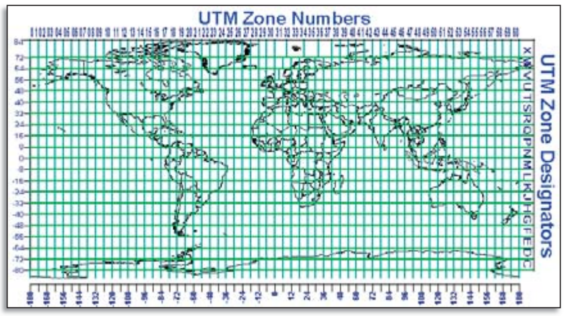
Georeferencing

- Is the representation of the location of real world features within the spatial framework of a particular coordinate system.
- Relationship between coordinate systems and map projections:
  - Map projections define how positions on the Earth's curved surface are transformed onto a flat map surface
  - Coordinate systems provide a referencing framework by which positions are measured and computed.

Coordinate Systems: Spatial Referencing

- Spherical Coordinate Systems
  - Geographical coordinate system (Latitude & Longitude)

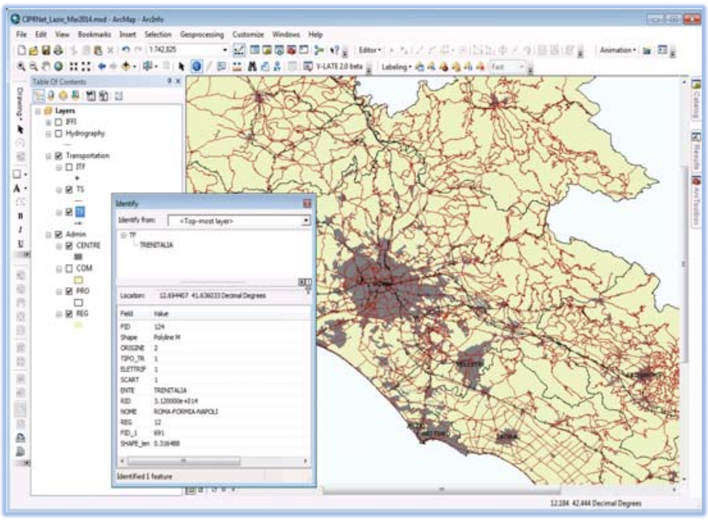




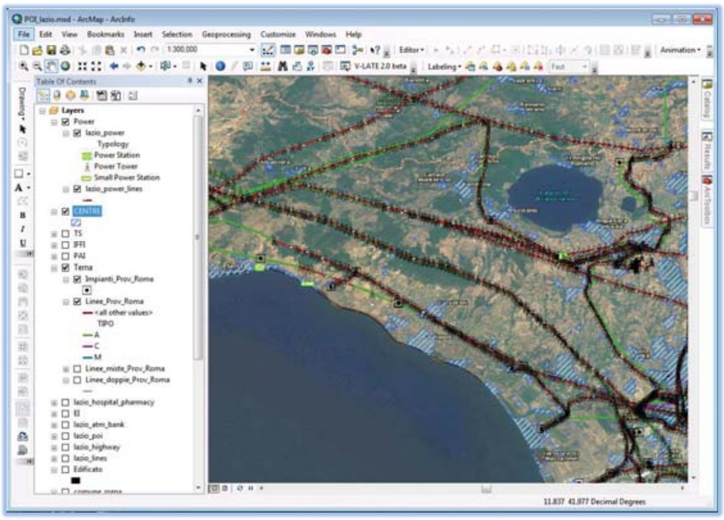
- Rectangular Coordinate Systems
  - UTM (Universal Transverse Mercator)
  - UPS
  - National Grids

To learn more: Peter Dana (University of Colorado): http://www.colorado.edu/geography/gcraft/notes/mapproj/mapproj_f.html

GIS Desktop interface: examples



Transportation network

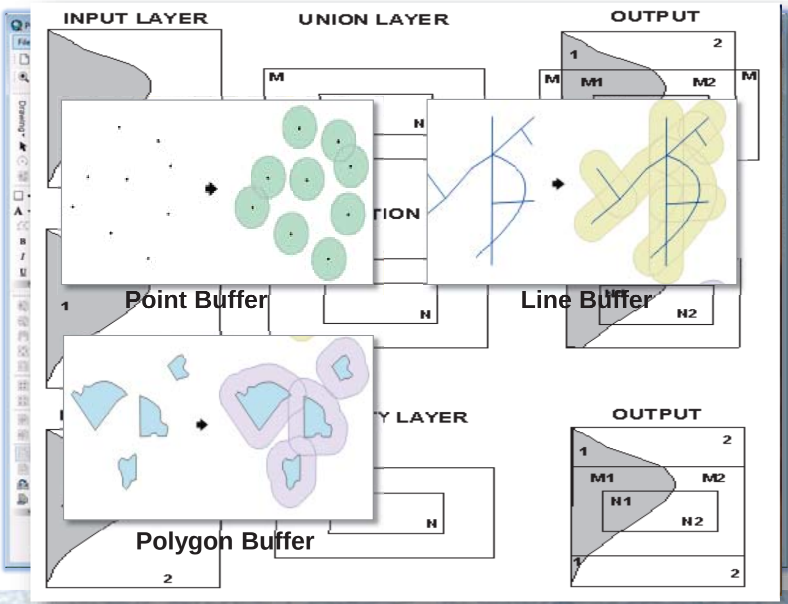


Power Lines and Elements

GIS Analysis Functions

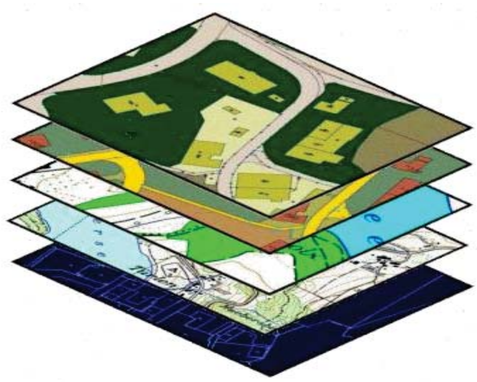
Main categories:

- Visualization
- Retrieval, Classification and Measurement
- Overlay
- Extraction
- Proximity
- Map algebra (Raster)



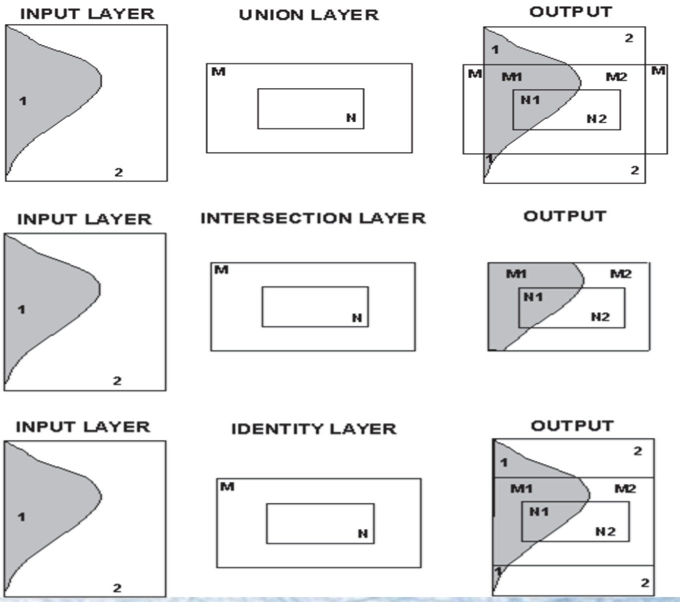
Overlay Functions

- Overlay analyses:
  - Operate on spatial entities from two or more maps to determine spatial overlap, combination, containment, intersection…etc.
  - One of the most "fundamental" of GIS operations
  - Basic part of the GIS toolbox
- Vector overlays:
  - combine point, line, and polygon features
  - computationally complex
- Raster overlays:
  - cell-by-cell comparison, combination, or operation
  - computationally less demanding



Overlay: Union, Intersect, and Identity

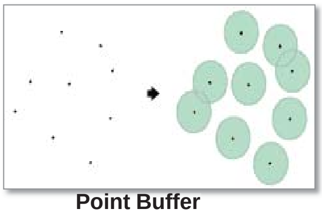
- UNION:
  - overlay polygons and keep areas from both layers.
- INTERSECTION:
  - overlay polygons and keep only areas in the input layer that fall within the intersection layer.
- IDENTITY:
  - overlay polygons and keep areas from input layer.



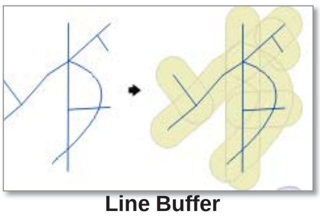
Proximity

Buffer (Vector):

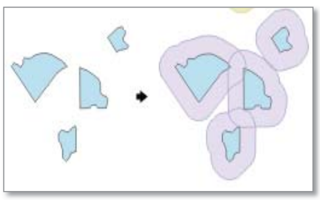
- Creates buffer polygons around input features to a specified distance.



Point Buffer



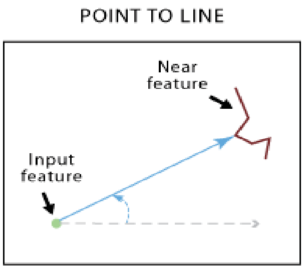
Line Buffer

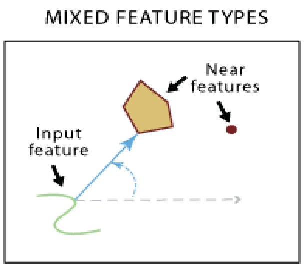


Polygon Buffer

Near:

- Determines the distance from each feature in the input features to the nearest feature in the near features, within the search radius.



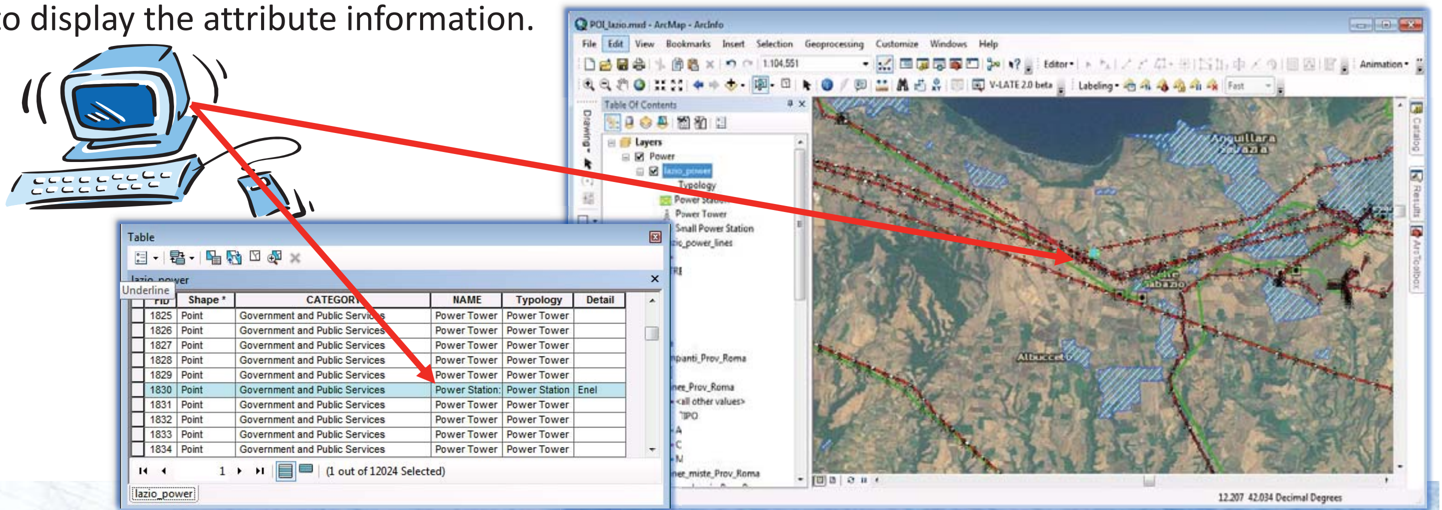


Methods of Spatial Data Analysis

- The GIS can perform a spatial analysis.
- Spatial relationships among the features and their attributes and the persistent link with their geometry (shape and position) make the GIS a tool able to simulate the real world and hence to help decision makers in solving actual problems.
- Operations can be carried out on a single data layer or by combining two or more data layers.
- They can be grouped in three categories:
  - Spatial data analysis;
  - Attributes analysis;
  - Integrated analysis.

GIS and DBMS

- The location and attribute information is stored inside your computer and a <u>GIS links the two types of information together</u>. It uses a map to display the location information and a table to display the attribute information.

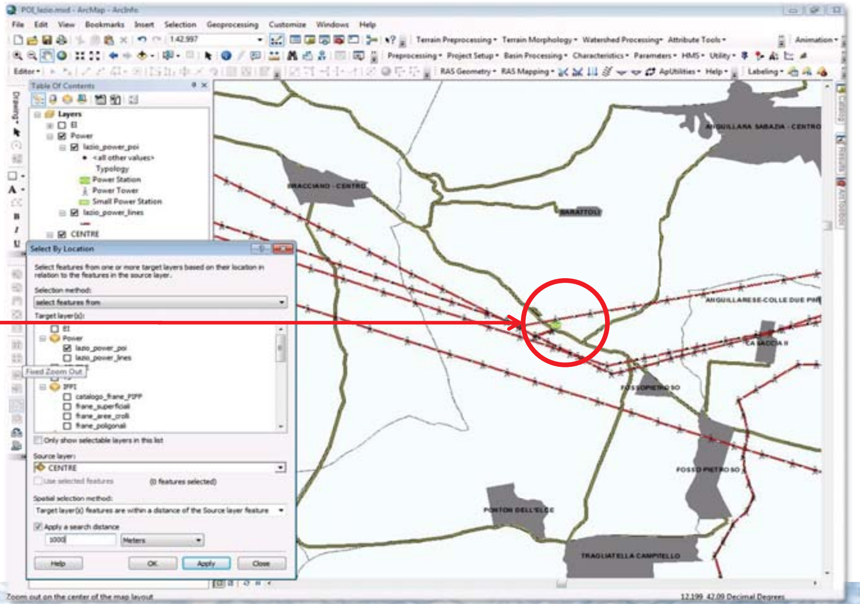


GIS query: example

- GIS software can answer questions about our world:

Spatial Questions:

Which Power Stations are closer than 1 km to a urban area?

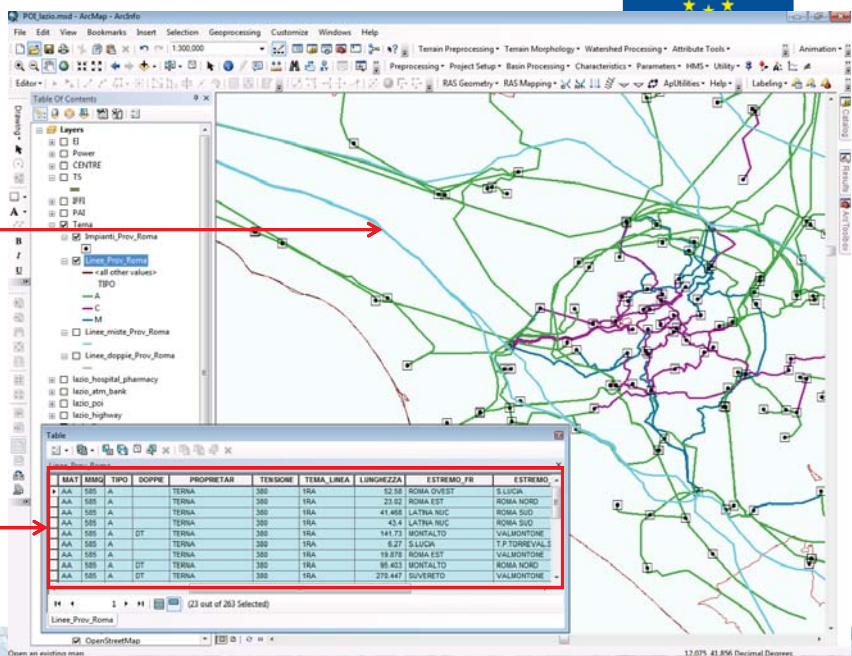


GIS query: another example

- GIS software can answer questions about our world:

Attribute Questions:

Select 380 kV high voltage transmission lines



Thematic mapping

Making Map with GIS:

- Output is the final goal of GIS projects. Two main types of output:
  - Maps
  - Visualizations
- Maps are good at summarizing and communicating.
- Primary goals in map design: to share information, highlight patterns and processes, illustrate results.

Maps and Cartography:

- Map is the digital or analog output from a GIS showing information using well established cartographic conventions
- Cartography is the art, science and techniques of making maps

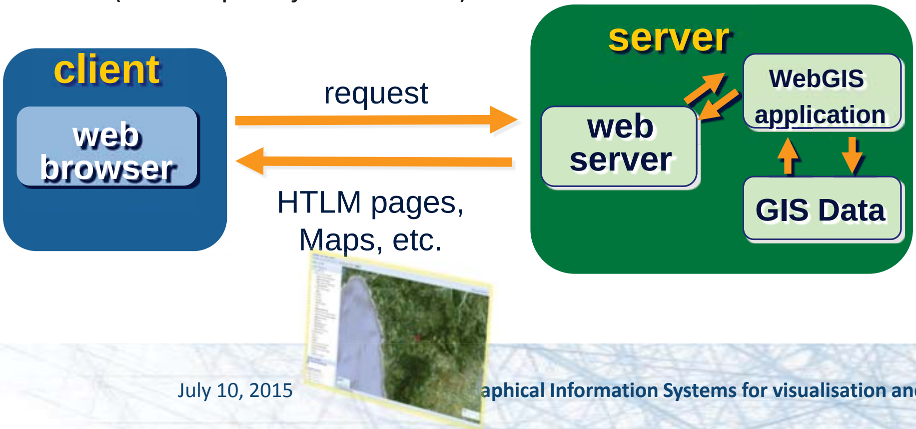
WebGIS and Web mapping

- Web mapping is the process of using maps delivered by GIS on the WWW, where it is both served and consumed. Web mapping is more than just web cartography, it is both a service activity and consumer activity.
- Web GIS is a type of distributed information system, comprising at least a server and a client, where the server is a GIS server and the client is a web browser, desktop application, or mobile application.
- In its simplest form, WebGIS can be defined as any GIS that uses web technology to communicate between a server and a client.

WebGIS and Web mapping

Web GIS basic schema:

- The server has a URL so that clients can find it on the web.
- The client relies on HTTP specifications to send requests to the server.
- The server performs the requested GIS operations and sends responses to the client via HTTP.
- The format of the response sent to the client can be in many formats, such as HTML, binary image, XML or JSON (JavaScript Object Notation).



➢ Open Geospatial Consortium (OGC) standards:

Web Services
WCS: Web Coverage Service
WFS: Web Feature Service
WMS: Web Mapping Service
WMTS: Web Map Tile Service
WPS: Web Processing Service

WebGIS advantages

- A global reach: you can present web GIS applications to the world, and the world can access them from their computers or mobile devices.
- A large number of users: in general, a traditional desktop GIS is used by only one user at a time, while a web GIS can be used by dozens or hundreds of users simultaneously.
- Better cross-platform capability: The majority of web GIS clients are web browsers. You do not need to install/buy specific software or pay to use WebGIS.
- Easy to use: Desktop GIS is intended for professional users with months of training and experience in GIS. WebGIS is intended for a broad audience, including public users who may know nothing about GIS. They expect web GIS to be as easy as using a regular website. WebGIS is commonly designed for simplicity, intuition, and convenience, making it typically much easier to use than desktop GIS.

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Platforms for Large & Complex Scenarios

Alberto Tofani – ENEA, Rome, Italy

alberto.tofani}@enea.it

CIPRNet Course inside the Master in Homeland Security
Second Edition

UCBM – Rome (Italy) – 9-10 July 2015

Classification of interdependencies M&S simulation approaches

- Ouyang categorisation
    - Empirical approaches
    - Agent based approaches
    - System dynamics
    - Economic theory based
    - Network based

Min Ouyang
Review on modeling and simulation of interdependent critical infrastructure systems,
Reliability Engineering & System Safety Volume 121, January 2014, Pages 43–60

- Satumtira,Duenas-Osorio classification method
    - Mathematical Method
    - Modeling objective
    - Scale of analysis
    - Quantity and Quality of Input data
    - Targeted discipline
    - End user type

Gesara Satumtira, Leonardo Dueñas-Osorio
Synthesis of Modeling and Simulation Methods on Critical Infrastructure Interdependencies Research,
Sustainable and Resilient Critical Infrastructure Systems 2010, pp 1-51

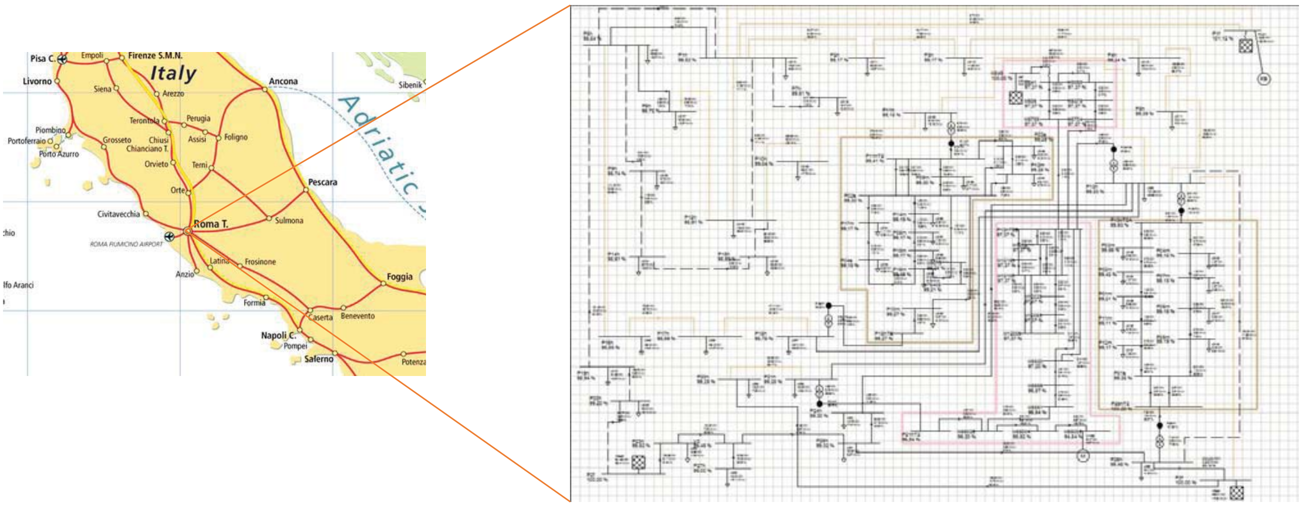
Large and complex scenario……..

- Possible dimensions of a scenario
  - Geographical extensions
    - City
    - Metropolitan area
    - Regional
    - National
  - Number of components in the scenario
    - Components complexity
    - Components heterogeneity
  - Independent domains vs interdependent domains

Large and complex scenario……..

e.g. Economic study – Leontief I/O model (purchase –sales relationships among different sectors/state members)

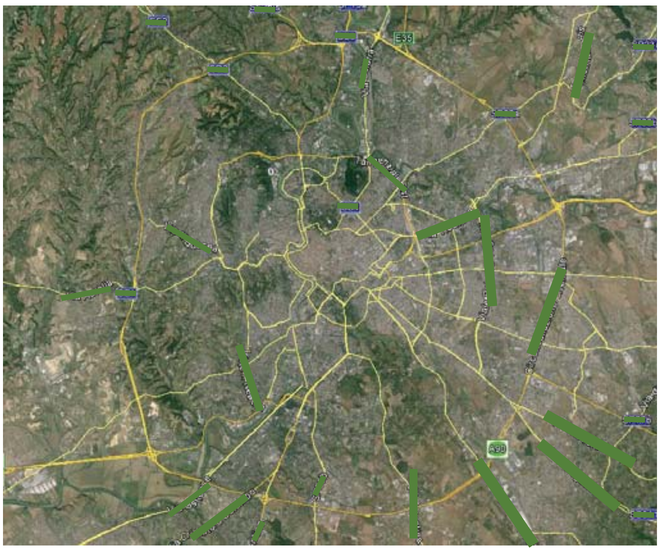
Large and complex scenario……..



Portion of an electrical distribution grid (Physical model)

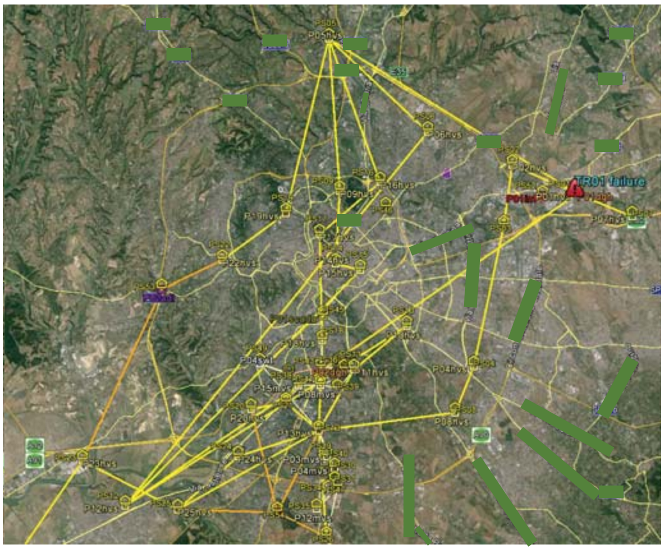
A large & complex scenario example

Geographical scale: Metropolitan area



A large & complex scenario example

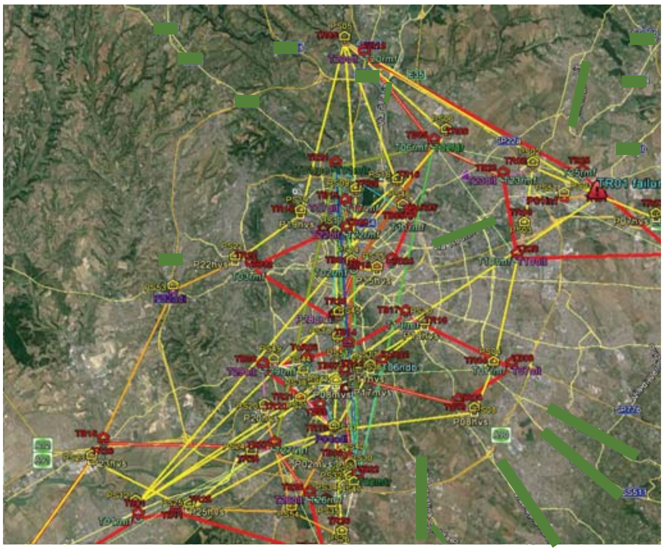
Geographical scale: Metropolitan area



Components
- Technological networks
  - Power network

A large & complex scenario example

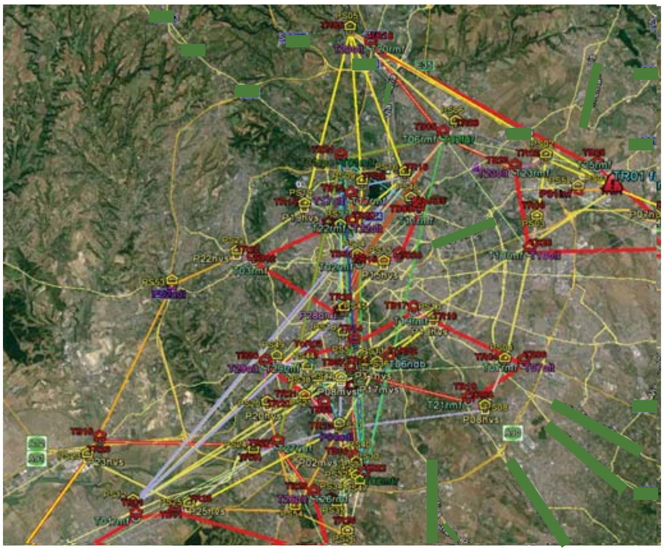
Geographical scale: Metropolitan area



Components
- Technological networks
  - Power network
  - Telco network

A large & complex scenario example

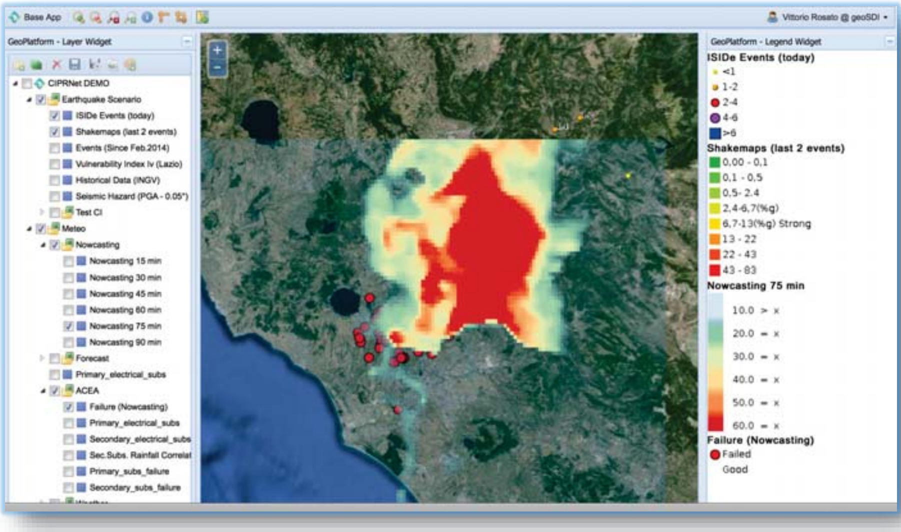
Geographical scale: Metropolitan area



Components
- Technological networks
  - Power network
  - Telco network
- Network dependencies

A large & complex scenario example

Geographical scale: Metropolitan area



Components
- Technological networks
  - Power network
  - Telco network
- Network dependencies

+

Threats (natural events….)

A large & complex scenario example

Geographical scale: Metropolitan area

Components
- Technological networks
  - Power network
  - Telco network
- Network dependencies

Threats (natural events....)

Societal system

Modeling Objectives

- Risk assessment
  - CI operators risk analysis improvement
  - Urban resilience improvement
  - Critical assets risk analysis in emergency situation
  - .....
- Vulnerability analysis
- Interdependency analysis
- Failure propagation analysis
- ....

Technological networks
Primary services
Critical assets

Threats (natural events....)

Context information

Infrastructure scale of analysis

- The infrastructure scale of analysis describes the level of granularity the infrastructure interdependencies are analyzed [Satumtira,Duenas-Osorio]

High Abstraction level

System of systems

Low Granularity level

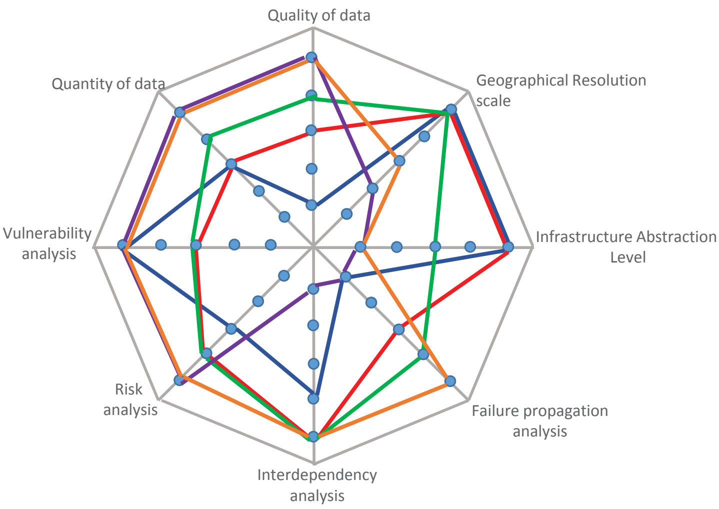
Network

Low Abstraction level

Advanced Network

High Granularity level

Learning by doing: the ENEA experience



Topology based

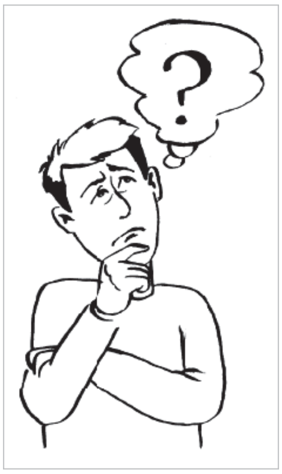
IIM

Agent Based

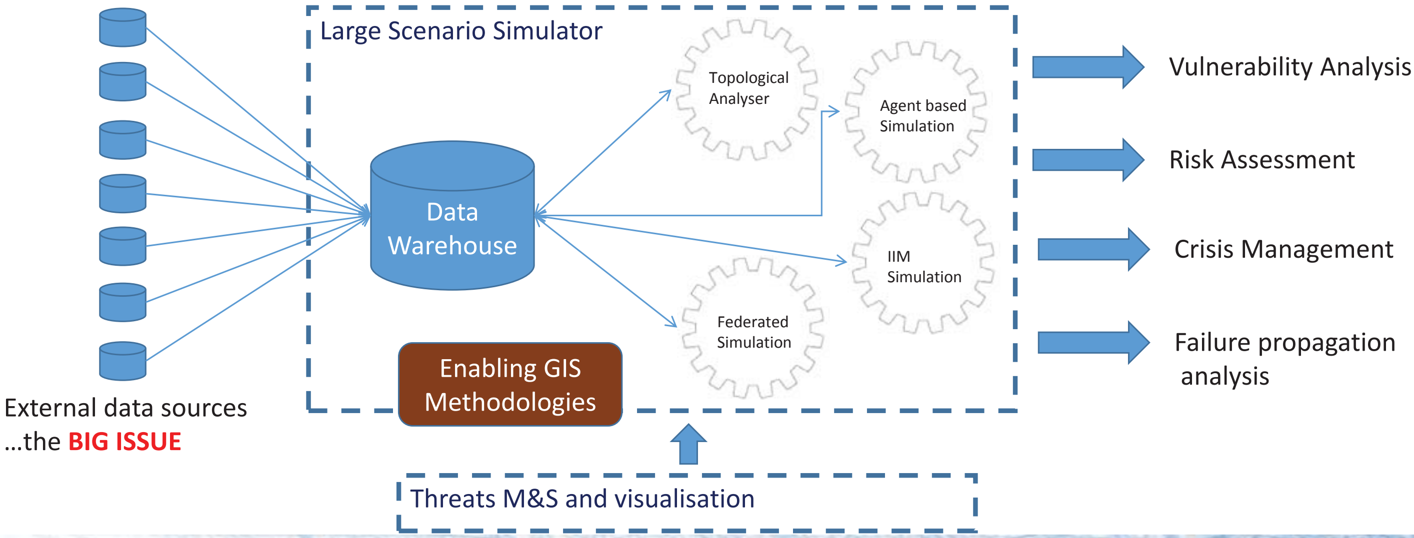
CI Domain simulators

Federated CI simulators

Simulation of large scenario.......



Simulation of large scenario: the solution architectural template



Conclusion

- NO “Silver-bullet” tool for large scenarios
- Solution: platforms for CIP contains models and tools of different categories
- Data gathering and homogenisation is the very BIG ISSUE

S. Rinaldi, J. Peerenboom, and T. Kelly.
“Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies,”
IEEE Control Systems Magazine, IEEE, December 2001, pp. 11-25

P. Pederson D. Dudenhoeffer S. Hartley M. Permann.
“Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research,”
INL/EXT-06-11464

Gesara Satumtira, Leonardo Dueñas-Osorio
Synthesis of Modeling and Simulation Methods on Critical Infrastructure Interdependencies Research,
Sustainable and Resilient Critical Infrastructure Systems 2010, pp 1-51

Min Ouyang
Review on modeling and simulation of interdependent critical infrastructure systems,
Reliability Engineering & System Safety Volume 121, January 2014, Pages 43–60

G. D’Agostino and A. Scala eds.
Networks of Networks: The Last Frontier of Complexity
Understanding Complex Systems. Springer International Publishing

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Decision Support System and Consequences Analysis part 1: DSS - The CIPRNet Idea

Vittorio Rosato
vittorio.rosato@enea.it

Master in Homeland Security 2015

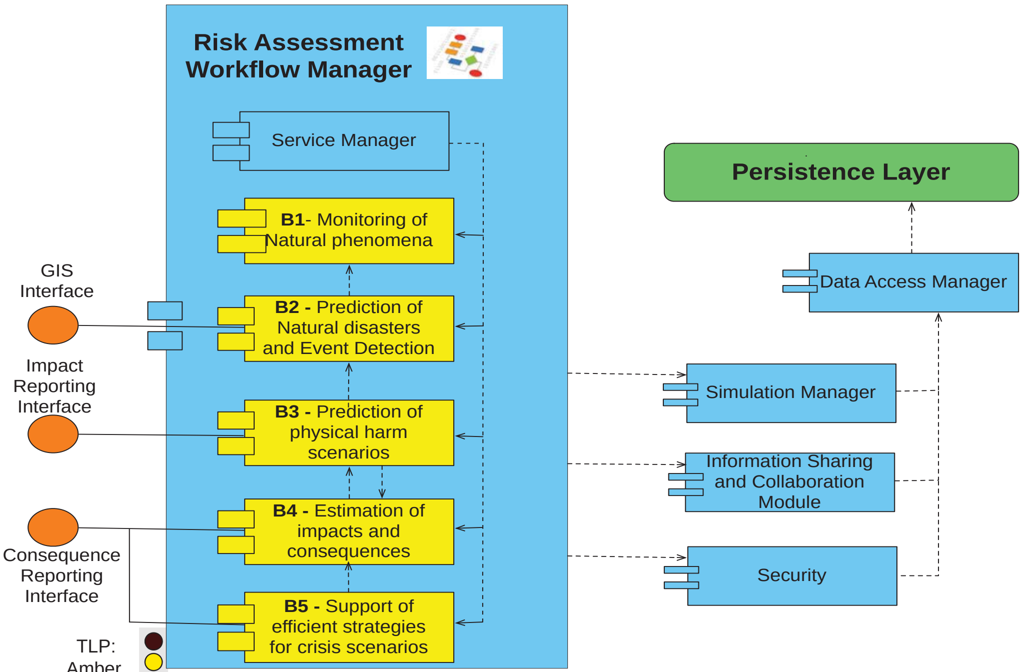
UCBM – Roma – July 9-10, 2015

Fraunhofer IAIS ENEA TNO UIC cea Deltares acris

Agenda

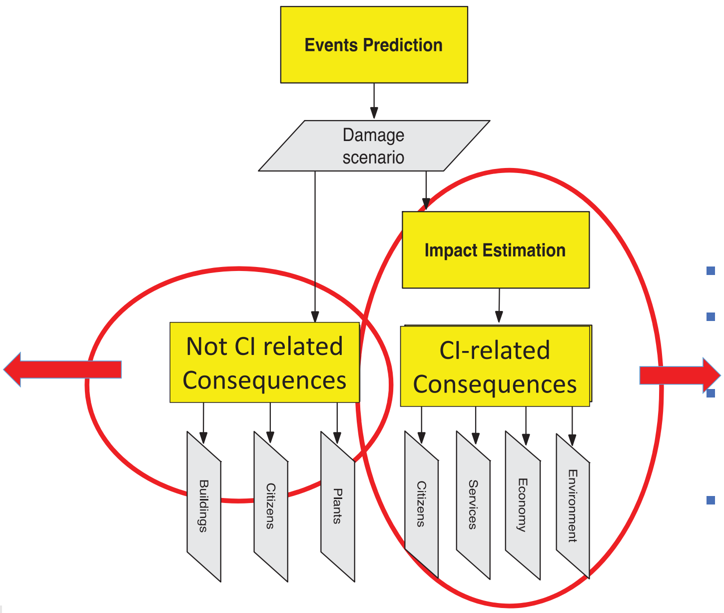
1. DSS: architecture
2. DSS: vulnerability analysis
3. DSS: impact analysis
4. DSS: interaction with the operators
5. DSS: an operational service and a Crisis Gaming tool
6. Conclusions

DSS architecture



DSS: Damages estimate

- damages to buildings and related casualties
- damages to industrial plants and related casualties
- damages to roads, railways and related losses in mobility
- damages to industrial plants and related GDP losses
- Expected flooded areas and number of involved citizens
- flooded areas and related GDP losses



- Damages to CI elements
- Impacts (loss of Service) to Power and telco systems
- Cascading effects to other CI and to some Essential Services (e.g. Hospitals)
- Consequences on 4 Criteria

DSS: Vulnerability analysis

The Damages estimation block transforms the predicted Events (with their predicted Strength) in Damages to CI elements and, wherever possible, to other types of assets (Buildings, Plants etc.)

The list of Events which will be monitored and whose effects will be “transformed” into Damages is the following:

- Earthquake
- Abundant rainfall
- Heat/Cold temperatures wave
- Strong Wind
- Lightning
- Heavy snowfall
- Ice/hail storm
- Landslide
- Flash flood
- Flooding
- Mud flow
- Debris avalanche
- Storm surge

DSS: Vulnerability analysis

Two different methods will be used to identify “vulnerability” of the different CI elements versus each considered threat

a.inferring vulnerability data thresholds from historical data (when available)

1. Elements with pronounced fault correlation with events
2. General trend of vulnerability versus event’s strength

b.getting vulnerability thresholds by CI elements technical data

1. Direct access (from explicit values, when available)
2. Indirect access (from empirical formulas)

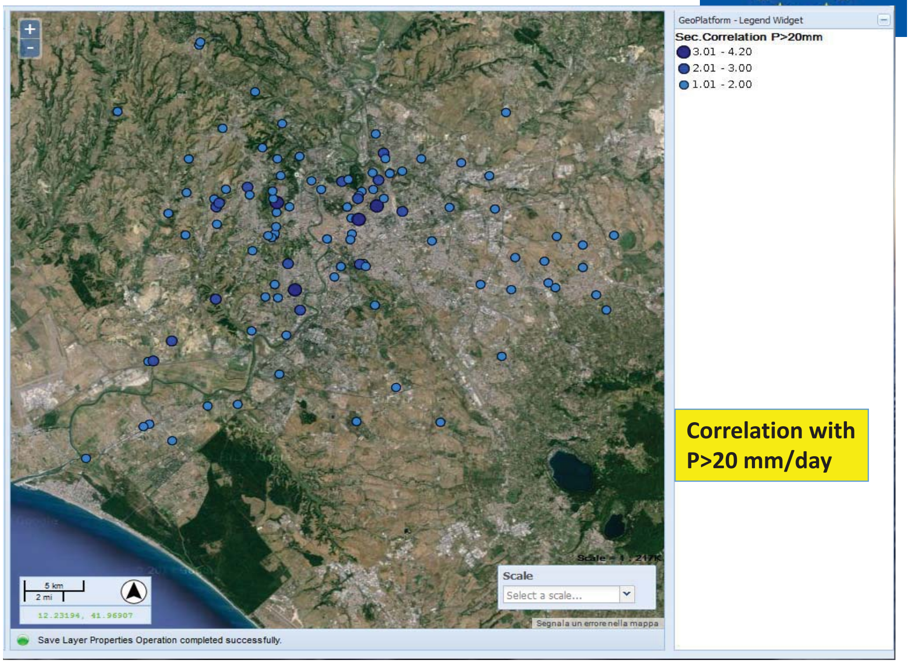
- Earthquake
- Abundant rainfall
- Heat/Cold temperatures wave
- Strong Wind
- Lightening
- Heavy snowfall
- Ice storm
- Landslide
- Flash flood
- Flooding
- Mud flow
- Debris avalanche
- Storm surge

DSS: Vulnerability analysis

Vulnerability to meteorological events

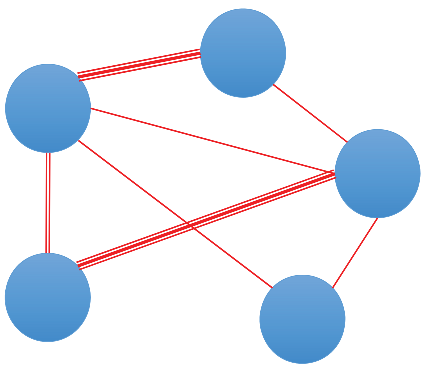
The vulnerability assessment is based on the statistical elaboration of:

- failure events/anomalies reported by CI owner;
- meteorological time series (last 10 years) of precipitation and temperature.



DSS: Impact analysis

Impact Analysis is the transformation of expected Damages into subsequent reductions (or losses) of Services supplied by CI, either those hit by damages and those hit via cascading (or dependency) mechanisms.



CI should be considered as a system whose elements are connected by forces having different force constants.
Tight connections produce dynamic responses characterized by high frequencies (small characteristic times) while loose couplings produce low frequencies (and higher characteristic times)

Electrical and Telecommunication systems seem to be the mostly thightly coupled infrastructures: thus their interaction takes place in a time scale much smaller than that pertaining to other systems. The times of mutual response to faults is very short: it could be “adiabatically” decoupled from that of the other systems.

DSS: Impact analysis

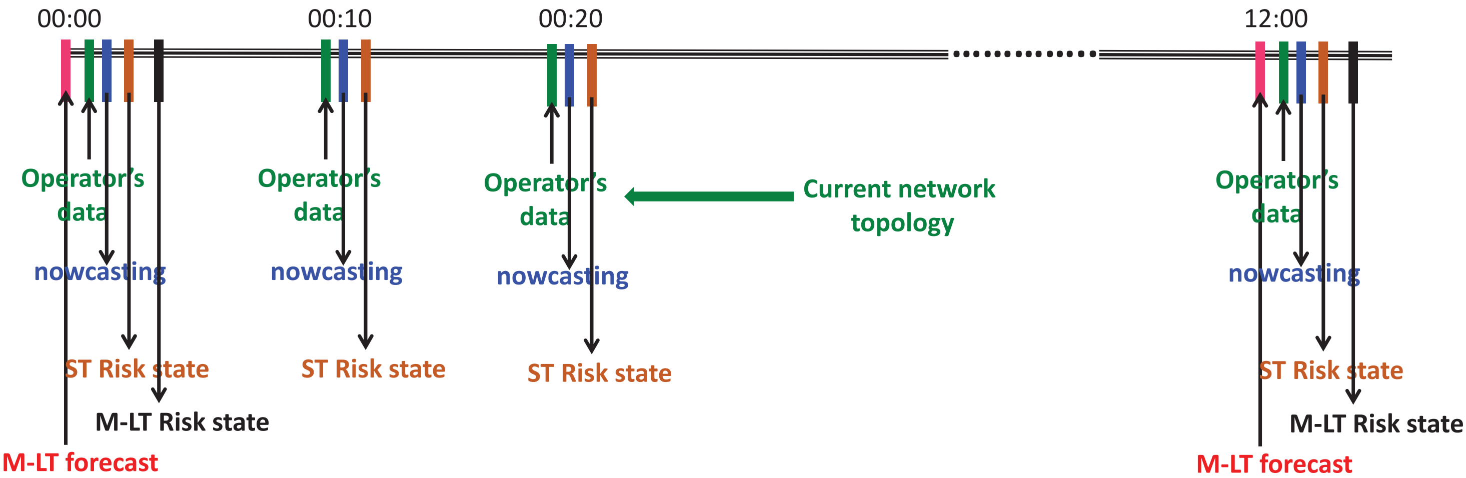
Impact Analysis has been thus split into two different modules:

1. An Electrical-Telecom interaction system, where eventual Damages occurring to one (or both) of these systems are analyzed and Impacts assessed.

   Time scale: from a few minutes to less than hours
2. An interaction scheme linking all other CI and connected to the Electrical-Telecom interaction system

DSS: Interaction with CI operators

The interaction with electrical operator ACEA (Roma multi-utility operator) will follow this workflow

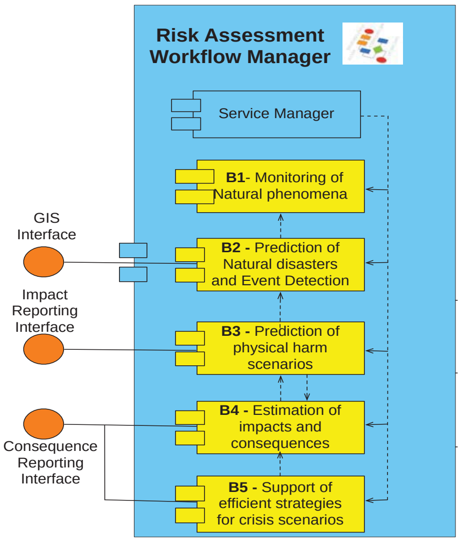


DSS: Consequence analysis

Consequence analysis estimates the severity of a crisis as a function of the ultimate effects that it can produce on

- Citizens
- Public Services
- Environment
- Economical sectors

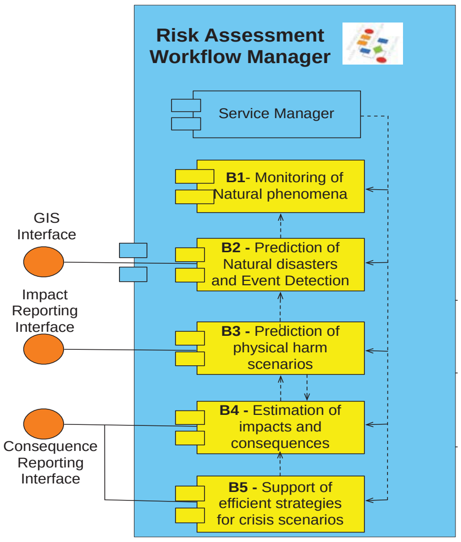
DSS: an Operational and a Crisis Gaming tool



When the DSS will receive as Input real-time data (forecast, predictions etc.) it operates as a Risk Analysis Forecast System, providing (with some anticipation) predictions on the course of events, the expected damages, the related impacts on the system of CI, the consequences to the different domains (Criteria).

It thus represents an Operational Tool which can be deployed (24/7) in favour of CI operators, Public Authorities

DSS: an Operational and a Crisis Gaming tool

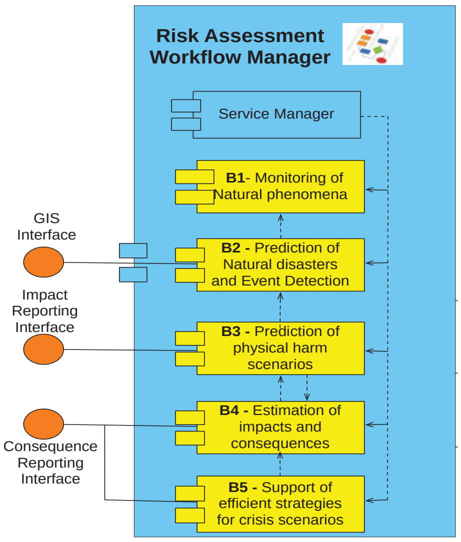


The DSS can also create synthetic scenario where the occurrence of natural events is simulated: the block getting data from true information sources can be substituted by a generator of synthetic perturbations such as:

- earthquake
- abundant rainfall
- cold or hot wave

The DSS could be used for stress testing and/or to evaluate complex systems response to predicted (but not yet occurred) natural manifestations

DSS: an Operational and a Crisis Gaming tool



The DSS can also create synthetic damages, to simulate scenarios which are not directly related to physical manifestations but rather to attacks or other types of home-made perturbations (with no specific or predictable patterns)

The DSS could be thus used for stress testing and/or to evaluate complex systems response to possible damages.

CIPR Net

End of first part

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Decision Support System and Consequences Analysis part 2: Consequence analysis concepts

Vittorio Rosato
vittorio.rosato@enea.it

Master in Homeland Security 2015

ENEA

UCBM – Roma – July 9-10, 2015

Fraunhofer IAIS ENEA TNO uic cea Deltares acris

Agenda

1. Consequence Analysis: the CIPRNet approach
2. Service Access Wealth Indices
3. A test case
4. Conclusions

Consequence Analysis

We define the **Wealth** as being the measure (expressed in a specific scale) of the well-being of a specific Criterion element. **Wealth** can be expressed in different terms, as a function of the chosen Criterion.

Assume the $\boldsymbol{W(t_{ij})}$ is the Wealth of the Criterion $\boldsymbol{t_{ij}}$ It can be described in terms of a Metrics $\boldsymbol{M(t_{ij})}$ providing the optimal value of some property ensuring the achievement of the Wealth

$$W(t_{ij}) = M(t_{ij}) \sum_{k=1}^{N_k} r_k(t_{ij}) Q_k$$

The Wealth achievement can be related to the availability of specific assets (International Wealth Index [1]) **or to the availability of Primary Services**. Our model thus considers the $\boldsymbol{Q_k}$ as being the Primary Services availability and $\boldsymbol{r_k(t_{ij})}$ the "relevance" of Service $\boldsymbol{k}$ for allowing Wealth achievement of the specific Criterion $\boldsymbol{t_{ij}}$.

[1] http://ddw.ruhost.nl/iwi/intro.php (Nijmegen Center for Economics, Institute for Management Research)

Consequence Analysis: a new model theory

The **Consequence** can be expressed as a difference between the "expected" Wealth and that effectively achieved due to **the loss of Primary Services.**

If the Crisis Scenario is expected to last a period ***T*** and the ordinary Wealth is $\boldsymbol{W_0}$, the Consequence of the Crisis (on a specific Criterion $\boldsymbol{t_{ij}}$) could be expressed as

$$C = W_0 T - M \int_0^T \sum_{k=1}^{N_k} r_k Q_k(t) dt$$

As $\boldsymbol{M=W_0}$ then

$$C = M[T - \sum_{k=1}^{N_k} r_k \int_0^T Q_k(t) dt]$$

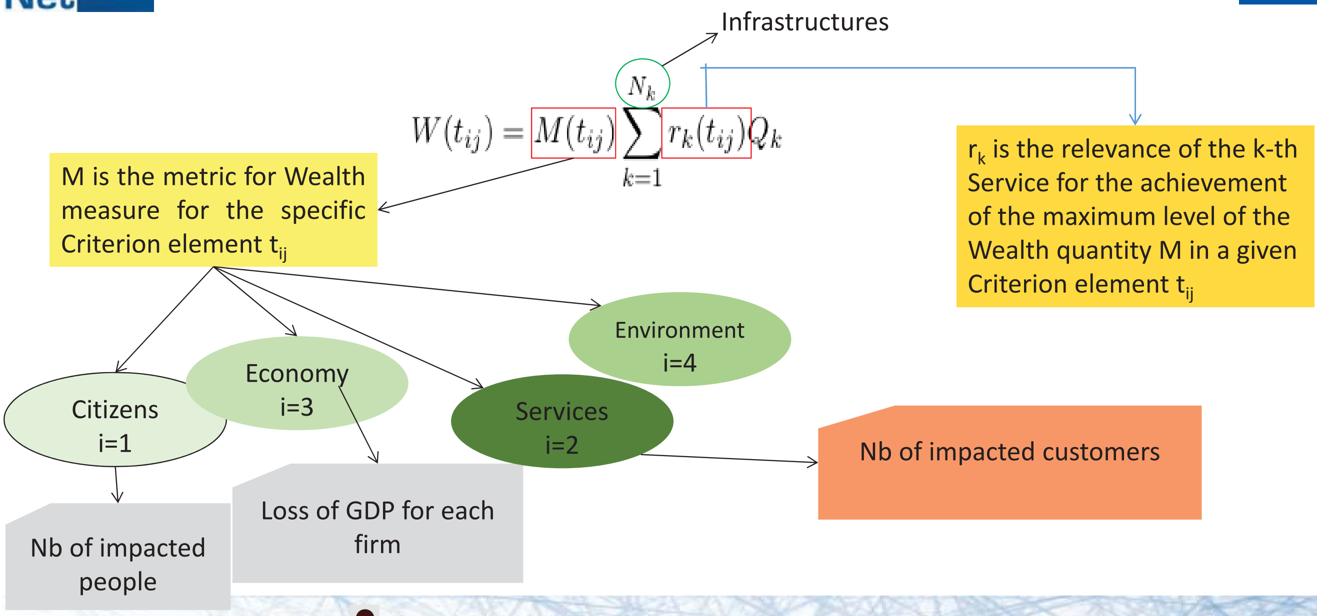
Service Access Wealth (SAW) Indices

$\boldsymbol{Q_k(t)}$ are the expected output of Impact Analysis, $\mathbf{r}_k$ are what we called **SAW (Services Access Wealth) Indices**.

They are different from one Criterion to another (electricity could be more relevant for the Wealth achievement depending on the class of age or the presence of physical disabilities)

Criterion element	Electricity	Telecom.	Water	Gas	Mobility	Total
citizens age <5 years	$r_1(t_{11})$	$r_2(t_{11})$	$r_3(t_{11})$	$r_4(t_{11})$	$r_5(t_{11})$	100
citizens age > 65 years	$r_1(t_{12})$	$r_2(t_{12})$	$r_3(t_{12})$	$r_4(t_{12})$	$r_5(t_{12})$	100
citizens 35<age < 65 years	$r_1(t_{13})$	$r_2(t_{13})$	$r_3(t_{13})$	$r_4(t_{13})$	$r_5(t_{13})$	100
citizens with disabilities	$r_1(t_{14})$	$r_2(t_{14})$	$r_3(t_{14})$	$r_4(t_{14})$	$r_5(t_{14})$	100

Service Access Wealth (SAW) Indices



Service Access Wealth (SAW) Indices

Tavola 8.8 **Persone di 3 anni e più per frequenza con cui usano un personal computer e persone di 6 anni e più per frequenza con cui usano Internet per sesso, classe di età, regione, ripartizione e tipo di comune**
Anno 2014, per 100 persone della stessa classe di età, sesso e zona

ANNI CLASSI DI ETÀ	Uso del personal computer (a)					Non usano il pc	Uso di Internet (b)					Non usano Internet
	Sì	Tutti i giorni	Una o più volte alla settimana	Qualche volta al mese	Qualche volta all'anno		Sì	Tutti i giorni	Una o più volte alla settimana	Qualche volta al mese	Qualche volta all'anno	
3-5	22,0	4,6	12,8	2,7	1,9	74,7	-	-	-	-	-	-
6-10	52,8	11,4	30,5	8,3	2,6	45,6	44,4	9,0	25,6	7,2	2,6	53,8
11-14	80,2	31,4	41,3	6,1	1,4	18,1	80,8	44,5	31,6	3,8	0,9	17,2
15-17	85,8	51,6	30,4	3,1	0,6	12,8	90,9	70,2	18,5	1,8	0,3	7,9
18-19	89,1	58,7	27,1	2,8	0,5	9,1	93,8	76,2	15,7	1,5	0,4	4,0
20-24	83,7	58,9	21,5	2,5	0,8	13,7	89,1	70,6	16,1	1,9	0,5	8,4
25-34	77,8	52,1	21,7	3,1	0,9	20,1	83,5	61,0	19,9	1,8	0,8	14,6
35-44	73,1	48,2	20,6	2,9	1,4	25,7	76,1	50,2	21,9	3,0	1,0	22,6
45-54	64,0	43,0	17,2	2,7	1,1	34,4	65,6	40,7	20,6	3,1	1,2	32,9
55-59	50,9	34,0	13,3	2,9	0,7	47,4	52,5	30,9	17,3	3,2	1,1	46,1
60-64	40,8	25,8	12,9	1,4	0,7	57,0	41,6	23,4	15,7	1,9	0,6	57,2
65-74	21,2	11,0	8,3	1,5	0,4	77,1	21,1	10,2	8,9	1,6	0,5	77,1
75 e oltre	4,7	2,3	1,9	0,4	0,1	93,4	4,3	1,9	1,8	0,4	0,2	93,9
Totale	**54,7**	**33,5**	**17,4**	**2,7**	**1,0**	**43,6**	**57,3**	**36,9**	**17,1**	**2,5**	**0,9**	**41,0**

Official italian Census data (2014)
Telecom relevance

Service Access Wealth (SAW) Indices

Tabella 15. Popolazione residente che si è recata il mercoledì precedente la data del censimento al luogo abituale di studio o di lavoro per classe di età in Italia e nel Lazio

Classe età	Italia N	Italia %	Lazio N	Lazio %
0-5	1.526.052	5,96	136.473	5,81
6-10	2.470.900	9,64	215.094	9,16
11-14	2.010.673	7,85	175319	7,47
15-19	2.197.139	8,57	201.236	8,57
20-24	1.676.995	6,54	146.018	6,22
25-29	2.249.258	8,78	196.398	8,36
30-34	**2.582.706**	**10,08**	**231.759**	**9,87**
35-54	**9.300.244**	**36,29**	**865.212**	**36,84**
55 e più	1.610.032	6,29	180.878	7,70
Totale	**25.624.599**	100,00	**2.348.387**	100,00

Fonte: ISTAT, 2001. "14°Censimento della popolazione e delle abitazioni"

Official italian Census data (2014)

Transport relevance

Regional breakdown

Tabella 19. Occupati che si sono recati il mercoledì precedente la data del censimento al luogo abituale di lavoro per mezzo utilizzato - Lazio (dettaglio provinciale) - Valori percentuali

Province	Treno, tram, metro	Autobus urbano, filobus, corriera, autobus extra-urbano	Autobus aziendale o scolastico	Auto privata (come conducente)	Auto privata (come passeggero)	Motocicletta ciclomotore scooter	Bicicletta	Altro mezzo	A piedi	Totale
Viterbo	2,89	3,65	0,80	73,07	5,30	2,40	0,30	0,29	11,31	100
Rieti	3,88	4,22	0,69	71,22	5,05	0,76	0,40	0,27	13,52	100
Roma	9,34	8,90	1,14	56,81	4,53	10,12	0,29	0,16	8,70	100
Latina	4,53	2,71	1,69	69,96	5,74	1,91	0,92	0,39	12,15	100
Frosinone	2,84	3,93	1,97	73,96	6,24	0,54	0,25	0,16	10,11	100
Lazio	**7,92**	**7,57**	**1,22**	**60,55**	**4,83**	**8,00**	**0,35**	**0,19**	**9,38**	**100**

Fonte: ISTAT, 2001. "14°Censimento della popolazio ne e delle abitazioni"

Service Access Wealth (SAW) Indices

Relevance of Power and Gas

3 Territorio	Italia
4 Tipo dato	spesa media mensile familiare
5 Misura	valori medi
6 Numero di componenti	totale
7 Condizione professionale	totale
8 Anno	2012

9 Tipologia familiare	persona sola con 35-64 anni	persona sola con meno di 35 anni	persona sola con 65 anni o più	coppia senza figli con p.r. con 35-64 anni	coppia senza figli con p.r.con meno di 35 anni	coppia senza figli con p.r. con 65 anni o più	coppia con 1 figlio	coppia con 2 figli	coppia con 3 e più figli
10 **Gruppo di spesa**									
11 totale	2008,48	1906,83	1539,11	2710,33	2534,72	2397,15	2841,95	3023,33	3034,53
+ 12 alimentari e bevande	344,42	323,48	324,65	467,51	386,07	489,94	536,07	586,18	659,19
40 non alimentari	1664,07	1583,35	1214,47	2242,82	2148,64	1907,2	2305,87	2437,15	2375,34
41 tabacchi	22,48	21,58	6,67	27,63	29,51	11,08	23,94	26,62	31,15
+ 42 abbigliamento e calzature	98,96	108,56	51,11	138,4	125,78	80,06	153,13	180,68	178,7
+ 46 abitazione (principale e secondaria)	628,87	559,12	604,39	779,76	683,44	813,55	745,87	738,32	658,26
52 combustibili ed energia	97,96	81,44	110,45	134,97	106,16	146,78	151,2	161,39	162,51
53 energia elettrica	32,8	29,56	32,12	46,56	36,13	47,97	56,06	63,51	73,43
54 gas	44,85	39,5	54,48	66,53	47,3	71,48	73,48	74,42	69,05
55 riscaldamento centralizzato	11,15	7,2	13,43	11,6	13,59	12,49	10,44	9,8	6,29
+ 56 mobili, elettrod. e servizi per la casa	87,62	95,95	96,54	123,75	148,2	119,36	131,09	128,24	145,12
+ 67 sanità	52,8	39,73	72,62	96,73	94,64	127,24	100,01	99,28	84,72
+ 70 trasporti	311,66	298,84	83,36	451,7	459,94	292,44	477	487,47	539,82
79 comunicazioni	37,32	33,3	30,1	47,14	47,67	40,46	54,96	58,29	61,58

$r_1(t_{11})/ r_1(t_{12}) = 32/9$

$r_1(t_{11})/ r_1(t_{14}) = 32/23$

$r_4(t_{11})/ r_4(t_{12}) = 49/16$

$r_4(t_{11})/ r_4(t_{14}) = 49/32$

Service Access Wealth (SAW) Indices

After a thorough analysis of available data we should be able to solve the following system of equations (20 unknown for ***Criteria*** element 1 (citizens))

$$\left\{\begin{array}{l} \left.\begin{array}{l} r_1^{11}+r_2^{11}+r_3^{11}+r_4^{11}+r_5^{11}=100 \\ r_1^{12}+r_2^{12}+r_3^{12}+r_4^{12}+r_5^{12}=100 \\ r_1^{13}+r_2^{13}+r_3^{13}+r_4^{13}+r_5^{13}=100 \\ r_1^{14}+r_2^{14}+r_3^{14}+r_4^{14}+r_5^{14}=100 \end{array}\right\} \text{normalisation} \\ \left.\begin{array}{l} r_2^{11}/r_2^{12}=\alpha_2 \\ r_2^{11}/r_2^{13}=\beta_2 \\ r_2^{11}/r_2^{14}=\gamma_2 \\ r_2^{12}/r_2^{13}=\delta_2 \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots \end{array}\right\} \text{from available data} \end{array}\right.$$

Service Access Wealth (SAW) Indices

At the end of Consequences evaluation, each Criterion will be characterised by a value of the Consequences that the predicted Crisis Scenario will produce on it.

Thus, the outcome of the Consequence Analysis module will be a vector ***C***

$$\boldsymbol{C} = \begin{bmatrix} C_1 \\ C_2 \\ C_3 \\ C_4 \end{bmatrix}$$

Each C_i value will be described by its own metrics (euros, #people affected, land surface polluted etc.); thus a classical Norm definition of the ***C*** vector will not be attempted nor wanted.

Service Access Wealth (SAW) Indices

In order to discriminate the different "severities" of the involved Scenarios, let us define a threshold Vector **T** which will define the limiting value of a Criterion Consequences leading a transition from "**Light**" to "**Severe**" crisis

$$\boldsymbol{T} = \begin{bmatrix} T_1 \\ T_2 \\ T_3 \\ T_4 \end{bmatrix}$$

According to the definition of these Vectors, we could establish a Grade Scale **G** indicating the Crisis Severity

$\mathcal{G}$ **= 1** No significant Consequences

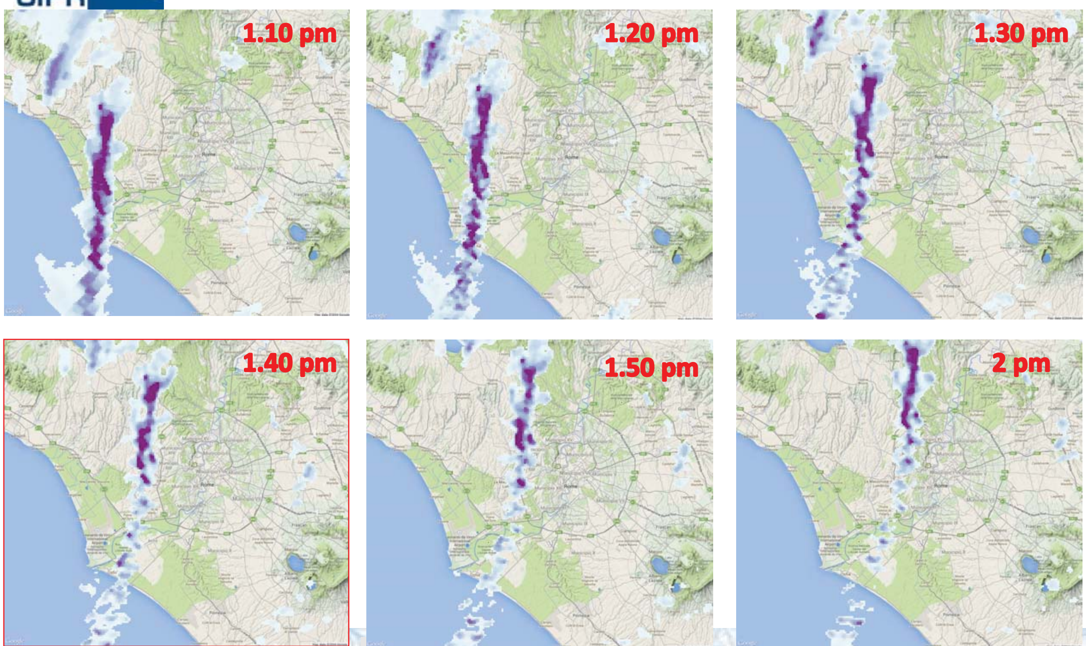
$\mathcal{G}$ **= 2** Consequences can be detected in geographical extent OR in time duration. C's are lower than thresholds

$\mathcal{G}$ **= 3** Consequences can be detected in geographical extent AND in time duration. C's are lower than thresholds

$\mathcal{G}$ **= 4** Consequences can be detected in geographical extent AND in time duration. At least one C higher than threshold

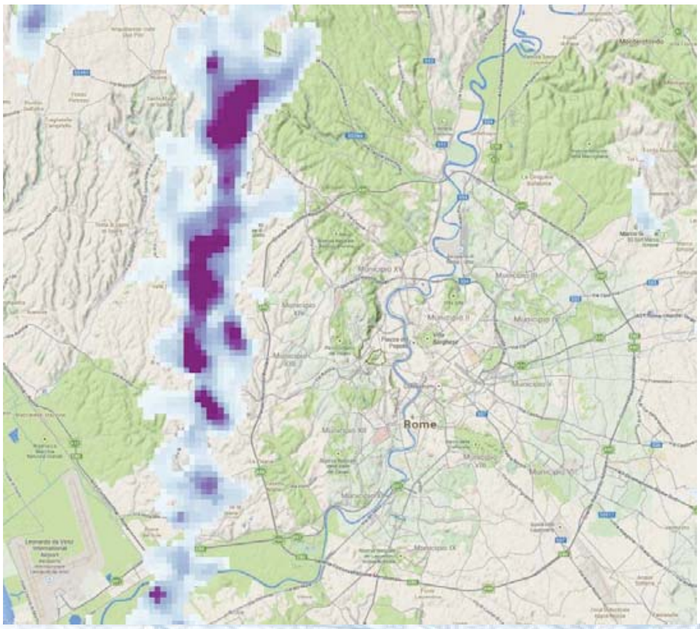
$\mathcal{G}$ **= 5** Consequences can be detected in geographical extent AND in time duration. Many C higher than thresholds

Test case



Nowcasting
Jan 31st 2014

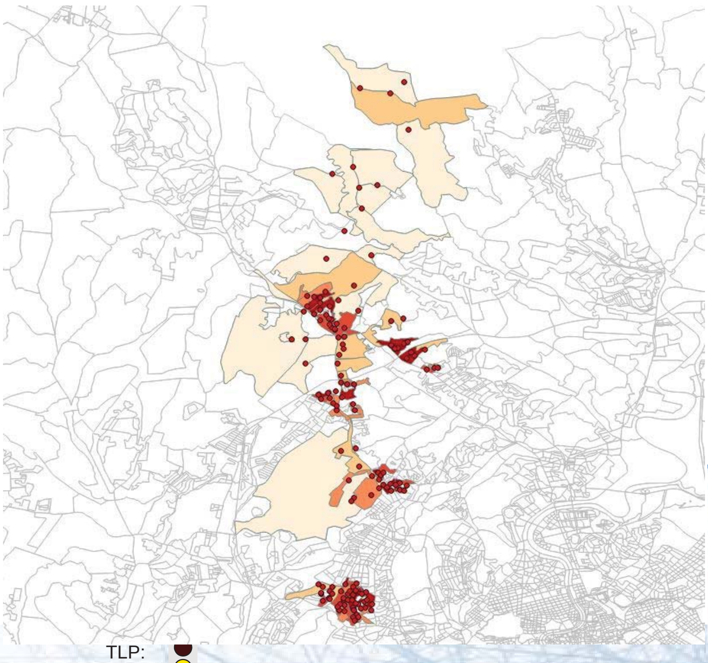
Test case



Case study:
Jan 31st 1.40 pm

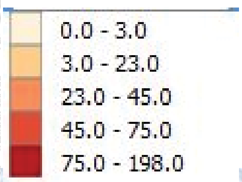
Predicted impact:
prolonged electrical outage
(> 1 hour)

Test case

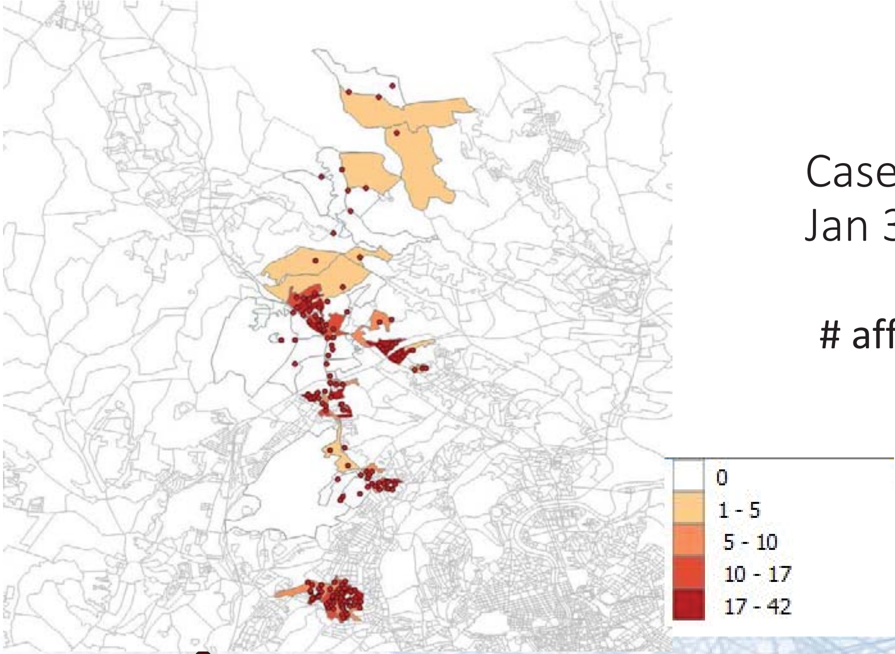


Case study:
Jan 31st 1.40 pm

affected people (y> 65)



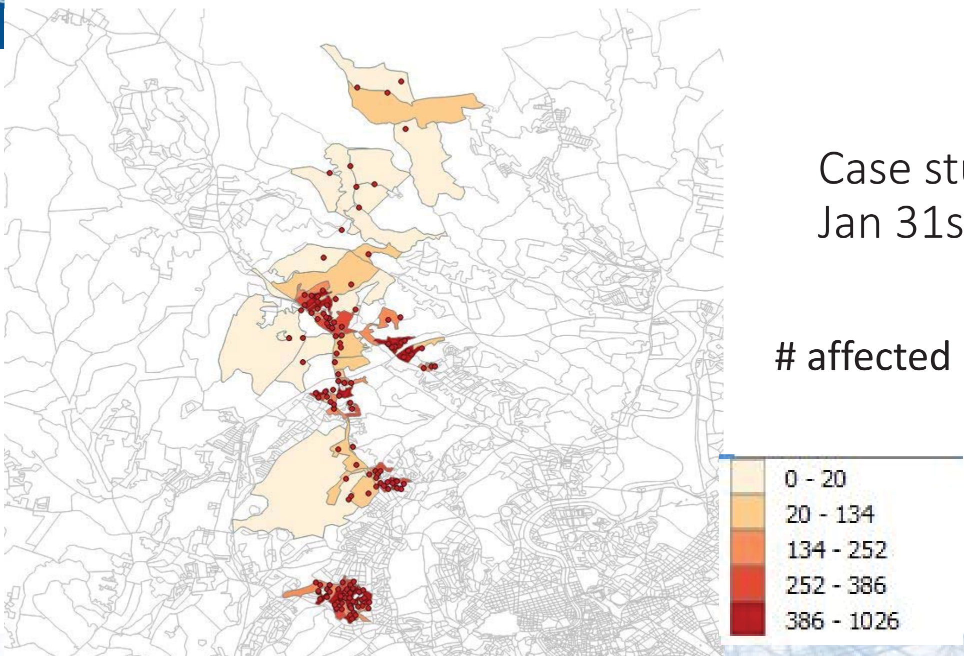
Test case



Case study:
Jan 31st 1.40 pm

affected people (y<5)

Test case

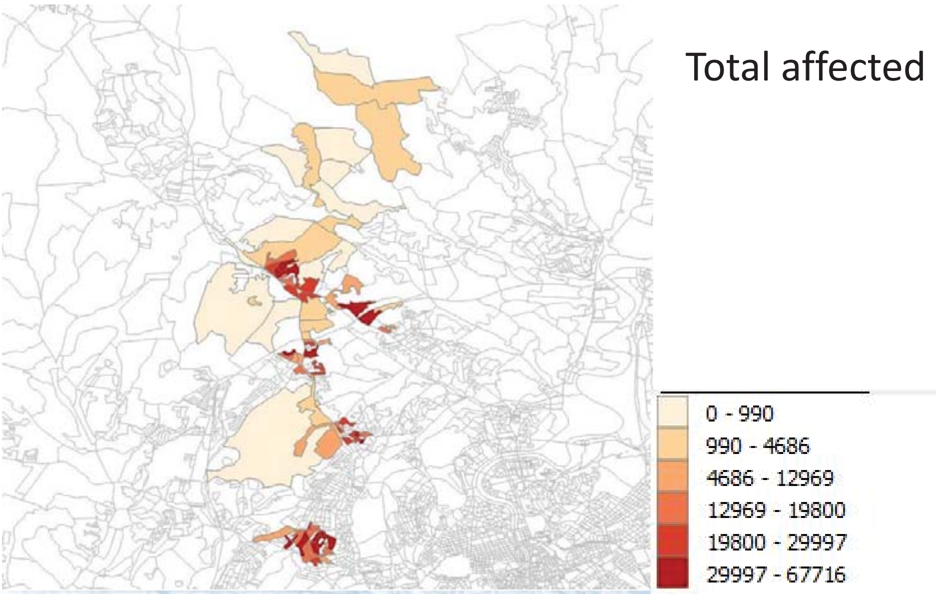


Case study:
Jan 31st 1.40 pm

affected people (35<y<65)

Test case

Total affected citizens



Conclusions

Consequences Analysis will thus end providing

- A Consequence vector ***C*** containing the expected Consequences for the different ***Criteria*** elements
- The Severity Grade of the predicted Crisis
- In particular cases, the DSS will provide indications on strategies to cope with the Crisis
  - Prediction of PV production (under development)
  - Resources optimisation: # CI elements to be restored ***F*** larger than the available Resources ***R*** (***F***> or >> ***R***) (under development)
  - Tracking of technical resources on the field: path optimisation by considering traffic jams (under development)

Conclusions

Consequences Analysis will thus provide

- A Consequence vector ***C*** containing the expected Consequences for the different ***Criteria*** elements
- The Severity Grade of the predicted Crisis
- In particular cases, the DSS will provide indications on strategies to cope with the Crisis
  - Prediction of PV production (under development)
  - **Resources optimisation: # CI elements to be restored *F* larger than the available Resources *R* (*F*> or >> *R*) (under development)**
  - Tracking of technical resources on the field: path optimisation by considering traffic jams (under development)

Conclusions

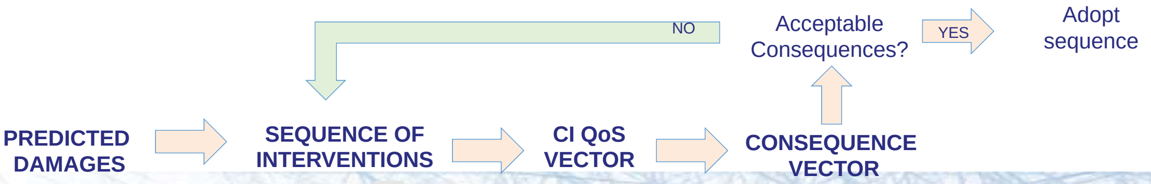
$F = [F_1, F_2, \ldots F_N]$

$R = [R_1, R_2, \ldots R_k]$

K< or << N

Optimization procedure

1. Select a Sequence of interventions $S = [S_1(R_j \rightarrow F_k), .. S_N]$
2. Estimate the Consequences associated to S
3. Generate S' (genetic algorithm)
4. Estimate the Consequences associated to S'
5. Compare C(S) with C(S')
6. If C(S')<C(S) then
   - $S' = S_{good}$
   - Go to 3
7. End when $C(S_{good}) < \varepsilon$



Thank you

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Events prediction and environmental sensing

Maurizio Pollino – ENEA (with Annette Zijderveld – Deltares contributions)
maurizio.pollino@enea.it

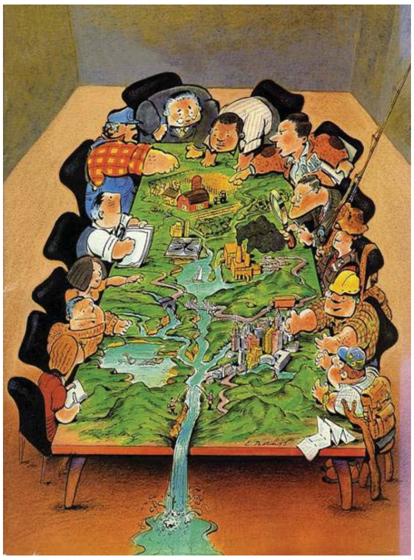
CIPRNet Course inside the Master in Homeland Security
Second Edition

University Campus Bio-Medico of Rome, 09-10July 2014

Fraunhofer IAIS ENEA TNO uic cea European Commission Deltares acris

Overview lecture

- Hazard prediction
- Weather, floods and landslide forecasting
- Forecasting process and lead time
- Vulnerability analysis
- Heavy rainfalls/heat waves example



Hazards: what can we predict?

Flash floods
Local precipitation of high intensity

Coastal flooding
Spring tides and storm surge

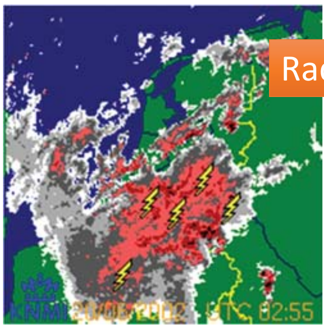
caused by rain or wind

Weather forecast

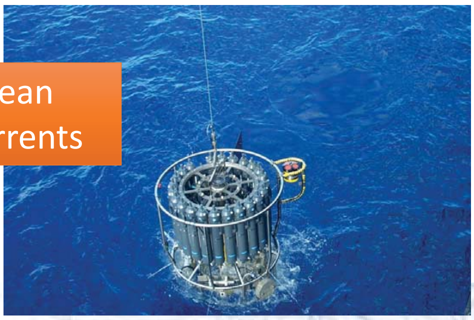
Landslide
Heavy long lasting precipitation / snow melt

Large scale flooding
Heavy long lasting precipitation / snow melt

Measurement data

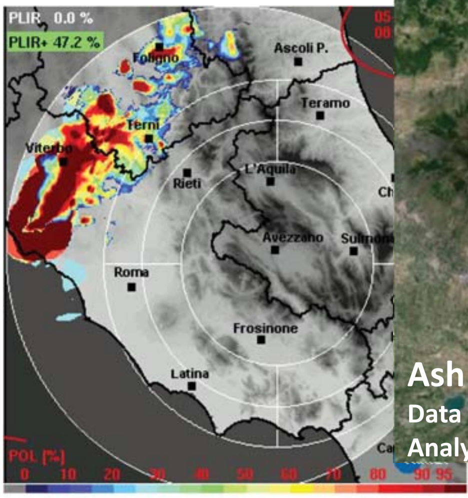


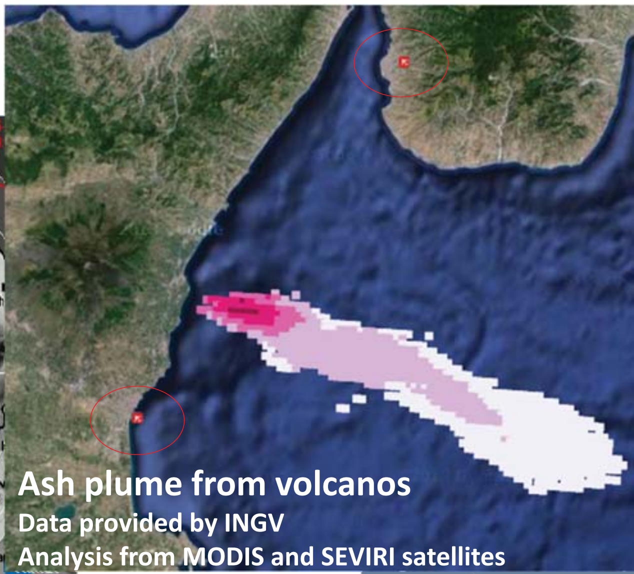
- Data availability increasing
- New sensor techniques
- Satellite information



…other measurement data

Lightning prediction





Weather forecast models

Time frame

Now-casting
Short range
Medium range
Monthly
Seasonal

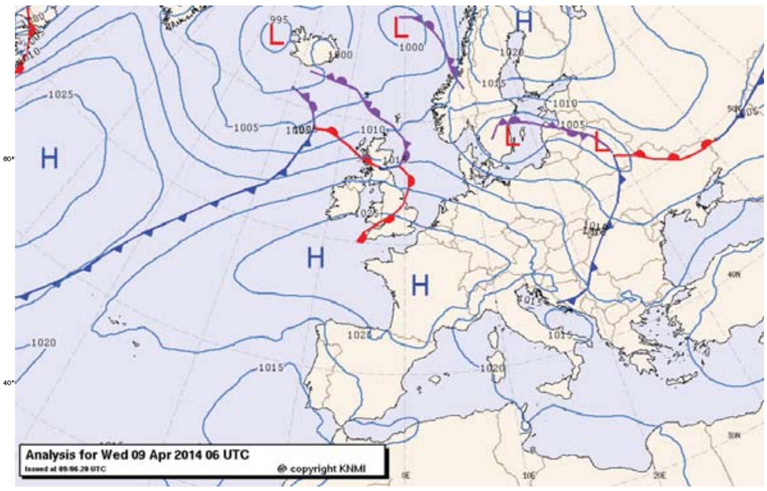
Spatial coverage

Global
Regional
Downscaling to local level

Modelling concepts

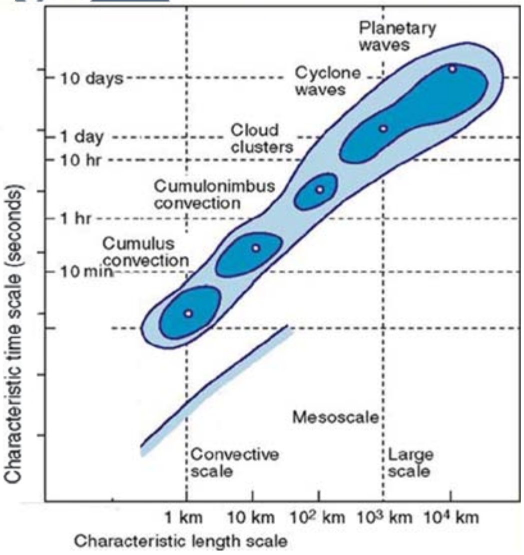
→ Deterministic models – 1 model run
→ Probabilistic models (ensemble of model runs)

Difference between models largest in extreme situations!



Source: KNMI, regional HiRLAM model

Weather forecasts: predictive skill



Time Range	0-12h	12 - 48 h	48 - 120 h
Type of Warning	WARNING	Pre-WARNING	Early WARNING
Product/ Area	**Actual local warnings**	**Regional warnings**	**Weather risk forecast**
Based on	Observations, Now-casting, Short range forecasting models	Deterministic and probabilistic models	Probabilistic models

Relation between atmospheric scale and time scale (adapted from ECMWF website)

Weather forecast example

•Numerical Weather Prediction grids in **FEWS-NL** (Rhine):

•**KNMI-HIRLAM**
- 48 hrs lead time

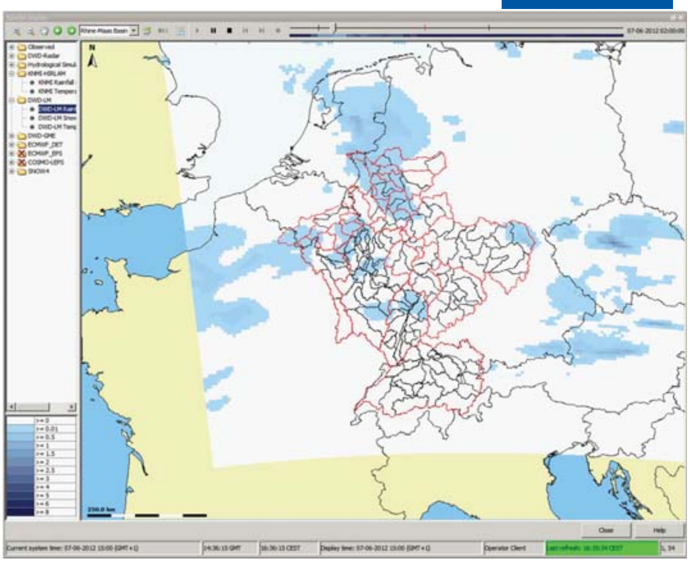
•**DWD-LM2**
- 78 hrs lead time

•**DWD-GME** (global)
- 174 hrs lead time

•**ECMWF deterministic**
- 240 hrs lead time

•**ECMWF ensemble**
- 240 hrs lead time
- 51 ensemble members

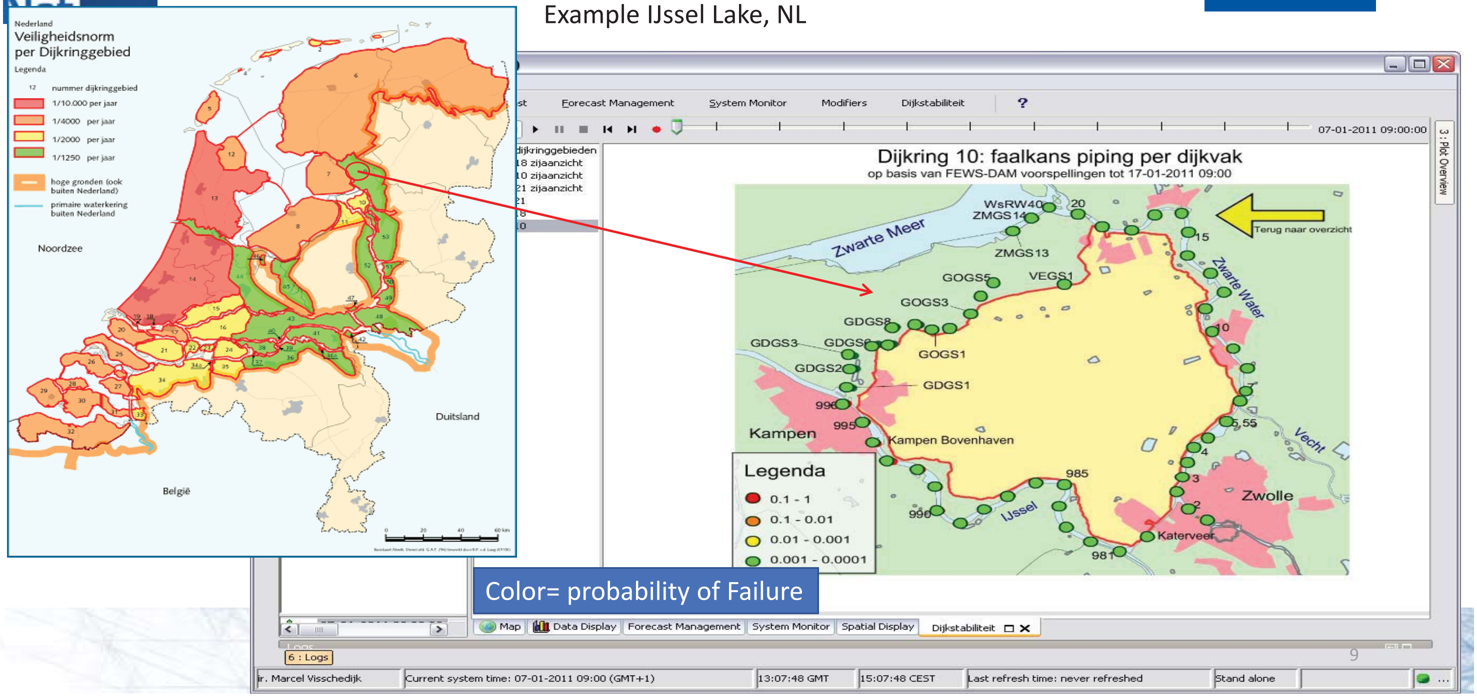
•**COSMO LEPS** (Limited-area Ensemble Prediction System)
- 160 hrs lead time
- 16 ensemble members



Dutch forecast system at RWS, weather forecast for River Rhine

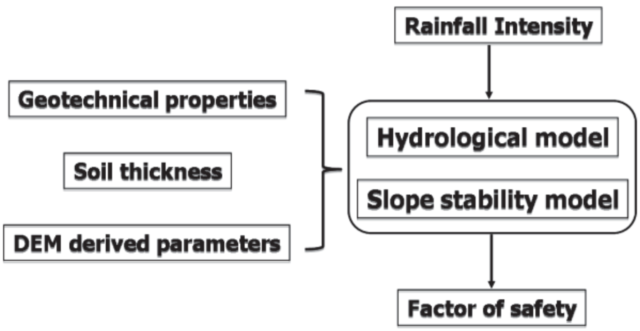
Real-time forecasts of levee strength

Example IJssel Lake, NL



Landslide prediction

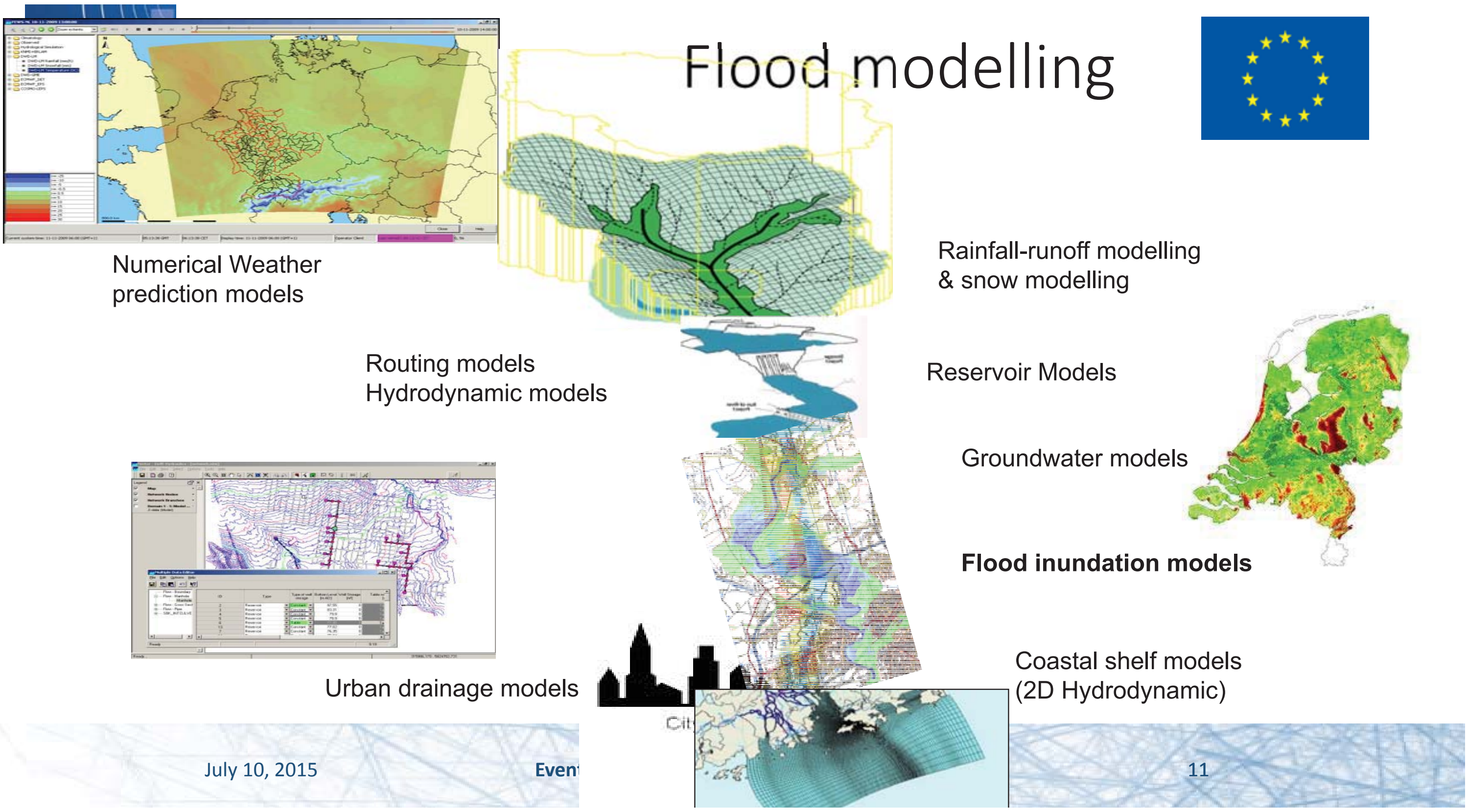
- Combination of different information sources and models
- Rain intensity and location important



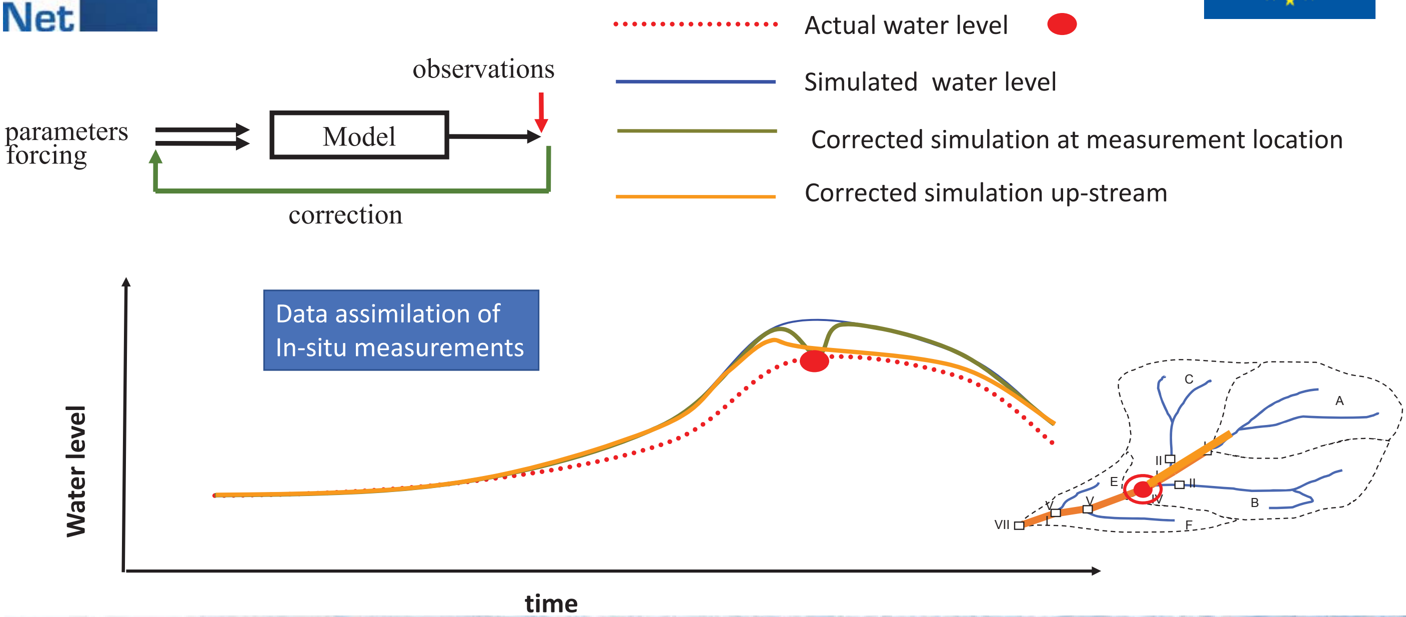
Forecast chain after S. Segoni et al, 2009

Source: SINAnet

Flood modelling

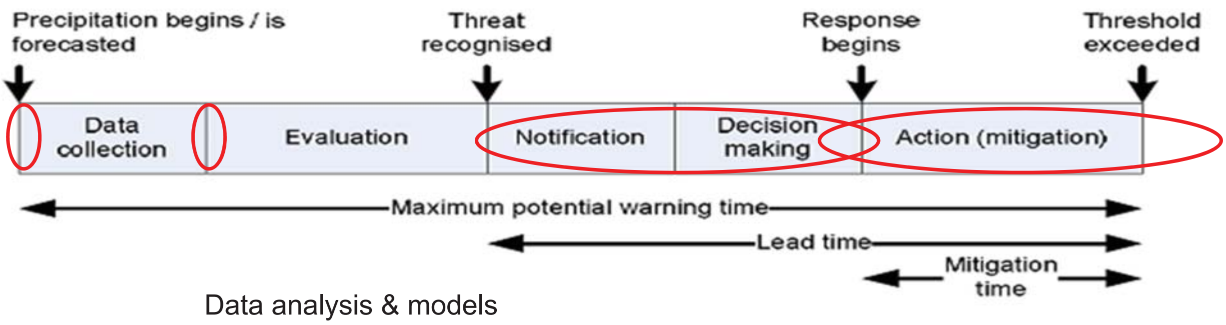


Data-Model integration



Concept of Lead time

Influencing factors



Data analysis & models

Carsell 2004; Verkade, 2008

Concept of Lead time

Examples: Response times of the river Rhine

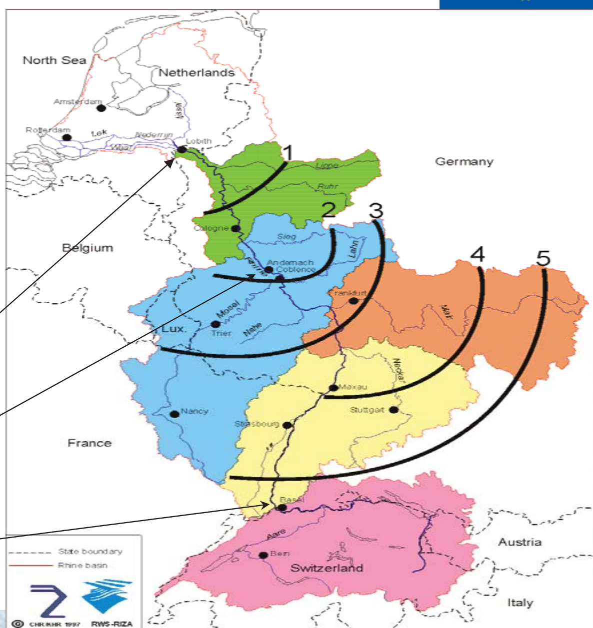
- Maximum response time of the flood wave is +/- 5 days
- Discharge entering NL at Lobith
- Largest contributions from the rivers Moselle and Main

Lead times not changed easily!

Lobith

Andernach

Rheinfelden

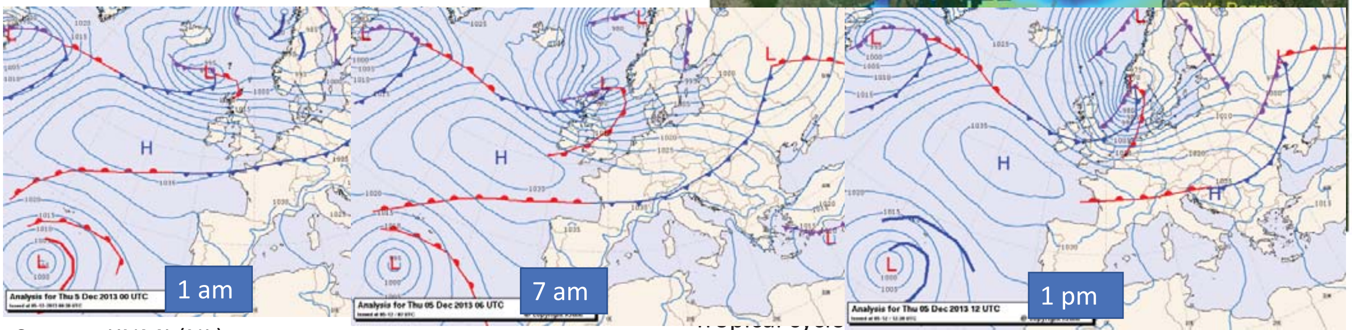


Concept of Lead time

Examples: coastal storm surges

- Tropical storm or North Sea: different behaviour
- Changes in tracks create uncertainty

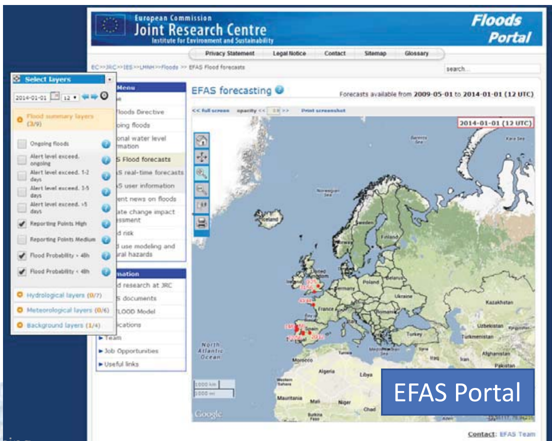
NW- storm at 5th December 2013
Higher water levels at UK coast than 1953
Highest water levels after 1953 in Belgium,
15 casualties in NW Europe



Source: KNMI (NL)

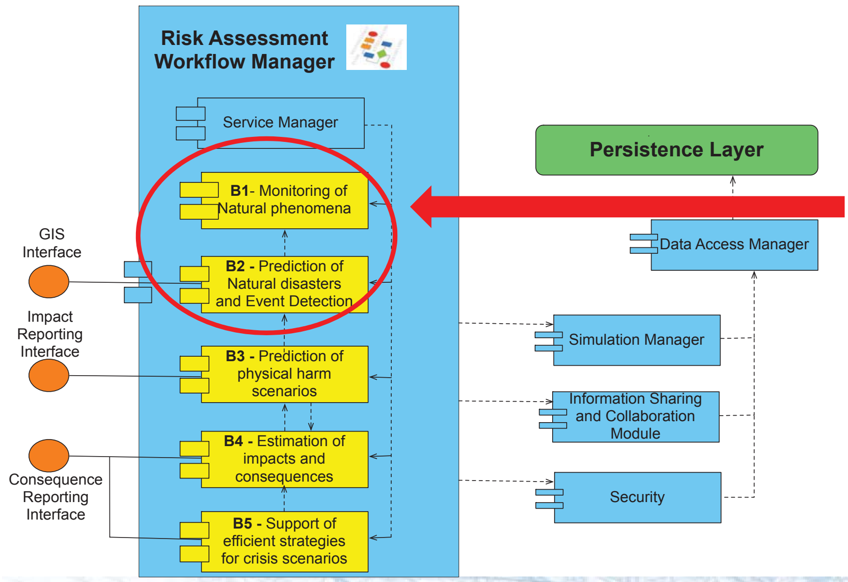
Available Forecasts in Europe

- Global Flood Awareness System (GloFAS) **http://www.globalfloods.eu/en/**
- Global Flood Partnership (GFP) **http://portal.gdacs.org/Global-Flood-Partnership**
- Copernicus Emergency Management Service (GMES) **http://www.copernicus.eu/**
- European Flood Awareness System (EFAS) **http://floods.jrc.ec.europa.eu/efas-flood-forecasts.html**
- National Forecasting Centres (Meteo/ Hydro)
- Civil Protection Agencies
- INGV (earthquake, Italy) **http://terremoti.ingv.it/en**
- CSEM-EMSC (earthquake, Europe) **http://www.emsc-csem.org/#2**



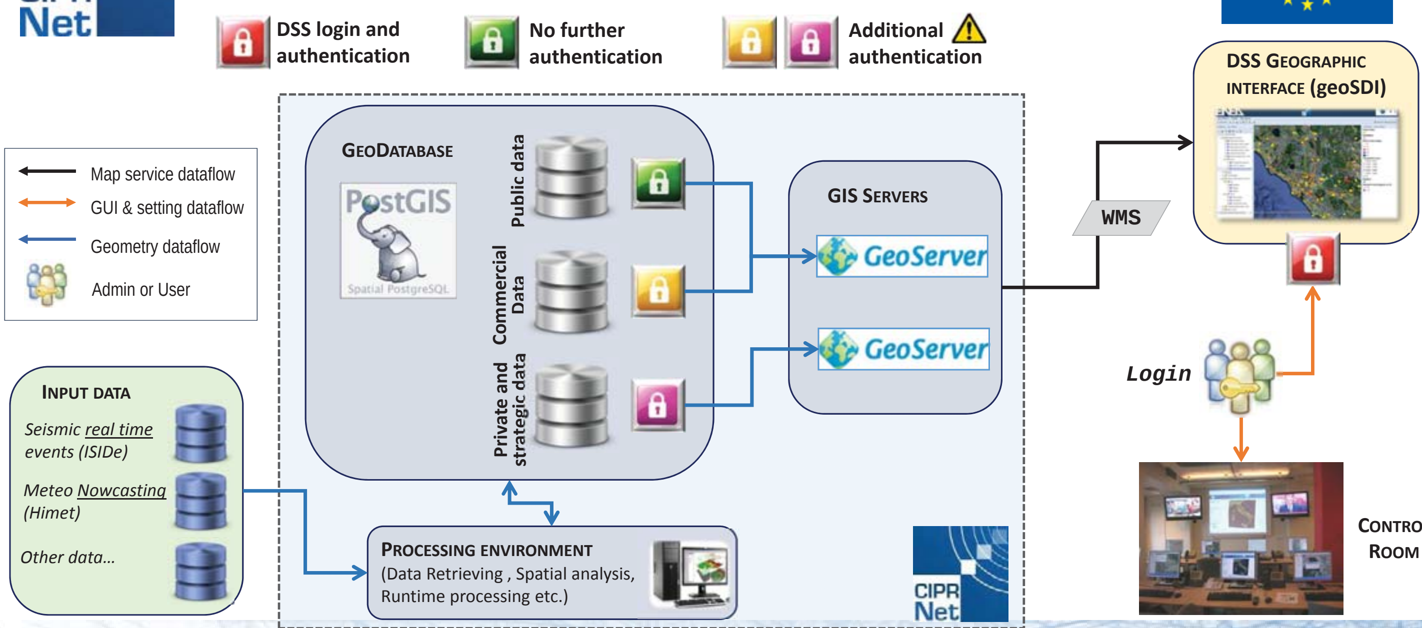
Output of Real-time Event Forecasting System
→ input for Decision Support System

DSS framework: blocks overview

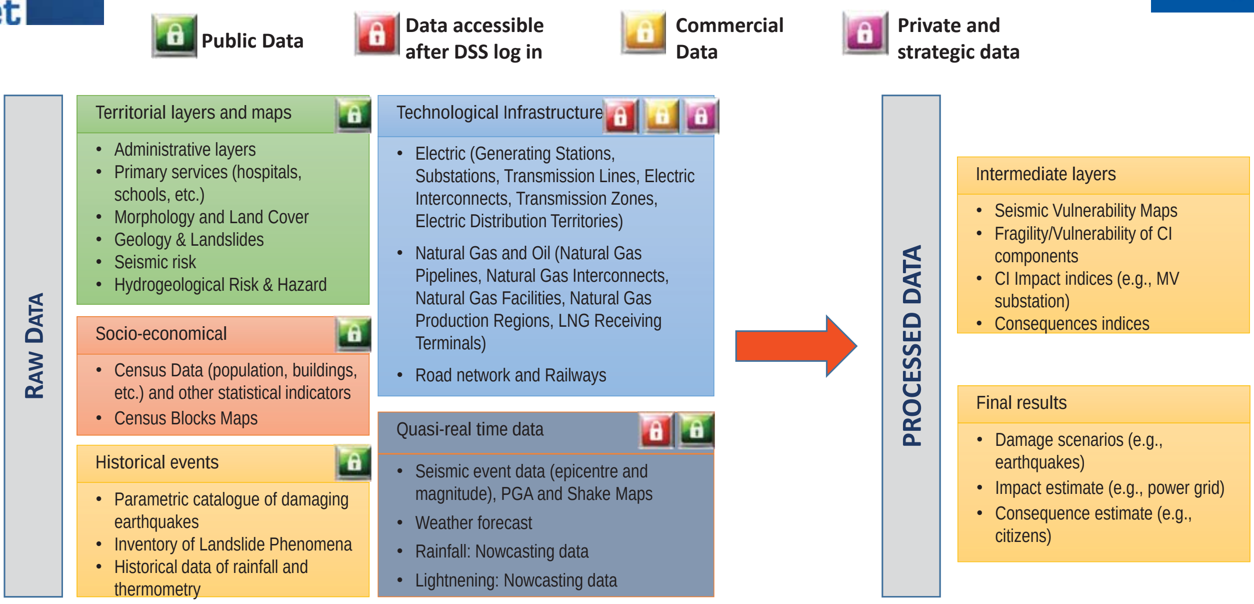


- **Monitoring of Natural phenomena**
- **Prediction of Natural disasters**

DSS data flow and processing



Data ontology and structure



Vulnerability analysis

The Damages estimation block transforms the predicted Events (with their predicted Strength) in Damages to CI elements and, wherever possible, to other types of assets (Buildings, Plants etc.)

The list of Events which will be monitored and whose effects will be “transformed” into Damages are the following:

- Earthquakes
- Abundant rainfalls
- Heat/Cold temperatures waves
- Strong Winds
- Lightning
- Heavy snowfall
- Ice/Frost
- Landslide
- Flash flood
- Flooding
- Mud flows
- Debris avalanches
- Storm surges

Vulnerability analysis

Two different methods will be used to identify "vulnerability" of the different CI elements versus each considered threat

a. inferring vulnerability data thresholds from historical data (when available)
   1. Elements with pronounced fault correlation with events
   2. General trend of vulnerability versus event's strength

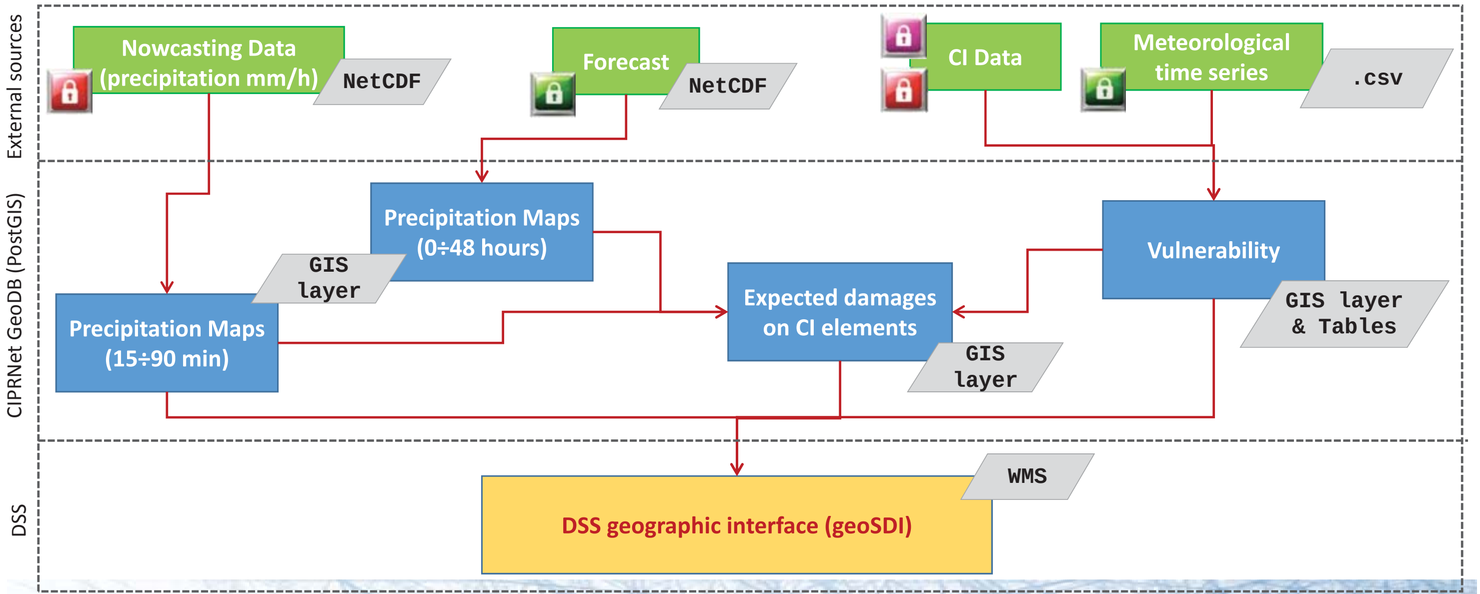
b. getting vulnerability thresholds by CI elements technical data
   1. Direct access (from explicit values, when available)
   2. Indirect access (from empirical formulas)

- Earthquakes
- Abundant rainfalls
- Heat/Cold temperatures waves
- Strong Winds
- Lightening
- Heavy snowfall
- Ice/Frost
- Landslide
- Flash flood
- Flooding
- Mud flows
- Debris avalanches
- Storm surges

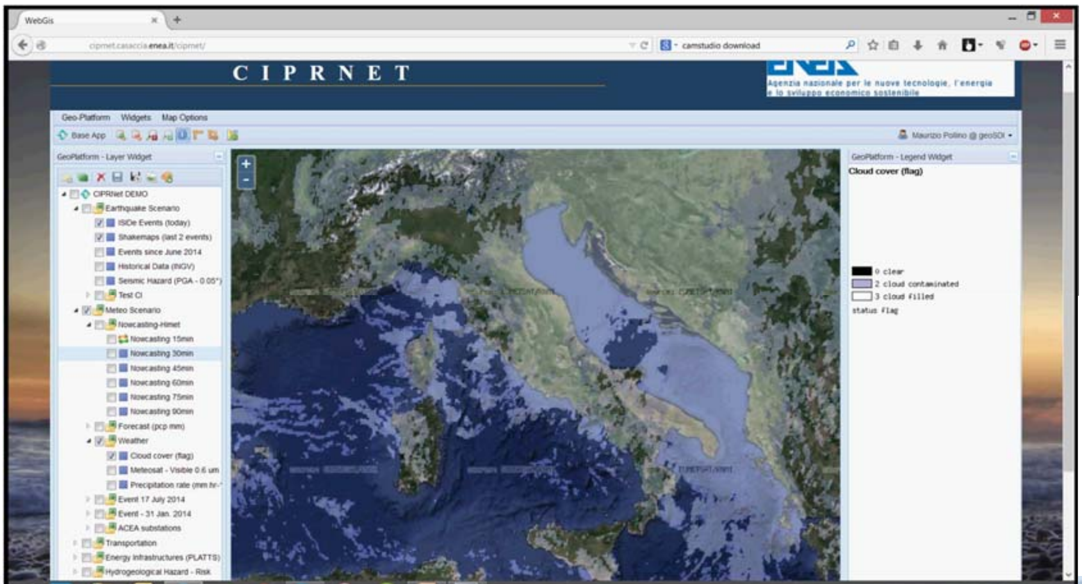
Vulnerability analysis: matrix

Natural threat	Historical fault data method (a1 and a2 options)	Data sheet method (b1 option)	Analytical based method (b2 option)
Earthquakes			✔
Abundant rainfalls	✔		
Heat/Cold waves	✔		
Strong Winds		✔	
Lightening		✔	
Heavy snowfall	✔		
Ice/Frost	✔		
Landslide	✔		
Flash flood	✔		
Flooding	✔		
Mud flows	✔		
Debris avalanches	✔		
Storm surges	✔		

Example of Data flow: Weather Forecast/Nowcasting



Weather Forecast/Nowcasting



Vulnerability analysis: abundant rainfalls and heat waves

Option (a)

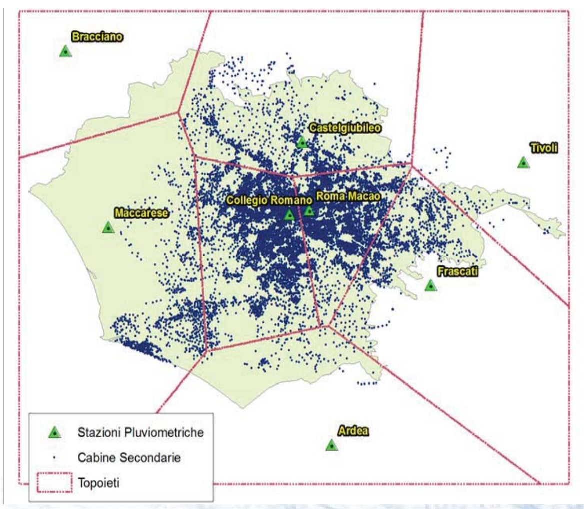
a. inferring vulnerability data thresholds from historical data (when available)
   1. Elements with pronounced fault correlation with events
   2. General trend of vulnerability versus event's strength

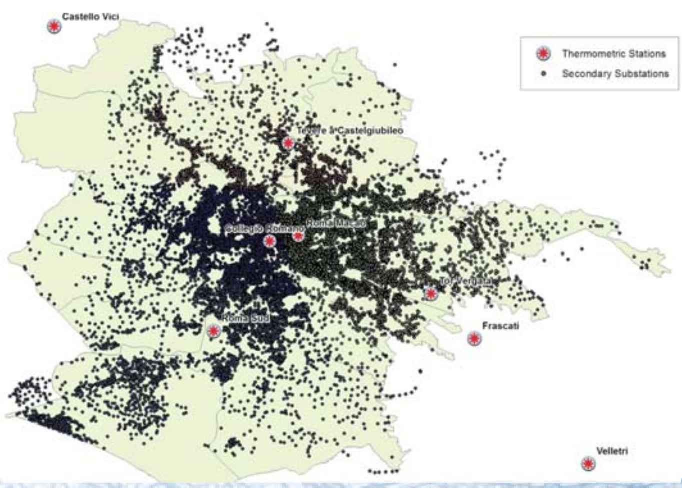
Available data

- historical data of *sparse* GIS-referenced weather stations (or any other types of sensors)
- Log file of faults in CI elements of a given operator
- GIS position of CI elements

Vulnerability analysis: abundant rainfalls and heat waves

Thiessen tassellation is used for dividing the area of Roma by using official Rain Gauges and Thermometers





Vulnerability analysis: abundant rainfalls and heat waves

Abundant rainfalls and heat waves

We used historical data of rain gauges and thermometers for correlating faults of electrical cabins EC repeatdly occurred in heavy rain days (P>20 mm/day) and hot days (T_{max}>30 °C).

We have defined the following quantity:

$$\delta(EC_i) = \text{(\#faults of } EC_i \text{ occurred in critical days)}^2 \,/\, \text{(\# critical days)}$$

If we set δ**(EC_i)** > 1, we get the following map of “vulnerable” EC to rain or to hot waves

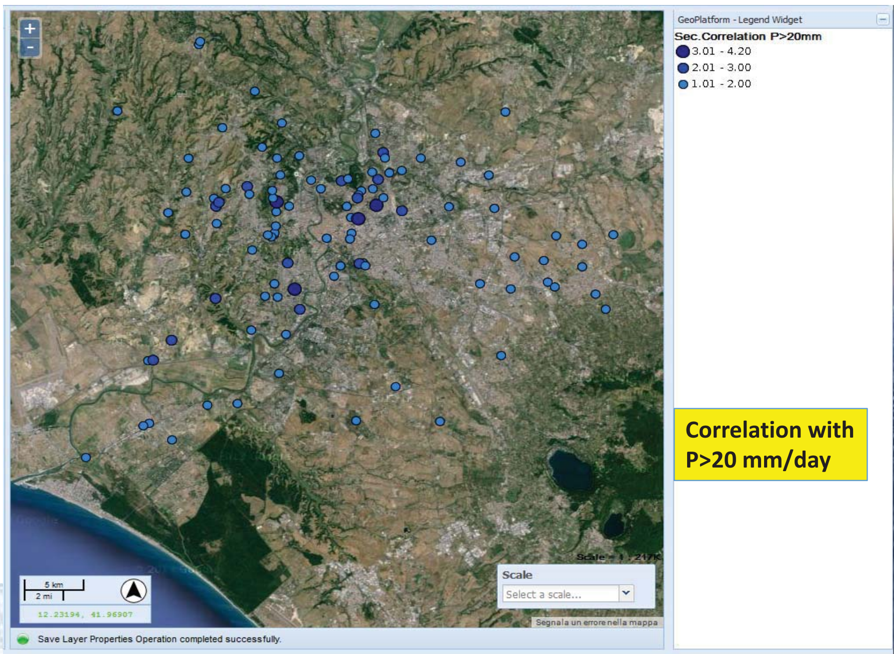
The square on the numerator allows to avoid to use a 1-norm value ($\delta(EC_i)$=1 could also occur in cases when EC_i is faulted once in a single rainy day).

Vulnerability analysis: abundant rainfalls and heat waves

Vulnerability to meteorological events

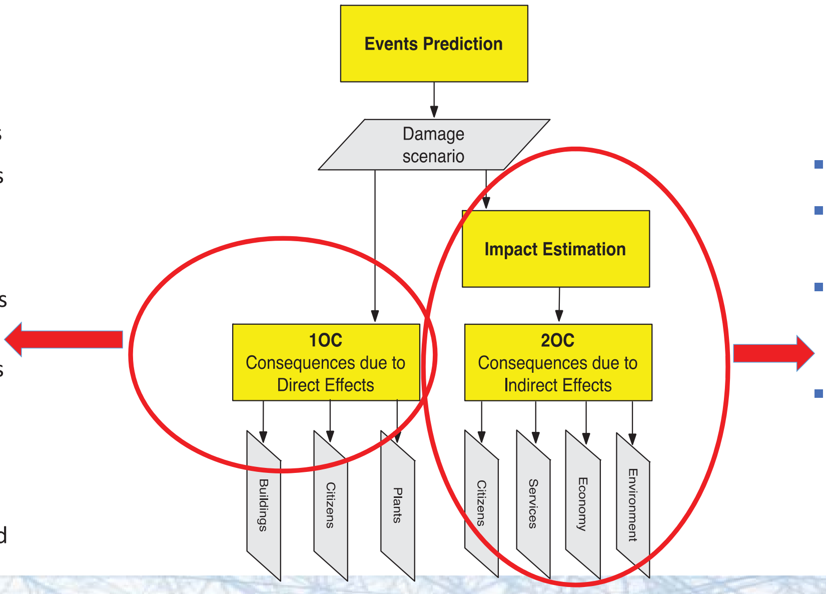
The vulnerability assessment is based on the statistical elaboration of:

- failure events/anomalies reported by CI owner;
- meteorological time series (last 10 years) of precipitation and temperature.



Damages estimate

- damages to buildings and estimated related casualties
- damages to industrial plants and estimated related casualties
- damages to roads, railways and estimated related losses in mobility
- damages to industrial plants and estimated related GDP losses
- Expected flooded areas and number of involved citizens
- flooded areas and estimated related GDP losses



- Damages to CI elements
- Impacts (loss of Service) to Power and telco systems
- Cascading effects to other CI and to some Essential Services (e.g. Hospitals)
- Consequences on 4 Criteria
  - Citizens
  - Primary Services
  - Economical
  - Environment

Conclusions

- Hazard prediction always combination of available measured data and model simulations, using different concepts
- Numerical model systems dominant in forecasting systems
- Leads times for warning depended on system behaviour
- Real-time services are increasing: both in quality as well in lead-time for different type of hazards
- The DSS could attempt to support the decision also through the finding of appropriate strategies which could be optimized by using the large amount of information present in the System

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Risk analysis tools for events and damages simulations

Maurizio Pollino - ENEA
maurizio.pollino@enea.it

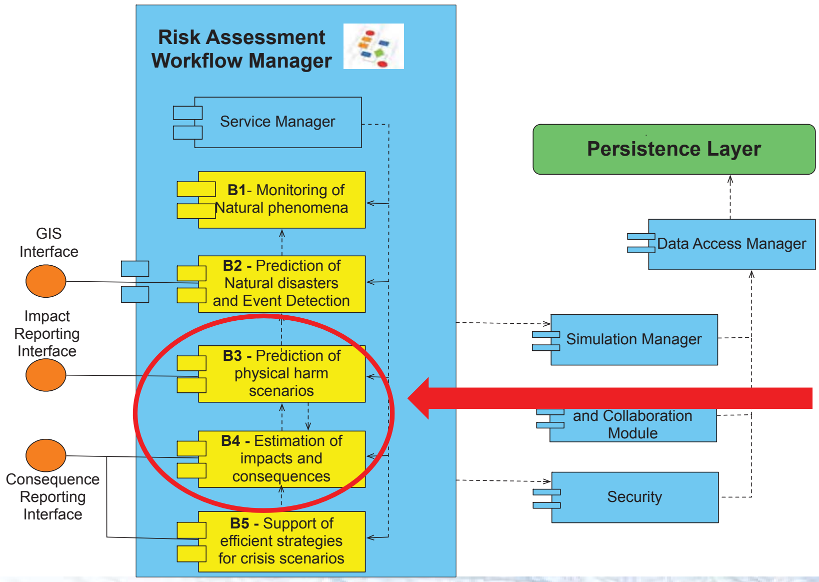
CIPRNet Course inside the Master in Homeland Security
Second Edition

University Campus Bio-Medico of Rome, 09-10July 2014

Outline

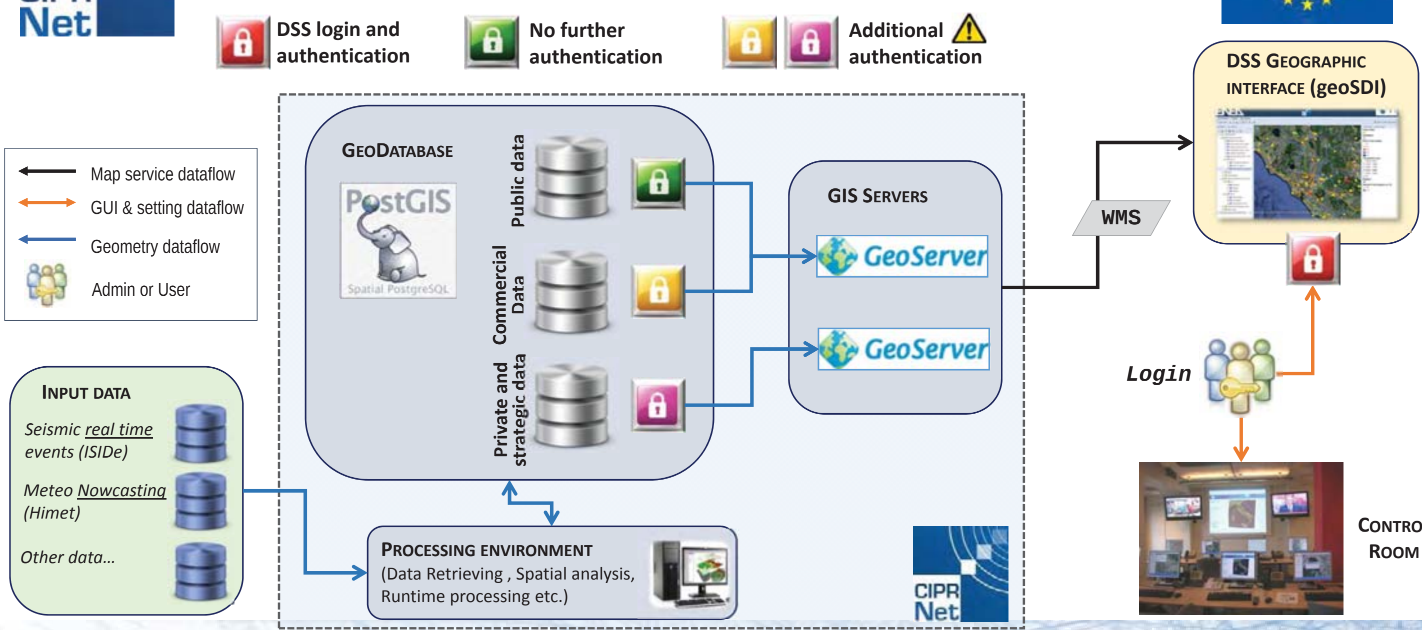
- DSS framework;
- Data flow and processing;
- GIS procedures;
- Vulnerability analisys;
- Earthquake event:
  - Real time monitoring
  - Simulation
- Conclusions

DSS framework: blocks overview



- **Earthquake Real Time Monitoring**
- **Earthquake Simulation**

DSS data flow and processing



Data ontology and structure

Public Data | Data accessible after DSS log in | Commercial Data | Private and strategic data

RAW DATA

Territorial layers and maps
- Administrative layers
- Primary services (hospitals, schools, etc.)
- Morphology and Land Cover
- Geology & Landslides
- Seismic risk
- Hydrogeological Risk & Hazard

Socio-economical
- Census Data (population, buildings, etc.) and other statistical indicators
- Census Blocks Maps

Historical events
- Parametric catalogue of damaging earthquakes
- Inventory of Landslide Phenomena
- Historical data of rainfall and thermometry

Technological Infrastructure
- Electric (Generating Stations, Substations, Transmission Lines, Electric Interconnects, Transmission Zones, Electric Distribution Territories)
- Natural Gas and Oil (Natural Gas Pipelines, Natural Gas Interconnects, Natural Gas Facilities, Natural Gas Production Regions, LNG Receiving Terminals)
- Road network and Railways

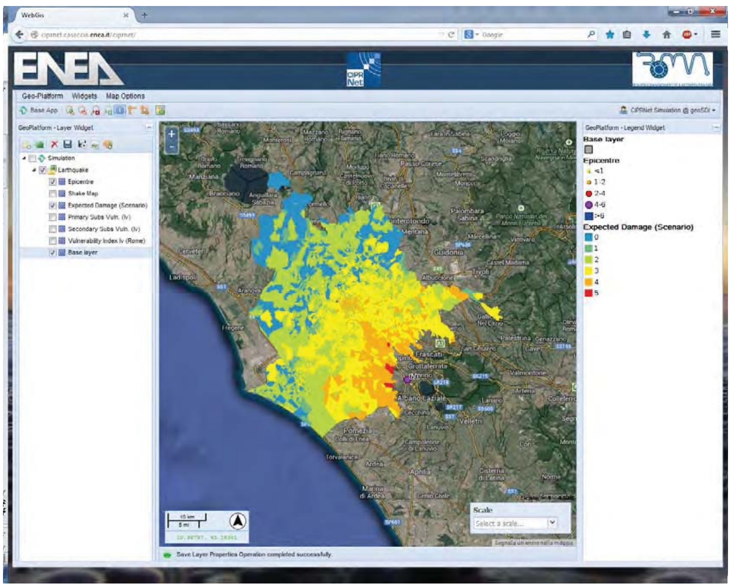
Quasi-real time data
- Seismic event data (epicentre and magnitude), PGA and Shake Maps
- Weather forecast
- Rainfall: Nowcasting data
- Lightnening: Nowcasting data

PROCESSED DATA

Intermediate layers
- Seismic Vulnerability Maps
- Fragility/Vulnerability of CI components
- CI Impact indices (e.g., MV substation)
- Consequences indices

Final results
- Damage scenarios (e.g., earthquakes)
- Impact estimate (e.g., power grid)
- Consequence estimate (e.g., citizens)

GIS spatial analysis and procedures



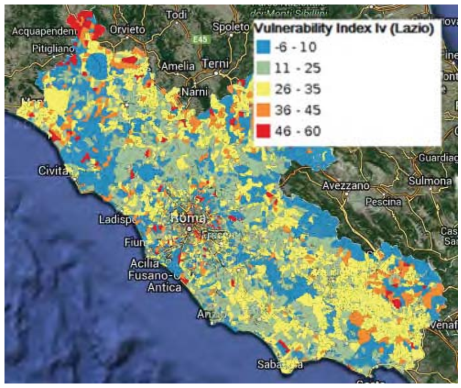
Spatial analysis procedures and geo-processing operations:
- Description and characterization of the study area (Geodatabase);
- Data management (Geomorphology, Seismic Risk, Census, Facilities and CI location, etc.);
- Shake maps processing (PGA/I_{MCS});
- Production of Vulnerability maps
- Elaboration of Damage Scenarios.

Results:
- **Real time monitoring** to support the management of near/post-event phases;
- Events **simulation**;
- Consultation via DSS WebGIS application.

Earthquake Event: DSS application example

- First information available immediately after a significant earthquake: magnitude and epicenter.
- Through geo-processing and visualization tools, shaking maps are overlaid with inventories of critical infrastructures (e.g., power/telco neteworks, gas pipelines, transportation, etc.) and vulnerable structures.
- Decision makers and responders, by knowing potential impacts and damages, can act more quickly and effectively, immediately after the seismic event.
- Moreover, considering the seismic characteristics and the vulnerability of an area, it is possible to simulate the potential impacts of an earthquake in that area: the results can be exploited to enhance the resilience of structure and infrastructure.

Vulnerability analysis



To evaluate the **seismic vulnerability** of structures, a detailed buildings inventory of the interest regional area is needed (source: ISTAT Census dataset).

Aggregated data related to buildings:

- structural typology (Masonry or Reinforced Concrete);
- age of construction;
- number of storeys.

The **vulnerability index (Iv)** for each census section has been calculated by using the Lagomarsino and Giovinazzi (2006) approach[1]. For each Census parcel the Map reports Iv values, ranging from -6 (min) to di 60 (max).

[1]: *Lagomarsino, S.; Giovinazzi, S. Macroseismic and mechanical models for the vulnerability and damage assessment of current buildings. Bull. Earthq. Eng. 2006, 4, 415–443*

Construction age	I_V	
	Masonry	RC
Before 1919	50	-
1919–1945	40	-
1946–1961	30	20
1962–1971	30	20
1972–1981	20	20
1982–1991	20	0
After 1991	20	0

No. of storeys \ Age	<1919	1919–1945	1946–1961	1962–1971	1972–1981	1982–1991	>1991
1	0	0	0	0	0	–6	–6
2	+5	+5	+5	+5	+5	0	0
3	+5	+5	+5	+5	+5	0	0
>4	+10	+10	+10	+10	+10	+6	+6

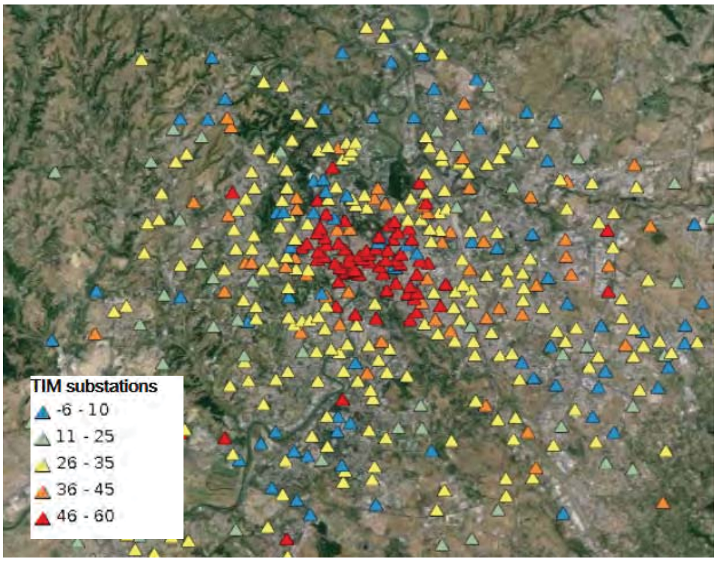
Vulnerability analysis

Starting from the detailed inventory of CI (e.g., electrical/telco substations, etc.), it has been extensively evaluated the **seismic vulnerability of each CI element**.

Vulnerability index (Iv) values have been derived from the corresponding Iv value of the building in which each element is located.

Such Iv value was opportunely reduced, taking into account the intrinsic characteristics of the element considered (for example, an electrical substation located under a trapdoor, situated at ground level, is characterised by a very low Iv value)

For each CI has been produced the relative Map reporting Iv values, ranging from -6 (min) to di 60 (max).



Vulnerability analysis

Shake Maps: empirical prediction of Peak Ground Acceleration (PGA) propagation

- Low magnitude (<4):

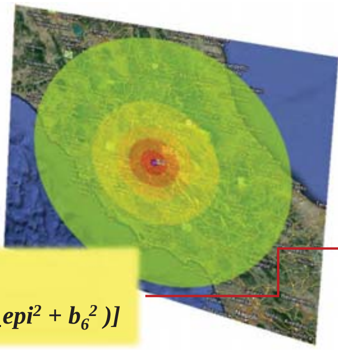
$$log_{10}(pga) = A + B \cdot (Mag - 6) + C \cdot log_{10}[sqrt(R\_epi^2 + H^2)]$$

Where:

A	B	C	H
4.037	0.572	-1.757	6.0

- High magnitude[2] (≥4):

$$log_{10}(pga) = b_1 + b_2 \cdot Mag + b3 \cdot Mag^2 + (b_4 + b_5 \cdot Mag) \cdot log_{10}[sqrt(R\_epi^2 + b_6^2)]$$



2. Akkar, S. and Bommer, J.J., 2007. "Empirical prediction equations for peak ground velocity derived from strong-motion records from Europe and the Middle East," Bulletin of the Seismological Society of America, Vol. 97(2), 511-530

Where:

b1	b2	b3	b4	b5	b6	s1	s1m	s2	s2m
1.647	0.767	-0.074	-3.162	0.321	7.682	0.557 -	0.049	0.189	-0.017

- PGA conversion to I_{MCS} (Macroseismic Intensity) by means the Decanini et al. formula[3] (1995):

$$log\ PGA = 0,594 + 0,197 \cdot I_{MCS}$$

3. Decanini, L., Gavarini, C. & Mollaioli, F., 1995. «Proposta di definizione delle relazioni tra intensità macrosismica e parametri del moto del suolo», Atti 7.mo Convegno L'ingegneria sismica in Italia, 1, 63-72

Vulnerability analysis

Expected damage
(Lagomarsino & Giovinazzi, 2006)

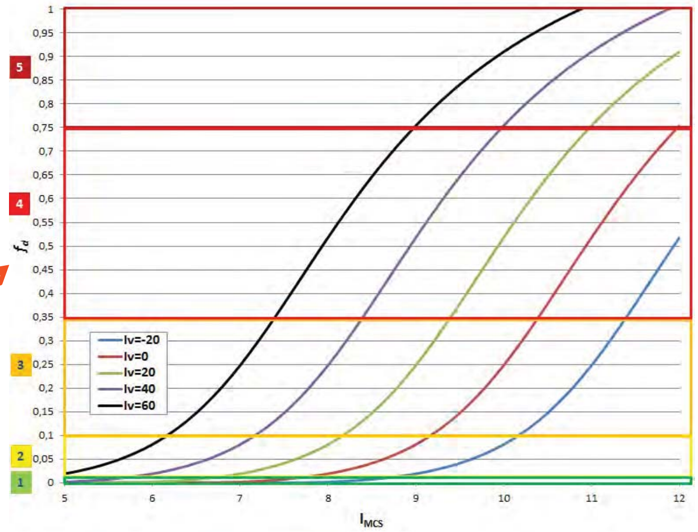
- Mean damage d:

$$d = 0.5 + 0.45\{\arctan[0.55(I_{MCS} - 10.2 + 0.05\,Iv)]\}$$

- Transition from mean damage d to the **fragility index** f_d:

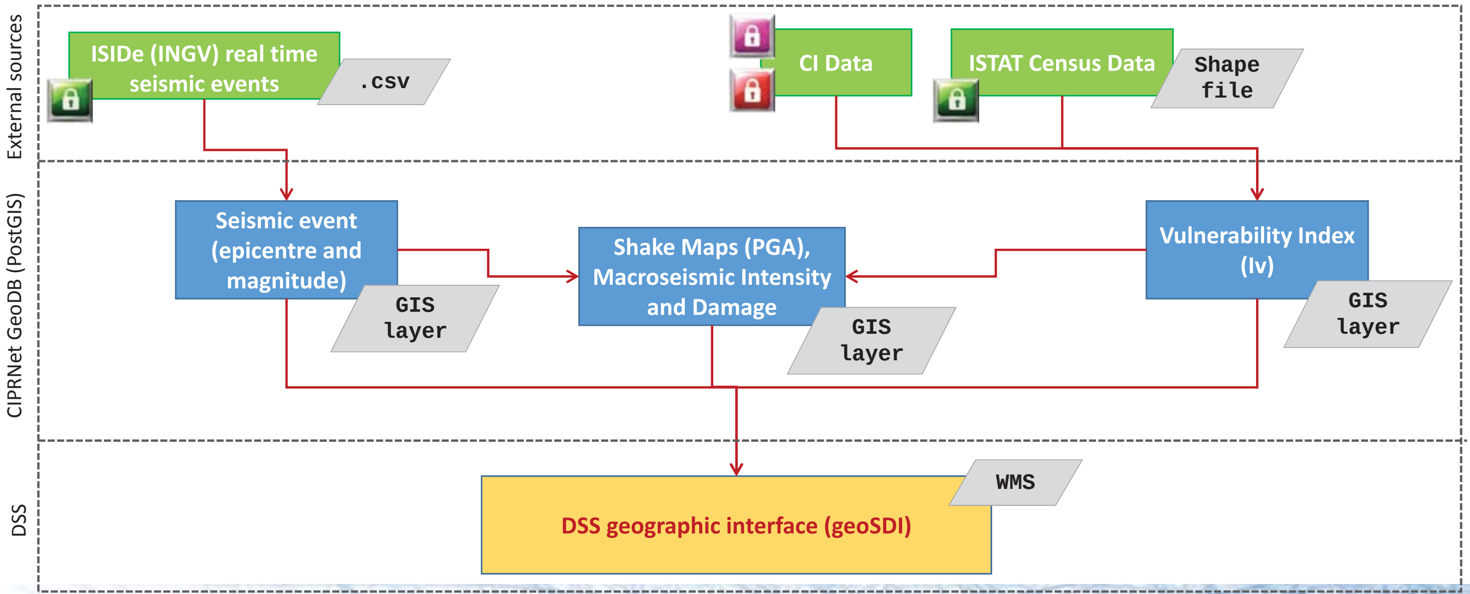
$$f_d = d^{1.75}$$

- **Level of damage** (1÷5)



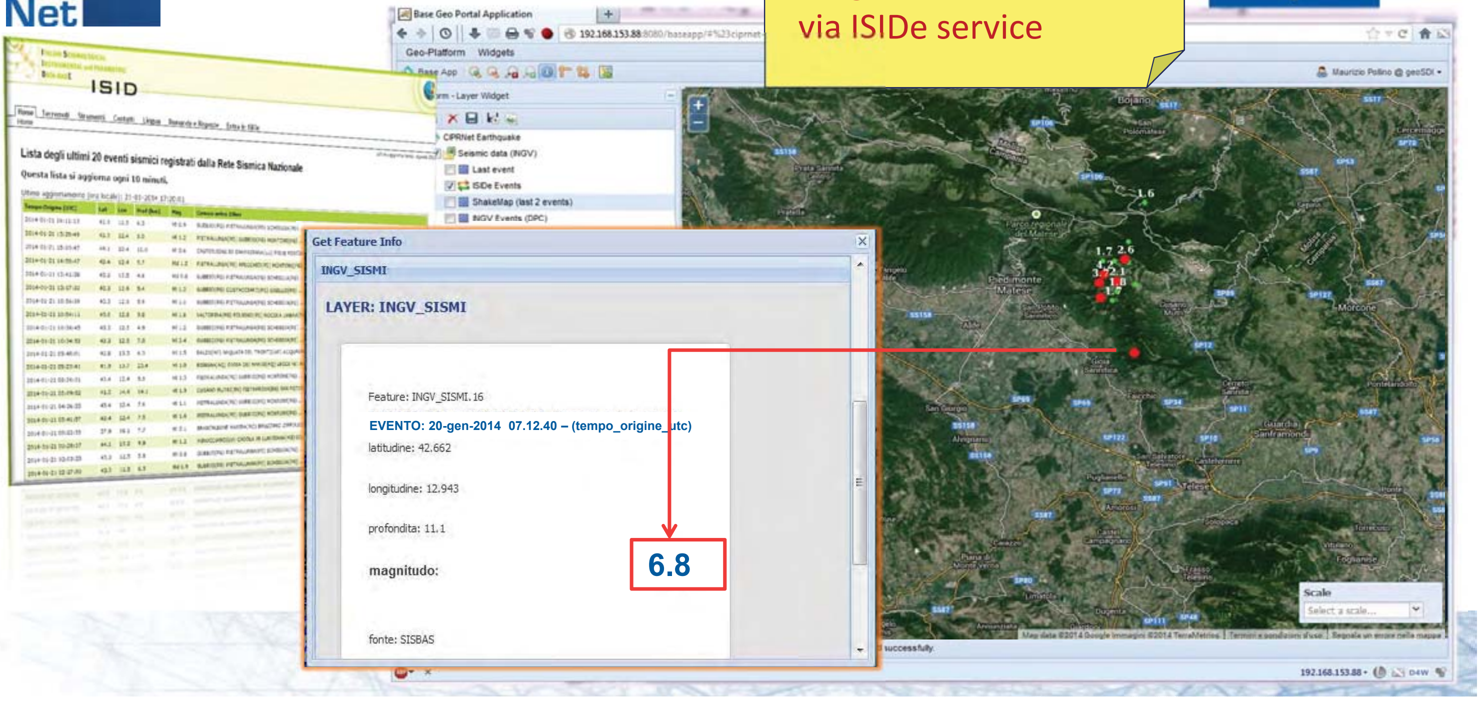
Factor of Damage (f_d)	0	0.01	0.1	0.35	0.75	1
Level of Damage	0	1	2	3	4	5

Example of Data flow:
Earthquake – Real Time Operational



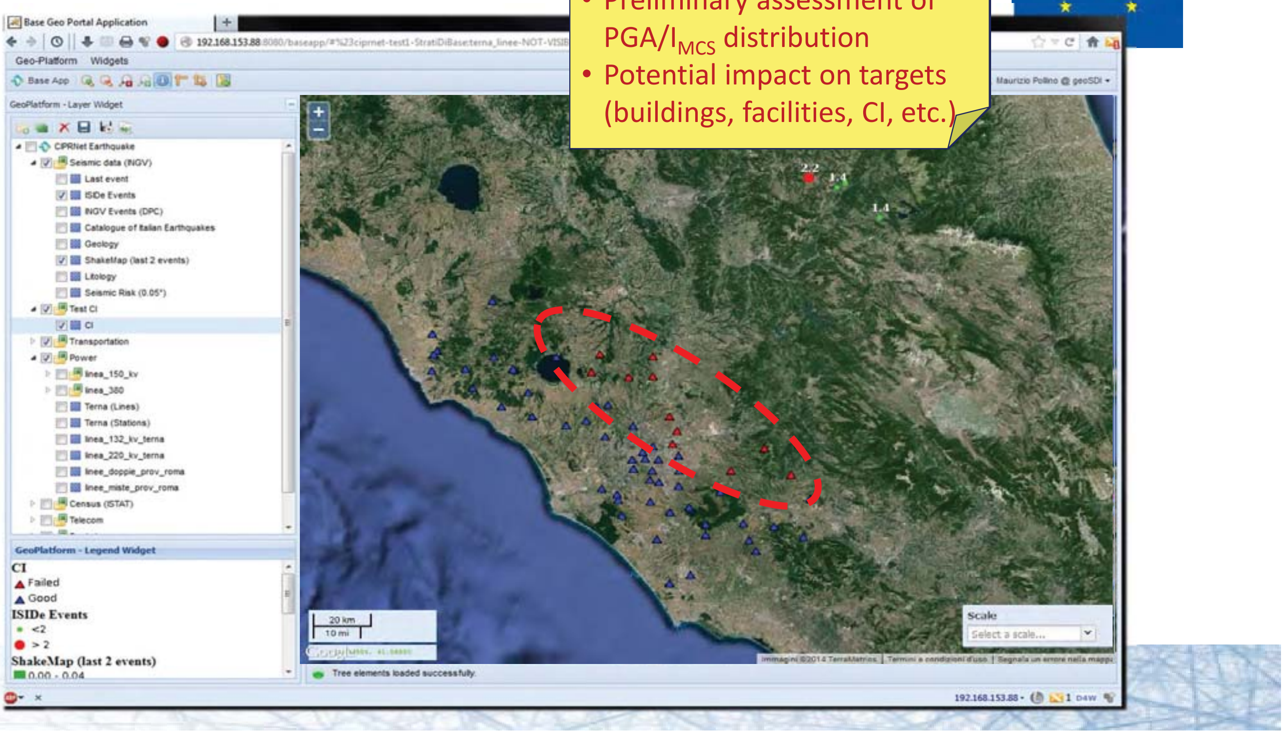
Earthquake Event – Step 1
(T$_0$ ÷ few minutes)

- Get event data (Epicentre and Magnitude) from INGV, via ISIDe service



Earthquake Event – Step 1
(T$_0$ ÷ few minutes)

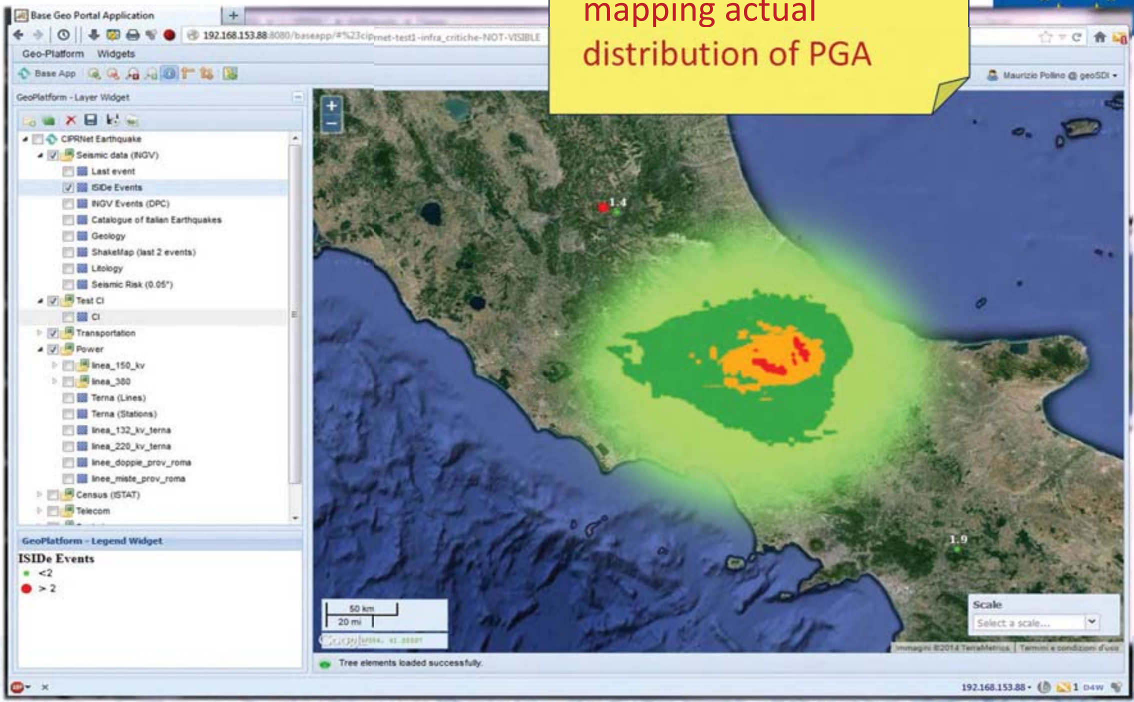
- Theoretical Shake-Maps production
- Preliminary assessment of PGA/I$_{MCS}$ distribution
- Potential impact on targets (buildings, facilities, CI, etc.)



Earthquake Event – Step 2

($T_0 \div$ 1-2 hours)

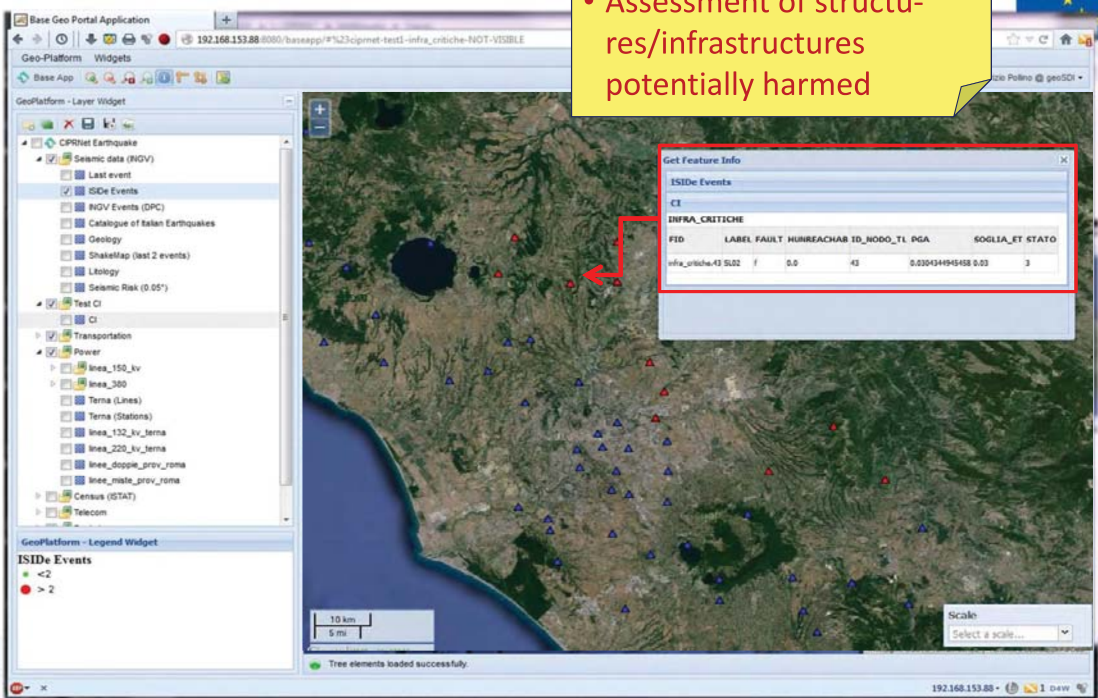
- Get Measured Shake-Maps from INGV: mapping actual distribution of PGA



Earthquake Event – Step 2

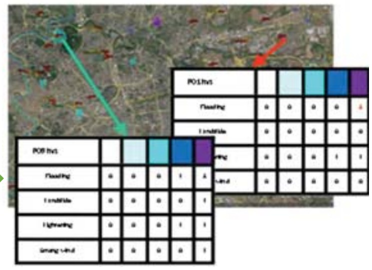
($T_0 \div$ 1-2 hours)

- Impact on CI after the main shock
- Assessment of structures/infrastructures potentially harmed



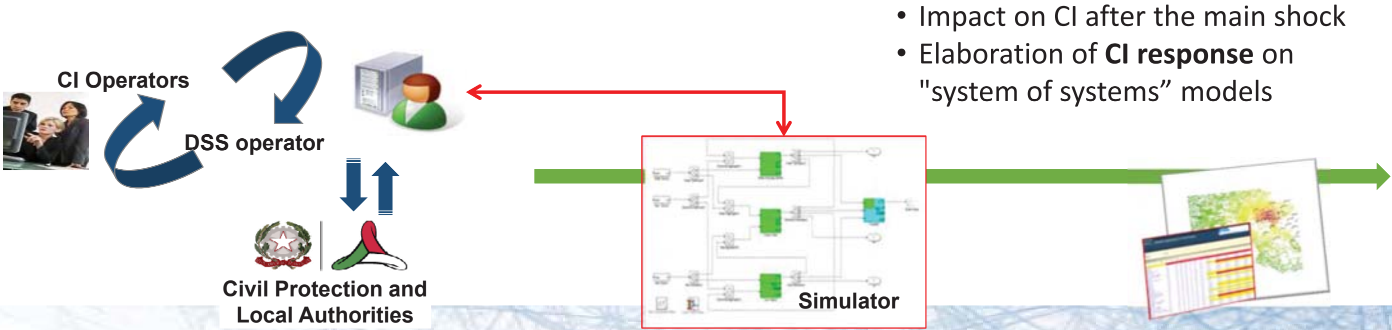
Earthquake Event – Step 2
($T_0 \div$ 1-2 hours)

- **Earthquake** event data (Epicentre and Magnitude) and **Shake Maps** from INGV
- Actual distribution of PGA. PGV and I_{MCS}



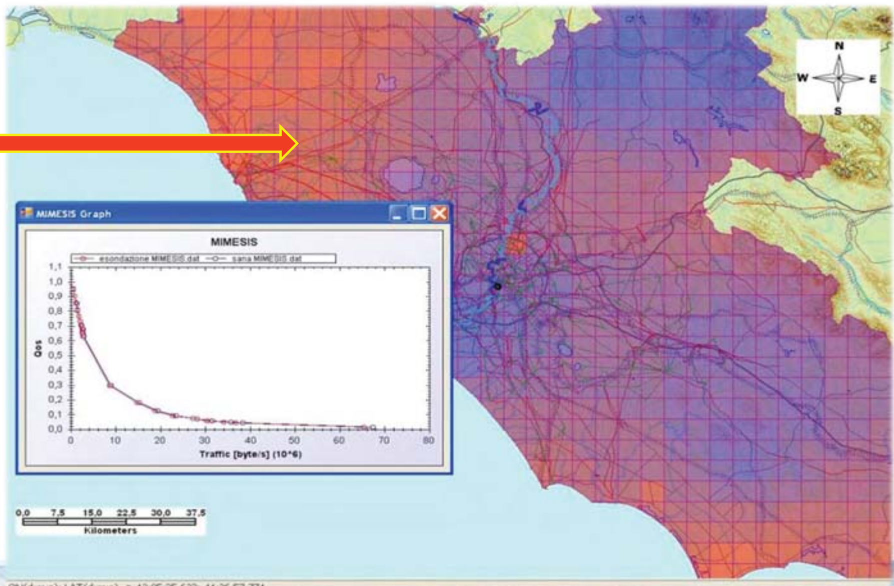
- Use vulnerability matrices to perform a **refined assessment** of potential **Harm Scenario**

- Impact on CI after the main shock
- Elaboration of **CI response** on "system of systems" models



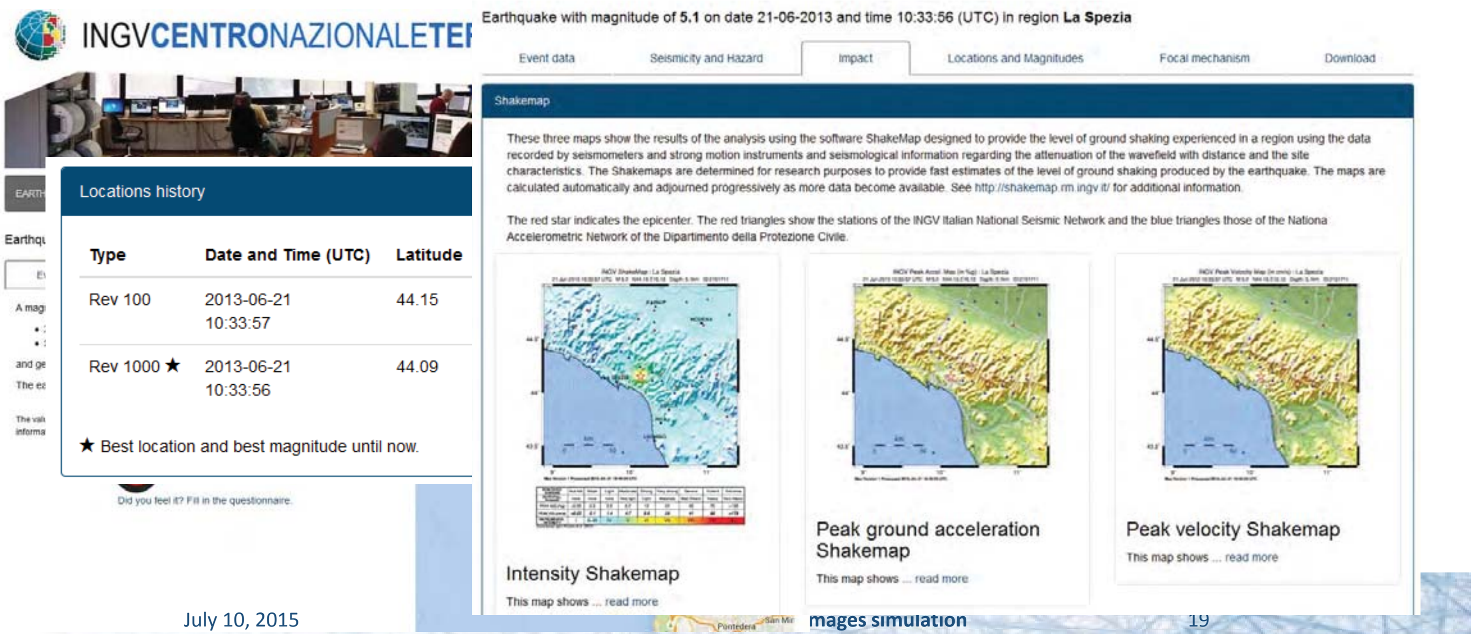
Earthquake Event – Step 2
($T_0 \div$ 1-2 hours)

Example:
- CI components QoS (Quality of Service) state evolution

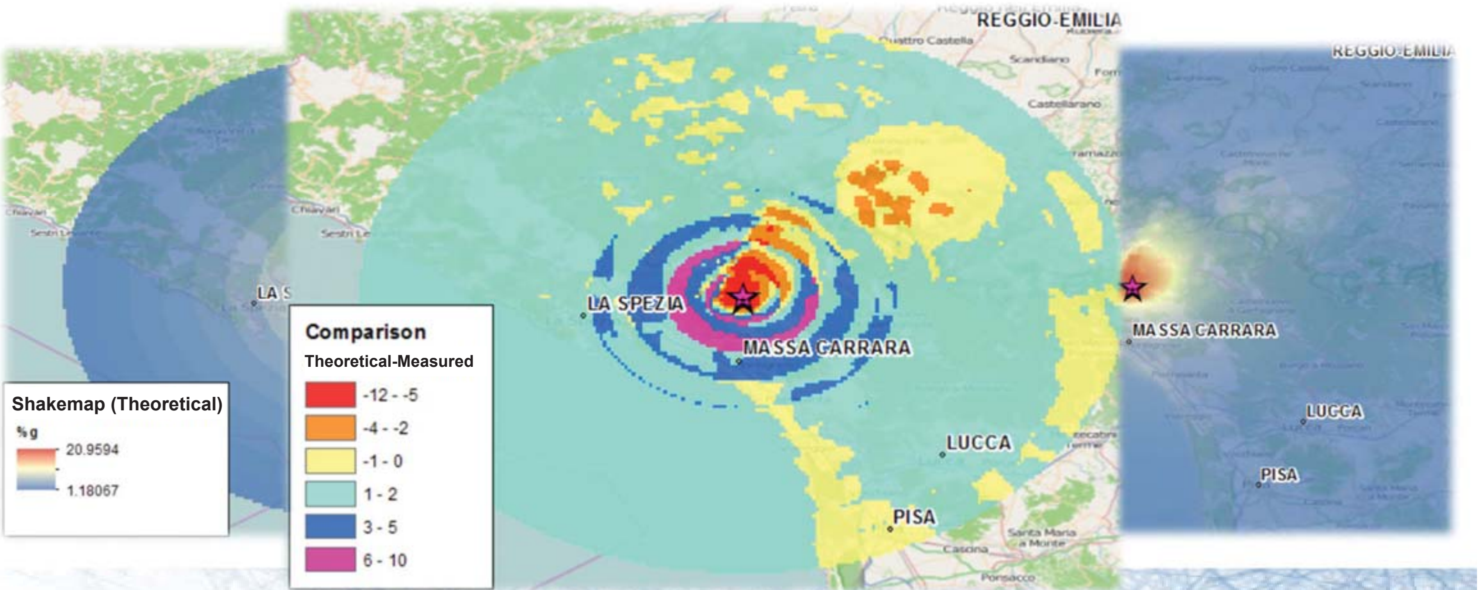


Estimate of consequences on:
- Population
- Services
- Industrial system
- Environment

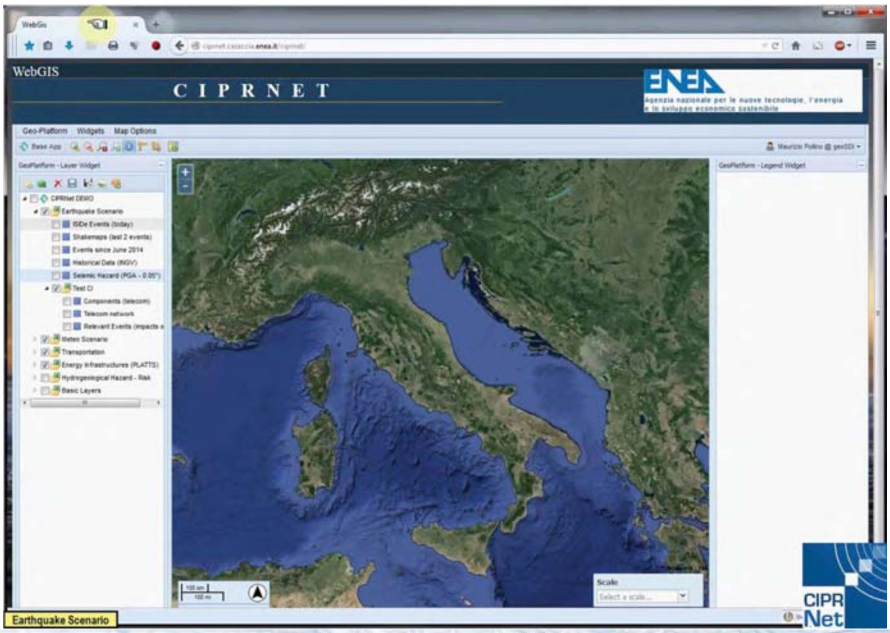
Earthquake with magnitude of 5.2 on date 21-06-2013 in La Spezia (Lunigiana)



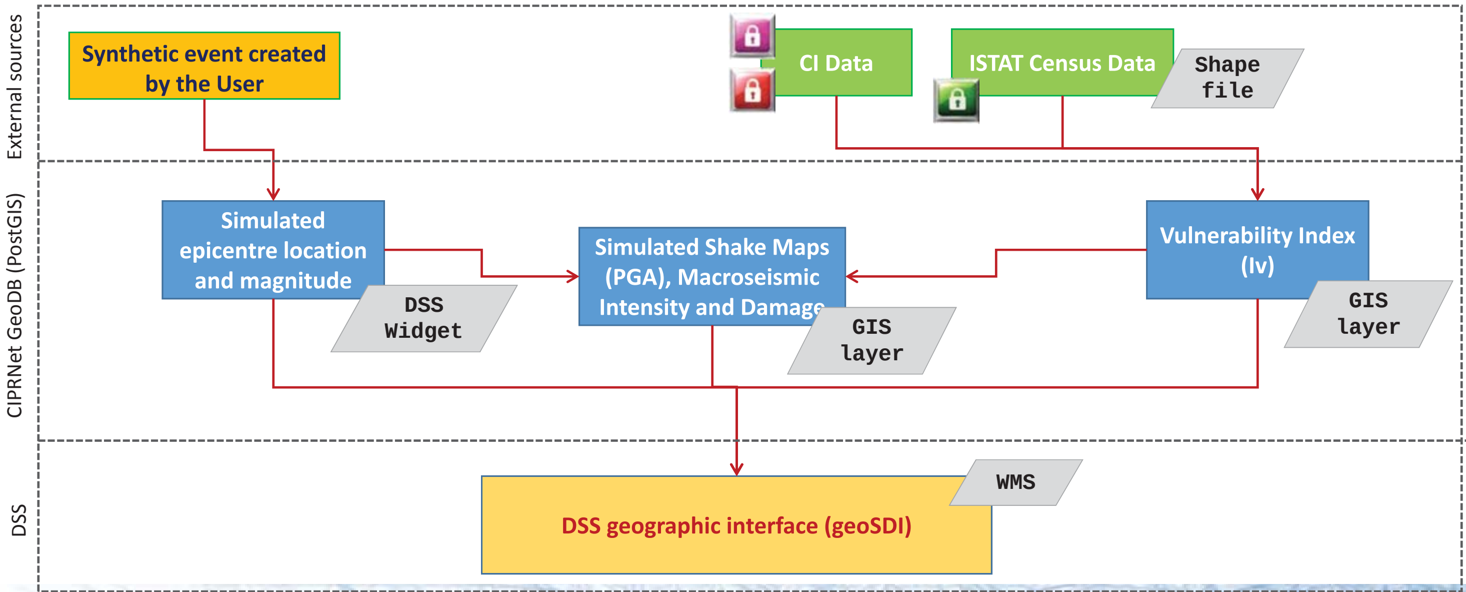
Comparison: Theoretical/Measured PGA



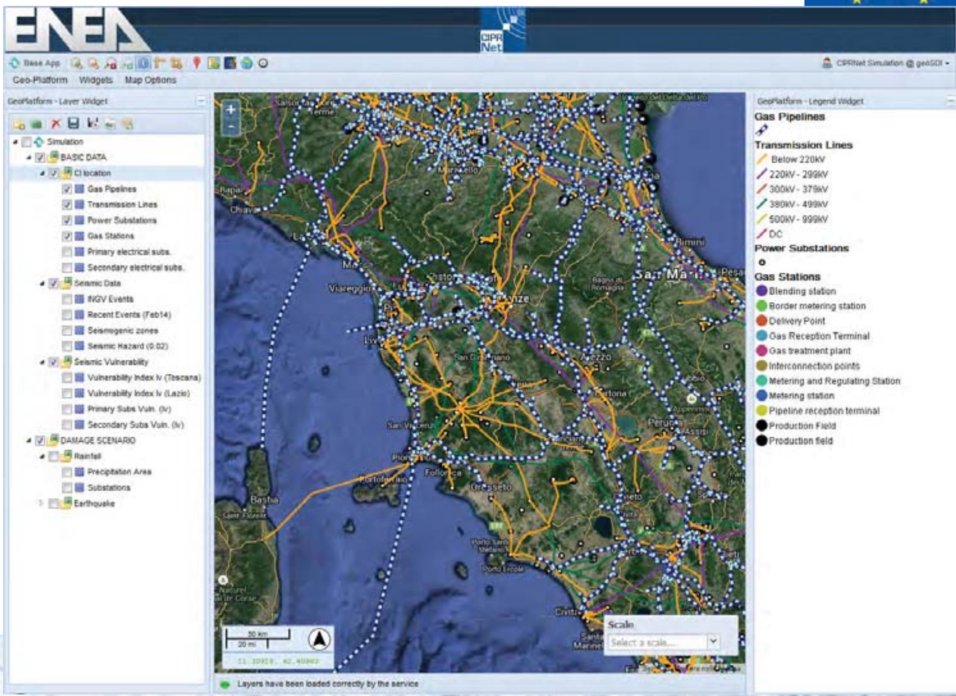
Earthquake – Real Time Operational



Example of Data flow:
Earthquake - Simulation

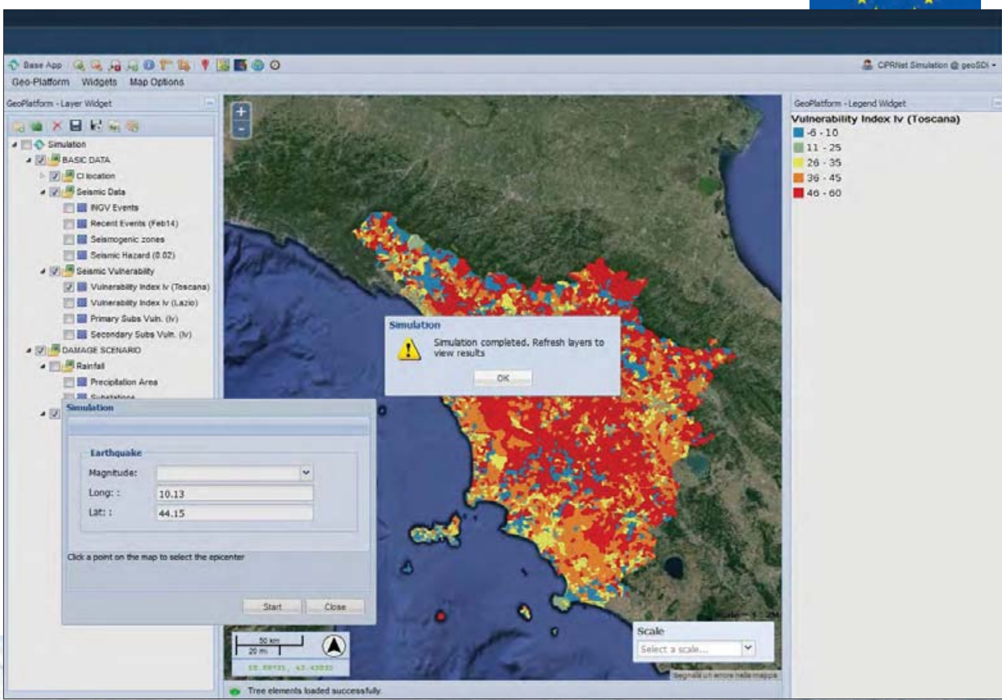


Earthquake simulation



- Seismic data
- Buildings vulnerability
- CI elements (transportation network, pipelines, power/telco networks, etc.)

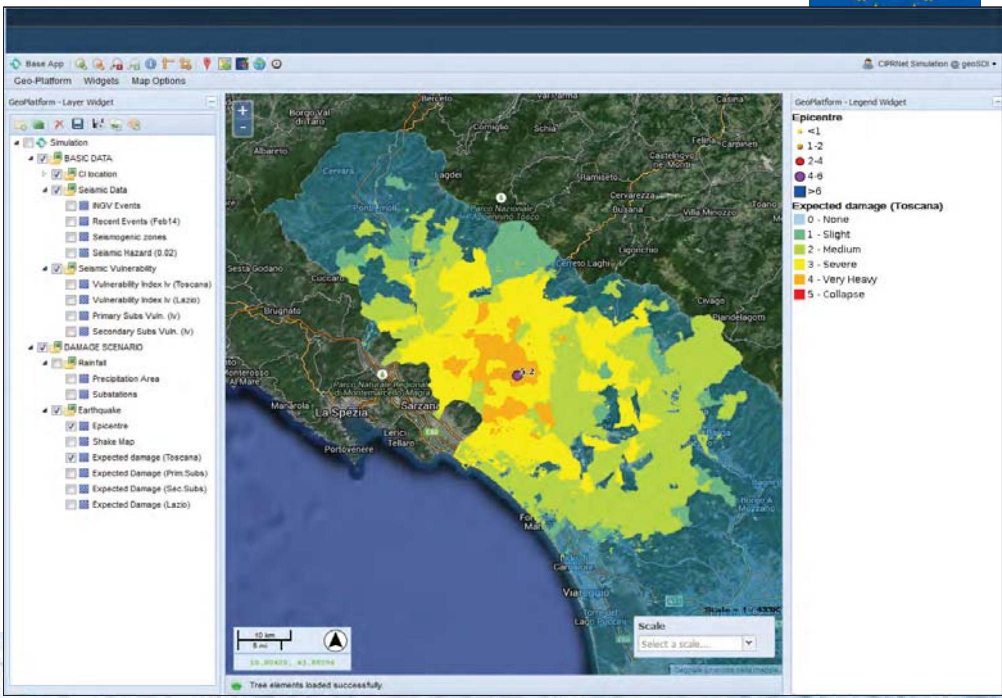
Earthquake simulation



- Earthquake simulation (via ad hoc developed widget)
- Selection of epicentre and magnitude
- Seismic parameters processing (PGA, I_{MCS} and Damage runtime calculation)

Earthquake simulation

- Shake Map (empirical prediction of PGA propagation)
- Earthquake damage scenario
- Level of damage for:
  - Buildings
  - CI elements



Earthquake simulation

Conclusions

- GIS-based Decision Support Systems (DSS) are effective tools to support, in an unique framework, risk assessment and consequence analysis based on events prediction/simulation and their impacts.
- With respect to the issues related to natural hazards (e.g. earthquakes), the recent advances in geo-informatics, communication and sensor technologies offer new opportunities.
- The WebGIS interface allows to visualize and analyse the geo-spatial data and thematic maps stored in the system by means of basic functionalities such as: description and characterization of the area of interest, production of thematic maps (e.g., vulnerability), scenarios (e.g. impacts on buildings and CI, etc.).
- The interactive DSS application developed is able to support public stakeholders and CI operators to quickly evaluate consequences and to address activities related to emergency management.

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

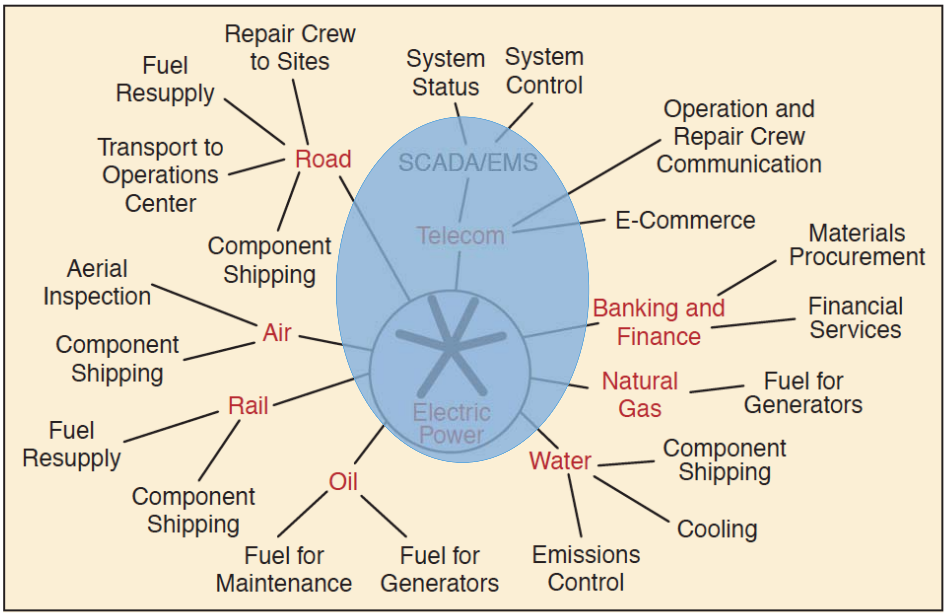
An Electric-SCADA-based Model to Implement Reconfiguration Procedures in Electric Distribution Grids

Antonio Di Pietro, PhD – ENEA
antonio.dipietro@enea.it

CIPRNet Course inside the Master in Homeland Security
Second Edition

Contents

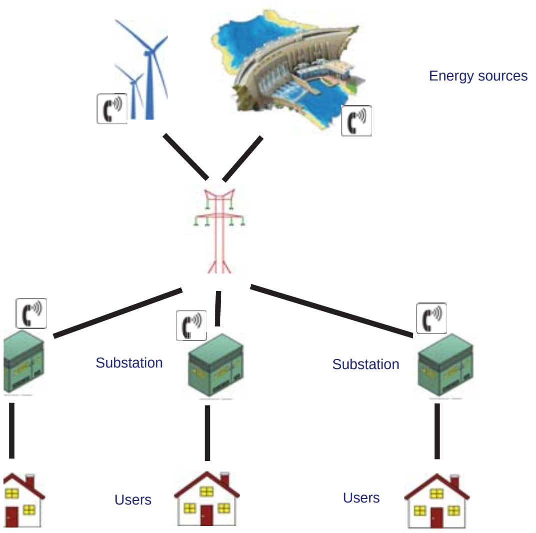
The Energy sector presents various types of dependencies [1]



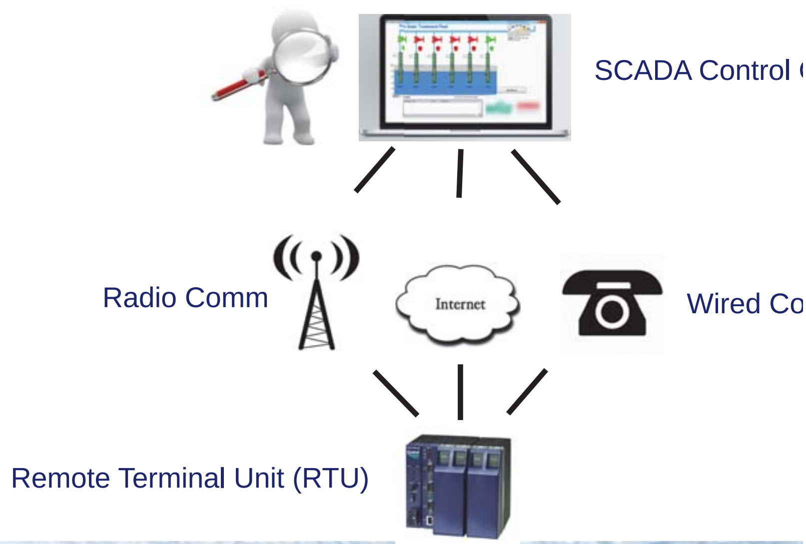
[Rinaldi, 2001]

The Electric Distribution Grid is controlled by a SCADA system

Power Grid



SCADA system



On January 2nd 2004, a failure in the Telecom node impacted the SCADA of the Rome grid [2]

elecom node faulted

iesel generator faulted

atteries run out energy

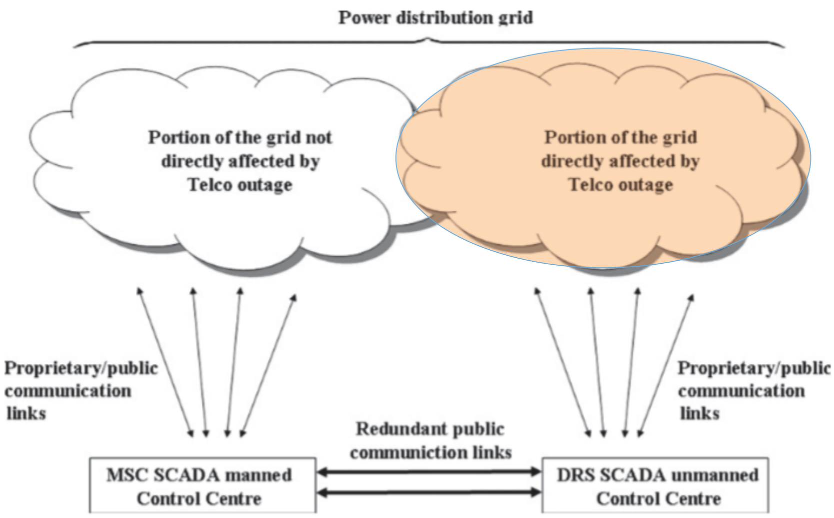
/ireless & Wired commun. tilted

CADA system affected

ome Electrical Grid affected

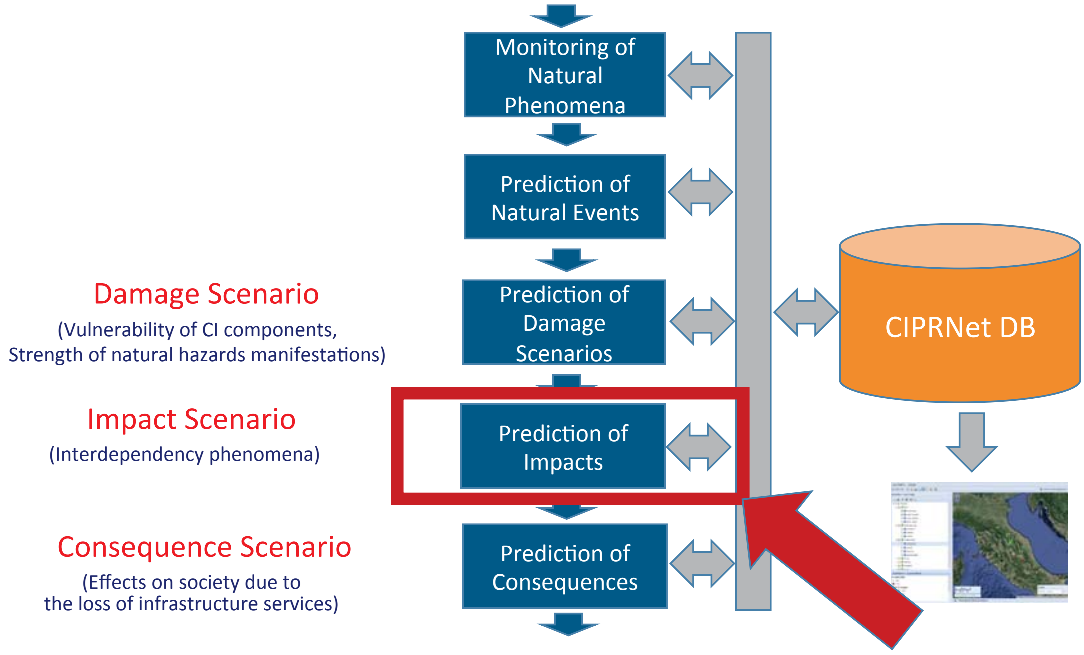
TMs tilted

er-SCADA: Short time scale impact!

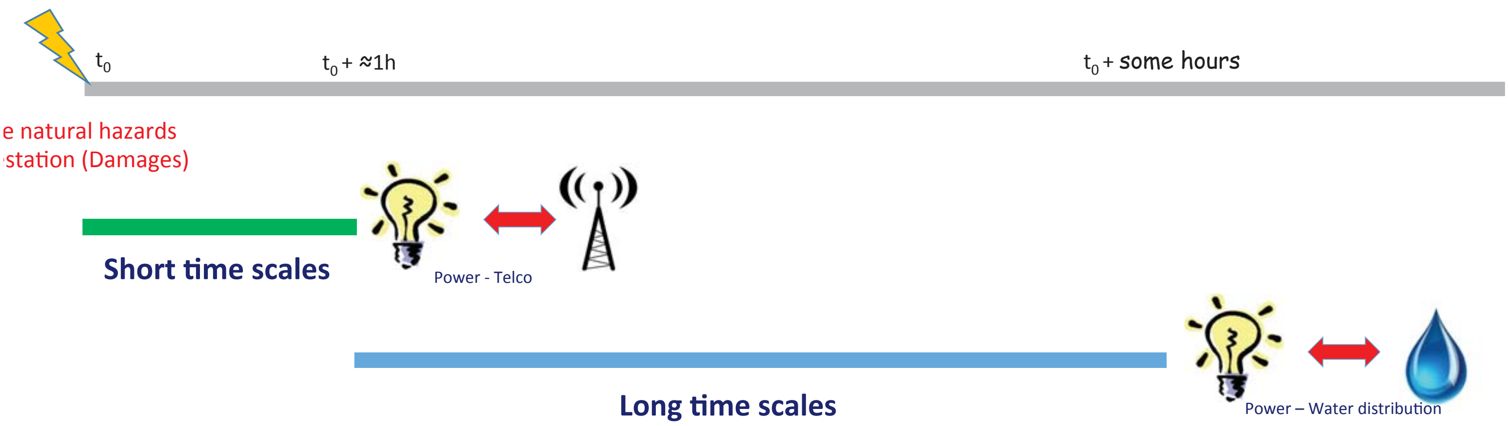


Contents

Starting from the Damage scenario, the DSS estimates the Impact scenario



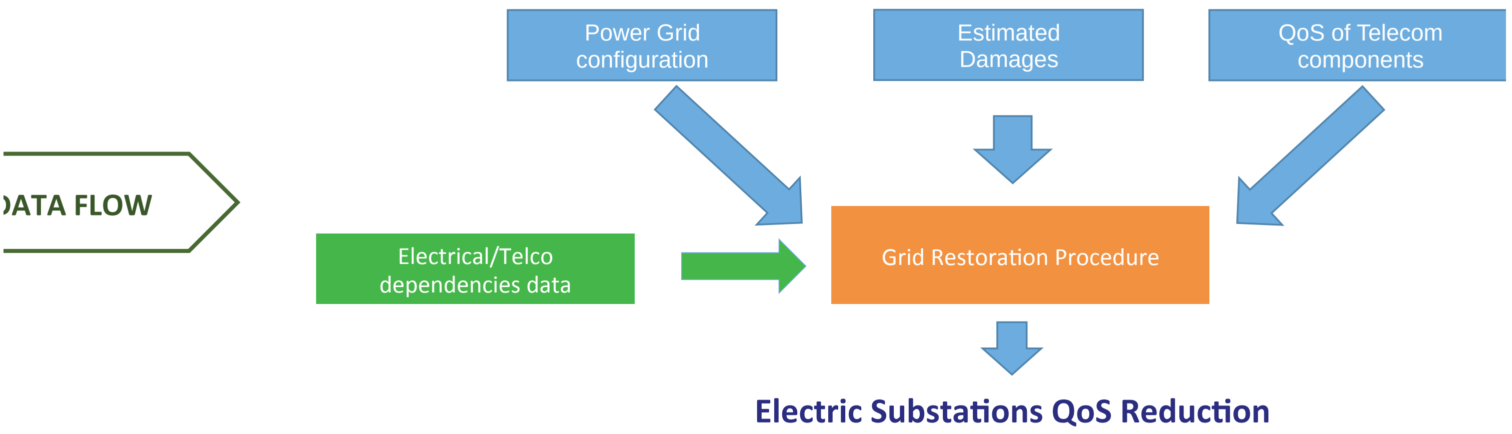
Impacts on infrastructures occur with different time scales



Our procedure for impact estimation addresses the short time scale

Contents

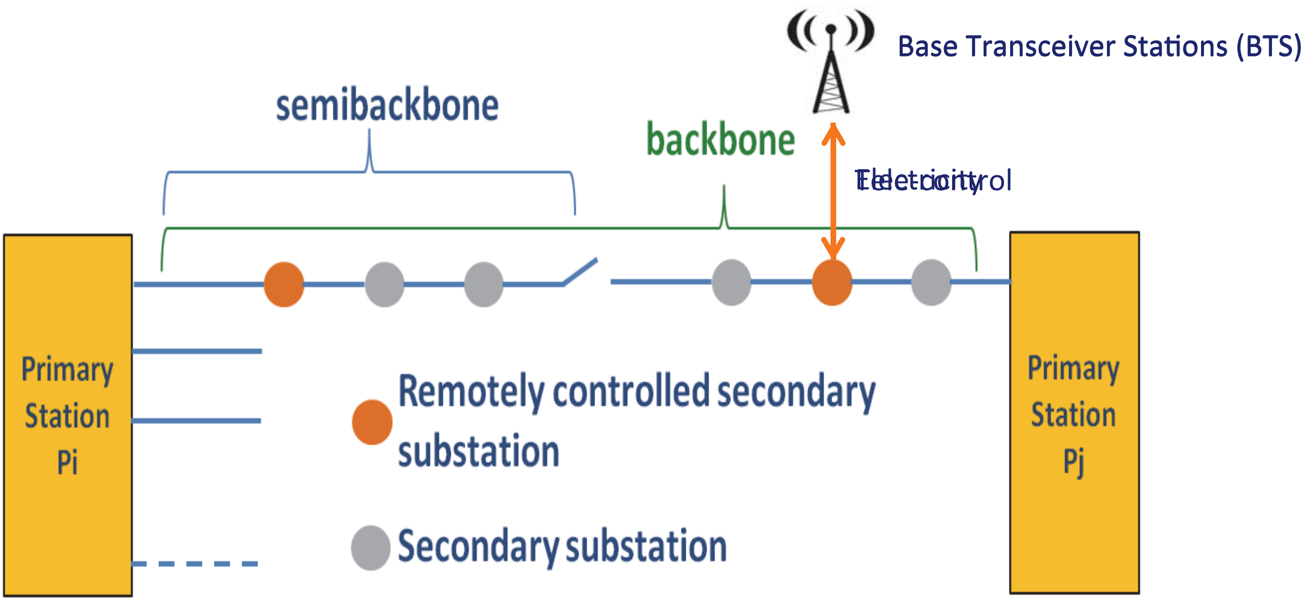
The Impact Estimation is implemented through a network-based procedure [3,4]



We modeled the Electrical Distribution Grid of Rome in normal configuration

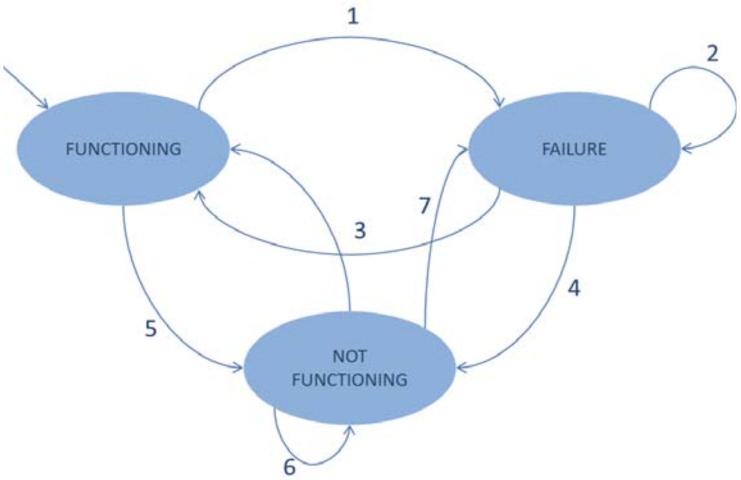
- ✓ **74 Primary Substations (PS) HV-MV** 220/150/60 kV – 20/8.4 kV)
- ✓ **≈13.500 Secondary Substations (SS) MV-LV** (20/8.4 kV – 220/380 V) connected in serial configuration
- ✓ **Remote Control** in specific SS

A normally open switch divides each backbones in two parts

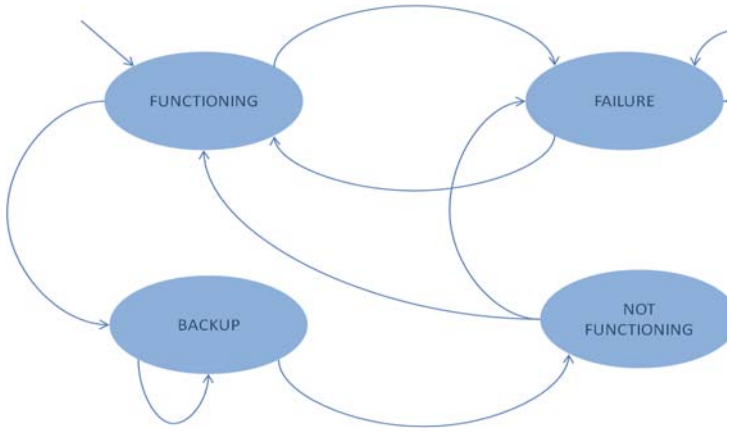


The electrical distribution grid model

Two Finite-State Machines to model Electric SS and Telecom BTS



Secondary Substation model



BTS model

The procedure considers Interdependencies & the restoration operations of the Electric operator

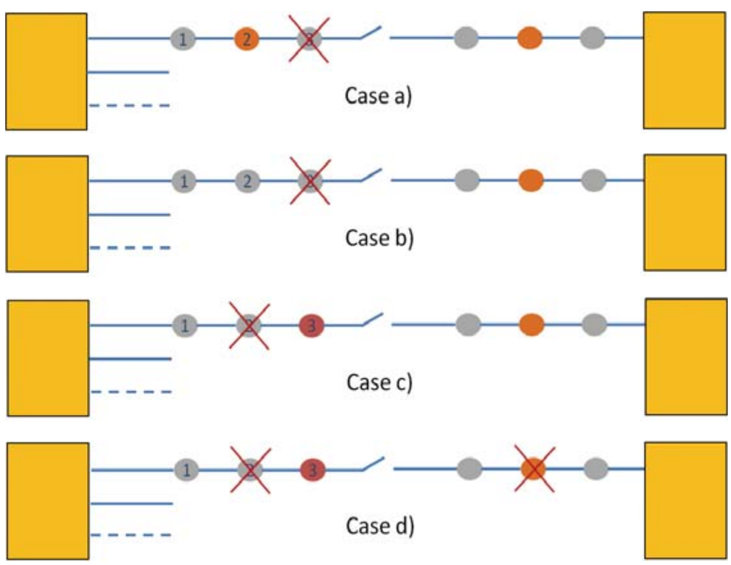
Features:

3TS that cannot work due to he loss of power

:lectric SS that cannot work lue to the loss of tele-control

\verage time duration to econnect the SS

:inal configuration of the grid



Possible failures of the electric grid

Contents

Electric – SCADA interdependencies

CIPRNet DSS Impact Analysis

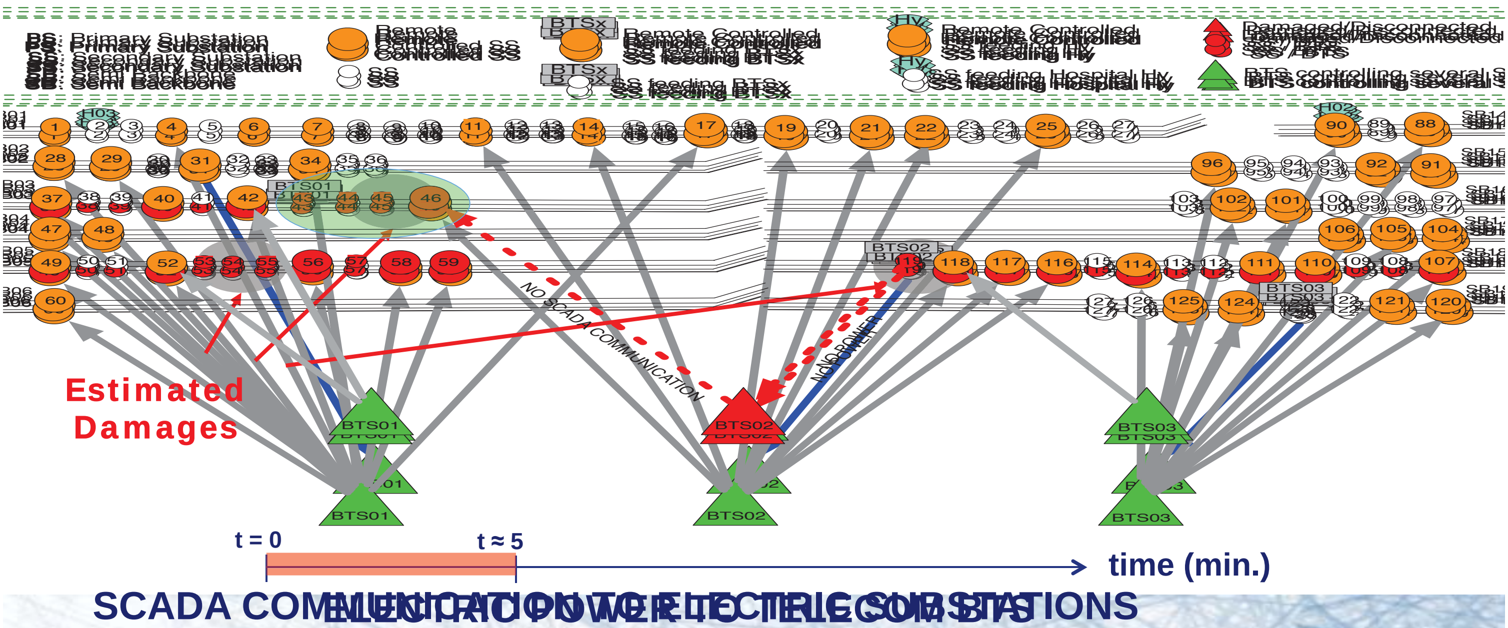
- ✓ From Damages of CI to CI QoS reduction
- ✓ Modeling Electric – SCADA interdependencies
- ✓ **The Rome Case Study**

Conclusions & Future Work

Lesson learnt

References

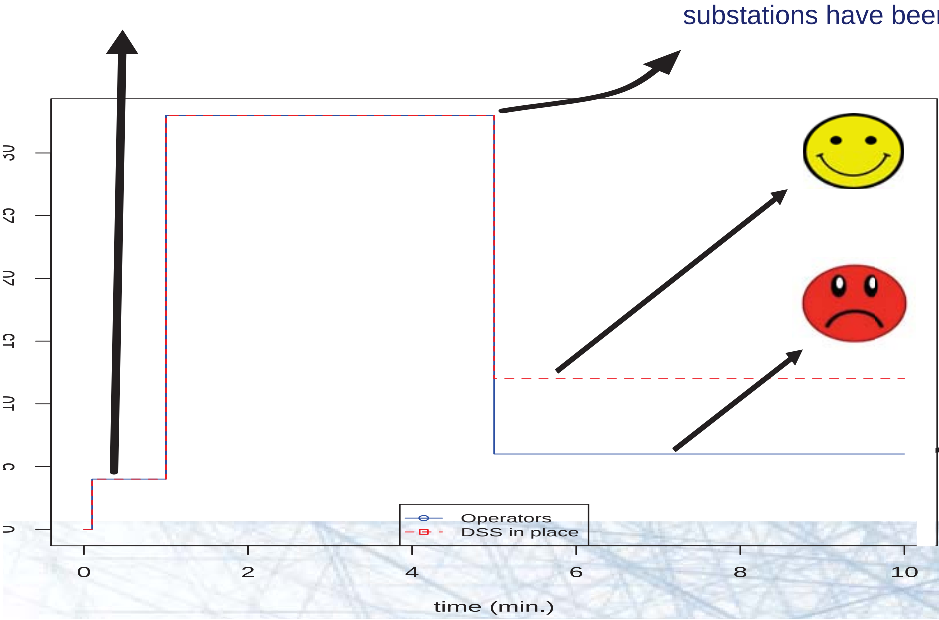
We estimate the electric substations disconnected due to SCADA outage dependencies



Results: Added value for the Electric operator

mated damaged substations

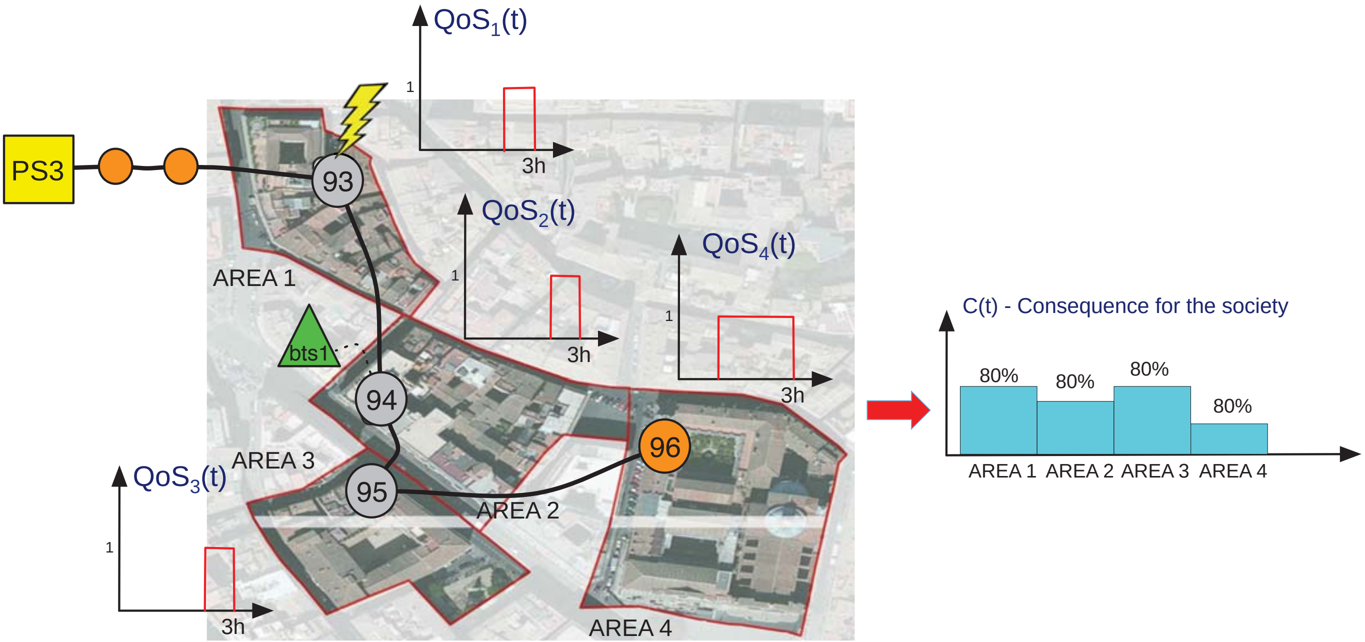
From its SCADA system, the Electric operator detects that some substations have been disconnected



The Electric operator estimates the possible **additional** faulted substations due to the loss SCADA control

With no information about the loss of BTS, only a **li** number of disconnected substations can be estim

The procedure returns the power profiles of each electric SS



Contents

Conclusions & Future Work

- We have implemented an Electrical Distribution Grid Internal Dependencies simulator
  - Tested on synthetic and realistic scenarios
- We started acquiring the “real” Electrical / Telecom interdependency information in the area of Rome
- We are working with CI Operators to design the interface between CIPRNet DSS and the Electric operator’s Information Systems
- We are working on the simulation algorithm to add new functionalities:
  - To consider traffic data impacts on the restoration procedures
  - To include optimization in restoration procedures

Contents

Lesson learnt

- Electric operators are very interested in tools that can relate the likehood of natural phenomena with the operability of their networks
  - E.g., hot waves, floods may produce disruptions on the electric grid
- The interdependency phenomena are often not well known to by CI operators
  - E.g., the electric operator does not know which BTS controls specific electric SS
- There not exist a specific software tool that models and evaluates the effects of impact on interdependent networks!
  - In general, existing tools should have been so much customized that a new development is preferable

Contents

Electric – SCADA interdependencies

CIPRNet DSS Impact Analysis

- ✓ From Damages of CI to CI QoS reduction
- ✓ Modeling Electric – SCADA interdependencies
- ✓ The Rome Case Study

Conclusions & Future Work

Lesson learnt

References

References

S.M. Rinaldi, J.P. Peerenboom, and T.K. Kelly. **Identifying, understanding, and analyzing critical infrastructu rdependencies**. Control Systems, IEEE, 21(6):11–25, Dec 2001.

A. Bobbio, G. Bonanni, E. Ciancamerla, R. Clemente, A. Iacomini, M. Minichino, A. Scarlatti, R. Terruggia, E. Zenc **vailability of critical SCADA communication links interconnecting a power grid and a Telco network**, Reliabil neering & System Safety, Volume 95, Issue 12, December 2010, Pages 1345-1357, ISSN 0951-8320, http://dx.doi.o 016/j.ress.2010.06.011.

A. Tofani, A. Di Pietro, L. Lavalle, M. Pollino, V. Rosato. **CIPRNet Decision Support System: Modelling Electric ribution Grid Internal Dependencies**. Journal of the Polish Society of Safety and Reliability, 2015, Accepted ication.

Min Ouyang. **Review on modeling and simulation of interdependent critical infrastructure systems**. Reliabil neering & System Safety, 121(0):43 – 60, 2014.

www.utmeacal.enea.it/dipietro/

antonio.dipietro@enea.it

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Application of system of systems model for impacts analysis in large scenarios

Alberto Tofani – ENEA, Rome, Italy

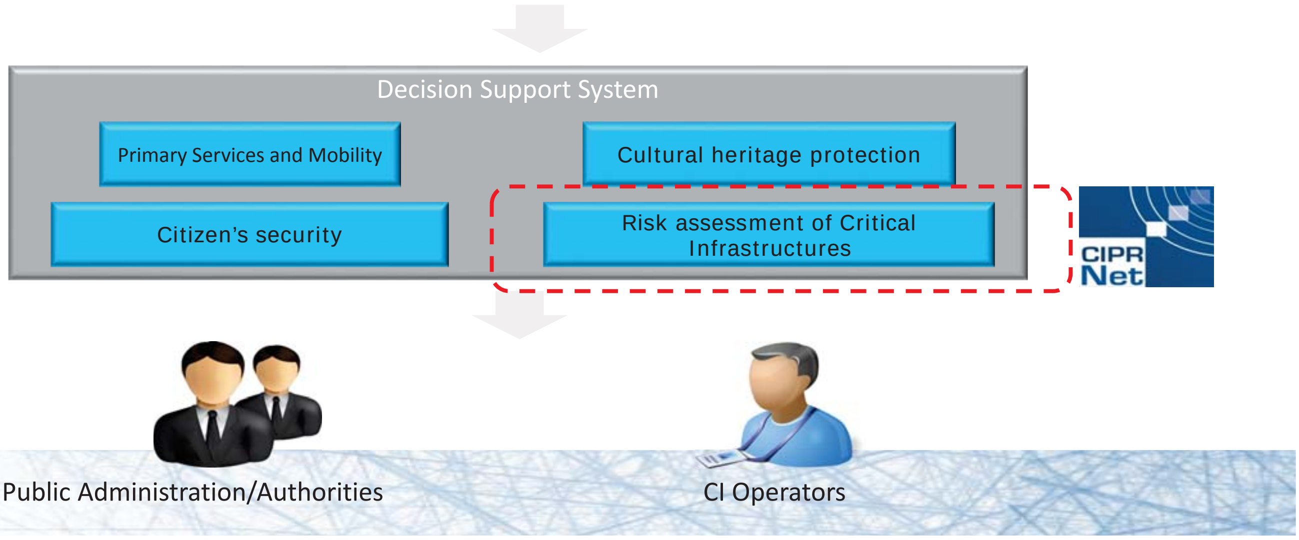
alberto.tofani}@enea.it

CIPRNet Course inside the Master in Homeland Security
Second Edition

UCBM – Rome (Italy) – 9-10 July 2015

ENEA CI Risk forecast platform

RESILIENCE ENHANCEMENT OF A METROPOLITAN AREA



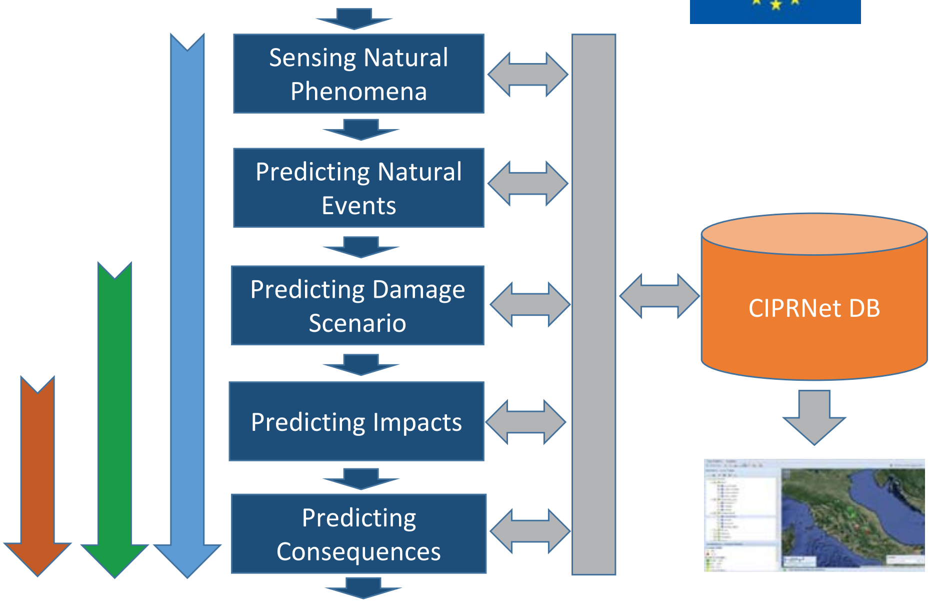
CIPRNet CI Risk Assessment Workflow

The Risk Assessment Loop
- 24/7 RA of CI components
in a given area .
Threats sources: natural events

Service on demand

Synthetic natural events simulator

Synthetic damage simulator



Predicting Impacts

- This block estimates the impact that damages will produce on the services delivered by the CI directly impacted by the damages and the impacts on all other CI network because of (inter)dependency phenomena

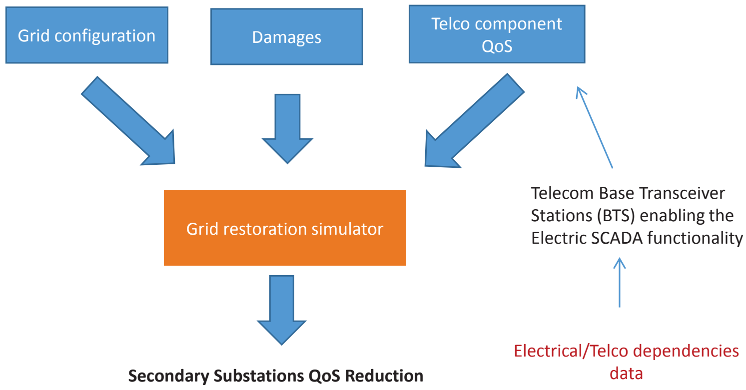
Severe natural event
Manifestation (Damages)

Short term impacts (Impacts on the electrical grid, electrical SCADA networks)

Long term impacts (Impacts on all CI networks: e.g. telecommunication networks, drinking water, gas pipeline)

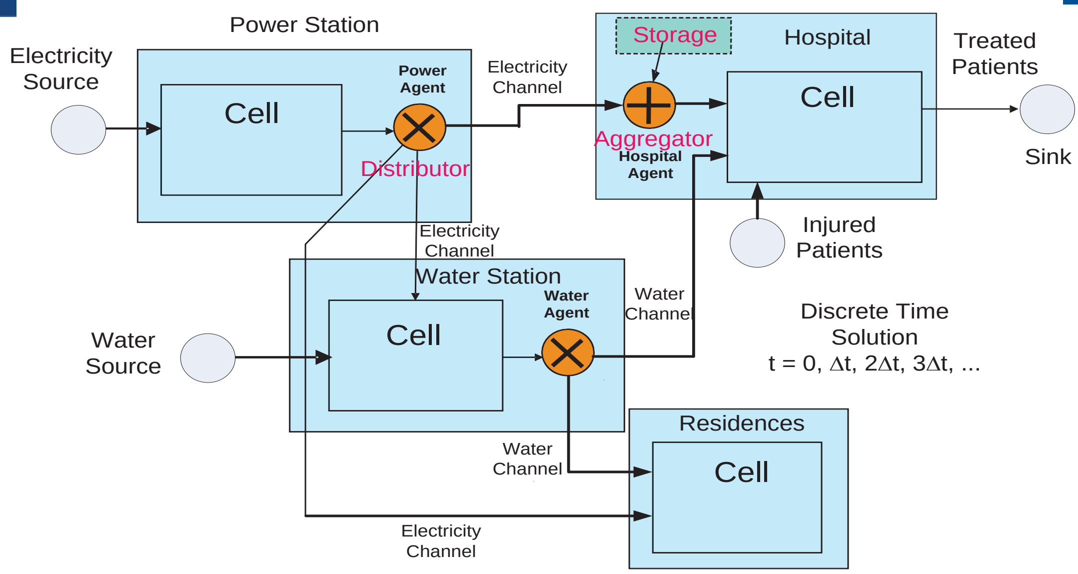
Predicting Impacts

Short term impacts



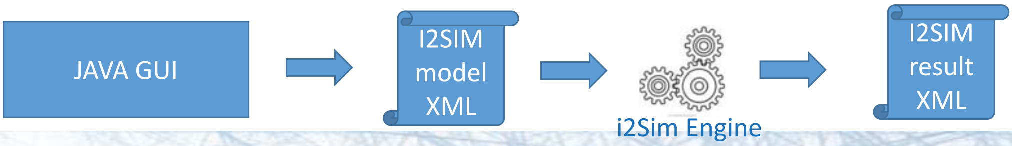
Long term impacts

i2Sim Ontology



The I2Sim simulator

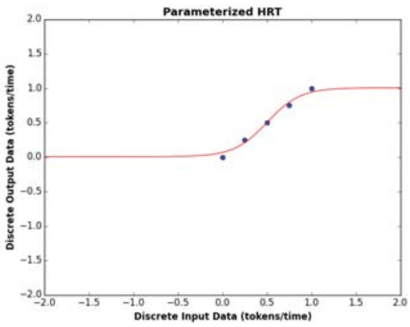
- The i2Sim GUI is written in Java.
  - Takes human input such as port connection, HRTs, etc.
  - Converts the data to the i2Sim Model
- The i2Sim Model is represented using XML
- The i2Sim Engine is written in Python
  - A compiled version of Python solver takes in a i2Sim Model and a event/scenario/timeline file (also in XML)
  - Perform the simulation
  - Generate a simulation result output file in XML format



The I2Sim engine

The HRT is parameterised into continuous functions.

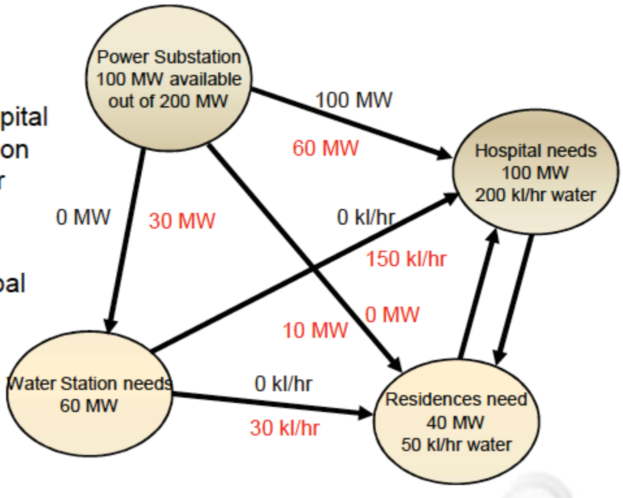
$y(t)$	$x_1(t)$	$x_2(t)$	$x_3(t)$	$x_4(t)$	$m_1(t)$
Patients per hours	Electricity (KW)	Water (KL/h)	Doctors	Nurses	Physical integrity
20	100	1,000	4	8	100%
15	50	500	3	6	80%
10	30	300	2	4	50%
7	20	200	2	3	20%
0	0	0	0	0	0%



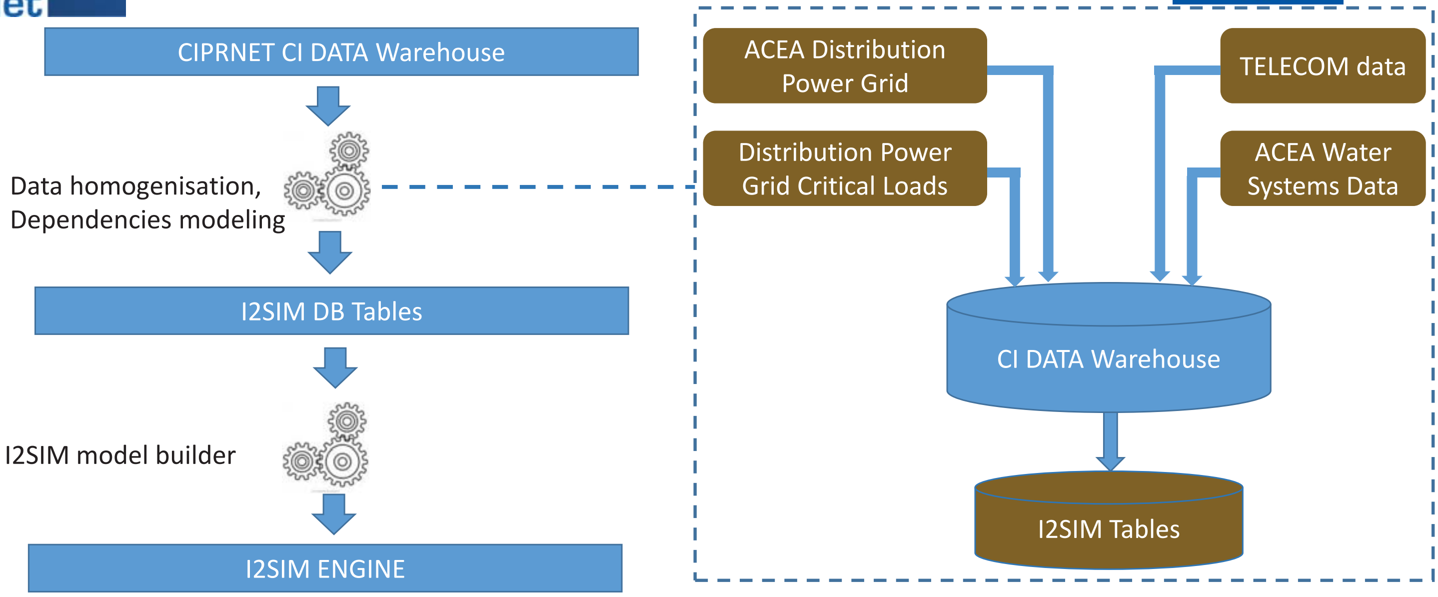
A system of equations is formed to solve for the operating states of each cell.

I2SIM for Resource Allocation Strategies

- **Black** bad decision because hospital cannot function without water
- **Red** good decision to optimize global objective



Predicting long term impacts



Predicting long term impacts

CIPRNET CI DATA Warehouse

Data homogenisation, Dependencies modeling

I2SIM DB Tables

I2SIM model builder

I2SIM ENGINE

Data ontology

CI Networks Tables

Electrical Networks	Telco Networks	Water Networks
Electrical Dependencies	Telco Dependencies	Water Dependencies

Ad hoc procedures

I2SIM tables

Predicting long term impacts

CIPRNET CI DATA Warehouse

Data homogenisation, Dependencies modeling

I2SIM DB Tables

I2SIM model builder

I2SIM ENGINE

Data ontology – I2SIM tables

Infrastructure_type

Infrastructures_components

	id [PK] serial	id_orig character vai	infrastructure integer	component_t integer	hrt_output text	source double precis	unit character vai	poi boolean
1	1	ps1	2	1	100,75,50,2	10	MW	FALSE
2	2	ps2	2	1	100,75,50,2	10	MW	FALSE
3	3	ps3	2	1	100,75,50,2	10	MW	FALSE
4	4	ps4	2	1	100,75,50,2	10	MW	FALSE
5	5	ps5	2	1	100,75,50,2	10	MW	FALSE
6	6	ps6	2	1	100,75,50,2	10	MW	FALSE
7	7	ps7	2	1	100,75,50,2	10	MW	FALSE
8	8	ps8	2	1	100,75,50,2	10	MW	FALSE
9	9	ps9	2	1	100,75,50,2	10	MW	FALSE
10	10	sb01	2	9	100,75,50,2	10	MW	FALSE
11	11	sb02	2	9	100,75,50,2	10	MW	FALSE
12	12	sb03	2	9	100,75,50,2	10	MW	FALSE
13	13	sb04	2	9	100,75,50,2	10	MW	FALSE

	id [PK] integer	name character varying(100)
11	11	PSTN Switch
12	12	GSM Mobile Switching Center
13	13	IP reuter
14	14	GSM Base Station Controller
15	15	Server

Predicting long term impacts

CIPRNET CI DATA Warehouse

Data homogenisation, Dependencies modeling

I2SIM DB Tables

I2SIM model builder

I2SIM ENGINE

Data ontology – I2SIM tables

CI Networks Dependencies tables

dependencies_table

	id_from [PK] integer	id_to [PK] integer
1	1	10
2	1	11
3	1	12
4	1	13
5	1	14
6	1	15
7	2	16
8	2	17
9	2	18
10	2	19
11	2	20
12	2	21
13	2	22
14	3	23
15	3	24
16	4	25
17	4	26
18	5	27
19	6	28

Predicting long term impacts

CIPRNET CI DATA Warehouse

Data homogenisation, Dependencies modeling

I2SIM DB Tables

I2SIM model builder

I2SIM ENGINE

Data ontology – I2SIM tables

Read POIs in the catalogue table

Back/Forward visit on dep. table

model_table

	id_from [PK] integer	id_to [PK] integer	default_hrt boolean
1	1	10	TRUE
2	2	22	TRUE
3	3	24	TRUE
4	4	26	TRUE
5	5	27	TRUE
6	6	28	TRUE
7	7	29	TRUE
8	8	30	TRUE
9	9	31	TRUE
10	10	23	TRUE
11	10	36	TRUE
12	10	37	TRUE
13	10	38	TRUE
14	10	39	TRUE
15	10	40	TRUE
16	10	41	TRUE
17	10	42	TRUE
18	10	43	TRUE
19	10	44	TRUE
20	10	45	TRUE
21	10	101	TRUE
22	10	114	TRUE

Predicting long term impacts

CIPRNET CI DATA Warehouse

Data homogenisation, Dependencies modeling

I2SIM DB Tables

I2SIM model builder

I2SIM ENGINE

Data ontology – I2SIM tables

default_hrt

	id_to_infr_ty [PK] integer	id_to_comp_ [PK] integer	id_from_infr_ [PK] integer	id_from_com [PK] integer	hrt text
1	2	2	2	9	1,0.0,0.0,0.0,0.0
2	2	9	2	1	1,0.0,0.0,0.0,0.0
3	3	3	2	2	1,0.75,0.5,0.3,0
4	6	4	2	2	1, 0.7, 0.6, 0.3, 0
5	6	4	3	3	1, 0.8,0.5, 0.4, 0
*					

detailed_hrt

	id_to [PK] integer	id_from [PK] integer	hrt text
*			

Predicting long term impacts

CIPRNET CI DATA Warehouse

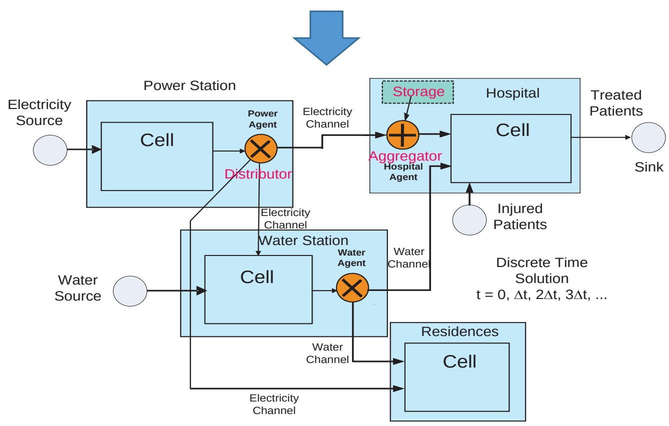
Data homogenisation, Dependencies modeling

I2SIM DB Tables

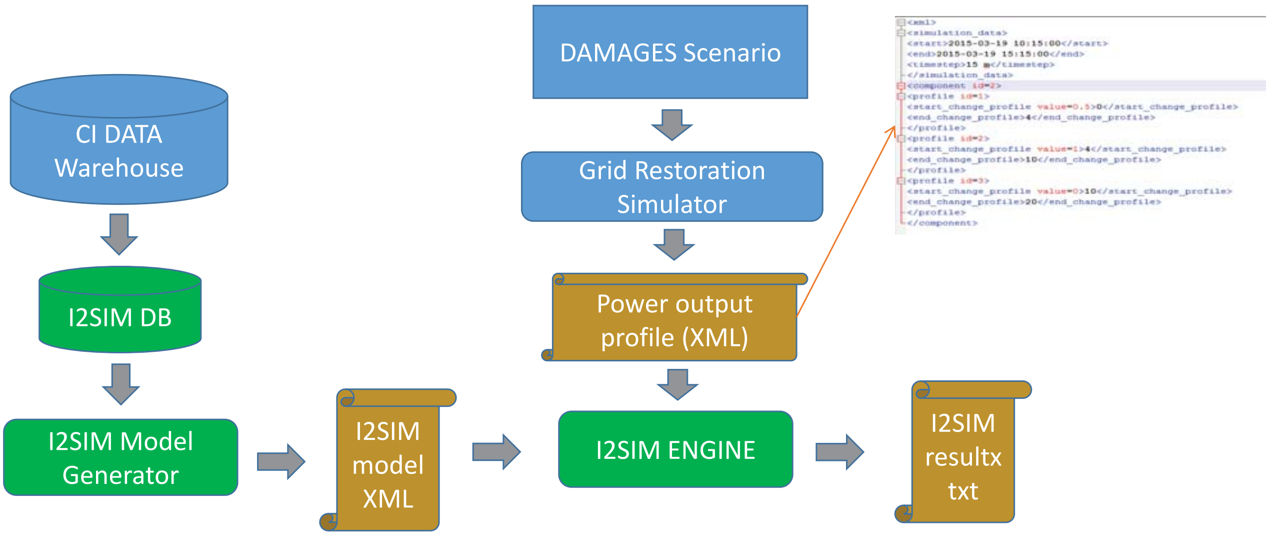
I2SIM model builder

I2SIM ENGINE

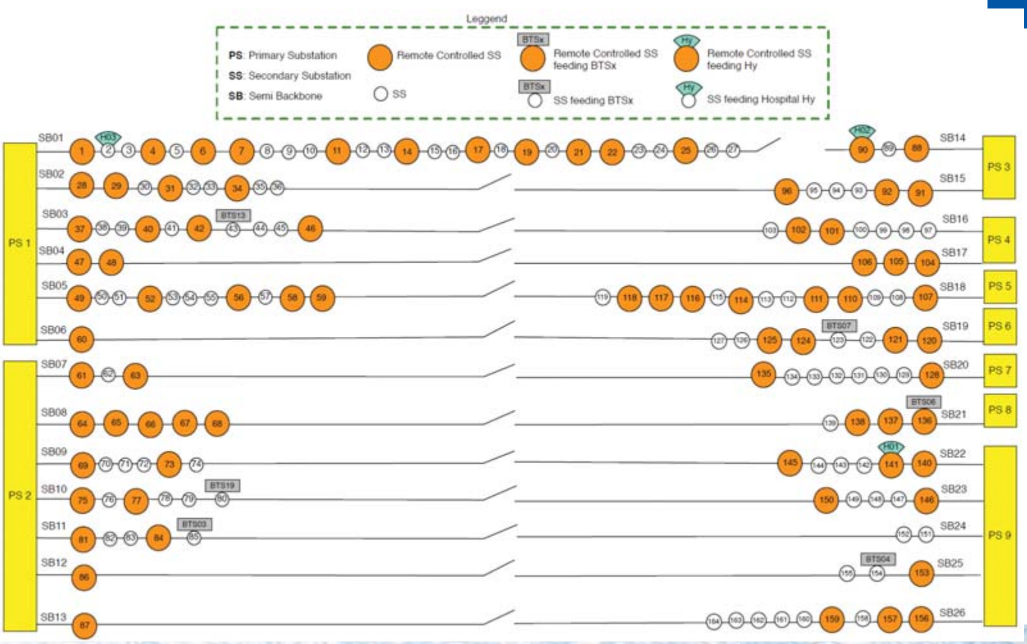
Infrastructures_components,model_table, hrt tables



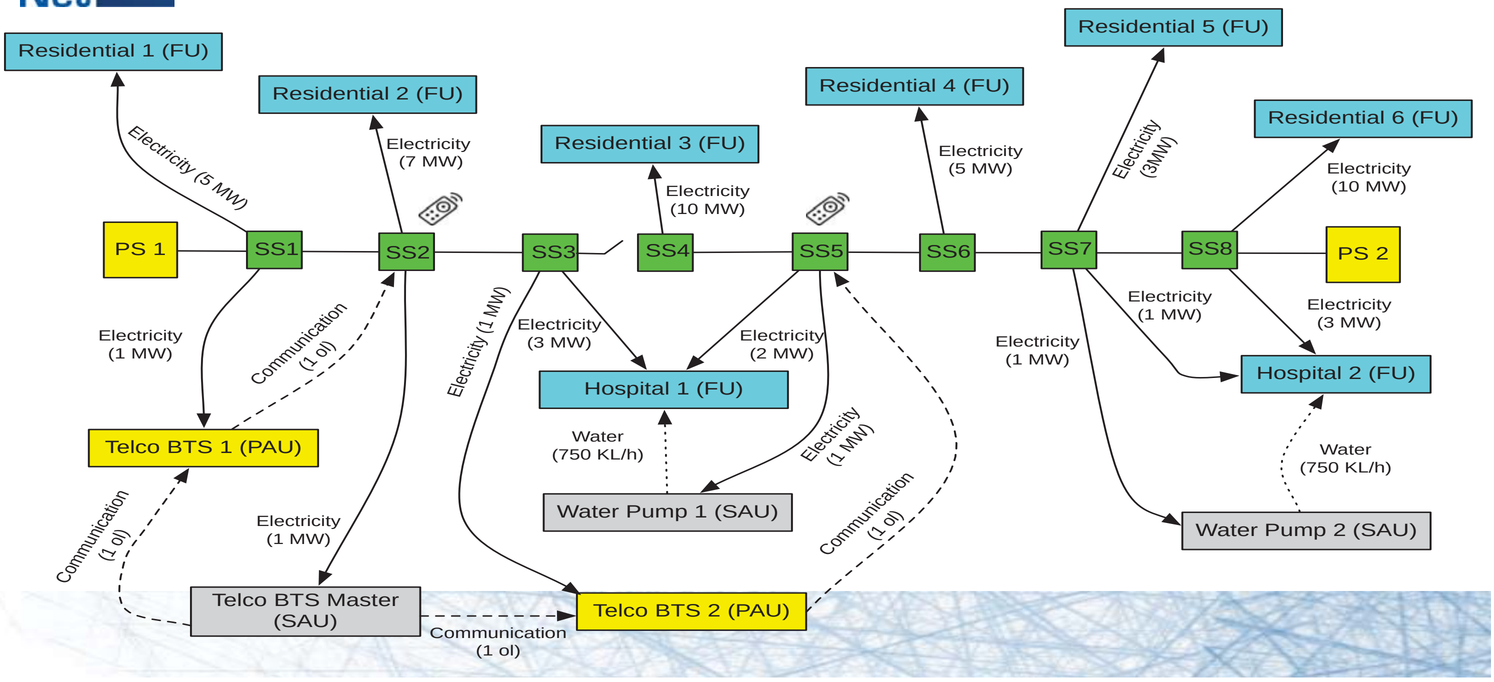
Predicting long term impacts



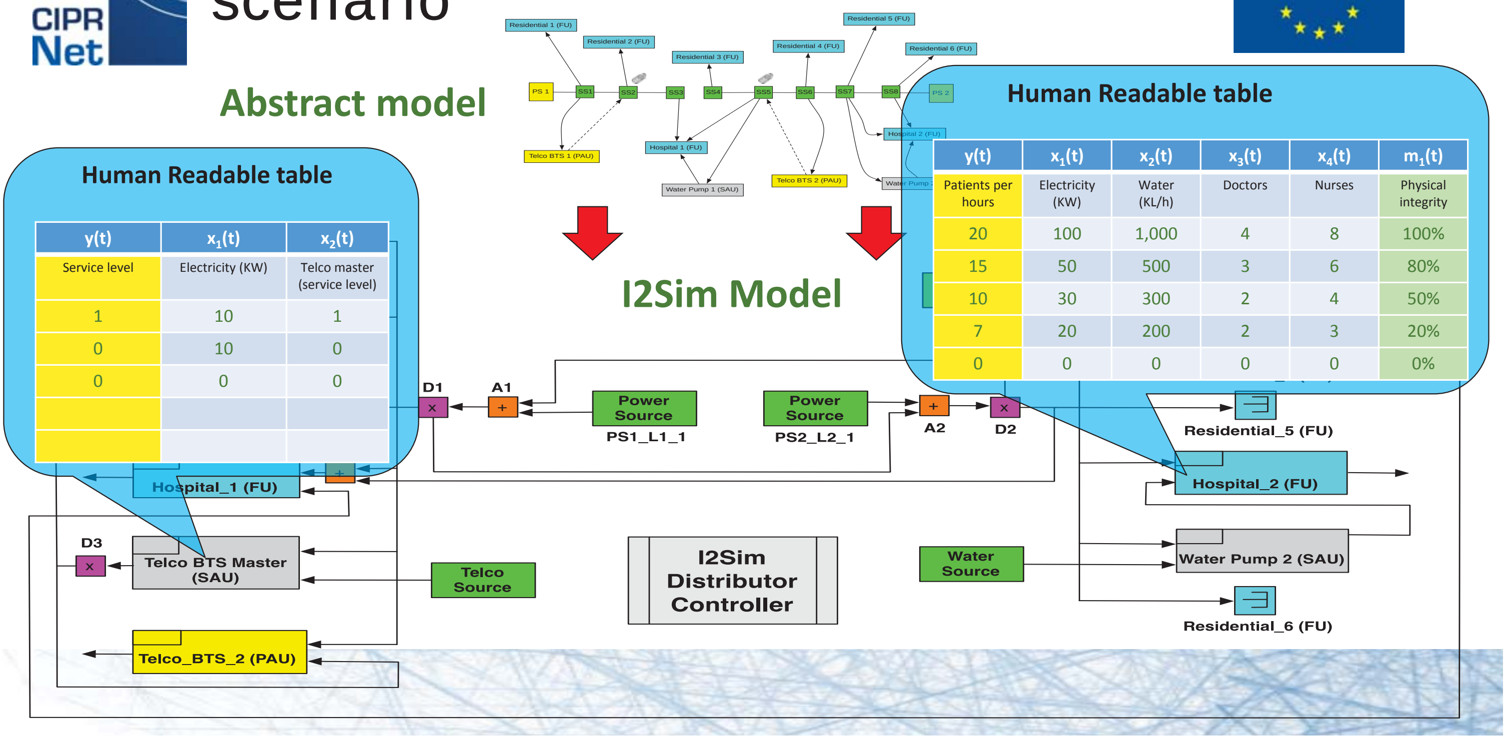
Use case scenario



Scenario example



I2Sim model for the example scenario



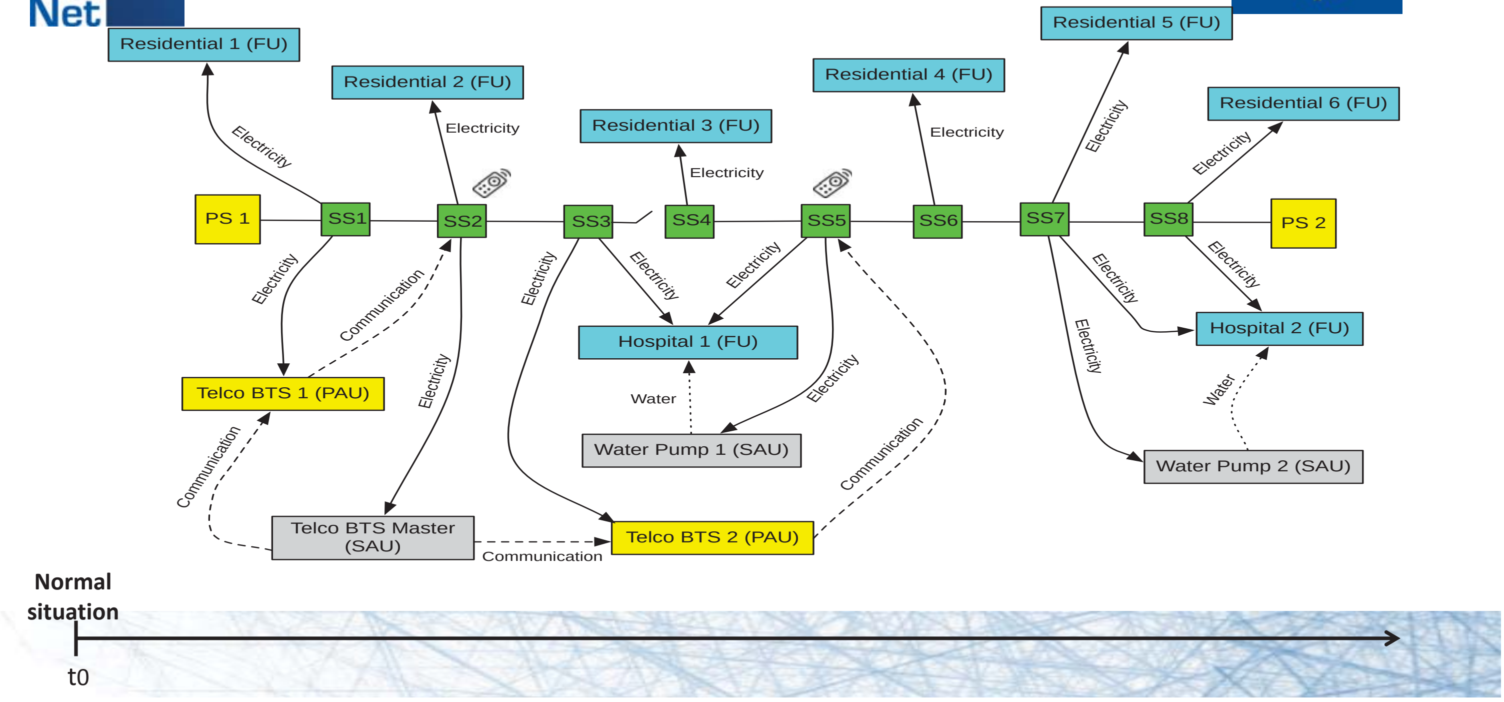
Human Readable table

y(t)	x_1(t)	x_2(t)
Service level	Electricity (KW)	Telco master (service level)
1	10	1
0	10	0
0	0	0

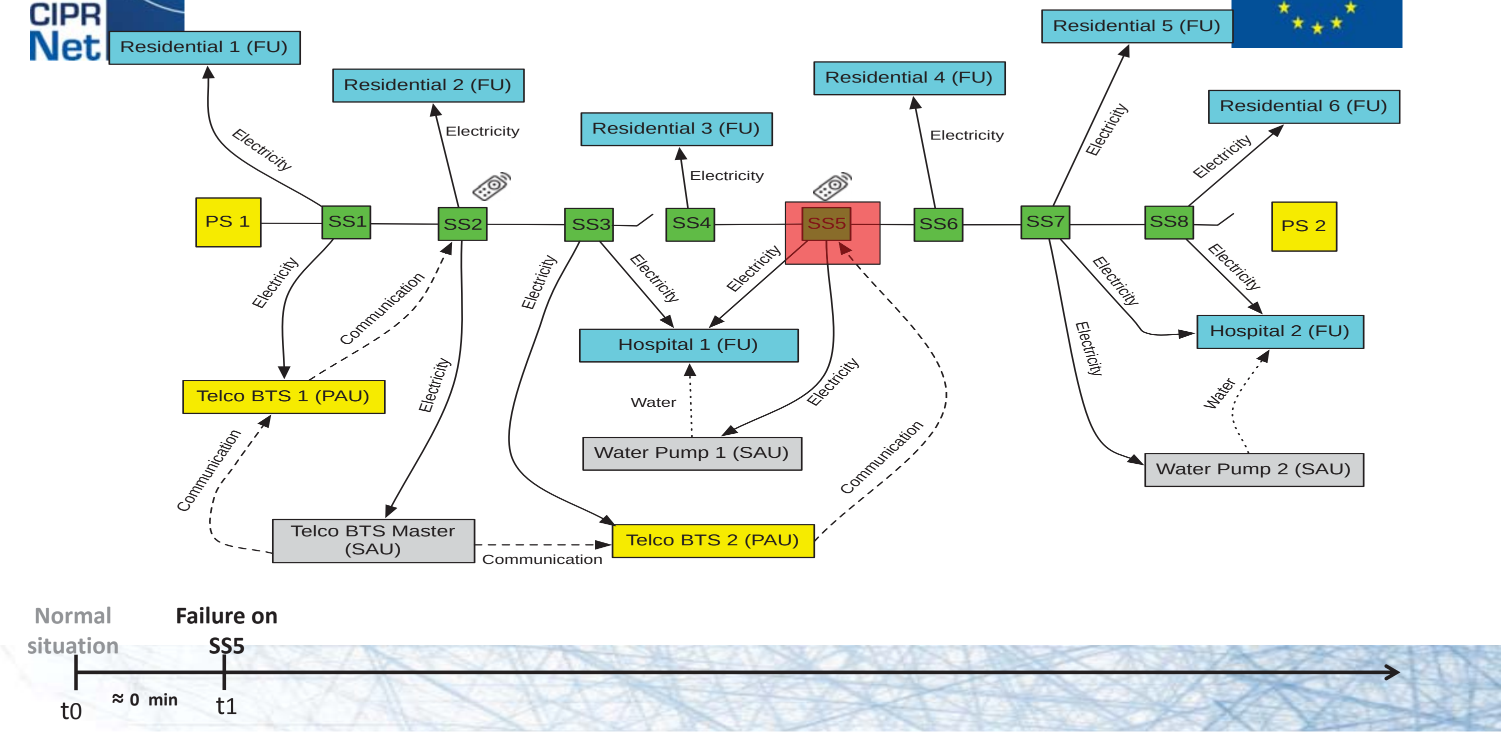
Human Readable table

y(t)	x_1(t)	x_2(t)	x_3(t)	x_4(t)	m_1(t)
Patients per hours	Electricity (KW)	Water (KL/h)	Doctors	Nurses	Physical integrity
20	100	1,000	4	8	100%
15	50	500	3	6	80%
10	30	300	2	4	50%
7	20	200	2	3	20%
0	0	0	0	0	0%

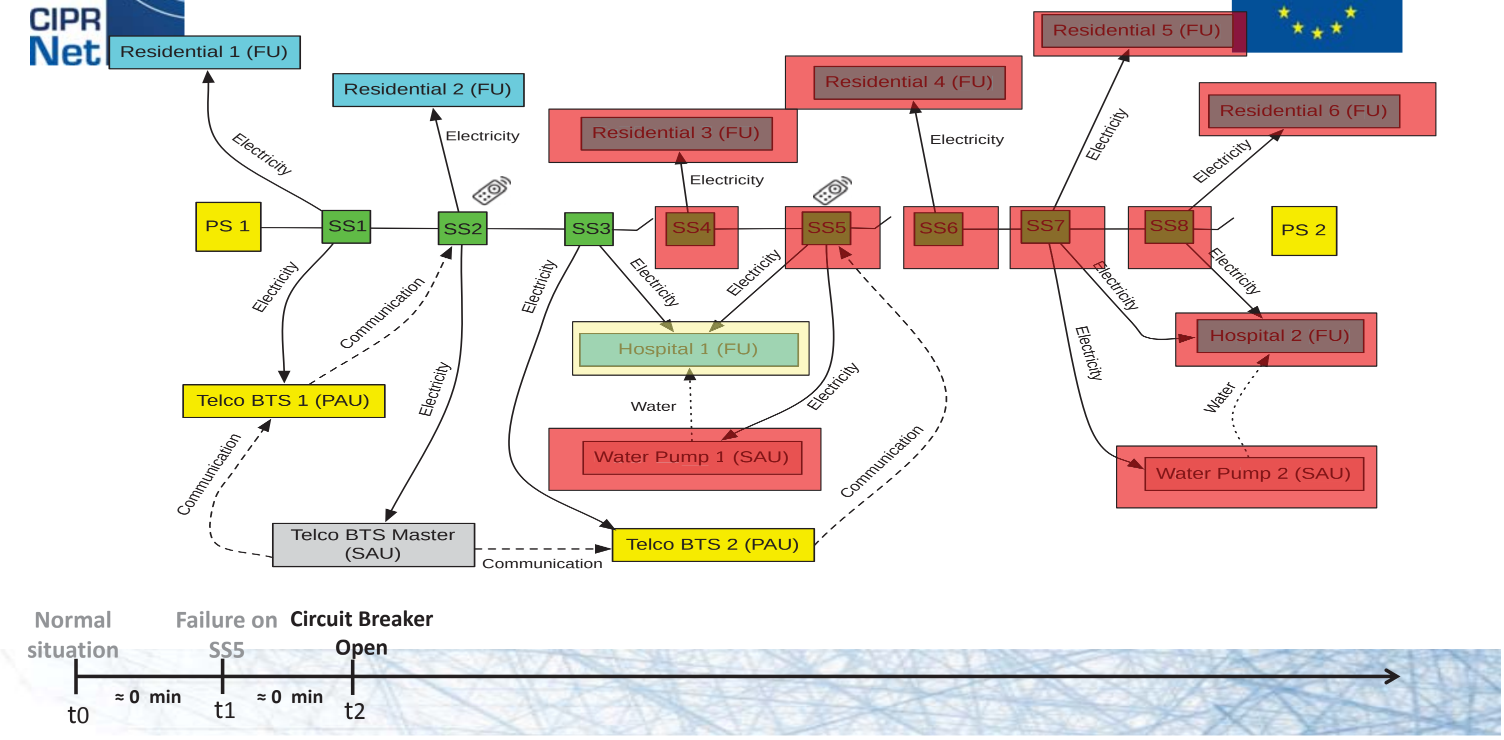
Case 1: Example scenario



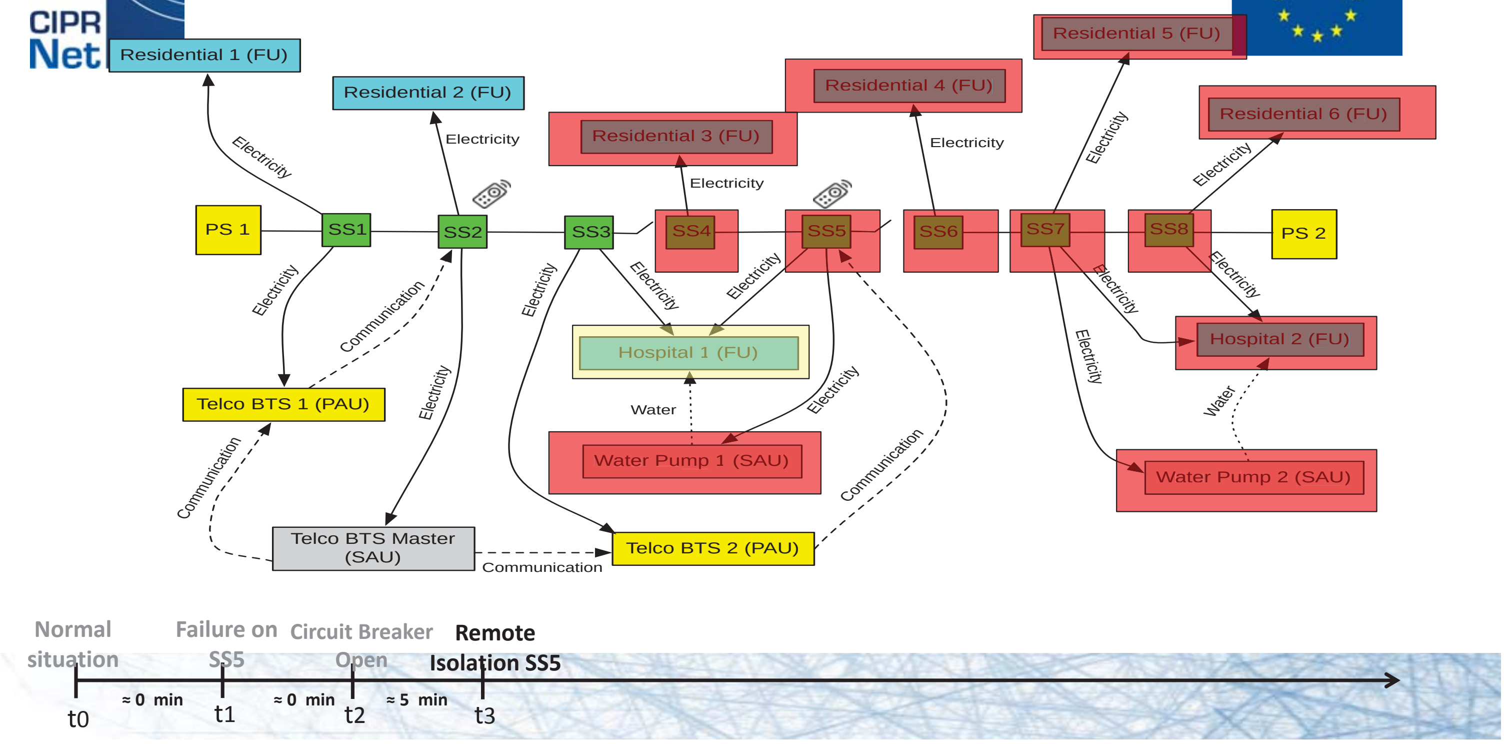
Case 1: Example scenario



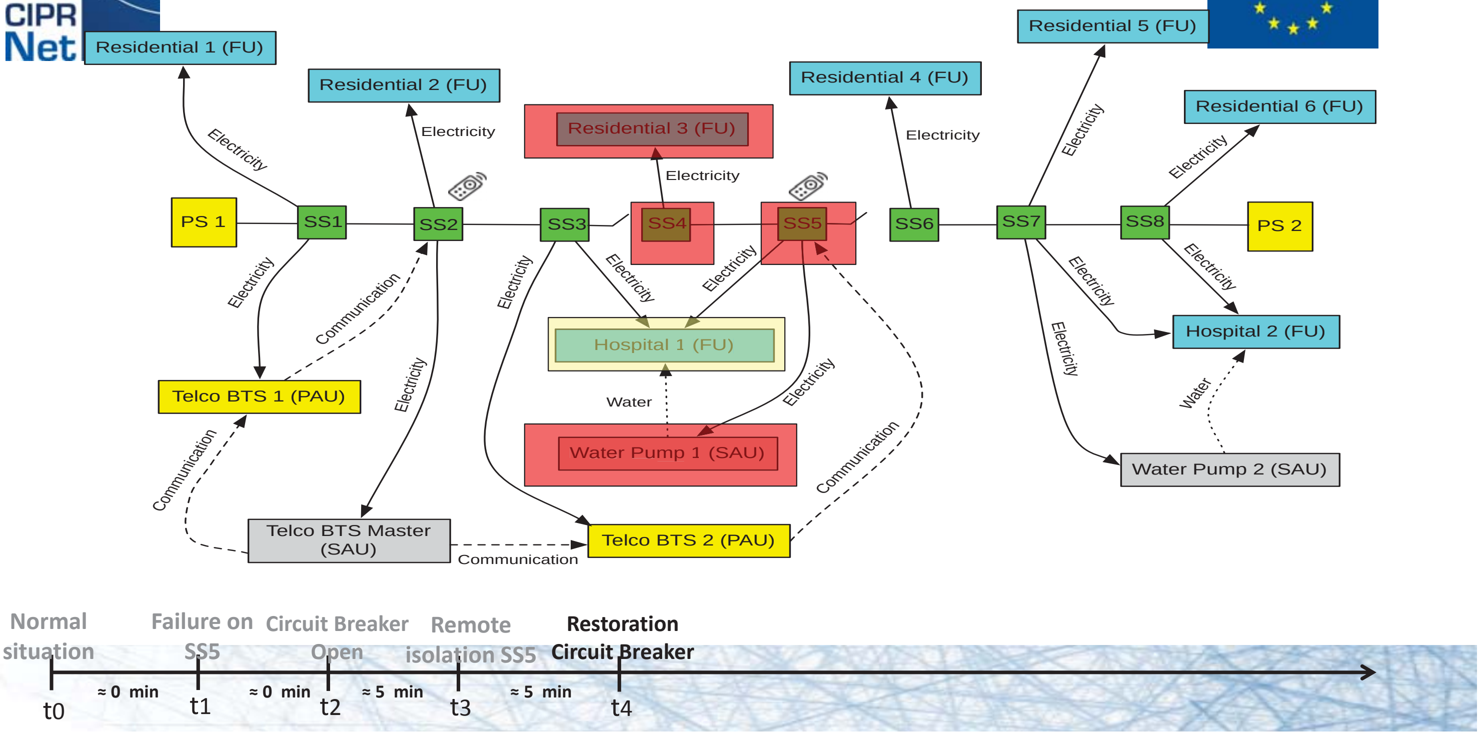
Case 1: Example scenario



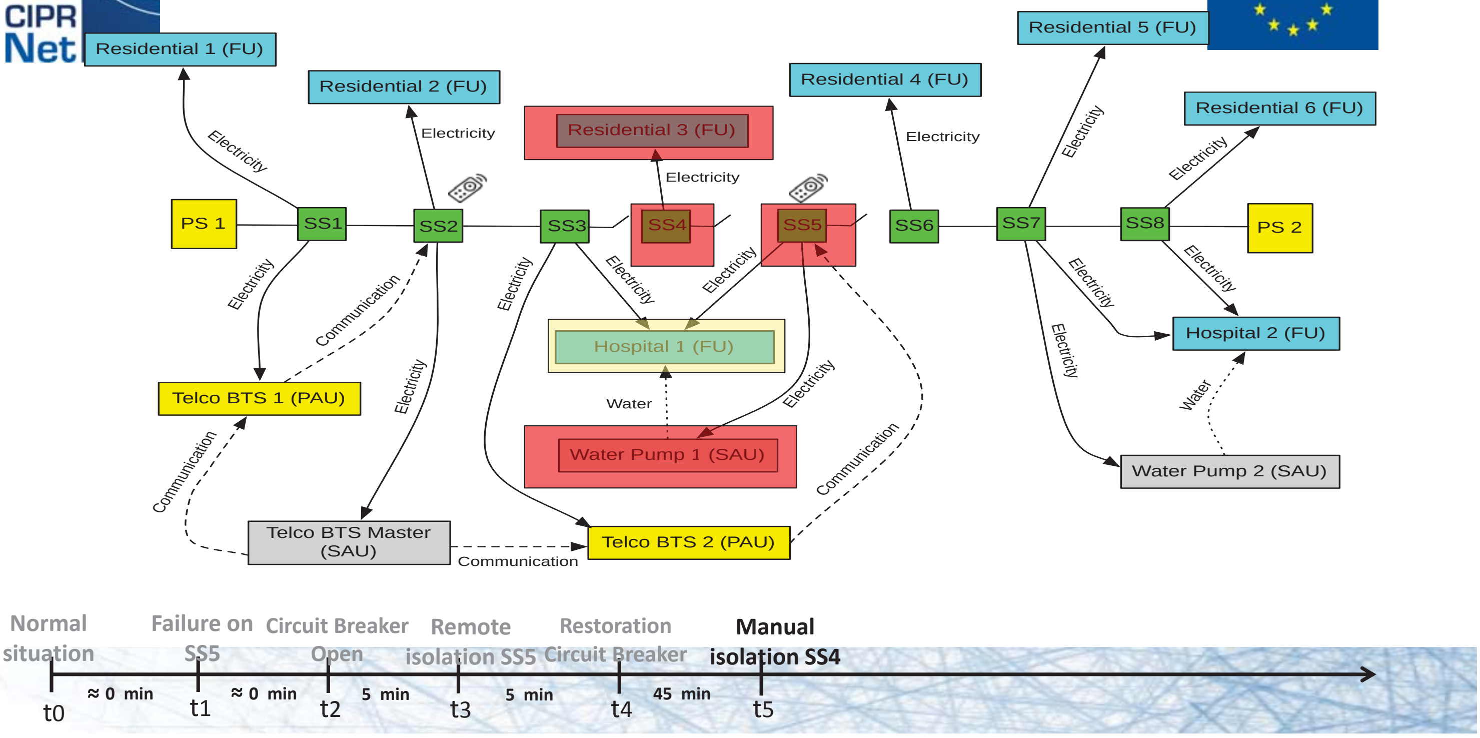
Case 1: Example scenario



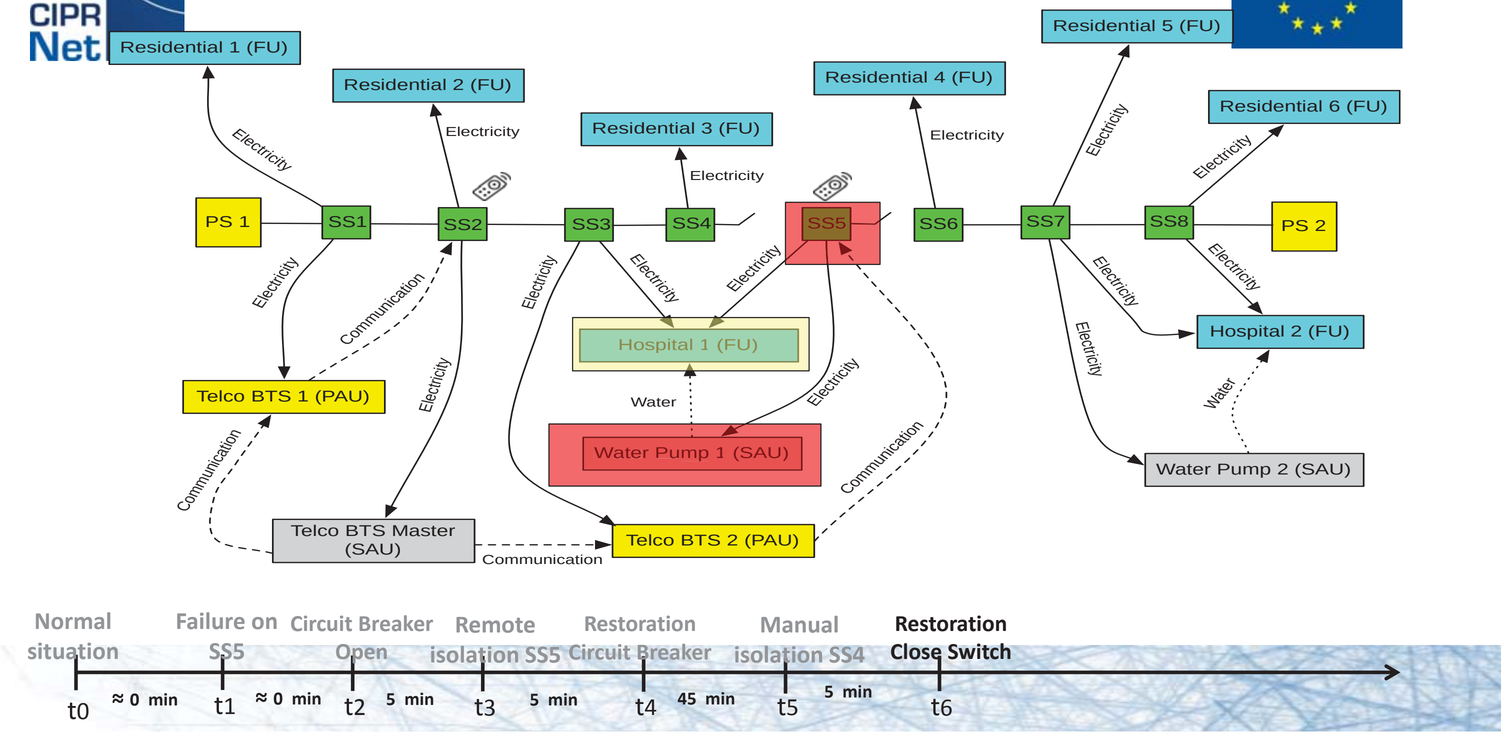
Case 1: Example scenario



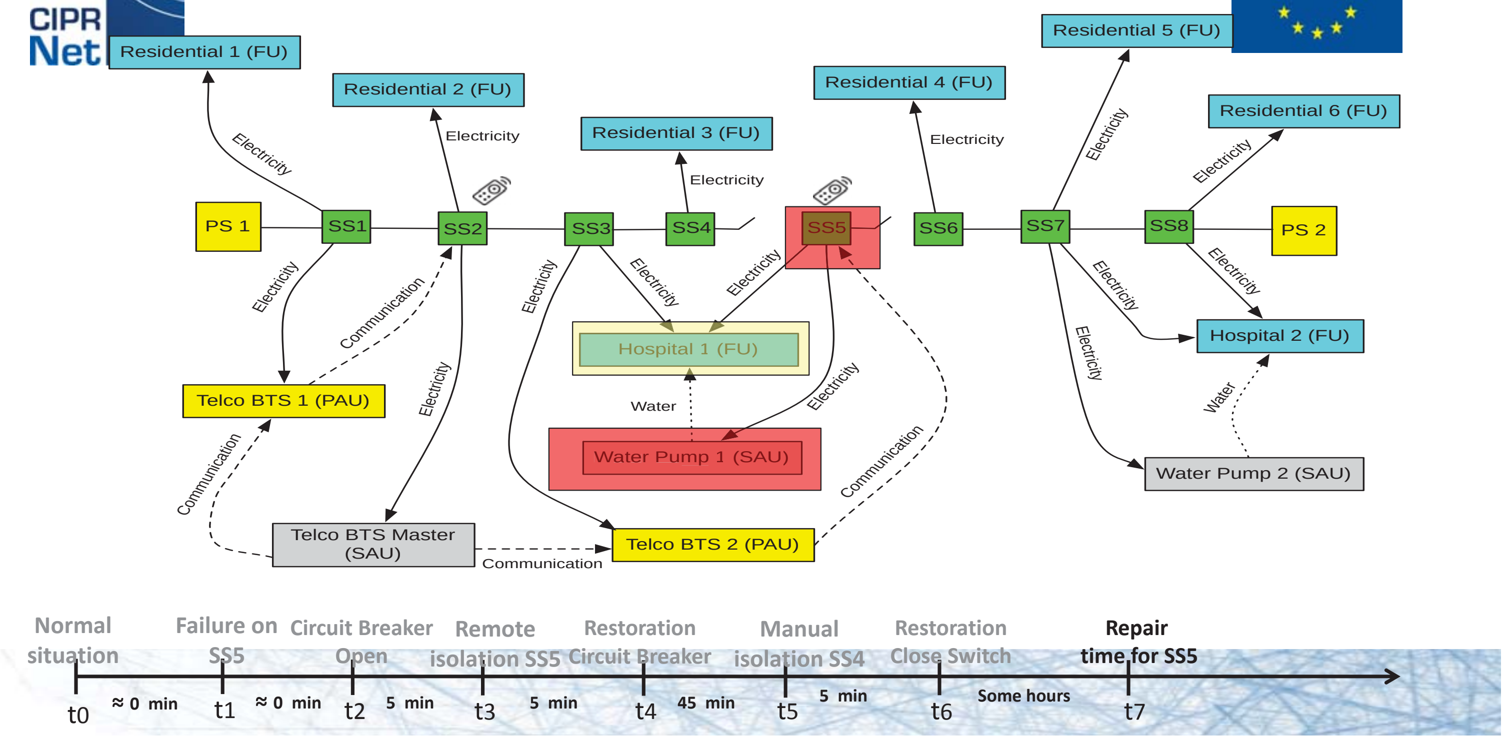
Case 1: Example scenario



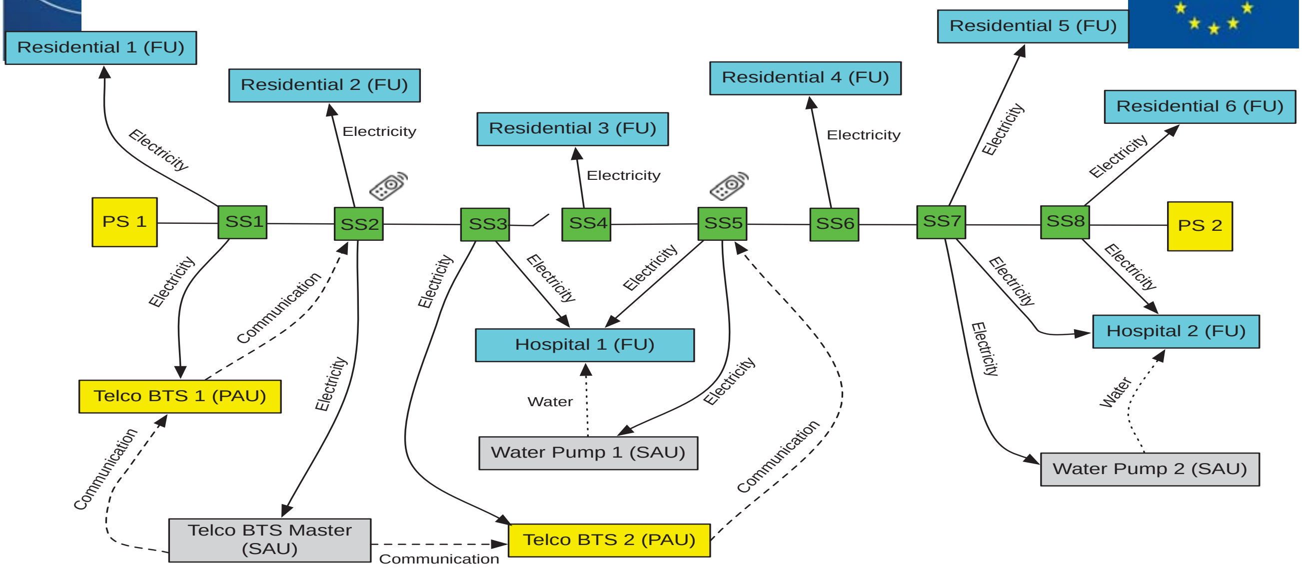
Case 1: Example scenario

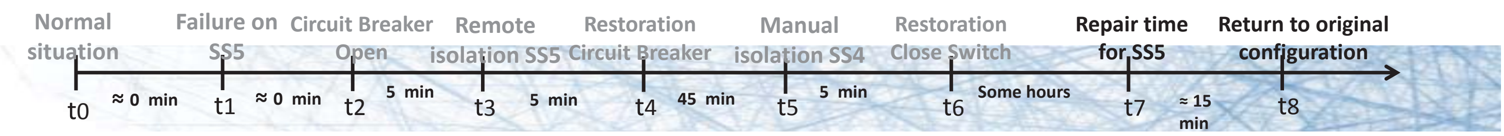


Case 1: Example scenario

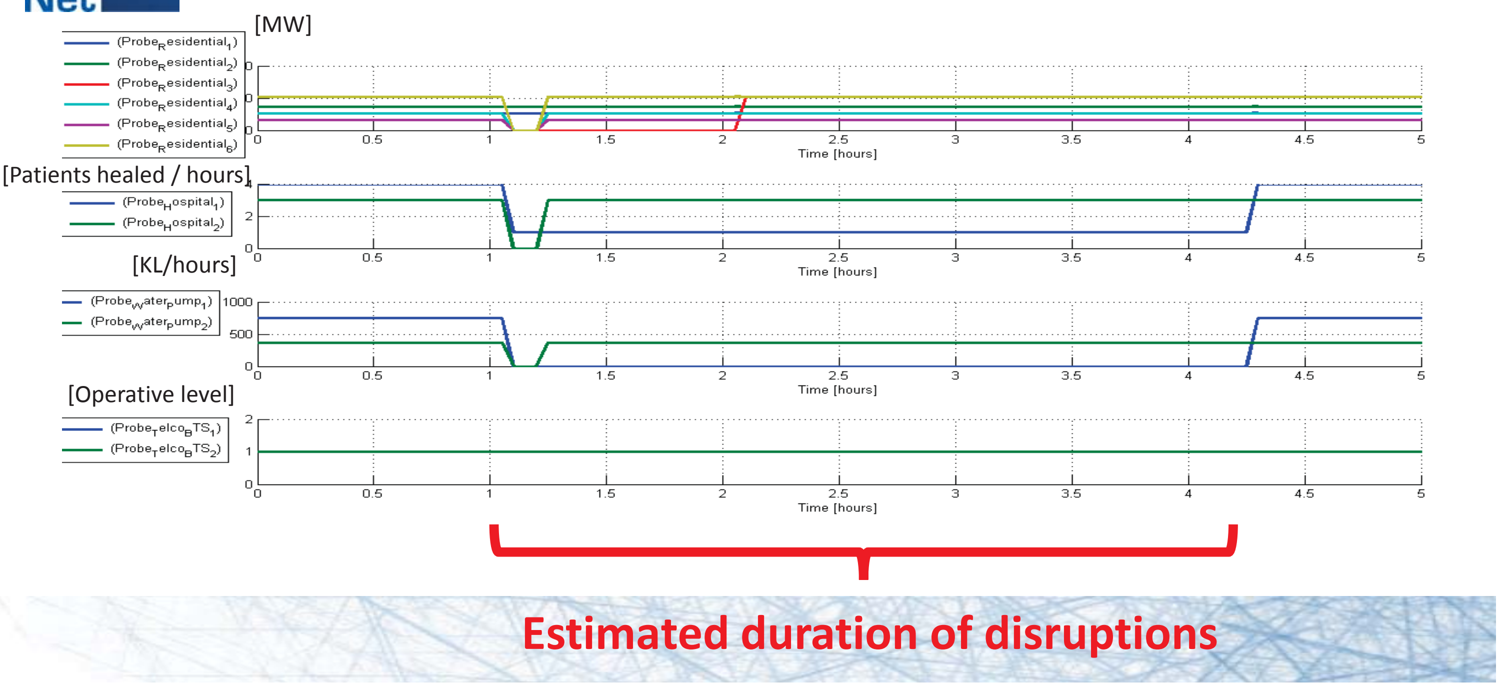


Case 1: Example scenario





I2Sim results



Conclusion

- CIPRNET approach for long term impacts assessment in large scenario
- ISSUES
  - Data gathering
    - A long term process just started!
  - Data homogenisation
    - Different formats
    - Levels of detail
    - Completeness
  - Interdependencies simulation
- CIPRNet approach
  - Integration of i2Sim in the loop
  - Ad hoc procedures + GIS methodologies for data homogenisation
  - Maturity level: low
    - Tested on a small scenario
- Future developments
  - I2Sim new functionalities (backups….)
  - Use of standards for data homogenisation
  - Optimization algorithms

Next Step