European Commission

Risk Assessment and Resilience for Critical Infrastructures

Workshop Proceedings
25-26 April 2012
Ranco, Italy

Editors:
Georgios Giannopoulos, Roberto Filippini

2012

Report EUR 25398 EN

Joint Research Centre

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Forename Surname
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 210, 21027 Ispra (VA), Italy
E-mail: georgios.giannopoulos@jrc.ec.europa.eu
Tel.: +39 0332 78 6211
Fax: +39 0332 78 5469

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

Legal Notice
Neither the European Commission nor any person acting on behalf of the Commission
is responsible for the use which might be made of this publication.

Europe Direct is a service to help you find answers to your questions about the European Union
Freephone number (*): 00 800 6 7 8 9 10 11
(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

A great deal of additional information on the European Union is available on the Internet.
It can be accessed through the Europa server http://europa.eu/.

JRC71923

EUR 25398 EN

ISBN 978-92-79-25589-2 (pdf)
ISBN 978-92-79-25590-8 (print)

ISSN 1831-9424 (online)
ISSN 1018-5593 (print)

doi:10.2788/35908

Luxembourg: Publications Office of the European Union, 2012

© European Union, 2012

Reproduction is authorised provided the source is acknowledged.

Printed in Italy

Contents

Proceedings of Workshop on Risk Assessment and Resilience for Critical Infrastructures

1 Background and purpose of the Workshop

Critical Infrastructures are essential for supporting everyday functions of modern societies. These functions depend on an extensive network of infrastructures that nowadays are highly connected, forming a complex mesh of interdependencies which facilitate exchange of services of various forms. The benefits from networking are accompanied by new threats and risks. In particular, disruptions in certain infrastructures can cause rippling effects that may render unstable the whole infrastructures network.

The issue of preserving and protecting infrastructures is a priority for modern societies and economies. However, because of their unprecedented complexity, gaps exist on the methodologies used to assess the risks and the identification of those measures necessary to preserve their functionality. The majority of researchers, scientists and policy makers have been concentrated on assessing the risk in case of infrastructure functioning disruption. This approach in fact implies a thorough understanding of the functioning of the various parts of the infrastructure and in particular their behavior under off-nominal operation conditions. The main hurdle for the application of this approach stands in the fact that data are incomplete. The continuously evolving nature of critical infrastructures (in topology) is another hurdle. Similarly, the idea of performing tests by inducing disruptive events is unrealistic and non-acceptable. In view of this, a different approach is necessary.

Systemic approaches overcome the limitations of risk assessment as they focus on attributes that an infrastructure possesses at systemic level, therefore globally. Resilience is one of these attributes. Resilience is applied to complex systems, of which infrastructures are a significant instance. In simple terms, resilience extends control disciplines at a higher level of abstraction. Any infrastructure is a system which is able to sense reality and take decisions, either by controls or procedures, in response to undesired events, and under given constraints and goals.

The concept of resilience can be seen as a superset in which typical risk assessment is a complementary part. A number of methodologies exist for performing risk assessment for critical infrastructures. These mainly focus on three elements: threats, vulnerabilities and impact. The business as usual ap-

proach is the one that prioritises threats, identifies vulnerable points for these threats in a certain system and finally evaluates impact. Of course, because of the aforementioned reasons, this analysis is unsuccessful if proceeds for the whole set of possible scenarios. In this respect, a resilience analysis may return those scenarios for which there is the risk that the infrastructure will collapse. When these scenarios prioritisation is done, a risk assessment can be performed. The systemic approach is developed here in a methodology, which consists of three stages: 1) system representation, 2) structural analysis and 3) dynamic (resilience) analysis. The representation of relationships among any component of the infrastructure returns a dependency network. This network is analysed in order to identify criticalities, vulnerabilities and interdependencies. The same model serves for the dynamic analysis. The scope is the propagation of disturbances, generated in one system, throughout the infrastructure and the ability of the same network to withstand disturbance and recover in case of failure. A number of critical scenarios can be identified from the latter analysis stage.

The identification of these critical scenarios is of outmost importance. The resilience analysis proves that the infrastructure is able to withstand a number of scenarios (e,g. under control), those that not lead to failure but stay rather within the limits for which the infrastructure has got internal resilience measures (e.g. buffering capacity, recovery). A minority of the identified failure scenarios will instead ask for more investigation, either by simulation or by a traditional risk assessment approach. Risk and resilience may be seen as complementary and they are here applied in synergy within the methodology. The dedicated session on Risk Assessment for Critical Infrastructures will provide an exhaustive introduction to the above mentioned concepts and methodologies, with the objective of supporting the following theses:

- A systemic approach is necessary in order to fully grasp the dynamics of modern infrastructures
- Risk assessment is not the final target but rather a supportive element of a more general framework for assessing the performance of infrastructures/systems
- Resilience analysis, resilience control measures and resilience informed design are issues that operators of critical infrastructures should consider as priority

2 Summary of the elements presented during the Workshop

There has been a substantial effort to prepare this workshop in a way to represent a variety of aspects related to critical infrastructures modelling. The majority of representatives provided a view from the academic/research world on the modelling of risk and resilience on critical infrastructures. However, the view of the operators was also presented (Eurocontrol) in order to obtain an operational view of risk and resilience in a big organisation.

In principle most of presentations that were dealing with complex systems interdependencies are related to electricity grids. These networks are well studied, data are available and in addition they have a European aspect with interdependencies that overcome the limits of one single country. In addition the

dependencies of other infrastructures on the electricity grid are clear. What is important to stress out is that the methodologies presented focused on the electricity grids can be also extended to other interconnected infrastructures. They can be considered as a specific proof of concept for generic methodologies.

Among the different elements that were presented, interdependencies between infrastructures of the same or different sectors were among the most dominant ones. Different types of interdependencies exist. In principle geographical and cyber interdependencies are dominating the discussions but functional interdependencies are also important. This depends also on the level of abstraction that is used for the representation of a complex system.

Modelling of complex systems requires the set up of sophisticated simulation tools in order to account for the necessary complexity. The approach of federation is presented b a number of participants where different models can be plugged-in on a common platform in order to simulate complex interoperable inhomogeneous infrastructures. On the counterpart of this approach, connectivity details between the different elements can be obscured.

3 Annexes

- Terms of reference for the Risk Assessment and Resilience Workshop
- Risk Assessment and Resilience Workshop Agenda
- List of participants
- Risk assessment and resilience within the EPCIP: from policy to science
- System Analysis for Interdependent Infrastructures
- Mitigation of risks in air traffic control
- Understanding Complexity and Interdependency: A prerequisite to increase resilience
- Modelling and Simulation in CIP
- Safety of complex energy systems
- Risk assessment methodology for interdependent critical infrastructures
- Supporting PPP for CI resilience with proper modelling and assessment tools: from a regional experience to the European perspective
- Preliminary Interdependency Analysis of Critical Infrastructures: Models, Tool Support and Data Analysis
- Impact estimation: from questionnaires to interdependencies
- Wrap up.

Terms of Reference for the Risk Assessment and Resilience Workshop

EUROPEAN COMMISSION
DIRECTORATE GENERAL JRC
JOINT RESEARCH CENTRE
Institute for the Protection and the Security of the Citizen
Security Technology Assessment Unit

Ispra, 21 February 2012

7th Workshop on the Implementation and Application of the Directive, with Dedicated Session on Resilience and Risk Assessment for Critical Infrastructures

23-26 April 2012
JRC, Ispra

Via E. Fermi 2749 - Ispra, Italy
Organizing Committee: Georgios Giannopoulos, Roberto Filippini, Muriel Schimmer
DG Joint Research Centre - JRC
Tel. – Secr.: +39-0332 78 6038
Contact: georgios.giannopoulos@jrc.ec.europa.eu

1. Introduction

JRC will organize a series of events during the fourth week of April from the 23rd to the 26th. These are related to the review of the EPCIP Directive that has already started in January 2012. JRC actively supports this activity. As a consequence the relevant events should enable Member States to have a clear view on the review process and in addition provide them with the necessary technical elements for issues that are paramount for the assessment of critical infrastructures. Thus a mixture of policy support and technical sessions is foreseen.

The first event will be the **7th Workshop on the Implementation and Application of the Directive** that will continue the series of successful workshops that started in 2009. Considering the roadmap for the review of the Directive 2008/114/EC, the importance of this workshop for the review process is evident. A separate explanatory note as well as a draft agenda will follow in the next weeks concerning this event. The participation to this first workshop is restricted to Member States representatives (CIP Points of Contact). The duration of the event will be 2 days starting in the afternoon of Monday 23/04. It is foreseen that the core business of the workshop will last 1.5 days with the first half day dedicated on a special session for systems/networks in the gas and electricity sector in order to have an update on CIP related work for these networks.

A dedicated **session on Resilience and Risk Assessment for Critical Infrastructures** will conclude the program. The organizers will invite representatives from universities, research institutes, and private sector in order to have the state of the art on the new scientific challenges, developments and trends in this domain. This will be a full day event following the 7th workshop on the Implementation and Application of the Directive, thus starting in the afternoon of 25th of April and ending on the 26th of April at noon. Background information on this event is presented in the following paragraphs.

2. Background information and content of Resilience and Risk Assessment session

Critical Infrastructures are essential for supporting everyday functions of modern societies. These functions depend in an extensive network of infrastructures that nowadays are highly connected, forming a complex mesh of interdependencies which facilitate exchange of services of various forms. The benefits from networking are accompanied by new threats and risks. In particular, disruptions in certain infrastructures can cause rippling effects that may render unstable the whole infrastructures network.

The issue of preserving and protecting infrastructures is a priority for modern societies and economies. However, because of their unprecedented complexity, gaps exist on the methodologies used to assess the risks and the identification of those measures necessary to preserve their functionality. The majority of researchers, scientists and policy makers have been concentrated on assessing the risk in case of infrastructure functioning disruption. This approach in fact implies a thorough understanding of the functioning of the various parts of the infrastructure and in particular their behavior under off-nominal operation conditions. The main hurdle for the application of this approach stands in the fact that data are incomplete. The continuously evolving nature of critical infrastructures (in topology) is another hurdle. Similarly, the idea of performing test by inducing disruptive events is unrealistic and non-acceptable. In view of this, a different approach is necessary.

Systemic approaches overcome the limitations of risk assessment as they focus on attributes that an infrastructure possesses at systemic level, therefore globally. Resilience is one of these attributes. Resilience is applied to complex systems, of which infrastructures are a significant instance. In simple terms, resilience extends control disciplines at a higher level of abstraction. Any infrastructure is a system which is able to sense reality and take decisions, either by controls or procedures, in response to undesired events, and under given constraints and goals.

The concept of resilience can be seen as a superset in which typical risk assessment is a complementary part. A number of methodologies exist for performing risk assessment for critical infrastructures. These mainly focus on three elements: threats, vulnerabilities and impact. The *business as usual* approach is the one that prioritizes threats, identifies vulnerable points for these threats in a certain system and finally evaluates impact. Of course, because of the aforementioned reasons, this analysis is unsuccessful if proceeds for the whole set of possible scenarios. In this respect, a resilience analysis may return those scenarios for which there is the risk that the infrastructure will collapse. When these scenarios prioritization is done, a risk assessment can be performed.

The systemic approach is developed here in a methodology, which consists of three stages: 1) system representation, 2) structural analysis and 3) dynamic (resilience) analysis. The representation of relationships among any component of the infrastructure returns a

dependency network. This network is analyzed in order to identify criticalities, vulnerabilities and interdependencies. The same model serves for the dynamic analysis. The scope is the propagation of disturbances, generated in one system, throughout the infrastructure and the ability of the same network to withstand disturbance and recover in case of failure. A number of critical scenarios can be identified from the latter analysis stage.

The identification of these critical scenarios is of outmost importance. The resilience analysis proves that the infrastructure is able to withstand a number of scenarios (e,g. under control), those that not lead to failure but stay rather within the limits for which the infrastructure has got internal resilience measures (e.g. buffering capacity, recovery). A minority of the identified failure scenarios will instead ask for more investigation, either by simulation or by a traditional risk assessment approach. Risk and resilience may be seen as complementary and they are here applied in synergy within the methodology.

The dedicated session on Risk Assessment for Critical Infrastructures will provide an exhaustive introduction to the above mentioned concepts and methodologies, with the objective of supporting the following theses:

- A systemic approach is necessary in order to fully grasp the dynamics of modern infrastructures
- Risk assessment is not the final target but rather a supportive element of a more general framework for assessing the performance of infrastructures/systems
- Resilience analysis, resilience control measures and resilience informed design are issues that operators of critical infrastructures should consider as priority

Risk Assessment and Resilience Workshop Agenda

Institute for the Protection and Security of the Citizen
European Commission
Joint Research Centre (JRC)
Institute for the Protection and Security of the Citizen

Via E. Fermi, 2749
I-21027 Ispra (VA) - Italy

Tel.: +39 0332 78 6038
Fax: +39 0332 78 5469

Web: http://ipsc.jrc.ec.europa.eu/
E-mail: JRC-STA-SECRETARIAT@ec.europa.eu

VII EPCIP Workshop on the Implementation and application of Directive 2008/114/EC and Risk Assessment and Resilience Session

Hotel Conca Azzura, Ranco, Italy

24-26 April 2012

Final Agenda

Robust science for policy making

OUR MISSION

The mission of the Joint Research Centre is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of European Union policies. As a service of the European Commission, the Joint Research Centre functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

VII EPCIP Workshop on the Implementation and Application of Directive 2008/114/EC

24 April

12:30-14:00 **Lunch**

14:00-14:30 **Welcome and Introduction – Overview of the State-of-Play (DG HOME, JRC)**

14:30-16:00 **Implementation issues – Tour de table. Views from the MS.**

16:00-16:15 **Coffee Break**

16:15-17:30 **ENTSOE Brussels workshop follow up (Joachim Vanzetta, ENTSOE)**

25 April

09:30-10:15 **Presentation of the status of the impact assessment study. (DG HOME, Contractor)**

10:15-10:30 **Coffee Break**

10:30-12:30 **General discussion on the policy options and input from MS**

12:30-14:00 **Lunch**

14:00-16:00 **Overall discussion, way forward, discussion of topics and date and content of next workshop**

Risk Assessment and Resilience session

16:00-17:30 **Introduction (JRC).**

19:00 **Dinner**

26 April

09:00-09:30 **Mitigation of risks in air traffic control (**Mr. Fred Konnemann, Mr. Matteo Sottile, Eurocontrol**)**

9:30-10:00 **Understanding Complexity and Interdependency: A prerequisite to increase resilience (**Prof. Wolfang Kröger, ETH Risk Centre)

10:00-10:30 **Modelling and Simulation in CIP (**Dr. Rüdiger Klein, Fraunhofer IAIS, Germany**)**

10:30-11:00 **Safety of complex energy systems (**Prof. Enrico Zio, Systems Science and Energetic Challenge, Ecole Centrale Paris and Supelec, Paris, France**)**

11:00-11:15 **Coffee Break**

11:15-11:45 **Risk assessment methodology for interdependent critical infrastructures (**Prof. Marianthi Theoharidou, Department of Informatics, Athens University, Athens, Greece**)**

11:45-12:15 **Supporting PPP for CI resilience with proper modelling and assessment tools: from a regional experience to the European perspective (**Prof. Paolo Trucco, Dipartimento Ingegneria Gestionale, Polytechnic of Milan, Italy**)**

12:15-12:45 **Preliminary Interdependency Analysis of Critical Infrastructures: Models, Tool Support and Data Analysis (**Prof. Peter Popov, Centre of Software Reliability, City University of London**)**

12:45-13:15 **Impact estimation: from questionnaires to interdependencies (**Prof. Stefano Panzieri, Department of Informatics and Automation University Roma 3, Italy**)**

13:30-14:45 **Lunch**

14:45-16:00 **Wrap up, conclusions and way forward**

16:00 **End of Workshop**

Practical details

All participants have to register through this link:
https://jrc-meeting-registration.jrc.ec.europa.eu/

The meeting will be held in:
Hotel Conca Azzurra, Angera (VA), Italy

Airports in Milan are:
Milano Malpensa and Milano Linate

Local transports
Transport from and to these airports and from and to the agreed hotels will be organized by JRC.

Hotel rooms have been pre-booked in the area. Please register by April 13rd to secure a hotel room.

For **information on the contents** of the workshop please contact:

Mr. Christian Krassnig
+32 (0)2 29 86 445.
Christian.KRASSNIG@ec.europa.eu

Mr. Georgios Giannopoulos
+39 0332 786211
Georgios.GIANNOPOULOS@jrc.ec.europa.eu

Mr. Roberto Filippini
+390332789936
Roberto.Filippini@jrc.ec.europa.eu

Ms.Muriel Schimmer
+39 0332 785295
muriel.schimmer@jrc.ec.europa.eu

For **organizational issues** please contact:
Ms. Laurence Campé :
+39 0332 785032
Laurence.CAMPE@ec.europa.eu

List of participants

JRC
EUROPEAN COMMISSION

Resiliance and risk assessment for critical infrastructures

25/04/2012 - 26/04/2012

TOTAL PARTICIPANTS: 15

SARA BOUCHON
Risk Governance Solutions S.r.l.
Via Fratelli d'Italia, 7
21052 BUSTO ARSIZIO (VA) (Italy)
tel: 00393491959490

E-mail: sbouchon.rgs@tiscali.it

DIMAURO CARMELO
Risk Governance Solutions S.r.l.
via Fratelli d'Italia
21052 BUSTO ARSIZIO (VA) (Italy)

E-mail: carmelo.dimauro@riskgovernancesolutions.eu

PETER DIEBEN
Eurocontrol
96, Rue de la Fusee
1130 BRUSSELS (Belgium)

E-mail: peter.dieben@eurocontrol.int

ROBERTO FILIPPINI
Joint Research Centre
Via Fermi 2749
21027 ISPRA (Italy)

E-mail: roberto.filippini@jrc.ec.europa.eu

RÜDIGER KLEIN
Fraunhofer IAIS
Schloss Birlinghoven
53754 SANKT AUGUSTIN (Germany)
tel: 00492241142608
fax: 004922412342
E-mail: Ruediger.Klein@IAIS.Fraunhofer.de

FRED KONNEMANN
EUROCONTROL
Horsterweg 11
6199AC MAASTRICHT AIRPORT (Netherlands)
tel: +31 43 3661247
fax: +31 43 3661400
E-mail: fred.konnemann@eurocontrol.int

WOLFGANG KROEGER
ETH Zurich, Risk Center
Scheuchzerstrasse 7
8092 ZURICH (Switzerland)
tel: +41 44 632 64 18
fax: +41 44 632 10 94
E-mail: wkroeger@ethz.ch

STEFANO PANZIERI
University ROMA TRE
Via della vasca Navale, 79
00146 ROMA (Italy)
tel: +39 0657333376

E-mail: panzieri@uniroma3.it

PETER POPOV
City University London
Northampton Square
EC1V 0HB LONDON (United Kingdom)

E-mail: ptp@csr.city.ac.uk

GIOVANNI SANSAVINI
Politecnico di Milano
Via Ponzio 34/3
20133 MILANO (Italy)

E-mail: giovanni.sansavini@polimi.it

HANS-RUDOLF SCHAEFER
IABG mbH
Einsteinstrasse 20
85521 OTTOBRUNN (Germany)
tel: +49 89 6088-3061

E-mail: Schaefer Hans-Rudolf [SchaeferRu@iabg.de]

MATTEO SOTTILE
EUROCONTROL
Horsterweg 11
6199 MAASTRICHT-AIRPORT (Netherlands)

E-mail: matteo.sottile@eurocontrol.int

MARIANTHI THEOCHARIDOU
Athens University of Economincs and Business
76 Patission Ave.
10434 ATHENS (Greece)

E-mail: mtheohar@aueb.gr

PAOLO TRUCCO
Politecnico di Milano - School of Management
Via Lambruschini 4/b
20156 MILAN (Italy)
tel: +39 02 2399 4053

E-mail: paolo.trucco@polimi.it

ENRICO ZIO
Ecole Centrale Paris
Grande Voie des Vignes
92295 CHATENAY-MALABRY (France)
tel: 0033(0)141131606
fax: 0033(0)141131272
E-mail: enrico.zio@ecp.fr

Risk assessment and resilience within the EPCIP: from policy to science

Georgios Giannopoulos
EC, DG JRC
Unit G.6 Security Technology Assessment
email: georgios.giannopoulos@jrc.ec.europa.eu

Summary

The first part of the presentation from JRC was focused on the support of JRC to the policy making process and how this is translated to concrete scientific work. The presentation provided an overview of the current process for the identification of critical infrastructures at European level and the steps that are necessary in order to apply resilience and improve the protection of European Critical Infrastructures responding to the findings of the Directive review study.

Risk assessment and resilience within the EPCIP: from policy to science

Georgios Giannopoulos

Outline

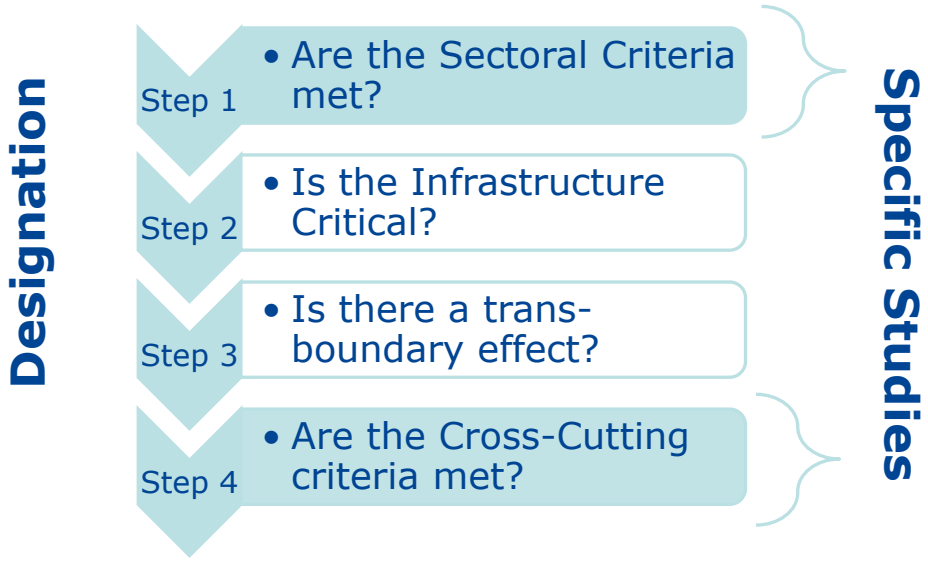
- EPCIP and directive review
- Which tools for the analysis of CI
- The risk and resilience assessment framework

Why the RA and Resilience workshop?

Arguments on

- Global vs Local approach
- Risk assessment as an integral part of resilience
- Resilience analysis – Resilience control measures and relevant actors

EPCIP Directive State of the art



Evaluation study evidence

Designation

- Sectoral – cross cutting criteria appropriateness
- Difficult to follow CI evolution and emerging threats
- Bottom-up approach no provision for European wide infrastructures

Protection

- No clear evidence of increased protection for ECIs following application of Directive

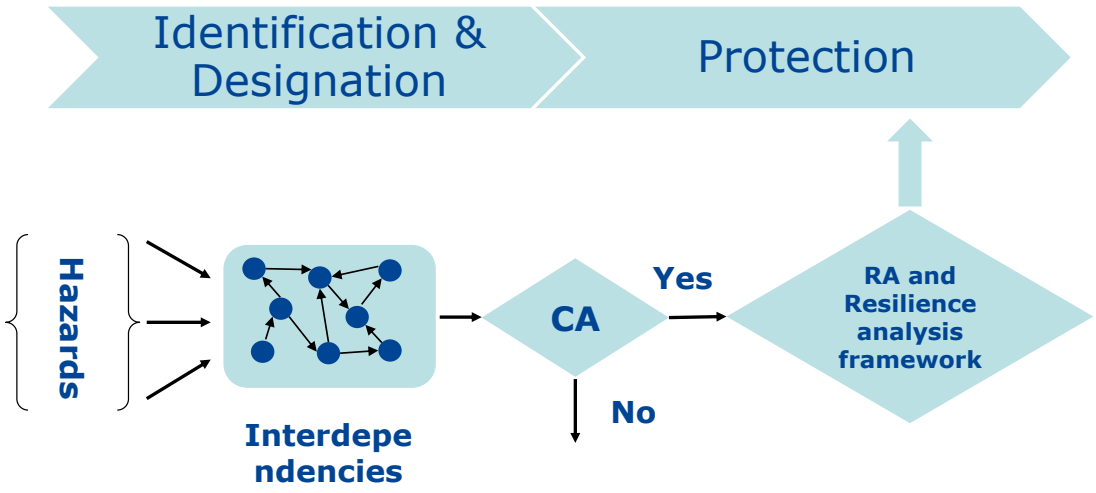
Objective: Respond to the evaluation study findings

Improve identification process

Improve protection

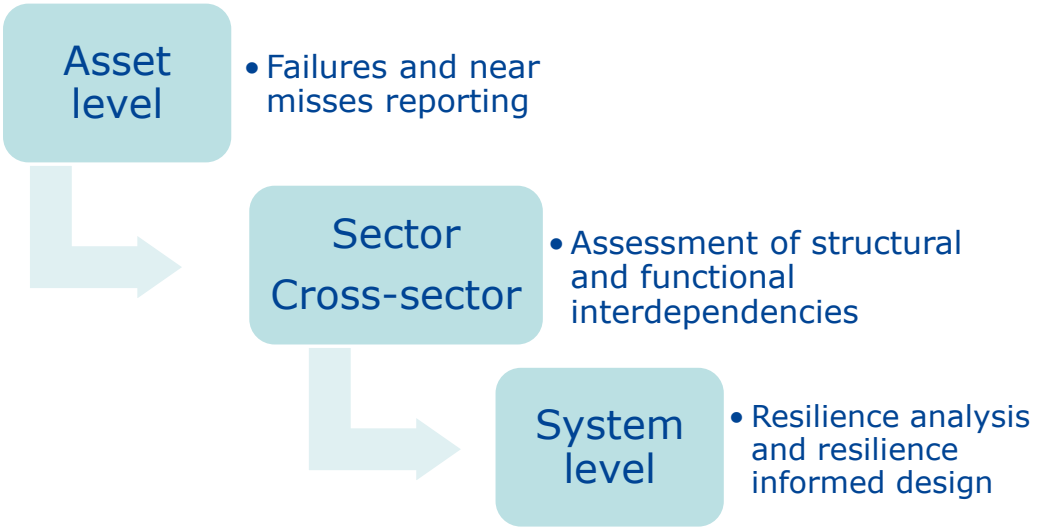
Common framework at EU level

Directive Review: Process, tools, methods



Protection: Resilience analysis Framework

Examples of Implementation Tools



System Analysis for Interdependent Infrastructures

Roberto Filippini
EC, DG JRC
Unit G.6 Security Technology Assessment
email: roberto.filippini@jrc.ec.europa.eu

Summary

The presentation from Dr. Filippini introduced to the research activities that focus on resilience assessment of systems of systems with critical infrastructures being a special instance. The methodologies are based on on the functional representation of system interconnections. From this presentation tools for structural and resilience analysis are devised and arranged in comprehensive modelling and analysis framework for resilience and risk assessment.

System Analysis for Interdependent Infrastructures

Roberto Filippini

Outline

- Scope and objectives
- Modeling interdependencies
- Structural Analysis of interdependencies
- Resilience analysis
- The system analysis framework
- Conclusions

Scope and objectives: background

Analysis issues

- Represent complexity/ cross-sector heterogeneity
- Modeling failure pathologies due to interdependencies
- Return useful quantities, structural, resilience and risk related

Design/management issues

- Protect local and global assets
- Managing emergencies, large scale, cross-sector
- Incorporate new design principles for resilience

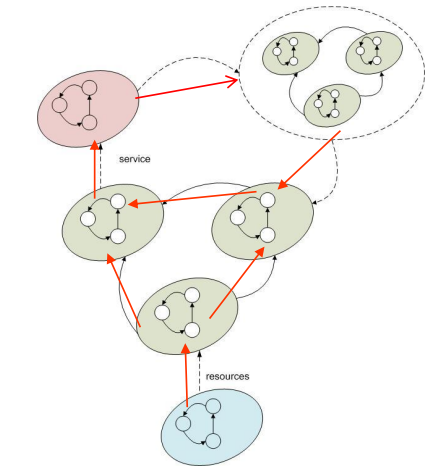
Scope and objectives: our view

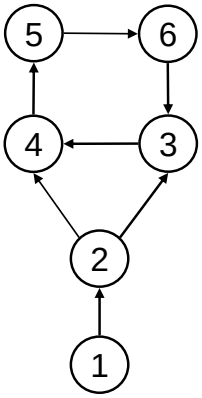
- **System representation**
  - Abstraction => interfaces, interconnections
- **System analysis**
  - Structural => vulnerability, criticality, interdependency
  - Dynamics => system response to failures => resilience
- **Resilience oriented design**
  - Outcomes to be used by operators and decision makers
  - Cross sector/intra-dependency measures to master system variability

Modeling interdependencies

1. Identify relationships at the interfaces
   - Producer/consumer, provider/user, controller/controlled
2. Transform relationships into functional dependencies
   - The dependency is a-dimensional

- **Outcome** => Network of functional dependencies
  - The network topology is a directed graph





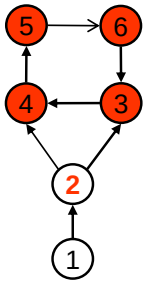
System of systems
Heterogeneous

Dependency network
Homogenous
Input/output dependencies

Structural analysis

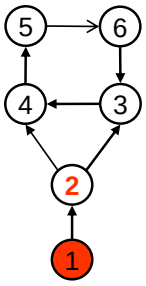
- **The dependency network** represents the topology of dependencies through which systems interact

- **Structural issues**
  - How to identify most critical nodes?
  - How to identify most vulnerable nodes?
  - How to discover interdependent nodes?
  - How strict a node is coupled to the others (average distance)?
  - How many interdependency are established for a given node?
  - …



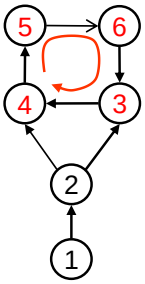
Criticality

Node 2 affects
3,4 (directly)
5,6 (indirectly



Vulnerability

Node 2 is
reachable from 1



Interdependency

Loop 3,4,5,6

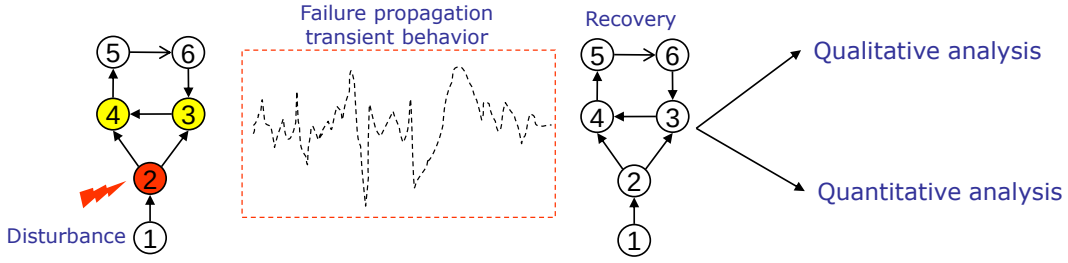
Resilience analysis

- **Resilience** is the ability of a system of preventing, withstanding, reacting and recovering from failures caused by a disturbance.

- **Resilience issues**
  - Is a system resilient to disturbance (locally) ?
  - Is a network resilient to disturbance (globally)?
  - Are the measures in place sufficient to resist/recover?
  - Do they exist scenarios that cannot be recovered?
  - …

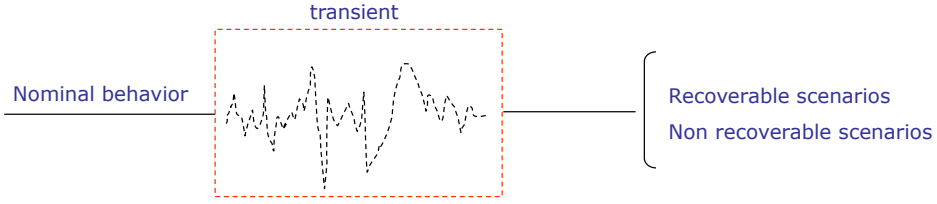
Resilience analysis

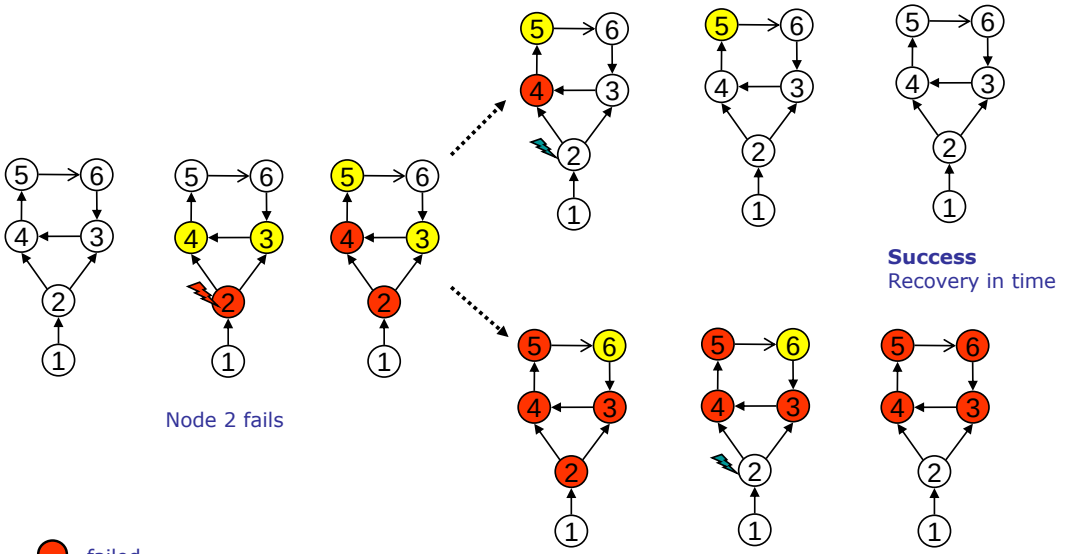
- **Event Driven dynamics**
  - Failures are triggered by input disturbances
  - Recovery is possible if input dependencies are available

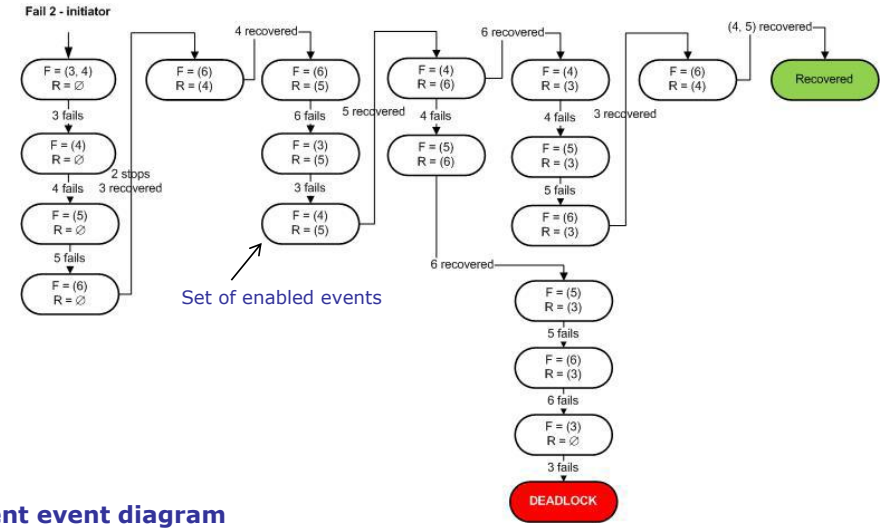


Resilience analysis: qualitative

- **The system response is a sequence of events**
  - The disturbance in a node is the initiating event
  - Next event is within a set of failure (F) and recovery (R) events
- **The tool => concurrent event sequence diagram**
  - **Outcome** => Resilience scenarios







Concurrent event diagram

Two possible scenarios are identified – which one will occur? Simulation is necessary

Resilience analysis: quantitative

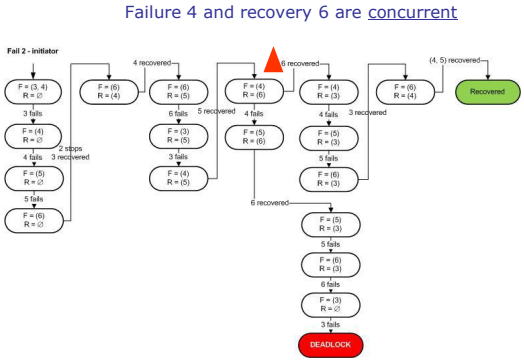
- **System response** is the transient behavior
- **Model parameters**
  1. Resilience related => resist to failure, and time to recovery
  2. Disturbance profile => where (which node) and duration
- **Tool => simulation**
  - Resilience as function of the system states

Resilience analysis: quantitative (2)

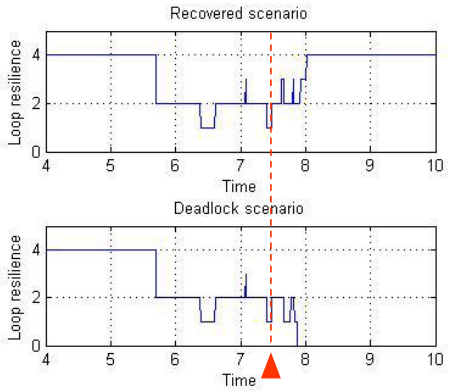
- **Input from the qualitative analysis**
  - Select most critical scenarios

1. **Deterministic analysis**
   - Resilience for the given settings and disturbance profile
   - Sensitivity analysis

2. **Stochastic analysis**
   - Probability of resilience for the given settings and disturbance profile



Failure 4 and recovery 6 are concurrent

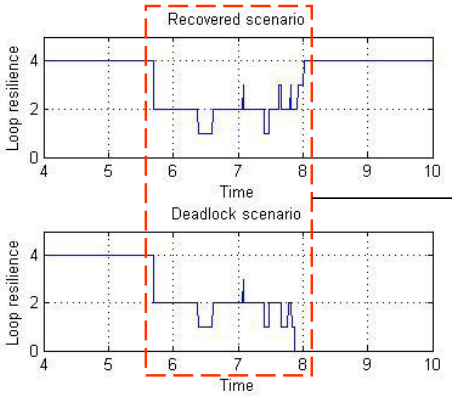


Simulation of scenarios (deterministic)

Resilience is the sum of the node's states (1 is functioning) in the loop 3, 4, 5 and 6.

Resilience and Risk assessment

- Estimate of consequences
- Evaluation of the likelihood



Transient behavior

Estimate costs for the duration of the service disruption, for each node affected

Resilience informed design (1)

- **Structural issues**
  - Does a system "see" indirect dependencies?
  - Does a system realize its criticality and vulnerability?
  - Does a system know of being part of interdependency?

- **Recommendations**
  - Modify topology in order to reduce criticality and vulnerability

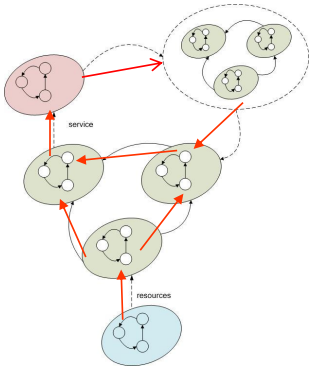
Resilience informed design (2)

- **Dynamic issues**
  - Does a system have sufficient measures not to fall into a deadlock?
  - Does a system coordinate with neighbors to stop failure propagation?
  - Is the overall system variability under control?

- **Recommendations**
  - Remove the possibility that certain failure scenarios may occur
  - Improve resilience measures (buffering, recovery)
  - Implement additional control layers, for supervision and coordination of clusters of interdependent nodes

Top down

Design of the system of systems



Bottom up

Design of each system

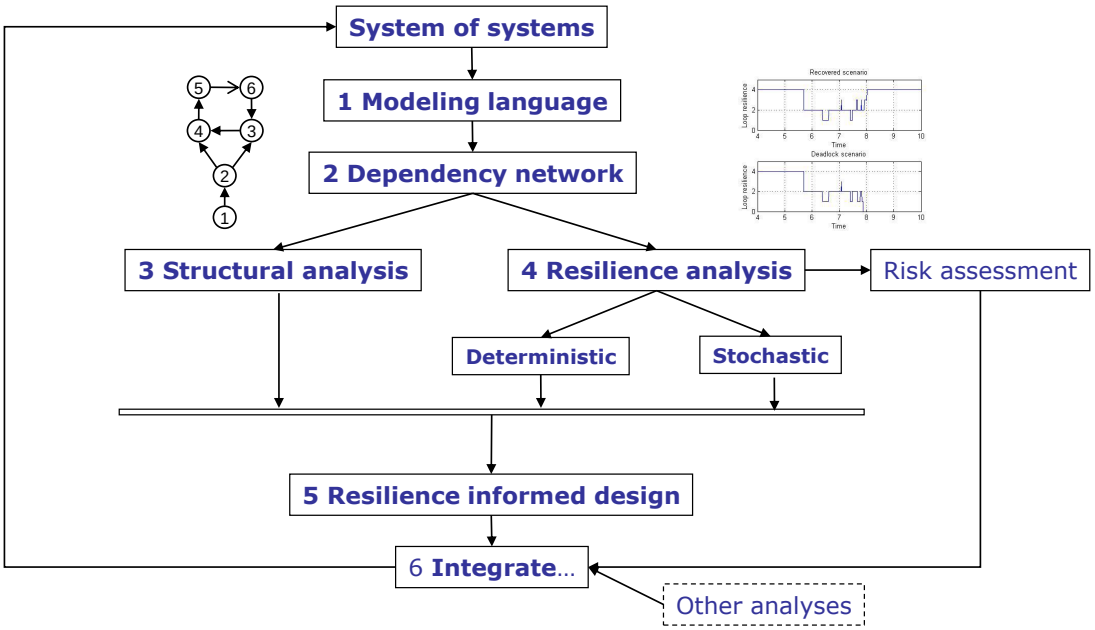
System variability

Is the (emerging) behavior predictable?

What about residual system variability?

Control variability

Cross-sector
Intra-dependencies



Conclusions

- **The underlying ideas**
  - Develop a methodology in which all relevant players in a interconnected infrastructure may be included within the same analysis framework
  - Focus on functional dependencies
  - Define simple failure/recovery mechanisms
  - Return structural quantities and resilience

- **Resilience informed design**
  - Reduce/control system variability
  - Control paradigm, cross-sector and intra-dependencies
  - Risk assessment of most critical scenarios

Mitigation of Risks in air traffic control

Fred Konnemman - Matteo Sottile
Eurocontrol - Maastricht Upper Area Control

Summary

The presentation from Eurocontrol identified safety as one of the most important issues but this has to be obtained without compromising performance. An additional element that renders the whole process more difficult is the fact that the decisions have to be taken in real time although planning takes place in advance for optimisation purposes. The resilience is not explicitly addressed in design/programming phase. Instead, a risk assessment process is undertaken. Finally in case of emergency, safety is the priority.

Resilience and Risk assessment for Critical Infrastructures workshop.

MITIGATING RISKS IN AIR TRAFFIC CONTROL

EUROCONTROL MAASTRICHT UAC

Matteo Sottile
Fred Könnemann

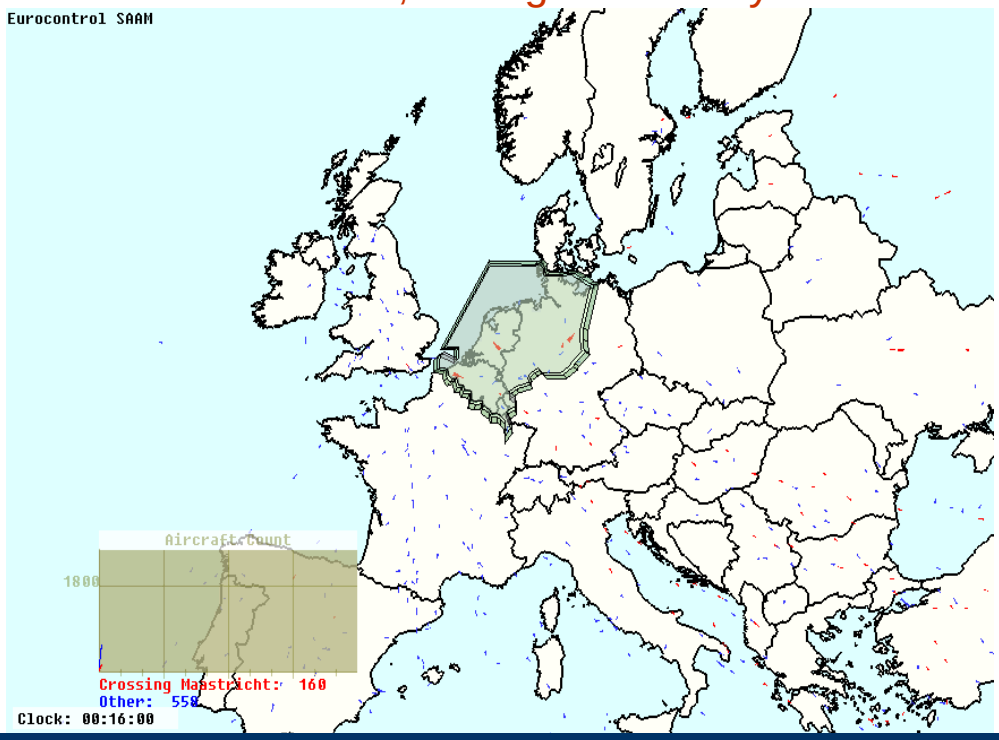
The European Organisation for the Safety of Air Navigation

CONTENT

- ❑ OVERVIEW OF EUROCONTROL MAASTRICHT UAC
- ❑ RISKS IN AIR TRAFFIC CONTROL
- ❑ ENSURING AVAILABILITY AND RELIABILITY

TRAFFIC

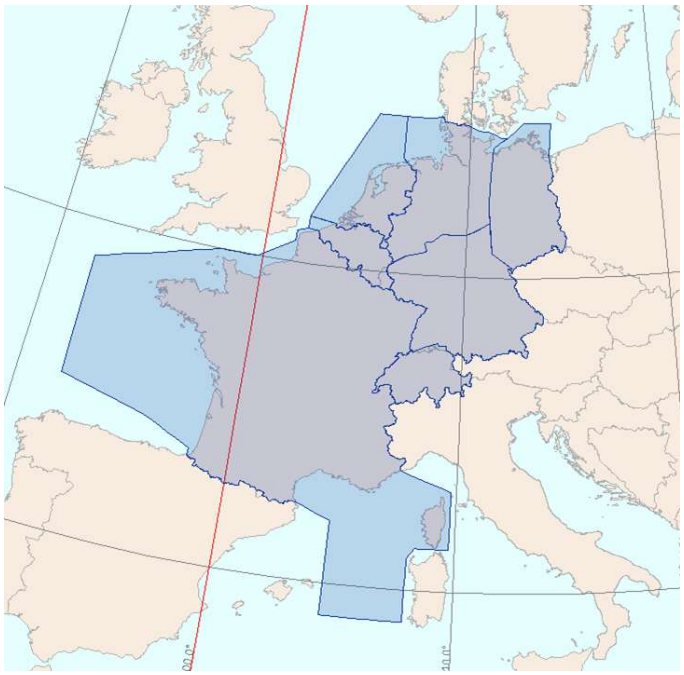
More than 5,000 flights on busy summer days



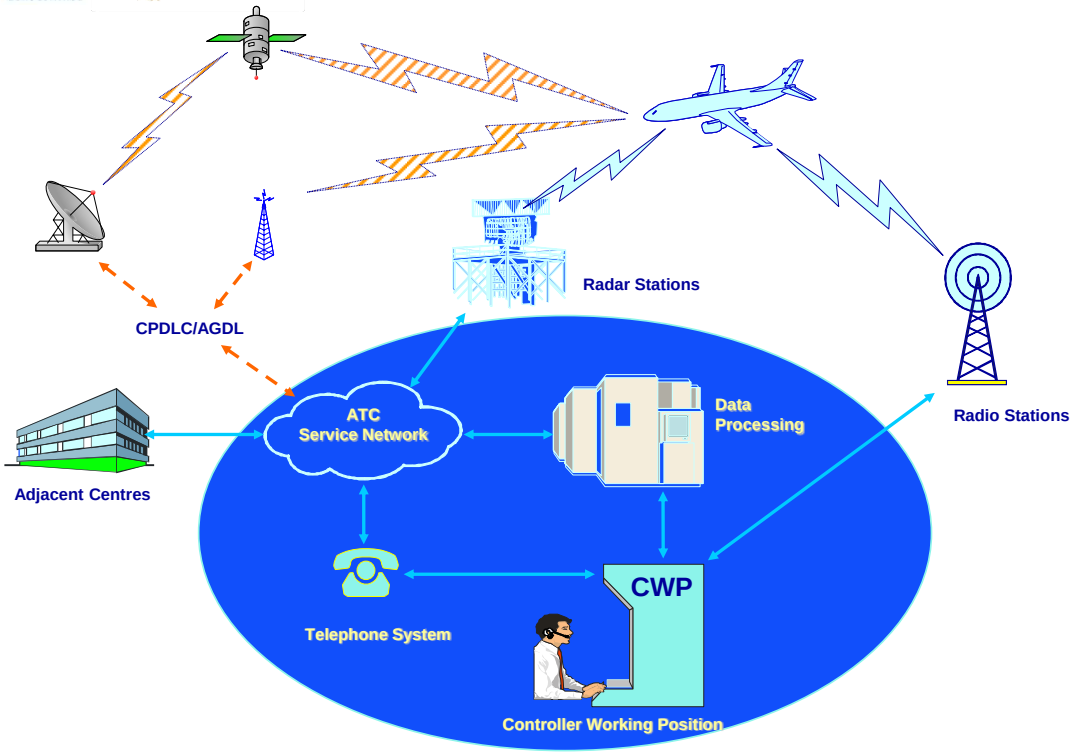
THE MAASTRICHT UPPER AREA CONTROL CENTRE

AREA OF RESPONSIBILITY

FUNCTIONAL AIRSPACE BLOCK EUROPE CENTRAL



AIR TRAFFIC CONTROL SYSTEM



40 years of uninterupted service

- **Redundancy of systems (50-100% performance)**
- Contingency Flight Level Allocation (max 50%)
- Internal Contingency (max 80% performance)
- External Contingency (10-40%)

CRITICALITY OF AIR TRAFFIC CONTROL

- IMPACT ON ECONOMY
- FINANCIAL IMPACT TO THE AIRLINES AND ASSOCIATED SECTOR – 1 min delay/aircraft = €82
  100 min system trouble at MUAC = €500.000
- IMPACT ON PUBLIC

EXAMPLE: CLOSING OF THE AIRSPACE DUE TO VOLCANIC ASH CAUSED BY THE ERUPTION OF *EYJAFJALLAJÖKULL*

MANAGING RISK

- SAFETY MANAGEMENT SYSTEM
- SECURITY MANAGEMENT SYSTEM
- QUALITY MANAGEMENT SYSTEM

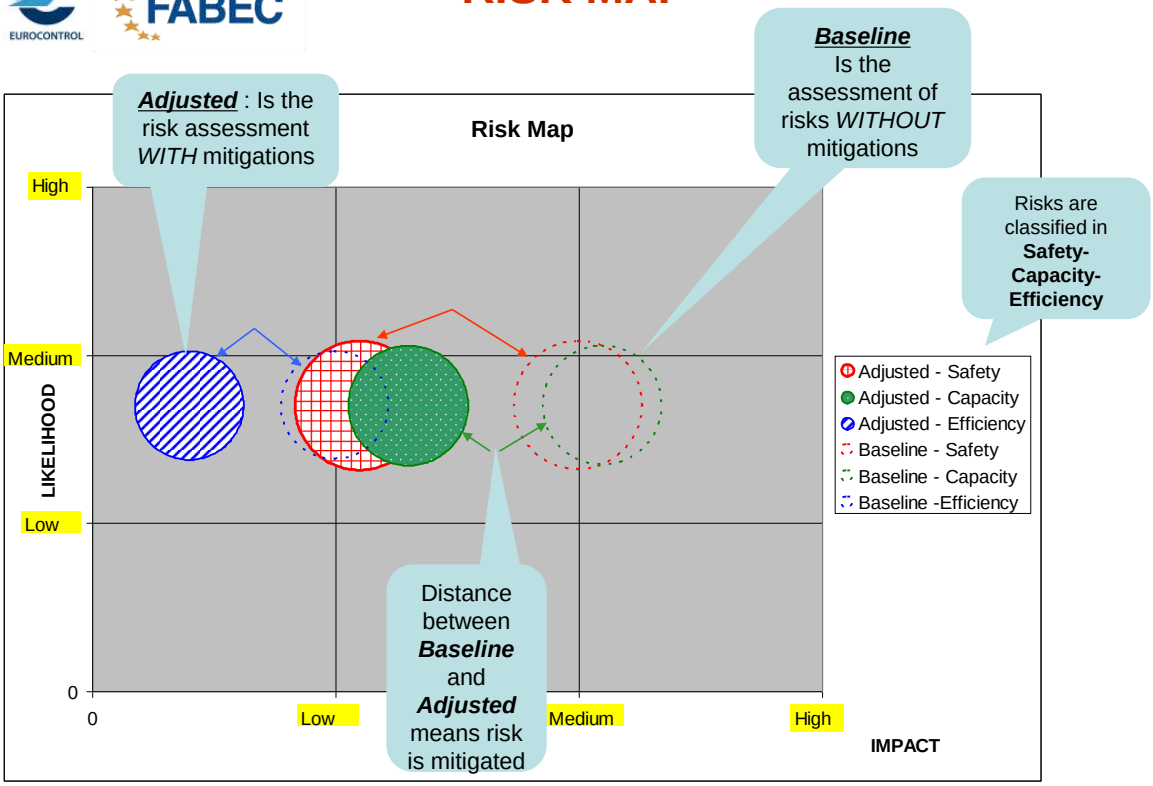
MAIN RISKS

- MID-AIR COLLISION
- SECURITY BREACH
- NATURAL CATSTROPHE
- TECHNICAL OUTAGE
- FIRE IN THE OPERATIONS FACILITY
- INDUSTRIAL DISRUPTION

PERSPECTIVES OF RISKS

- BUSINESS RISKS
- PROCESS RISKS
- SAFETY RISKS
- PROJECT RISKS

RISK MAP



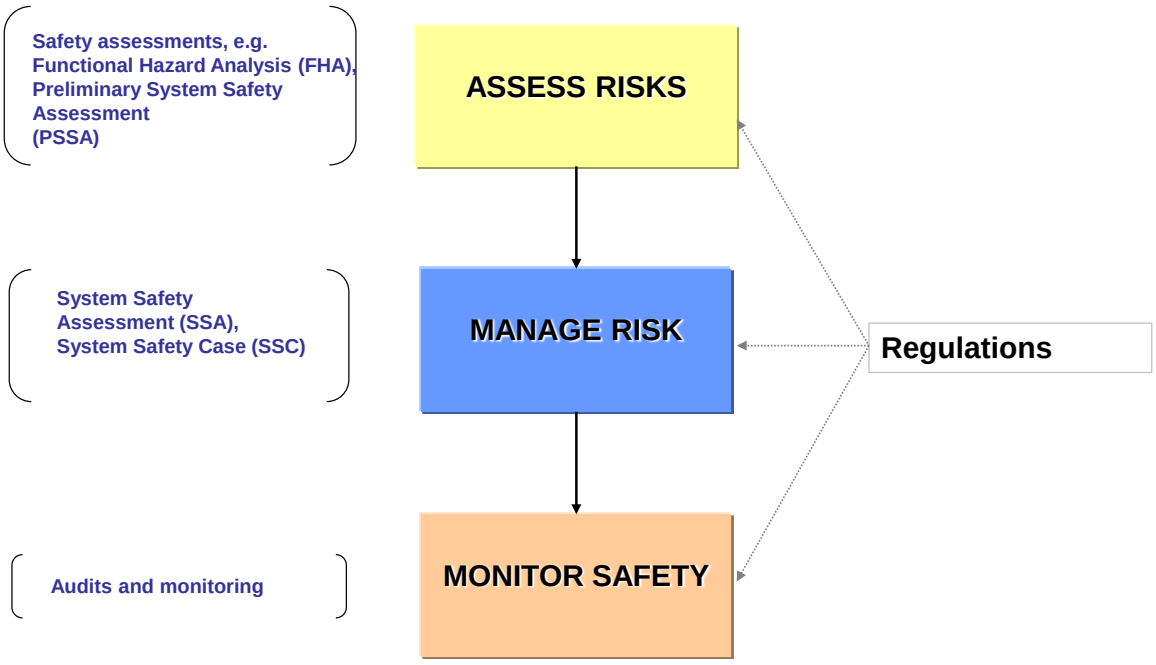
PROCESS RISK

- RISK ANALYSIS

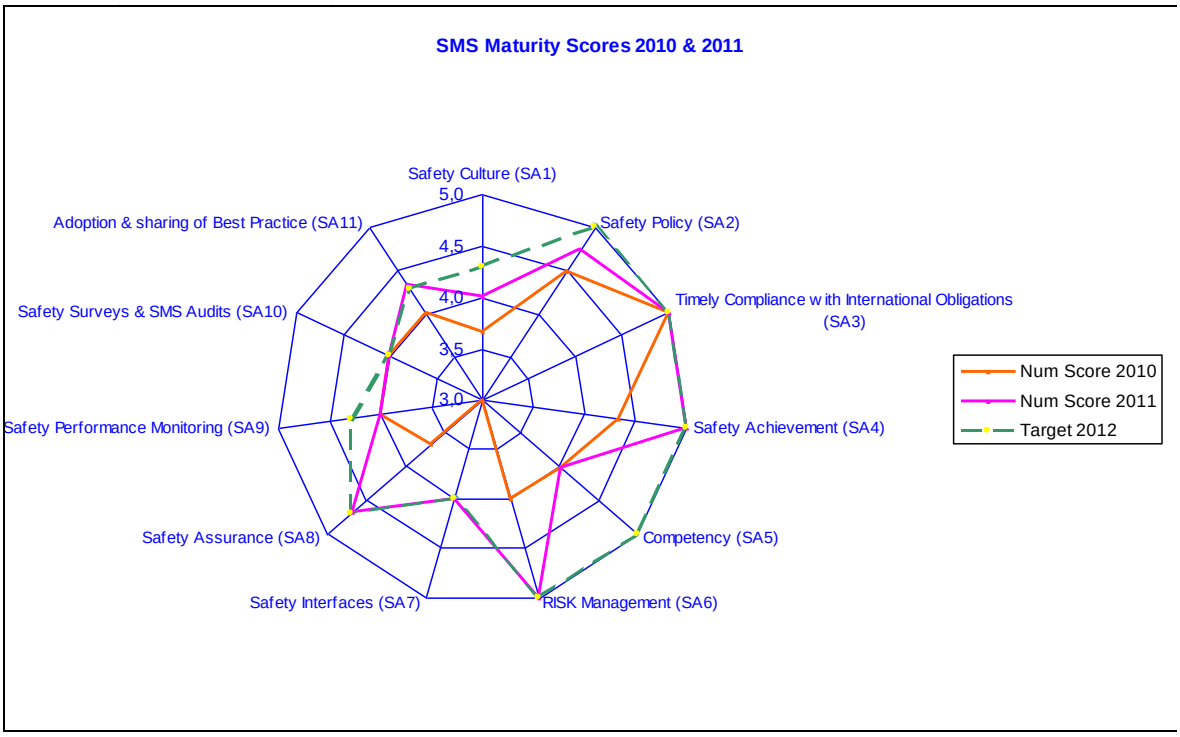
Risk	Identifier	Full name	Process	Risk Impact Description	Risk Control	Risk Categorisation	RISK ASSESSMENT BASELINE Safety	Capacity	Efficiency	Likelihood	ADJUSTED Safety	Capacity	Efficiency	Likelihood

What are the main risks? → What is the impact? → How is the risk controlled? → How severe is the risk? → Has the risk reduced? → What has changed

SAFETY MANAGEMENT SYSTEM



SAFETY MANAGEMENT SYSTEM MATURITY



Understanding Complexity and Interdependency: A prerequisite to increase resilience

Prof. Dr. Wolfgang Kröger
ETH Risk Centre, Zurich, Switzerland

Summary

The presentation from Prof. Kröger encompasses many aspects of system analysis for large infrastructures and networks, and especially Power Grids. The complexity is clearly related to the interconnections, and resulting emergent behaviours. The focus is therefore in the identification of all possible interconnections, which are source of interdependencies (physical, functional, geographic, etc.) among systems. The study proposes a "divide and conquer" approach in which system heterogeneity is dealt applying the principles of HLA (High Level Architecture) framework. The approach represents an effective engineering modular approach to the modeling and analysis of resilience.

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Understanding Complexity and Interdependency: A Prerequisite to Increase Resilience

Prof. Dr. Wolfgang Kröger
Head, former Laboratory of Safety Analysis (LSA)
Executive Director, Risk Center

Dedicated Session on Resilience and Risk Assessment for Critical Infrastructures,
JRC Ispra, 25–26 April 2012

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Characteristics of large-scale technical systems

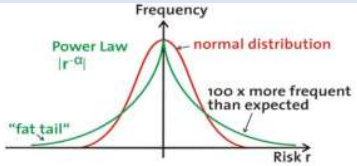
- A geospatially distributed network of physical-engineered systems that function synergistically to produce a continuous flow of essential goods and services
- They are subject to rapid technological and organizational changes and/or evolutionary developments; they face multiple threats (technical-human, natural, physical, cyber, contextual), may pose risks themselves
- Most “critical infrastructure” has become more tightly integrated as well as more interdependent; communication and control increasingly using real-time data (SCADA) and moving to open, commercialized structures
- Disruptions may cascade, accelerate (recall „blackouts“) and render to off-equilibrium conditions, hard to predict and tackle
- Large-scale systems in other sectors (financial, social, political) have similar characteristics and show similar (emergent) behaviors

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

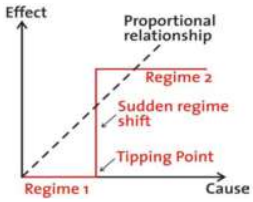
Complexity: Required paradigm shift in risk analysis/ evaluation

Examples: Power Grids, Railway Systems, Financial Markets, Large Supply Chains, etc.

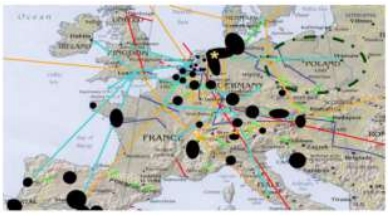
1. Large number of interacting (mutually coupled) system elements.



2. Element interactions are usually non-linear.



Causes & effects are not proportional to each other



Network interactions/interdependencies inducing cascading effects

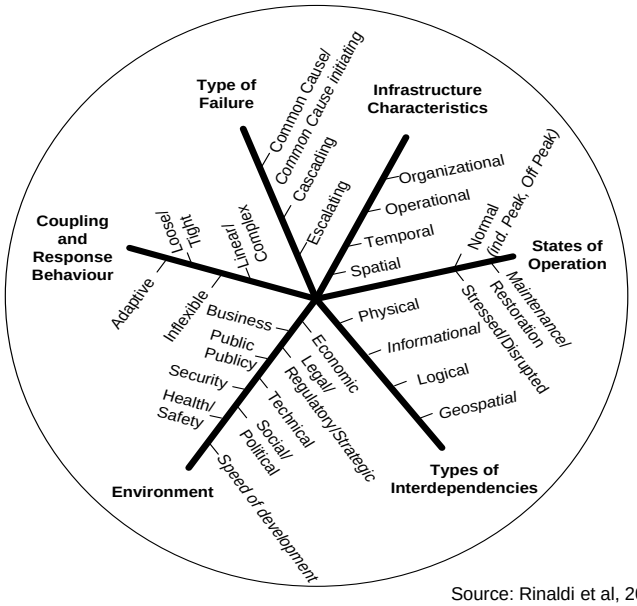
3. Dynamic rather than static & probabilistic rather than deterministic behavior.

Source: D. Helbing, 2010

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Addressing interdependency as key element of complexity

Note: Dependency defines an unidirectional relationship between infrastructures, while interdependency defines a bidirectional relationship



Source: Rinaldi et al, 2001, modifications Kröger in *italic*

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Classification of negative impacts arising from interdependencies

- **Common cause initiating events**: One event causing failure or loss of service of more than one infrastructure such as areal external events (earthquakes, extreme weather conditions, etc.), due to spatial proximity
- **Cascade initiating events:** Failure of one infrastructure causing failure or loss of service of at least another one, e.g., rupture of water mains
- **Cascade resulting events:** Failure or loss of service resulting from an event in another infrastructure, e.g., failure of gas lines due to loss of main power supply if compressors are electrically driven
- **Escalating events:** Failure or loss of service of one infrastructure escalating because of failure of another affected infrastructure, e.g., failure of the power system leading to failure of SCADA and by this affecting restoration of the power system

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Interdependency Studies

- **Goal:** To search for an approach capable to get deepened insights into cascading system behaviors as a result of interdependencies and to identify hidden vulnerabilities, inter alia in order to increase resilience
- In general, the interdependency study approaches can be divided into :
  - **Knowledge-based**: use of data collected or “mined” and/or analyzing past events to acquire information and improve the understanding of the dimensions including types of interdependencies
  - **Model-based**: intent to model/simulate interdependencies with advanced techniques, e.g., probabilistic dynamic modeling, complex network theory, agent-based modeling

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Application of model-based approach: CNT

Heuristic investigation of potential attacks

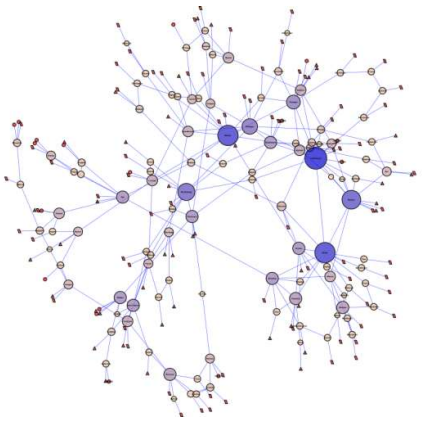
Important elements of the **Swiss transmission grid** are identified by **centrality analysis** for simulated

a) deterministic attacks, targeted on vital substations

b) stochastic attacks on lines (randomly removed)

Results based on response analysis:

- No highly unstable conditions emerged from the attack on the most critical substations (hubs)
- Although the **load flow model** is quasi-dynamic, the effect of cascading failures was very small
- Overloading of transmission lines in only a few scenarios shows good safety margins for the grid



Representation of the Swiss grid by 242 nodes for substations, loads, or power generating stations and 310 links for transmission lines. Node size is analog to node degree centrality.

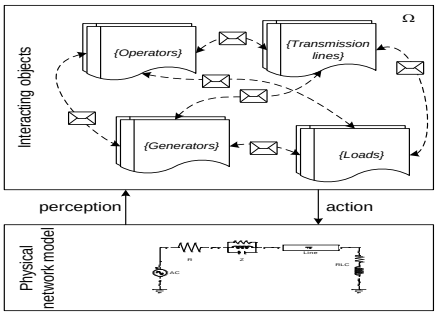
Source: E. Bilis, ETH-LSA, 2010

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Application of model-based approach: ABM

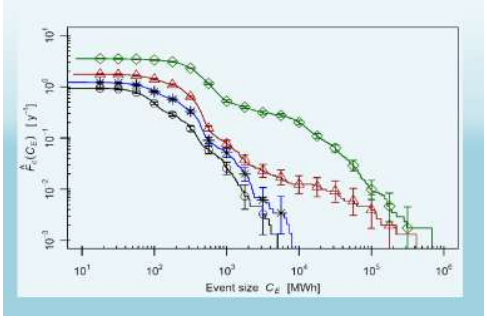
Model electric power grid

- A time-stepped model developed based on a two-layer ABM approach
- Simulates electrical power system scenarios in a continuous time by means of conventional techniques such as power flow calculations
- 587 agents are used to model technical components such as generators, lines and non-technical components such as grid operators



Results

- Cumulative blackout frequency; distribution law depending on initial grid loads levels

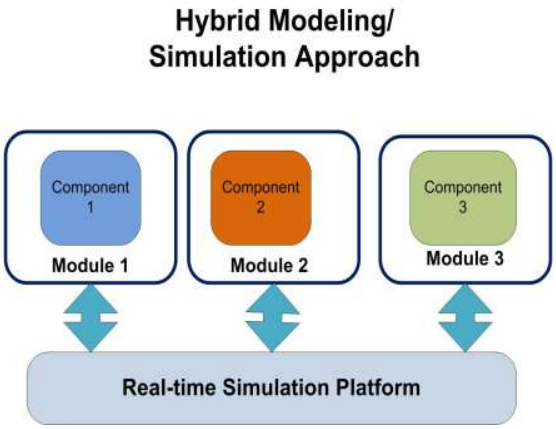


Blackout frequencies for different grid load levels (100% (circles), 110% (stars), 120% (triangles) and 137% (diamonds))

Source: Schläpfer, ETH-LSA, 2008

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Taking-up the challenge to go beyond single infrastructure system: Proposing a hybrid modeling/simulation approach



To fully utilize benefits of each approach, it is necessary to integrate different types of modeling approaches into one simulation platform

One of the key challenges is the required ability to create multiple-domain models and effectively exchange data among these models

The traditional simulation approach is generally challenged by two difficulties:

Lack of Performance

Lack of Simulation Interoperability

One possible solution is to adopt the distributed simulation approach using the modular design concept

Source: Kröger W, Zio E, Vulnerable Systems, Springer, 2011

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

…. Overview

- This “distributed simulation approach” can be considered as a successor of traditional simulation approach in case multiple systems need to be considered
- Instead of building a "heavy weight" simulation component, a number of "light weight" components are developed interacting with each other over the real-time simulation platform

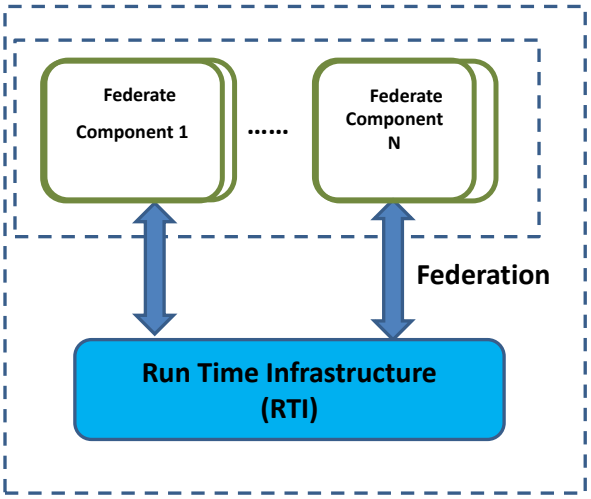
Limitations

- Not all simulation tasks can be solved using this approach, whether or not distributing multiple simulation components will affect the final output of the overall simulation is a main concern and key limitation
- Developing such a distributed simulation environment is time-consuming and labor-intensive

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Proposing a hybrid modeling/simulation approach: HLA

- A simulation standard is required to implement the hybrid approach
- High Level Architecture (**HLA**) is an open simulation standard (IEEE1516) that facilitates the interoperability of multiple-type models (simulators), supporting the distributed simulation
- Each single system model referred to as **Federate,** collection of federates referred to as **Federation**
- **Run Time Infrastructure (RTI)** is the middleware layer for information exchange



HLA-compliant simulation environment

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

…. HLA (cont.)

Drawbacks

- Significant increases of resources and time during implementation

  Resources including time required to implement an HLA-compliant simulation platform could be significantly higher compared to a non-HLA-compliant platform

- Update latency

  The interval between sending an update by one federate and receiving this update by another federate could be long enough to affect the outcomes of real-time simulation

- Not a "plug-and-play" standard

  All HLA-related (object and interaction) classes must be declared before the simulation

- Incompatibility between HLA standards

Despite these drawbacks, HLA is still a most applicable and feasible standard for the implementation of the proposed hybrid modeling/simulation approach

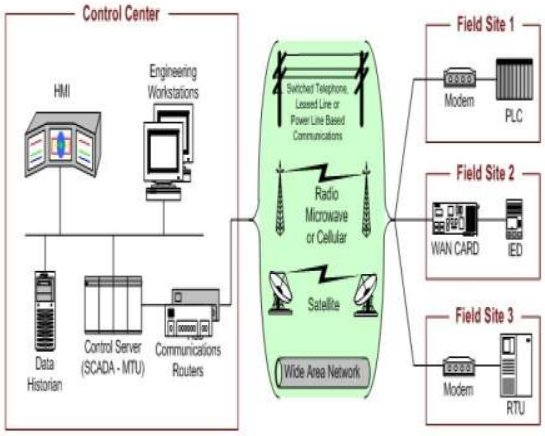
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Application of the hybrid approach

…to investigate interdependency-related vulnerabilities between SCADA and SUC (using Swiss power transmission network as reference)

- SCADA (Supervisory Control and Data Acquisition) is an example of Industrial Control System, widely used to to control industrial systems and processes such as power supply
- Current SCADA systems are often/increasingly linked to higher level business/trading systems
- Generally, SCADA was built for non-networked environment, lacking security features

General layout of a SCADA system



Source: Stouffer. K et al. Guide to Industrial Control Systems Security, 2008

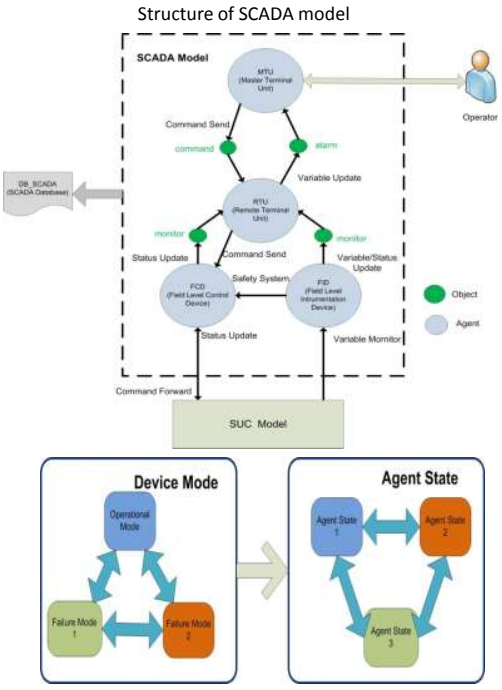
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Application of the hybrid approach: Modeling SCADA

Failure-oriented ABM approach

- SCADA model combines ABM with other modeling techniques, e.g., MC, Finite State Machine, Markov model, Fuzzy Logic, HRA.
- As an HLA-compliant model, it includes 583 agents and thousands of objects
- Each agent is developed based on failure-oriented modeling approach
- “Agent state" is defined as a location of control and “device mode” as status of corresponding simulated hardware devices (allowing modeling beyond functionalities)
- Continuous-time and discrete-state Markov models are used to describe the failure behavior of studied devices

Structure of SCADA model

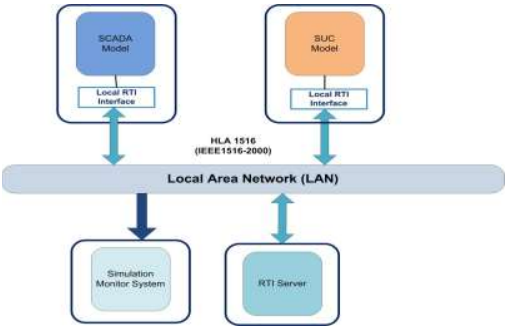


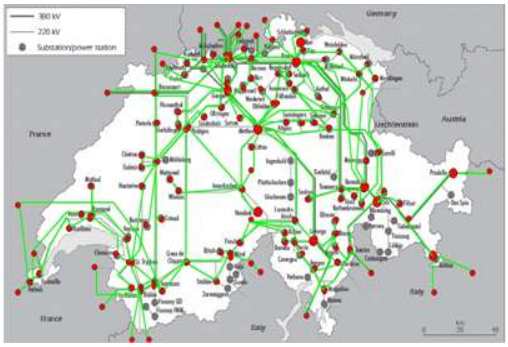
Source: Nan et al. Exploring Critical Infrastructure Interdependency by Hybrid Simulation Approach, 2011.

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Application of the hybrid approach: A simulation test-bed

- The experimental simulation test-bed consists of four major components: SUC and SCADA model, RTI server, and simulation monitor system, all connected over LAN
- SUC model, originally a stand-alone model, has been converted to become HLA-compliant
- RTI server acts as the centre of the test-bed, responsible for simulation synchronization and communication routing among all components
- Simulation monitor system is used to observe current simulation environment
- Experiments including a feasibility and single failure propagation experiment have been performed to demonstrate the capability and applicability of the approach





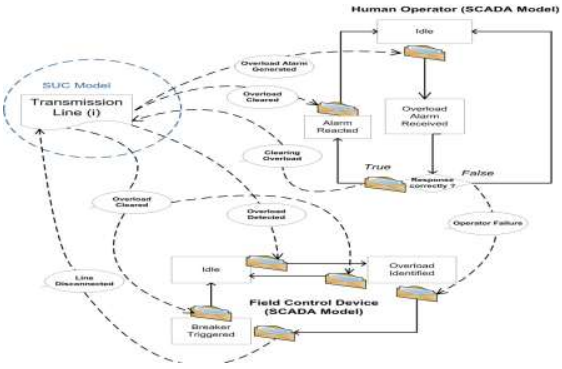
Screen shot of simulation monitor system

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Application of the hybrid approach: Failure propagation experiment

Goal

- Investigate the capability of the hybrid modelling/simulation approach for representing interdependencies
- Scenarios are developed in both models in order to trigger and handle power line overload alarm during the simulation



Results

- Propagation of failures crossing interlinked systems (SCADA/SUC) can be observed during the simulation
- Based on collected results of this experiment, three types of interdependencies can be simulated: physical, cyber and geospatial

Stamped Time (S)	Events
52.43	Line(i)'s FID calibration has been modified, offset is + 9.67 (FID)
140	Line(i) is overloaded and a warning has been generated (FID)
156.09	RTU has generated an alarm and sent it to MTU (RTU)
174.85	Operator recognizes the alarm (MTU)
183.24	Operator reacts correctly and distributing algorithm will be taken (MTU)
212.31	Command has been processed by operator successfully, redistribution command sent out (MTU)
223.05	Power flow of line(i) decreases (SUC model)

FID: Field Instrumentation Device

RTU: Remote Terminal Unit

MTU: Master Terminal Unit

Source: Eusgeld et al. "System-of-systems" Approach for Interdependent Critical Infrastructures, 2011

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

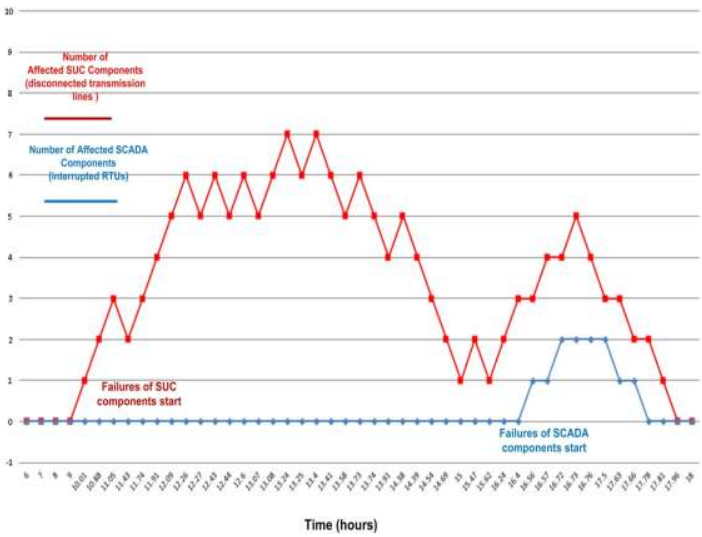
Application of the hybrid approach: "In-depth" experiments

Goal

- Investigate interdependency-related vulnerabilities between SCADA and SUC within electricity power supply system by performing "in-depth" experiments on the simulation test-bed

Key Results

- Importance of field level devices should not be underestimated in modeling efforts
- Propagation of failures crossing interlinked systems is not instantly but takes a certain period of time (hours), which is very important for minimizing negative effects caused by interdependencies.



The number of affected SUC and SCADA components recorded in one of "in-depth" experiments

Source: Nan, ETH-LSA, 2012

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

…an interim conclusion

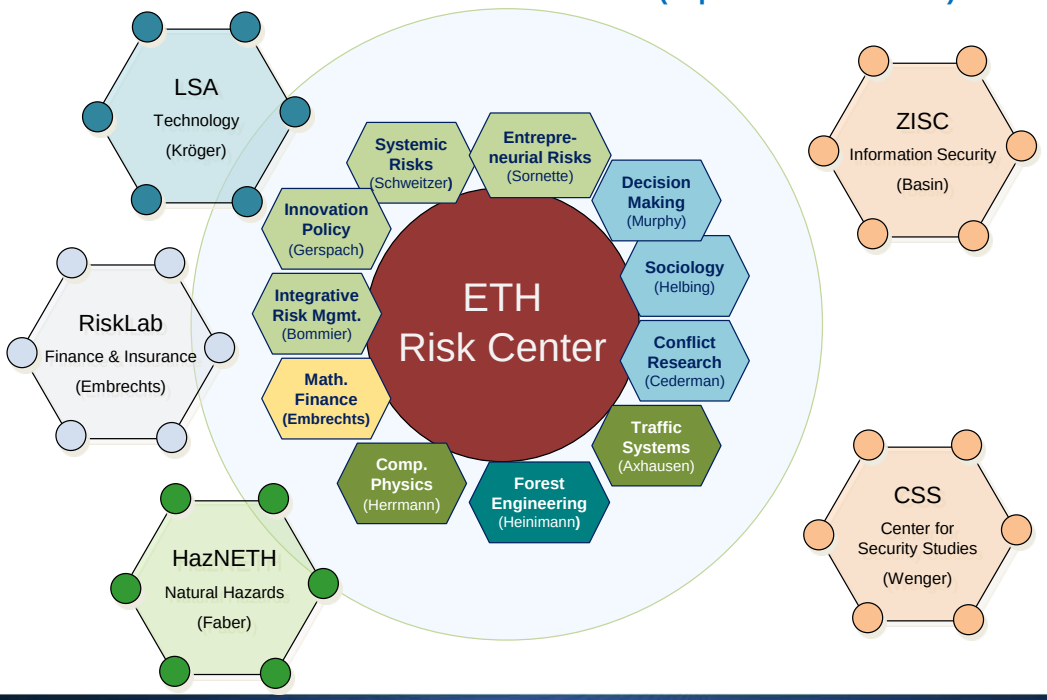
- Although progress has been made in modelling and simulating interdependencies within (and among) infrastructure systems, more efforts are needed to further improve the methods/tools and to scale them up to the level of "system-of-systems" and the systemic nature of risks

- Systems theory and related methods assume steady state or near-equilibrium processes and has difficulties explaining phenomena like emergence and adaptation which are typical for complex (interdependent) systems

- To support the design of resilient systems it is necessary to fully understand off-equilibrium conditions and to develop a solid interdisciplinary mindset

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Risk Center aims to develop a multidisciplinary mindset and collaborative research: Network of available resources (departments coloured)



ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

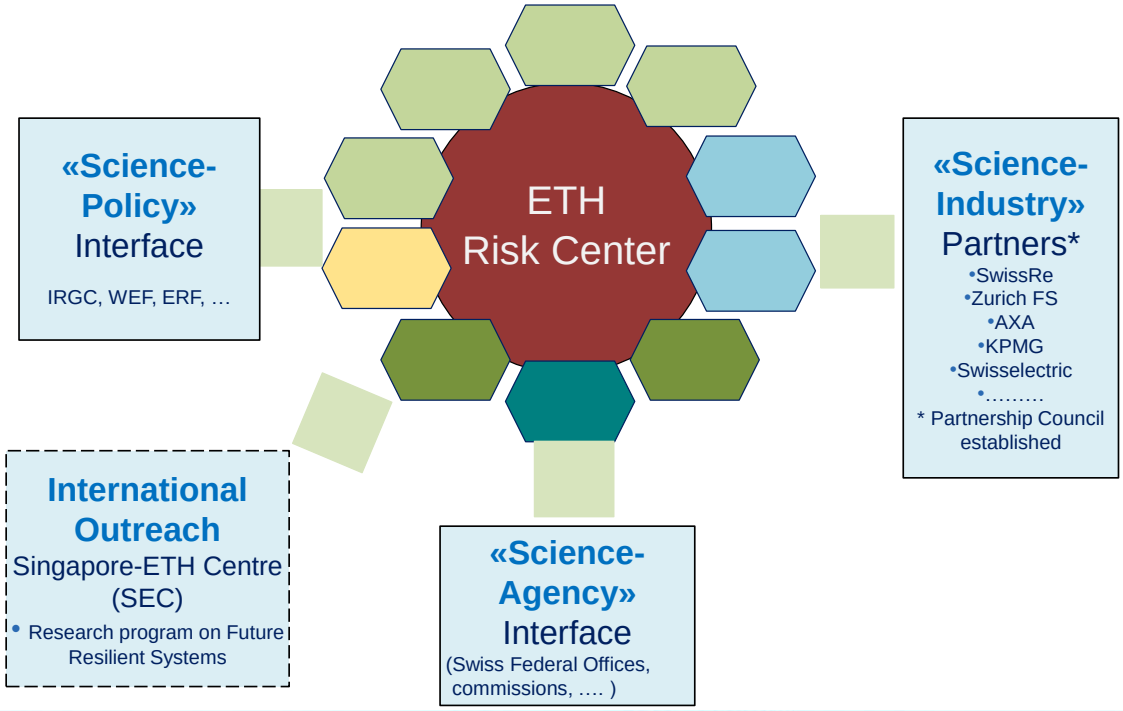
Guiding idea of the first joined research proposal - with 3 work packages and 8 core projects submitted to ETH (KPMG) for funding

Building on cross-disciplinary experience and cross-breeding it with expertise in traditional risk domains, such as finance, natural hazards, decision-making and physically-engineered systems, three research challenges are taken up:

- Link modern probabilistic and statistical methods with complexity science to improve our understanding of systemic risk phenomena, such as sudden regime shifts, cascading effects, or slow emerging risks [WP 1]
- Improve our understanding of the emergence and the spread of financial crisis and explore most robust institutional arrangements…[WP 2]
- Explore interdependencies between macro-systems, particularly resource extraction, energy production, and political stability, to improve our understanding of cross-system links [WP 3]

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Development Options of ETH Risk Center (established 6/2011)



ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Concluding remarks

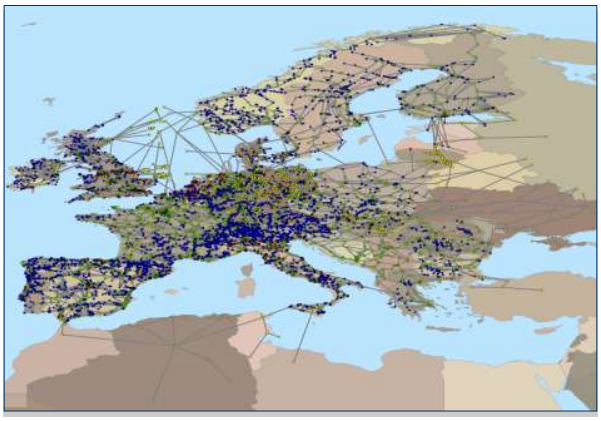
- There is still no single “silver bullet” approach to handle complexity and interdependency
- Boost research & development in the addressed areas
- Intensify efforts to develop a truly interdisciplinary mindset and “system-of-systems thinking”
- Provide a platform for dialogue among key actors (science, industry, users, authorities)

Modelling and Simulation in CIP

Dr Rüdiger Klein
Fraunhofer Institute for Intelligent Analysis and Information Systems (IAIS), Germany

Summary

The presentation of Dr. Klein focuses on interdependencies and dynamics, with application to Smart Cities. An important element of these are Smart Grids. The abstraction to cyber-layer throughout infrastructures is here addressed with a focus on control relationships of type sensor-model-actuators. The modelling scope is the system response to attacks, in which physical quantities are analysed. In the presentation there is also a shopping list of what is needed at modelling level in order to simulate the behavior of modern critical infrastructures.



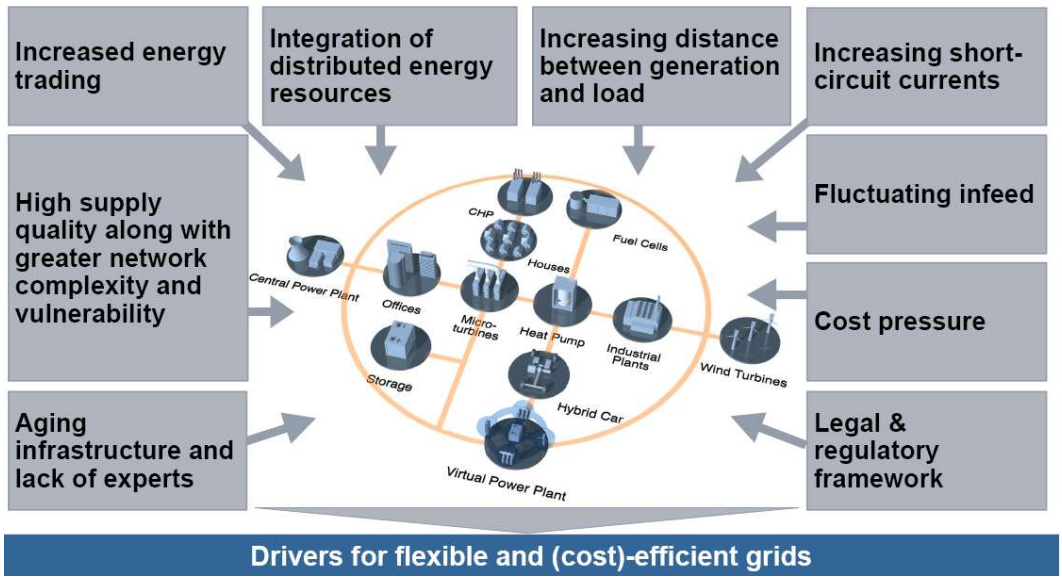
Modelling and Simulation for Critical Infrastructure Protection

Dr. Rüdiger Klein

Fraunhofer IAIS

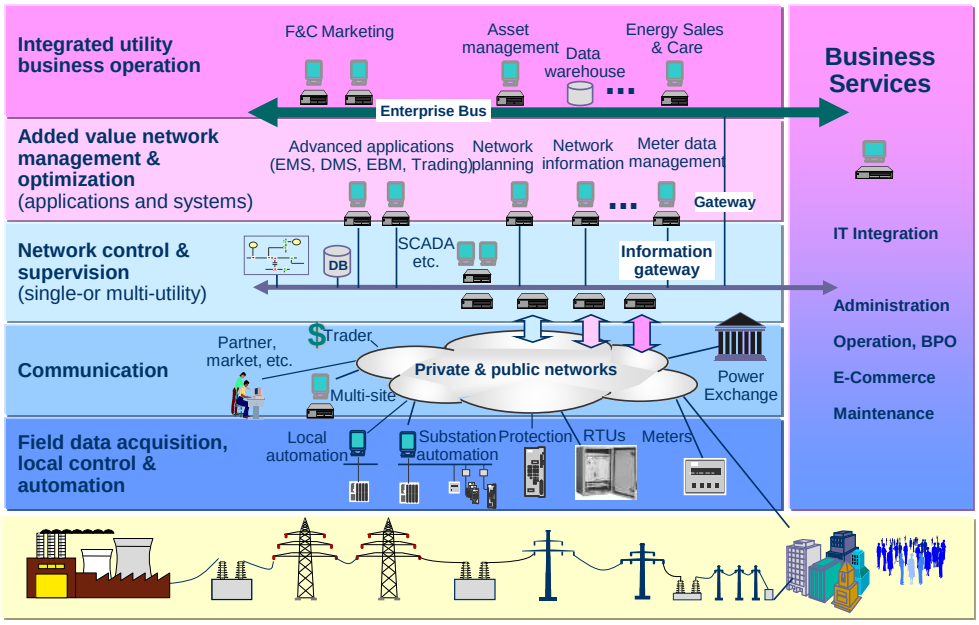
JRC EU Workshop
Ispra, 26.4.2012

Requirements to Future Power Grids



© Siemens AG (IRRIIS)

Vertical and Horizontal Interoperability in Control Centres

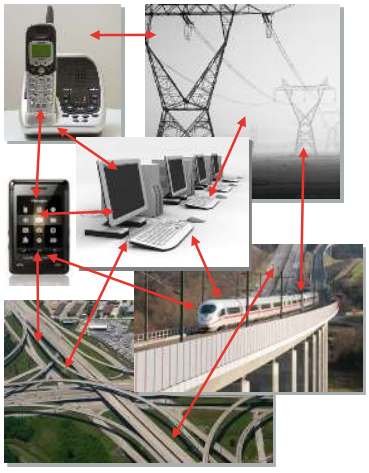


Fraunhofer IAIS

© Siemens AG (IRRIIS)

Motivation:
Critical Infrastructure Protection (CIP)

- CI are increasingly **complex** and **heterogeneous**
- and **interlinked** due to economical, political, technological and social reasons
- They **depend** on each other
- Networks of CIs
- up to “Smart Cities”, “Smart Planets”…
- **Multiple threats**: natural disasters, technical failures, human error, cyber and other attacks
- **ICT** is of central importance everywhere
- New opportunities: control, communication
- New challenges:
  - cyber security
  - Understanding dependencies and dynamics



© Fraunhofer Institut für intelligente Analyse- und Informationssysteme IAIS

Fraunhofer IAIS

Emergency Management in CI

Fraunhofer IAIS

We need new Information Technologies to manage this complexity

- **Understanding** dependencies and dynamcis needs modelling and simulation
- for CI **operation**: online/real time decision support
- There is **no** „one fits all“ solution. We need a large variety of IT solutions and their interoperability

© Fraunhofer Institut für intelligente Analyse- und Informationssysteme IAIS

IT Mega Trends

- Big data: the amount of data available is growing rapidly
- Web of data
- Ubiquituous computing: data are produced and processed „everywhere“
- Mobile commmunication
- Data cloud
- Internet of Things
- Social networks

© Fraunhofer Institut für intelligente
Analyse- und Informationssysteme IAIS

Cyber-Physical Systems

- Cyber-Physical Systems are systems which exist and act in the „real world“
- with dynamic behaviour following the rules of physics and technology

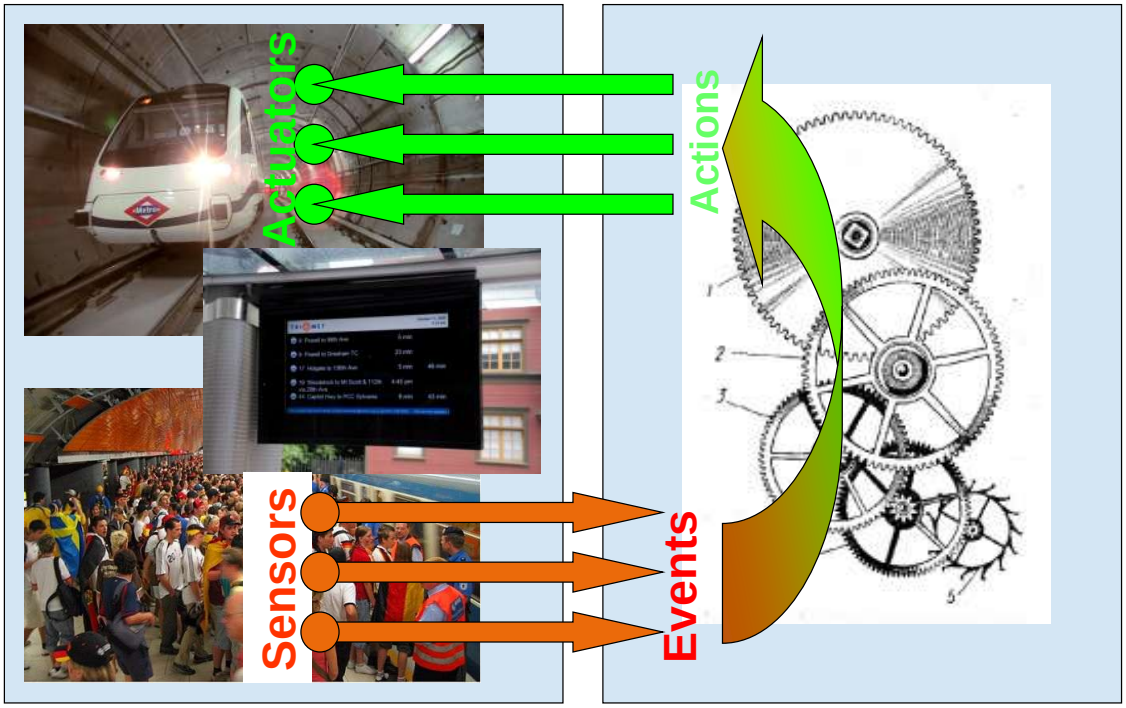
AND

- which are controlled by a computer or computer system
- following certain policy rules under normal, exceptional, and emergency conditions
- where the control system has to communicate with the physical system (ist sensors and ist actuators)

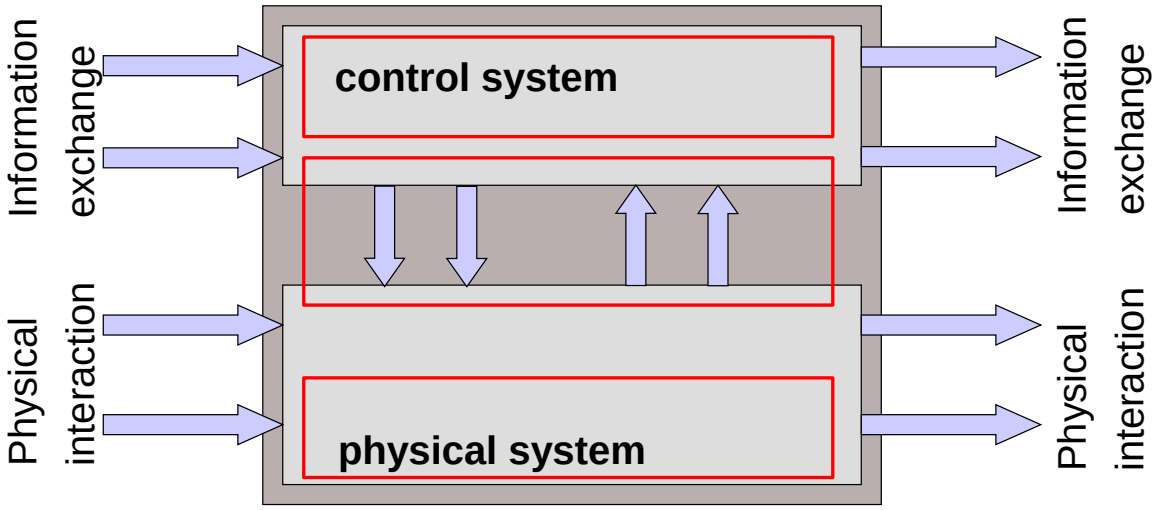
Critical Infrastructures are Cyber-Physical Systems

© Fraunhofer Institut für intelligente
Analyse- und Informationssysteme IAIS

2. Physical System and Control in CPS



2. Control of CPS



© Fraunhofer Institut für intelligente Analyse- und Informationssysteme IAIS

Why New Information Technologies?

1) Data, Semantics, and Information Exchange

- Critical Infrastructures are complex systems. Their models comprise a large variety of different kinds of data which depend on each other (structures, functional dependencies, geospatial/topological, physical, temporal aspects, …)
- CI depend on each other in many ways
- They have to work together: appropriate exchange of data
- These data are different across domains – but also within domains
- Their meaning is frequently not clear for others
- It is (too much) focused on what is needed within the own CI – not for others

We need semantic data and semantic interoperability

© Fraunhofer Institut für intelligente Analyse- und Informationssysteme IAIS

Why New Information Technologies?

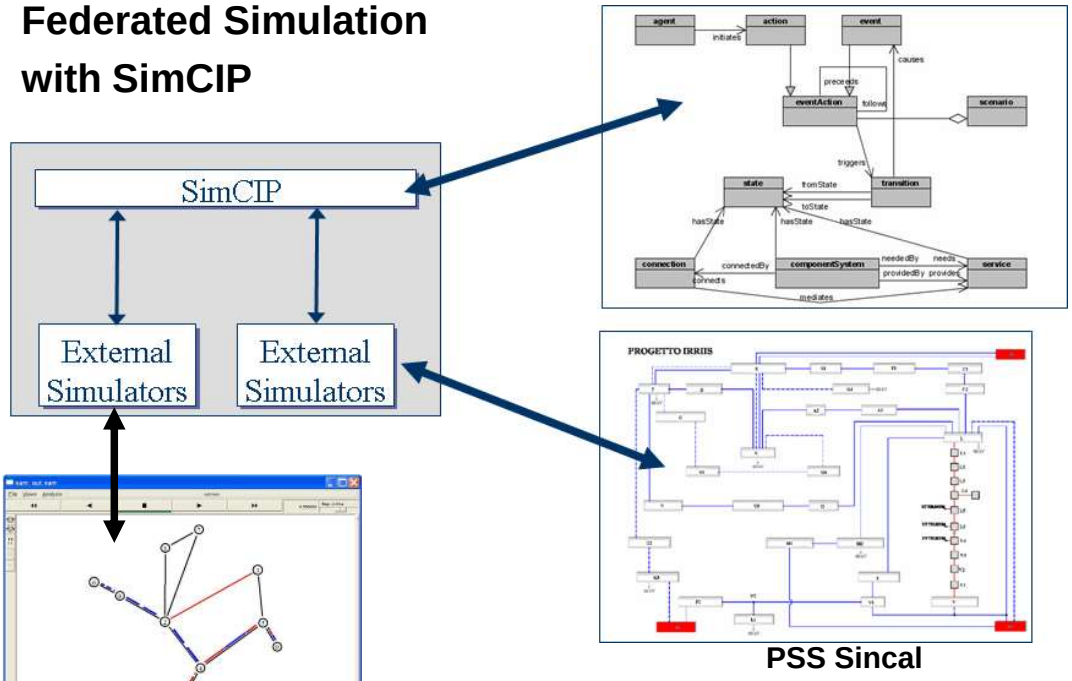
2) Simulations

- CI are too complex to be managed „by hand“ and understandable intuitively
- We need appropriate simulations which capture the typical behaviour of CI
- Due to the complex behaviour of CIs and their interdependencies

we need integrated or federated simulations of different kinds

© Fraunhofer Institut für intelligente Analyse- und Informationssysteme IAIS

Federated Simulation with SimCIP



PSS Sincal

Telco Simulator

NS-2

© Fraunhofer Institut für intelligente Analyse- und Informationssysteme IAIS
Fraunhofer IAIS

Why New Information Technologies?

3) Simulations as Services

- Can a single CI operator get a reasonable risk estimation and resiliance analysis ?
- Where do the external data come from?
- How to integrate them and use federated simulations?

Risk estimation and resiliance analysis for interdependent Critical Infrastructures needs new collaborative approaches between providers and institutions.

Simulations as Services can support this.

© Fraunhofer Institut für intelligente Analyse- und Informationssysteme IAIS
Fraunhofer IAIS

Why New Information Technologies?

4) The Dynamic Web

- The Internet with its data structures and protocolls is the central information infrastructure.
- It‘s currently mainly based on static information (HTML, XML, HTTP, …). All dynamic aspects have to be treated „by hand“ (programming).
- Critical Infrastructures are dynamic processes: Smart Grids, Internet of Things etc. need appropriate treatment of dynamics and changes.

We need a Dynamic Web with Complex Event Processing and Reactions.

Temporal aspects are very important in CIP! In real-time and in off-line simulations…

© Fraunhofer Institut für intelligente Analyse- und Informationssysteme IAIS

Why New Information Technologies?

5) Methodology

- Semantic Data Models, Dynamic Web, and federated simulations: a very complex approach

- How can we guarantee that these „components“ work together appropriately and that we run the right simulations in the right way?

We need a methodology which allows us to systematically create scenarios and evaluate them effectively!

© Fraunhofer Institut für intelligente Analyse- und Informationssysteme IAIS

Why New Information Technologies?

6) New Standards

- Semantic Data Models
- Dynamic Web
- Federated Simulations

We need new standards for semantic data formats, dynamic distributed data processing and federated simulations!

© Fraunhofer Institut für intelligente Analyse- und Informationssysteme IAIS

Why New Information Technologies?

7) User Interactions

- Complex semantic data models
- With dynamics: event processing and reactions
- and integrated/federated simulations

have to be managed by risk analysis experts and operators.

We need user interaction capabilities which allow experts to manage this complexity!

Visual Analytics

3D and 4D data visualisation

© Fraunhofer Institut für intelligente Analyse- und Informationssysteme IAIS

Summary

- Critical Infrastructures are getting more complex, more dependend, and more related to ICT
- The evolving paradigm of cyber-physical systems provides an attractive framework for understanding and controling CIs
- We need complex models and simulation for on-line decision support and off-line analysis and optimisation
- These models and simulations need new ICT
  - Semantic models
  - Dynamic technologies
  - Federated simulations
  - Advanced user interfaces and Visual Analytics
  - A comprehensive methodology for systematic scenario evaluation
  - New standards for data and interoperability

© Fraunhofer Institut für intelligente Analyse- und Informationssysteme IAIS

New Information Technologies – Embedded into an Interdisciplinary Holistic Approach

- Information Technologies are central for Critical Infrastructures:
  - for their normal operation
  - for understanding them: their behaviours, vulnerabilities, risks, resiliance, etc.
- Modelling and simulation are needed to manage this complexity

- Embedded into a holistic, interdisciplinary approach
- including human behaviours, social communication, decision making, etc.

© Fraunhofer Institut für intelligente Analyse- und Informationssysteme IAIS

THANK YOU FOR YOUR ATTENTION!!

© Fraunhofer Institut für intelligente
Analyse- und Informationssysteme IAIS

Safety of complex energy systems

Prof. Enrico Zio
Chaire SSDE-Foundation Europeenne pour l'Energie Nouvelle, EDF
Ecole Centrale Paris and Supelec, France
Department of Energy Politecnico di Milano, Italy

Summary

The presentation of Prof.Zio introduced the state of the art of system analysis methodologies (from reliability and risk assessment community) that are applicable to networked infrastructures. Both topological and dynamic view of a complex system was presented, together with tools and metrics. The topological analysis provides information on critical and vulnerable nodes. Though it is only by simulation that system properties, such as resilience, can be assessed. The approach is epidemiological, in the sense that a failure propagates through the network and triggers other events (either failure or recovery/defence actions) Sudden phase changes in the state space, like the ones that occur in non linear system, resulted form the analysis thus confirming the complexity of the emerging behaviour. Finally a global framework for the optimization of system parameters in order to make the network reliable and resilient is proposed.

Safety of Complex (Energy) Systems

Enrico Zio
Chaire SSDE-Foundation Europeenne pour l'Energie Nouvelle, EDF
Ecole Centrale Paris and Supelec
Department of Energy, Politecnico di Milano

Safety of Complex (Energy) Systems

COMPLEX (ENERGY) SYSTEMS:

physical attributes
{structure, dependencies and interdependencies, dynamics, …}

operation and management attributes
{communication, control, human and organizational factors, logistics…}

performance and safety attributes
{reliability, availability, maintainability, risk, vulnerability, …}

economic attributes
{life-cycle costs, costs-benefits, market drivers…}

social attributes
{supply-demand, active players, …}

environmental attributes
{pollution, sustainability, …}

COMPLEX (ENERGY) SYSTEMS:

logic representation and mathematical modeling

{From FT/ETs, Markov Diagrams to BDDs, BDMPs, Petri Nets, BBNs, Hybrid and Soft Models, …}

model quantification and simulation

{From analytical to Monte Carlo simulation, from physics-based to metamodeling by artificial intelligence, from system dynamics to agent-based modelling,…}

uncertainty modeling & quantification

{From Probability to Imprecise Probabilities, Possibility Theory, Evidence Theory, Fuzzy Interval Analysis, …}

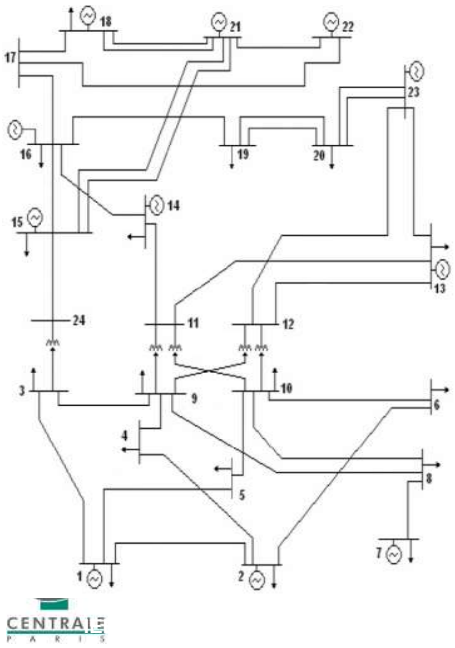
element importance and sensitivity analysis

{From Local-Differential to Global-Variance Decomposition, Polynomial Chaos Expansion…}

Safety
(Reliability, Vulnerability, …)

Safety of Complex (Energy) Systems

- Complex energy systems: connectivity structure + power flow + failure/recovery behavior

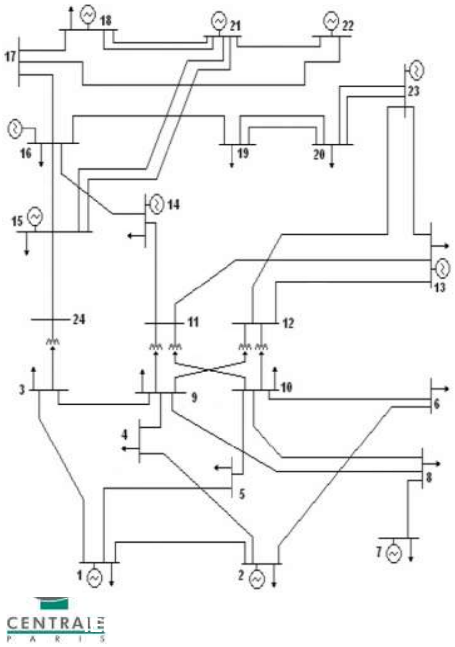


Robustness to failure?
Vulnerability to attacks?

Simulation | Reliability/Risk Analysis | Topological Analysis

Safety of Complex (Energy) Systems

- Complex energy systems: **connectivity structure** + power flow + failure/recovery behavior



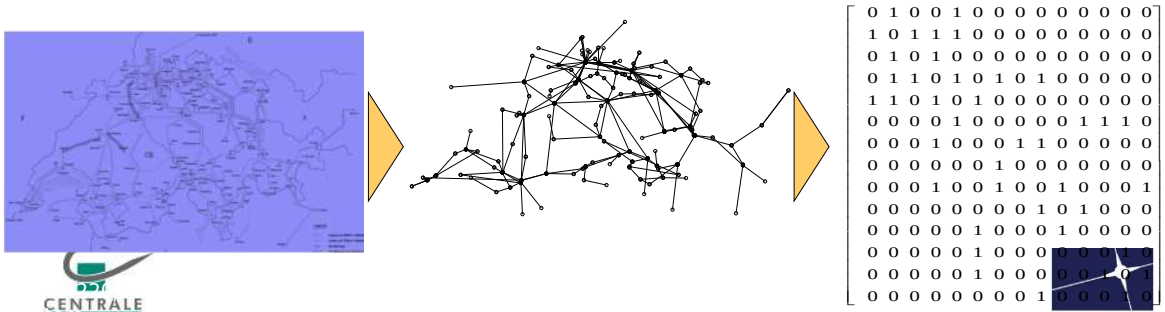
Robustness to failure?
Vulnerability to attacks?

Simulation | Reliability/Risk Analysis | **Topological Analysis**

Directed, connected graph $G=(N, K)$

Adjacency matrix $[a_{ij}]$: $a_{ij}=1$ if node i and node j are directly connected, 0 otherwise

"Unweighted" or "weighted" topological links



Safety of Complex (Energy) Systems
Topological Analysis (Graph theory)

Global properties

Connection degree per node distribution $P(k)$

Shortest path length distribution $P(d_{ij})$

Average global efficiency $$E_{glob}(G)=\frac{\sum_{i\neq j\in G}\frac{1}{d_{ij}}}{N(N-1)}$$

Local properties

Average local efficiency $$E_{loc}(G)=\frac{1}{N}\sum_{i\in G_i}E(G_i)$$

Element importance (centrality)

Topological betweenness centrality, C^B

$$C_i^B = \frac{1}{(N-1)(N-2)} \sum_{j,k \in G, j \neq k \neq i} \frac{n_{jk}(i)}{n_{jk}}$$

Node i is central if it is traversed by many of the shortest paths connecting pairs of nodes

Topological information centrality, C^I

$$C_i^I = \frac{\Delta E(i)}{E} = \frac{E[G] - E[G'(i)]}{E[G]}$$

Node i is central if the (connectivity) efficiency drops significantly upon its failure

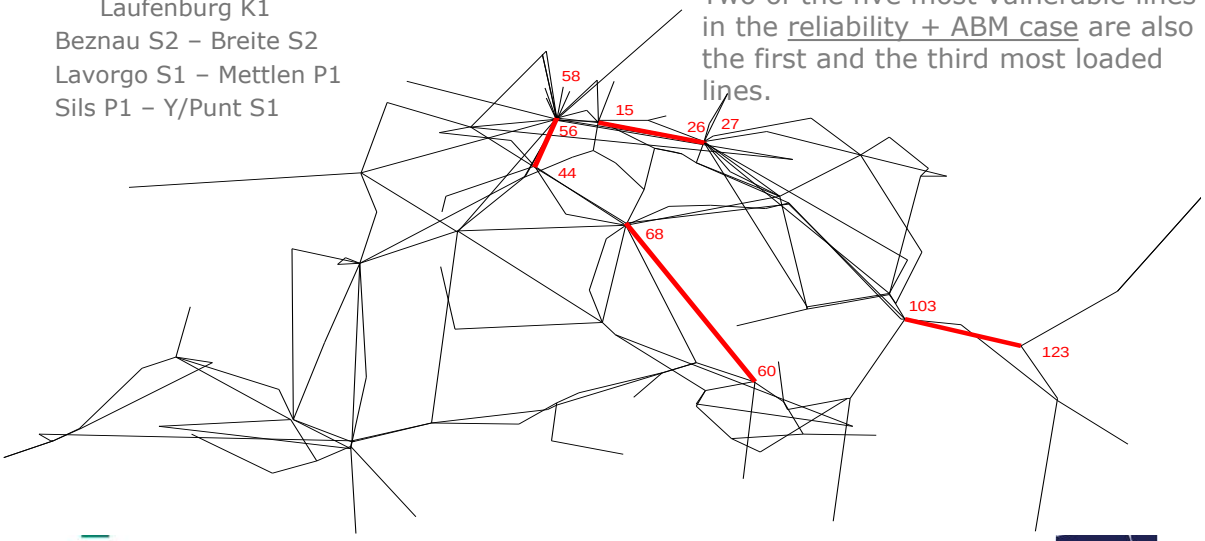
Safety of Complex (Energy) Systems
Topological Analysis

Swiss 220/380 kV transmission system

Goesgen S1 – Laufenburg 01
Laufenburg 01- Laufenburg K1
Beznau S2 – Breite S2
Lavorgo S1 – Mettlen P1
Sils P1 – Y/Punt S1

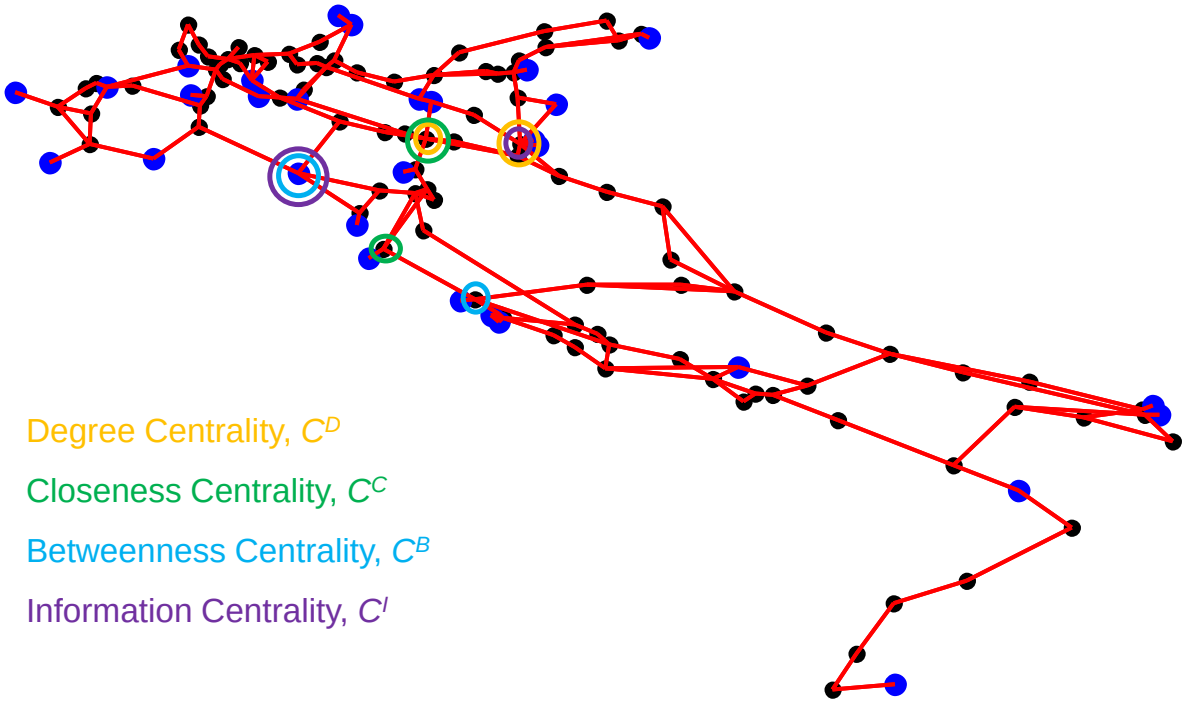
Beznau S2 – Breite S2 connection is among the most vulnerable ones in any case.

Two of the five most vulnerable lines in the reliability + ABM case are also the first and the third most loaded lines.



I. Eusgeld, W. Kroger, G. Sansavini, M. Schlapfer and E. Zio, *"The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures"*, Reliability Engineering and System Safety, vol 94, No. 5, 2009, pp. 954–963

Safety of Complex (Energy) Systems
Topological Analysis



Degree Centrality, C^D

Closeness Centrality, C^C

Betweenness Centrality, C^B

Information Centrality, C^I

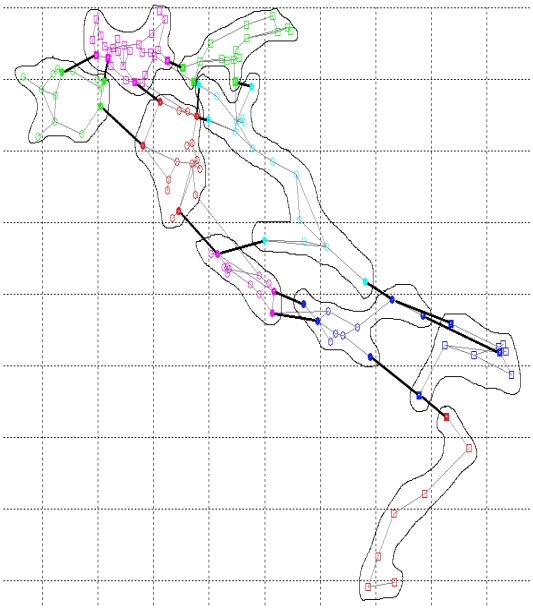
E. Zio & G. Sansavini, Component Criticality in Failure Cascade Processes of Network Systems, Risk Analysis, Volume 31, Issue 8, pages 1196–1210, August 2011

Supélec

Safety of Complex (Energy) Systems
Topological Analysis (Clustering)

Critical components identification by unsupervised spectral clustering

Cascading failure hierarchical modeling by successive clustering.

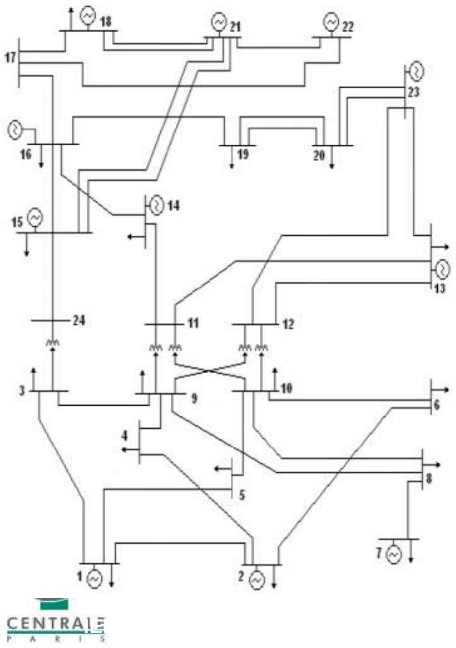


CENTRALE PARIS

Supélec

Safety of Complex (Energy) Systems

- Complex energy systems: connectivity structure + power flow + **failure/recovery behavior**



Robustness to failure?
Vulnerability to attacks?

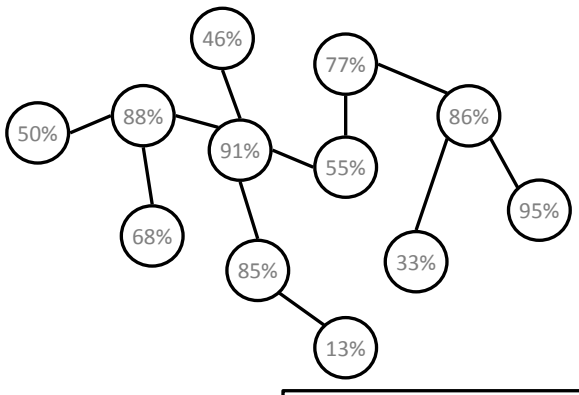
Simulation (Topological)

Reliability/Risk Analysis

Topological Analysis

Safety of Complex (Energy) Systems
Simulation of cascading failures

- Sequence of failures in interconnected systems
- Triggered by an initial event and spreading over the system according to the connectivity pattern (structure) and a **spreading rule** (dynamics)



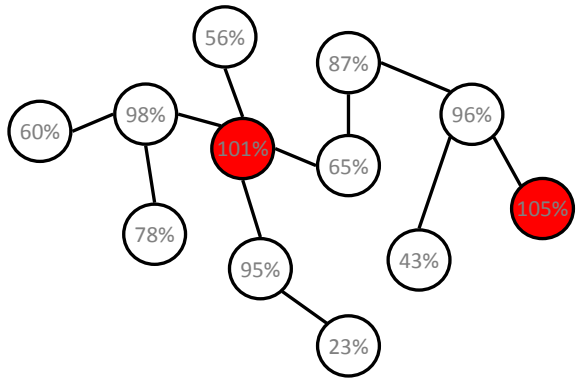
100% = component relative limit capacity
Initiating event: uniform disturbance (10%)

Safety of Complex (Energy) Systems
Simulation of cascading failures

- Sequence of failures in interconnected systems
- Triggered by an initial event and spreading over the system according to the connectivity pattern (structure) and a **spreading rule** (dynamics)

Spreading rule:

fixed load (5%) transferred after a failure to neighboring nodes



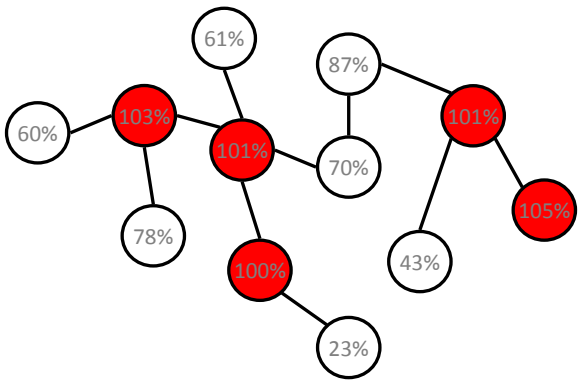
100% = component relative limit capacity
Initiating event: uniform disturbance (10%)

Safety of Complex (Energy) Systems
Simulation of cascading failures

- Sequence of failures in interconnected systems
- Triggered by an initial event and spreading over the system according to the connectivity pattern (structure) and a **spreading rule** (dynamics)

Spreading rule:

fixed load (5%) transferred after a failure to neighboring nodes



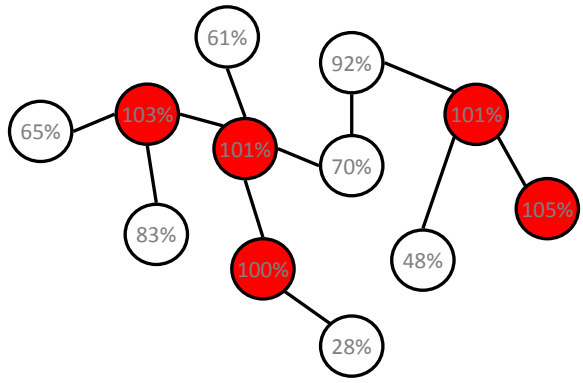
100% = component relative limit capacity
Initiating event: uniform disturbance (10%)

Safety of Complex (Energy) Systems
Simulation of cascading failures

- Sequence of failures in interconnected systems
- Triggered by an initial event and spreading over the system according to the connectivity pattern (structure) and a **spreading rule** (dynamics)

Spreading rule:

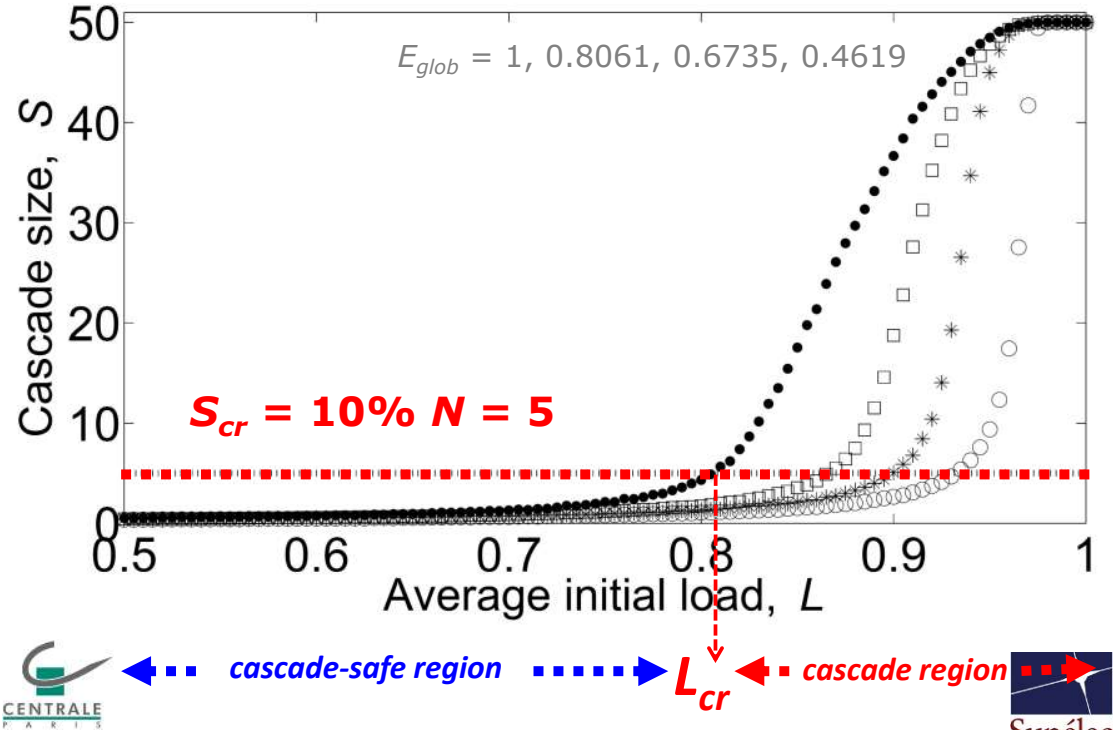
fixed load (5%) transferred after a failure to neighboring nodes



Propagation follows until no more working component can fail

100% = component relative limit capacity
Initiating event: uniform disturbance (10%)

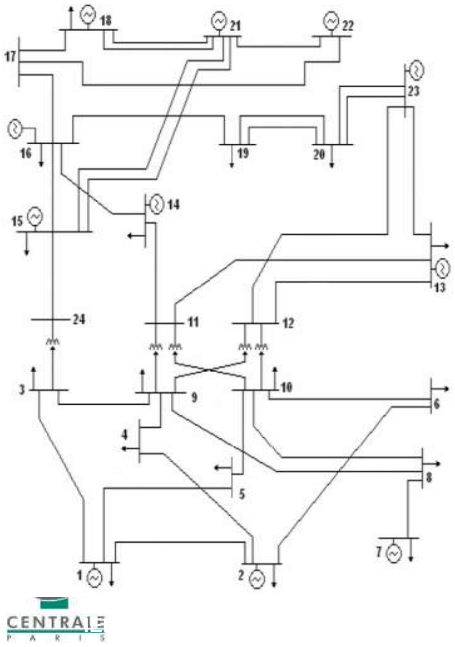
Safety of Complex (Energy) Systems
Simulation of cascading failures



G. Sansavini, M. R. Hajj, I. K. Puri and E. Zio, *"A Deterministic Representation of Cascade Spreading in Complex Networks"*, Europhysics Letters, 87(4), 48004, August 2009

Safety of Complex (Energy) Systems

- Complex energy systems: connectivity structure + **power flow** + failure/recovery behavior



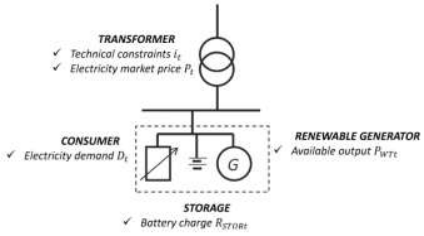
Robustness to failure?
Vulnerability to attacks?

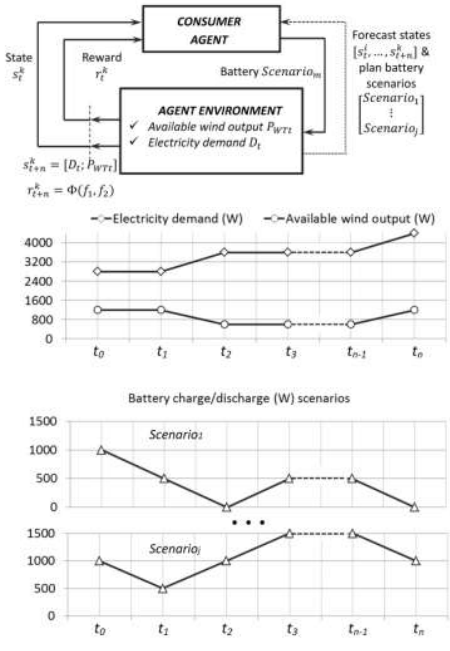
Simulation (Physical)

Reliability/Risk Analysis

Topological Analysis

Safety of Complex (Energy) Systems
Physical Simulation (Agent-based modeling+reinforcement learning)





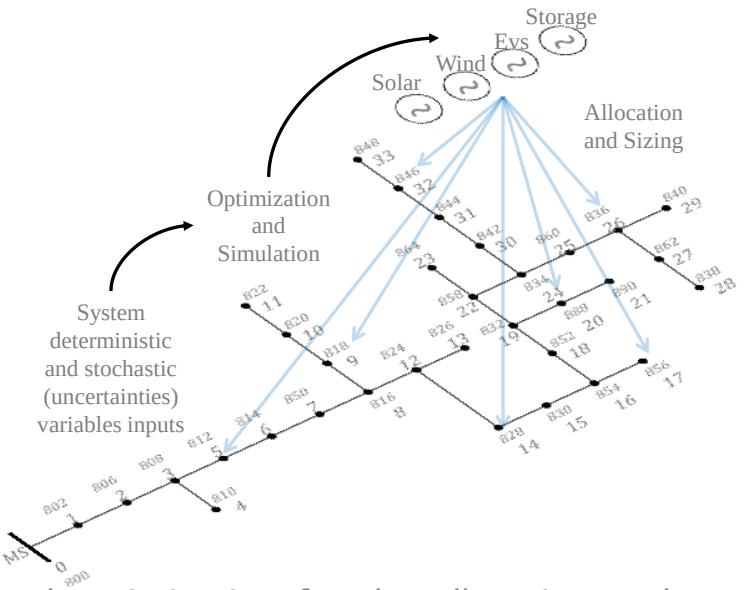
- Modeling framework for energy management in microgrids with locally installed renewable generators and storage facilities.
- Agent-based modeling and simulation of microgrid individual actors, each with explicit goals and interactions with the environment.

  Reinforcement learning → *to exploit the* environment → *decision of optimal scenario* to maximizing reward → multi-objective goals (costs, renewable energy, etc).

Optimization

Safety of Complex (Energy) Systems
Optimization under uncertainty

- Stochastic representation of the components operating/mechanical states and their physical-functional interrelation (Monte Carlo Simulation)
- Two stages stochastic formulation: multi-objective optimization by Genetic Algorithms with nested Power Flow Analysis.

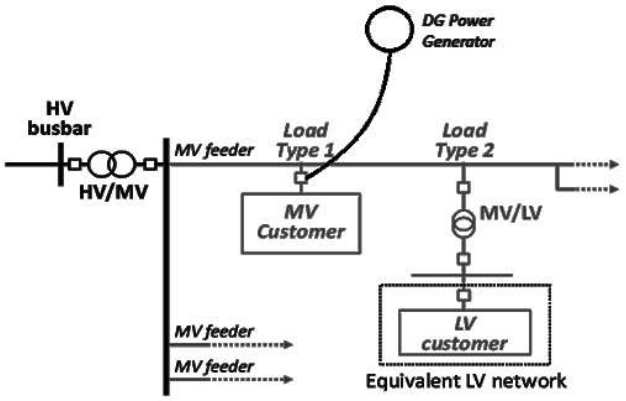


Modeling and optimization for the allocation and planning of distributed generation systems under uncertainties.

Safety of Complex (Energy) Systems
Optimization (DG Penetration Analysis in MV Networks)

Objective – To quantify the maximum DG hosting capacity of MV networks

Find the maximum distributed generation that can be connected to each network bus without violating operating limits



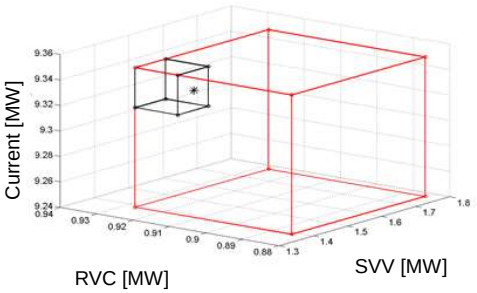
Operating Limits:

- •Rapid Voltage Change ⇨ ± 6%
- •Supply Voltage Variation ⇨ [-4%, 10%] of the nominal voltage
- •Current limits ⇨ 250 A

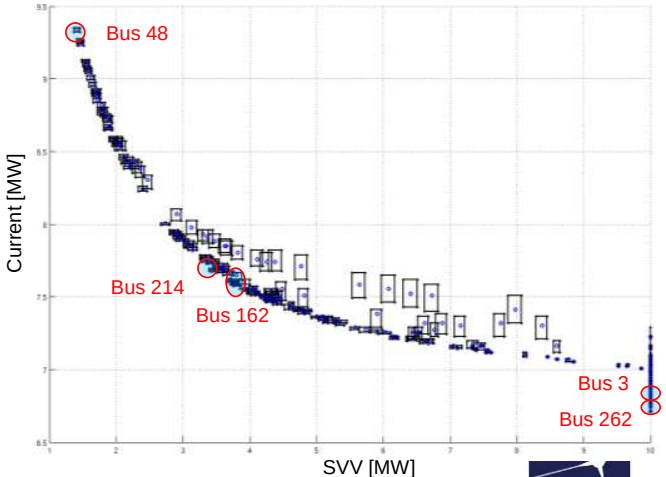
Safety of Complex (Energy) Systems
Physical Simulation (DG Penetration Analysis in MV Networks)

Application: 274-bus Network

Feeder	Bus	Month	TB	Constraint	DLF [MW]	μ PLF	σ PLF
1	3	4	5	Current	6.7734	6.7758	0.0137
2	48	4	5	SVV	1.4141	1.4203	0.0224
3	162	4	5	SVV	3.7891	3.7898	0.0357
4	214	4	5	SVV	3.4258	3.4252	0.0201
5	262	1	2	Current	6.7109	6.7109	0



Cube of bus 48, most limiting time band and all year comparison

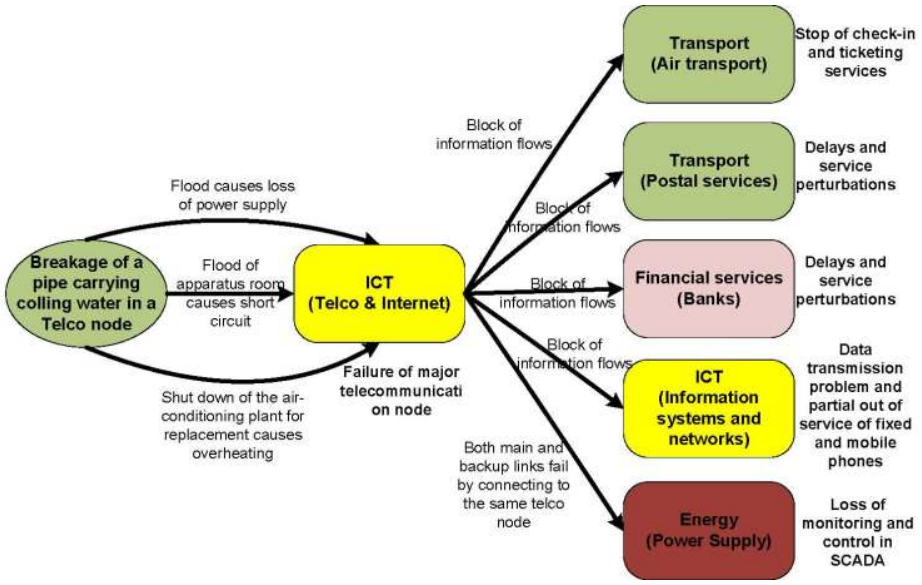


All buses in their most limiting time band

Probabilistic DG Penetration Analysis of Medium Voltage Distribution Networks by Monte Carlo Simulation
M. Delfanti, L. Giorgi, V. Olivieri, G. Sansavini, E. Zio. PMAPS 2012

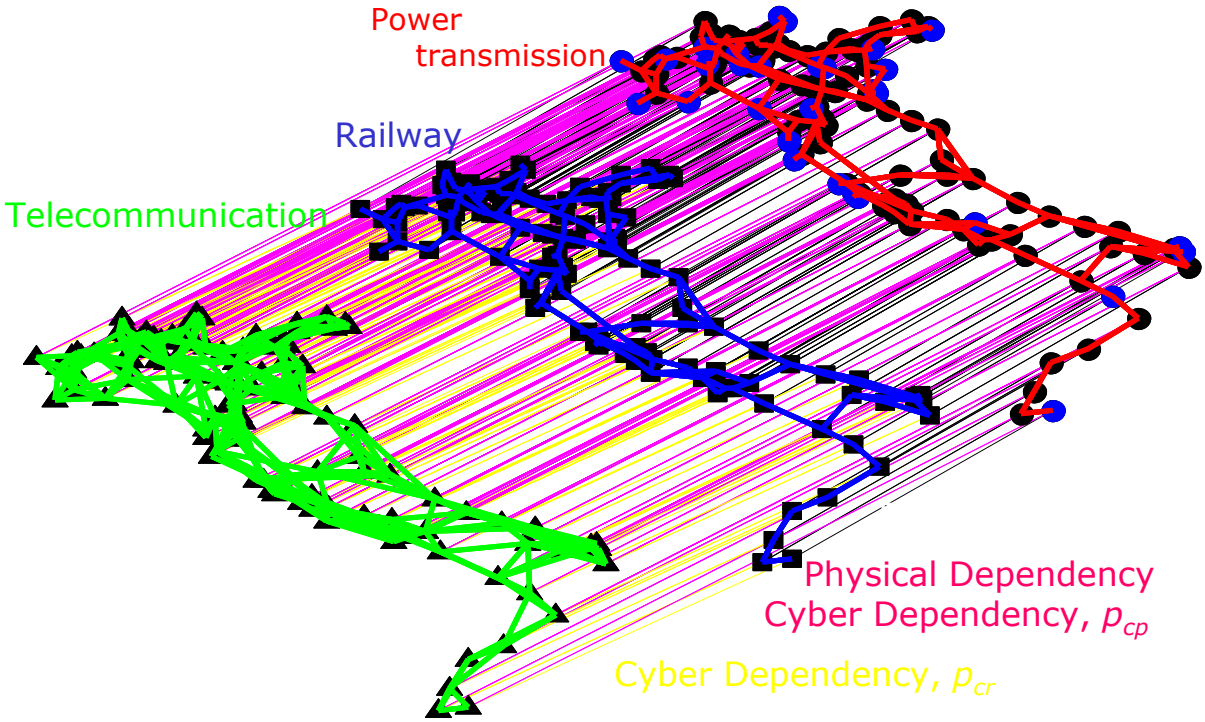
Systems of Systems

System of Systems



Infrastructures affected by the mini telecommunication blackout in Rome, 2004

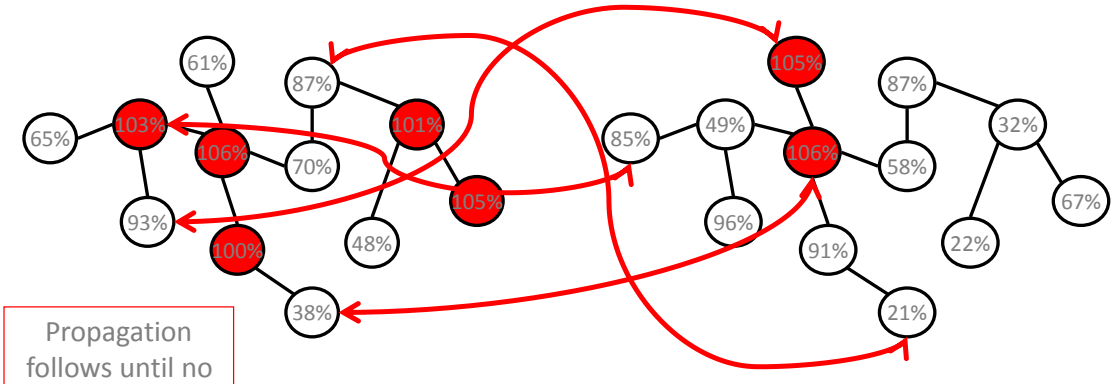
Inter-dependencies



27

Inter-dependencies: systems of systems

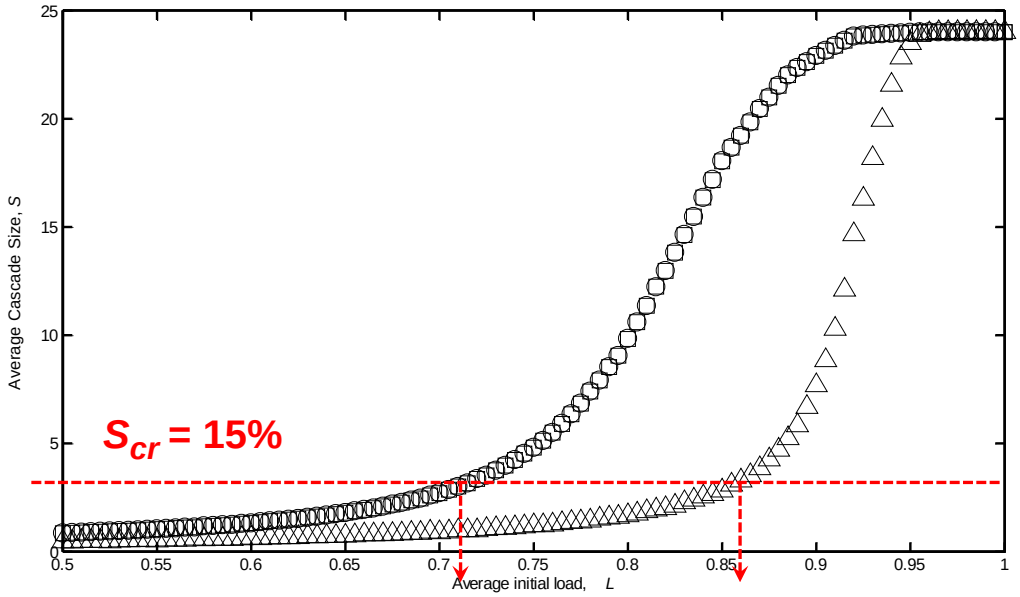
- **Spreading rules:**
  - fixed load (5%) transferred after a failure to neighboring nodes
  - fixed load, *l*, (10%) transferred after a failure to interdependent nodes



Propagation follows until no more working component can fail

100% = component relative limit capacity
Initiating event: uniform disturbance (10%)

Inter-dependencies: systems of systems



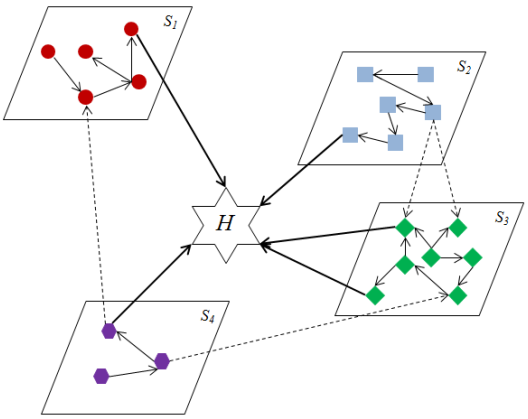
E. Zio and G. Sansavini, "*Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins*", IEEE Transactions on Reliability, 60(1), pp. 94-101, March 2011

Systems of systems: external events risk assessment

Safety of a critical plant, e.g., a nuclear power plant, exposed to risk from external events, e.g., earthquakes.

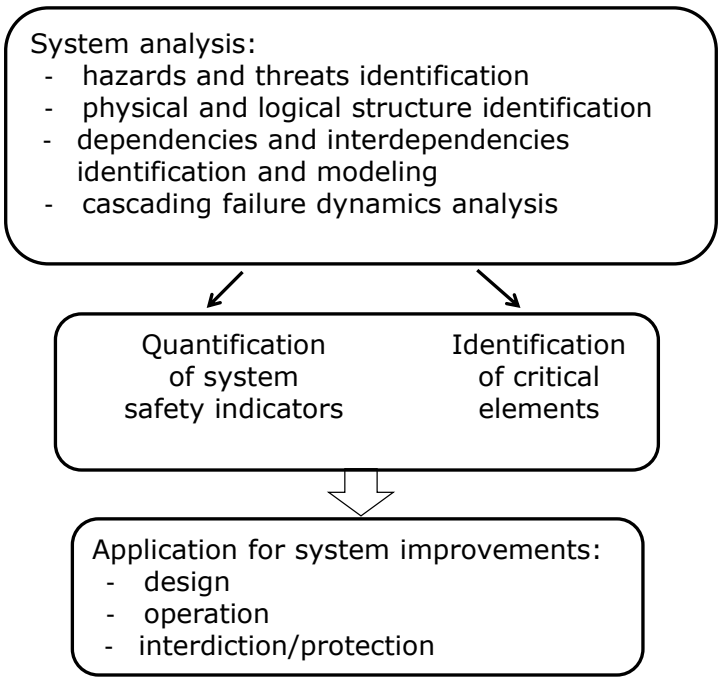
System-of-Systems analysis of the interdependent infrastructures that support the critical plant.

Muir Web and Fault Tree Analysis + Monte Carlo simulation



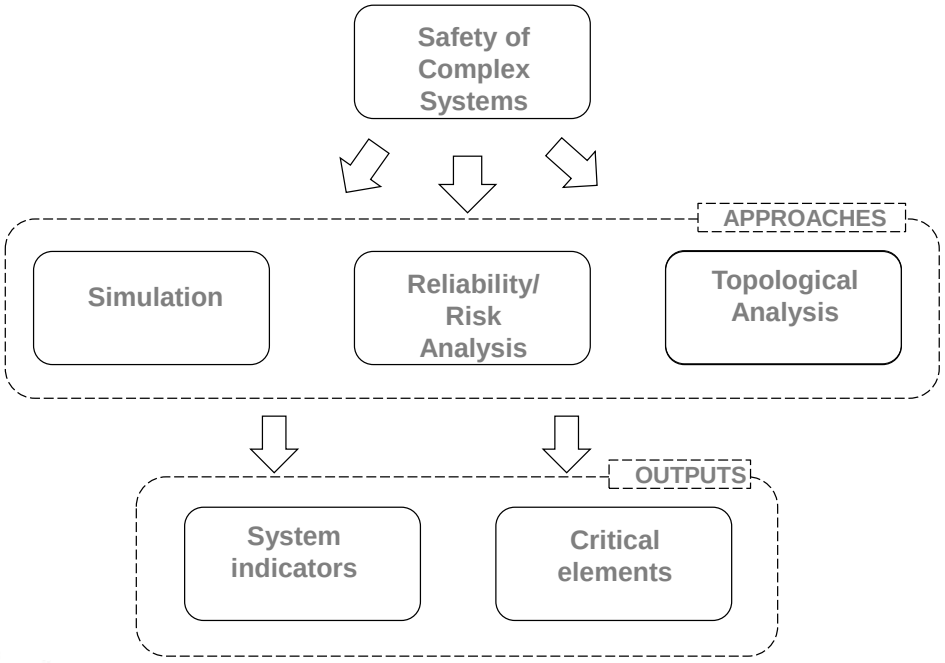
Safety of Complex (Energy) Systems

Safety of Complex (Energy) Systems
Conclusions: The Analysis Scheme

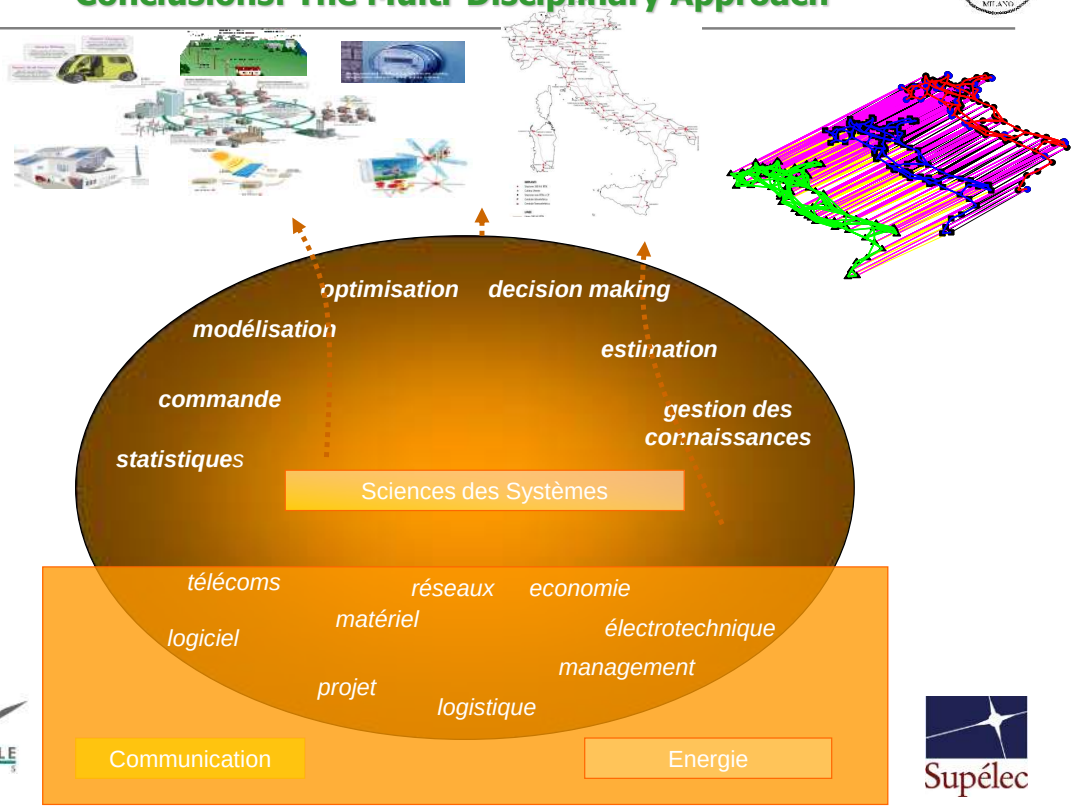


W. Kroger and E. Zio, *"Vulnerable Systems"*, Springer, 2011

Safety of Complex (Energy) Systems
Conclusions: The Analysis Framework



Safety of Complex (Energy) Systems
Conclusions: The Multi-Disciplinary Approach



Chaire « Sciences des Systèmes et Défis Energétiques (SSDE) »

Fondation Européenne pour les Energies de Demain — Électricité de France (EDF)

PRESENTATION

The Chair on Systems Science and the Energy Challenge is a research and education initiative shared between ECP and SUPELEC, with the support of EDF. Its activities focus on the development, implementation and use of computational models, methods and algorithms for the analysis of the failure behavior of complex energy systems and the related uncertainties.

The **research topics** of interest relate to complex systems modeling, reliability, availability and maintainability (RAM) engineering, risk assessment, safety and security evaluation, vulnerability analysis, failure diagnostics and prognostics.

The **research spirit** is intended to be exploratory and methodological. The Chair aims at complementing and integrating the different approaches to complex system analysis (from abstract network theory to detailed simulation, from analytical to empirical modeling, from probabilistic to non-probabilistic uncertainty analysis) to effectively respond at the specific scope of the different analyses (design, operation, maintenance, protection, etc.) on the different objects of analysis (components, plants, network systems, critical infrastructures, etc.).

RESEARCH SPIRIT
.Methodological
.Exploratory
.System analysis

RESEARCH AREAS
.Modeling
.Simulation
.Optimization

The Team

Two full-time faculty members

Yan-Fu LI — Assistant Professor
Enrico ZIO — Professor, Chair Director

Two post-docs

Carlos Ruiz MORA
Valeria VITELLI

Eight PhD students

Ronay AK
Yi-Ping FANG
Elisa FERRARIO
Elizaveta KUZNETSOVA
Jie LIU
Chung-Kung LO
Rodrigo MENA
Tairan WANG

COLLABORATIONS

Beihang University, China
City University, Hong Kong
Demark Technical University, Denmark
EDF R&D, France
Federal University of Pernambuco, Brasil
Institute of Nuclear Energy Research, Taiwan
Lund University, Sweden
Politecnico di Milano, Italy
Politecnico di Torino, Italy
Universidad Federico Santa Maria, Chile
University of Stavanger, Norway

RESEARCH LINES

1. Aging and failure processes in components of energy production plants

Component failure prognostics
Ronay AK, Jie LIU, Valeria VITELLI

Component degradation and maintenance modeling and simulation
Yan-Hui LIN

2. Energy network systems

Agent-based modeling
Elizaveta KUZNETSOVA, Carlos Ruiz MORA

Complexity Science
Yi-Ping FANG, Tairan WANG

System-of-Systems approach to External Events

Risk Assessment with uncertainties
Elisa FERRARIO, Chung-Kung LO

Optimization under uncertainty
Rodrigo MENA, Carlos Ruiz MORA

Risk assessment methodology for interdependent critical infrastructures

Dr. Marianthi Theoharidou
Department of Informatics, Athens University of Economics and Business, Athens, Greece

Summary

Dr. Theoharidou presented an analysis of criticality and impact assessment based on the structural description (topology) of the network interdependencies. The approach is static, and identifies interdependencies at three layers, organisational, sector, and intra-sector. On the basis of the arrangement of information in a look up table, the possible effects of failure are propagated and risk mitigation measures are suggested. Resilience is not addressed.

Risk assessment methodology for interdependent critical infrastructures

Dr. Marianthi Theoharidou
Department of Informatics
Athens University of Economics and Business

Workshop on Risk Assessment and Resilience for Critical Infrastructures
Joint Research Centre - Ispra
25-26 April 2012

Outline

1. Motivation
2. Research goals
3. The proposed method
4. Multi-order dependencies
5. Conclusions and future work

Publications:

1. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk assessment methodology for interdependent critical infrastructures", *International Journal of Risk Assessment and Management* (Special Issue on Risk Analysis of Critical Infrastructures), Vol. 15, Nos. 2/3, pp. 128-148, 2011.
2. Theoharidou M., Kotzanikolaou P., Gritzalis D., "A multi-layer Criticality Assessment methodology based on interdependencies", *Computers & Security*, Vol. 29, No. 6, pp. 643-658, 2010.

Motivation

- Which infrastructures are more critical?
- Which sectors are more critical?
- How dependencies affect risk?
- How can risk be mitigated?
  - Are there nodes or connections which are more cost-effective, when considering risk mitigation?

Research goals

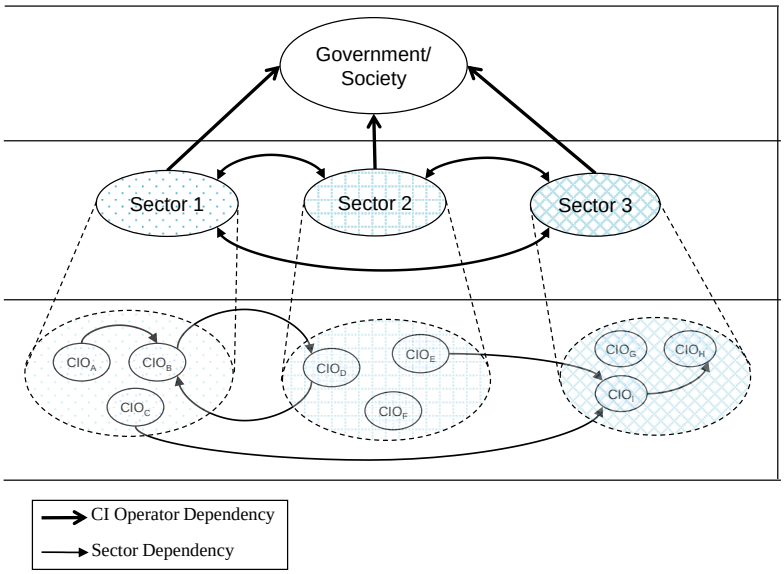
- Propose a method suitable for security experts, policy makers, national representatives or organizations dealing with CIP
- Assess:
  1. organizational and societal impacts of an infrastructure or a sector
  2. dependencies between infrastructures
  3. overall infrastructure risk
  4. cascading effects between infrastructures
- Provide useful input for a cost-effective risk mitigation for CIs
  - Provide alternatives for risk treatment by reducing threat, vulnerability or impact *within the complete chain of dependencies*

Risk assessment for CIP?

- Dependencies!
- Dual view of security risks:
  - *Organization-oriented*
    - It considers the security impacts, threats and risks for each examined organization (Critical Infrastructure – CI), in case of a security incident or scenario.
    - This can be based on existing risk assessment results.
  - *Society-oriented*
    - It needs to examine macroscopic impacts of a security incident or scenario, external for the examined organization (i.e. societal impacts) or impact to other CIs.

5

Risk assessment methodology for CIs



Three layers of analysis

Layer 3: Intra-sector /Society

- It examines the overall risks and evaluates the criticality of CIs and Sectors

Layer 2: Sector-layer

- Sector-layer analysis (the data are assessed by sector experts in order to assess the sector risks)

Layer 1: Organization-layer

- It is based on the 1st order dependencies of each CI
- It assumes that the CIs have conducted risk assessment

6

Organization-layer: Dependencies

- Goal: Identify the CIs on which a CI is most dependent on.

➔Organizational risk assessment based on dependencies, performed by the owner or operator of a CI.

- *Step 1* Identify all the requisite CIs and dependencies.
  - *Based on previous risk assessment results*
- *Step 2* Assess incoming risk *ri,j*
- *Step 3* Create the incoming risk matrix for each *CI*

7

Sector-layer: Societal Risk

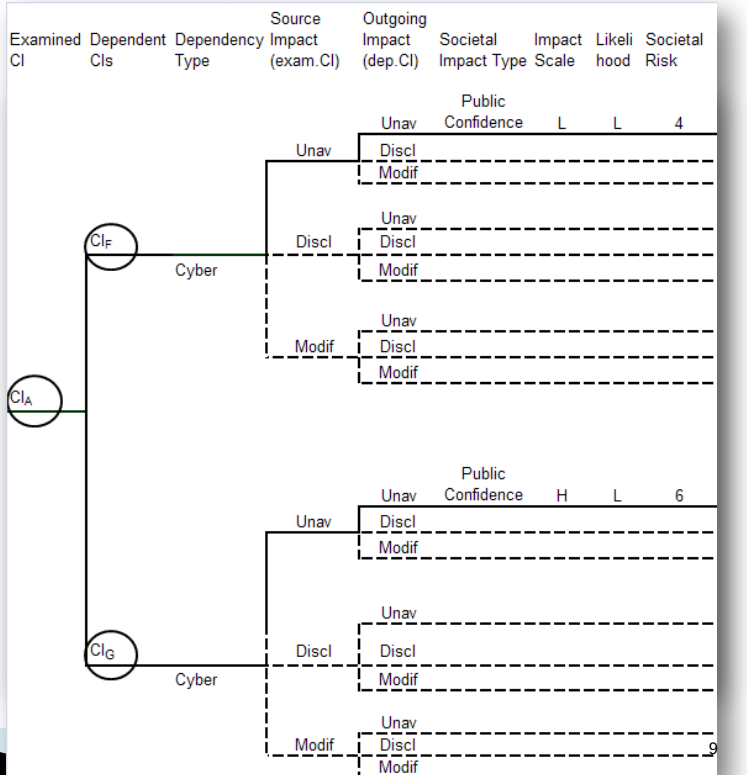
- Goal: Use the graphs from the previous step, but perform assessment on a societal and not organizational context.

- *Step 1* Identify the dependent CIs
- *Step 2* Assess the societal risk of each dependency (matrix, graph)
- *Step 3* Assess the societal risk of each CI (matrix)
- *Step 4* Estimate overall dependency and societal risk.

8

Sector Layer: Dependencies

Outgoing Societal Risk



Sector Layer: Societal Risk of Dependencies

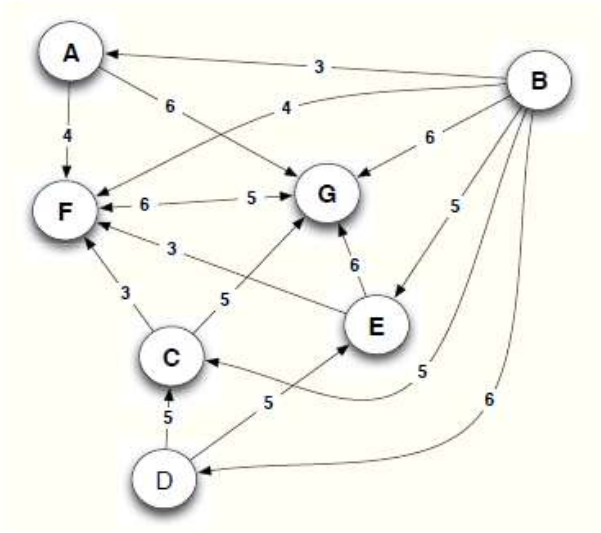
CI_A (Finance)

Dependent CIOs	Type	Description	Source Effect	Incoming Effect	Impact Type	Impact Scale	Likelihood	Outgoing Risk $sr_{i,j}$
CI_F (Gov.)	Cyber	Provides payment services	UA	UA	Public Confidence	L	L	**4**
CI_G (Gov.)	Cyber	Provides payment Services	UA	UA	Public Confidence	H	L	**6**

(UA: Unavailability, VH: Very High, H: High, M: Medium, L: Low, VL: Very Low)

Max Societal (Dependency) Risk of CI_i to CI_j $SR_{i,j} = \max_{\forall (i,j)} \{sr_{i,j}\}$ where $sr_{i,j}$, $SR_{i,j} \in [0,9]$

Dependency graph (first-order dependencies)



Sector Layer: Societal Risk of each Infrastructure (Node)

CI_C (ICT)					
Description	**Effect**	**Impact Type**	**Impact Scale**	**Likelihood**	**Societal Risk sr_i**
Provides network services to all public organizations.	UA for 3 hours	Public confidence	H	L	**6**

(UA: Unavailability, VH: Very High, H: High, M: Medium, L: Low, VL: Very Low)

Max Societal Risk of CI_i $\quad SR_i = \frac{1}{r_{max}} \max\{sr_i\}$ where $sr_i \in [0,9]$, $SR_i \in [0,1]$, $r_{max} = 9$

Sector Layer: Overall Dependency Risk

Sector	CI	Fin. CI_A	Ener. CI_B	ICT CI_C	ICT CI_D	ICT CI_E	Gov. CI_F	Gov. CI_G	ISR_i AVG	ISR_i STDEV	ISR_i MEAN	ISR_i MAX
Fin.	CI_A		3						0,056	0,000	0,333	0,333
Ener.	CI_B								0,000	0,000	0,000	0,000
ICT	CI_C		5		5				0,185	0,000	0,556	0,556
	CI_D		6						0,111	0,000	0,667	**0,667**
	CI_E		5		5				0,185	0,000	0,556	0,556
Gov.	CI_F	4	4	3		3		6	**0,370**	**0,136**	0,430	**0,667**
	CI_G	6	6	5		6	5		**0,519**	0,061	**0,620**	**0,667**
OSR_j	AVG	0,185	**0,537**	0,148	0,185	0,167	0,093	0,111				
	STDEV	0,328	0,216	0,271	0,309	0,324	0,386	0,463				
	MEAN	0,183	**0,383**	0,145	0,185	0,160	0,076	0,091				
	MAX	**0,667**	**0,667**	0,556	0,556	**0,667**	0,556	**0,667**				

Layer 3: National/intra-sector level

- *Step 1* Calculate overall risk for each CI.
  - We consider that a CI is critical for the society:
    - due to the inherent societal risk (*SRi*) or
    - due to the outgoing societal risk that occurs due to interdependencies (*OSRi*).
- *Step 2* Calculate overall risk for each sector.

Sector Layer: Overall CI Risk

- The risk level of a CI is based on two factors:
  - The *outgoing societal risk* (the potential risk caused to other CIs due to a security incident)
  - The *societal risk* (the risk that may be caused to the society or to a significant number of persons due to a security incident realized to the CI)
- Risk of infrastructure *i*: $R_i = f(OSR_i, SR_i)$
- For example

$R_i = a\ OSR_i + \beta\ Sr_i$ where $a+\beta = 1$ and $\alpha, \beta \in [0,1]$

	CI_A	CI_B	CI_C	CI_D	CI_E	CI_F	CI_G
OSRi	0,185	0,537	0,148	0,185	0,167	0,093	0,185
SRi	0,333	0,777	0,667	0,667	0,555	0,555	0,333
Ri	0,267	0,629	0,364	0,405	0,313	0,269	0,267

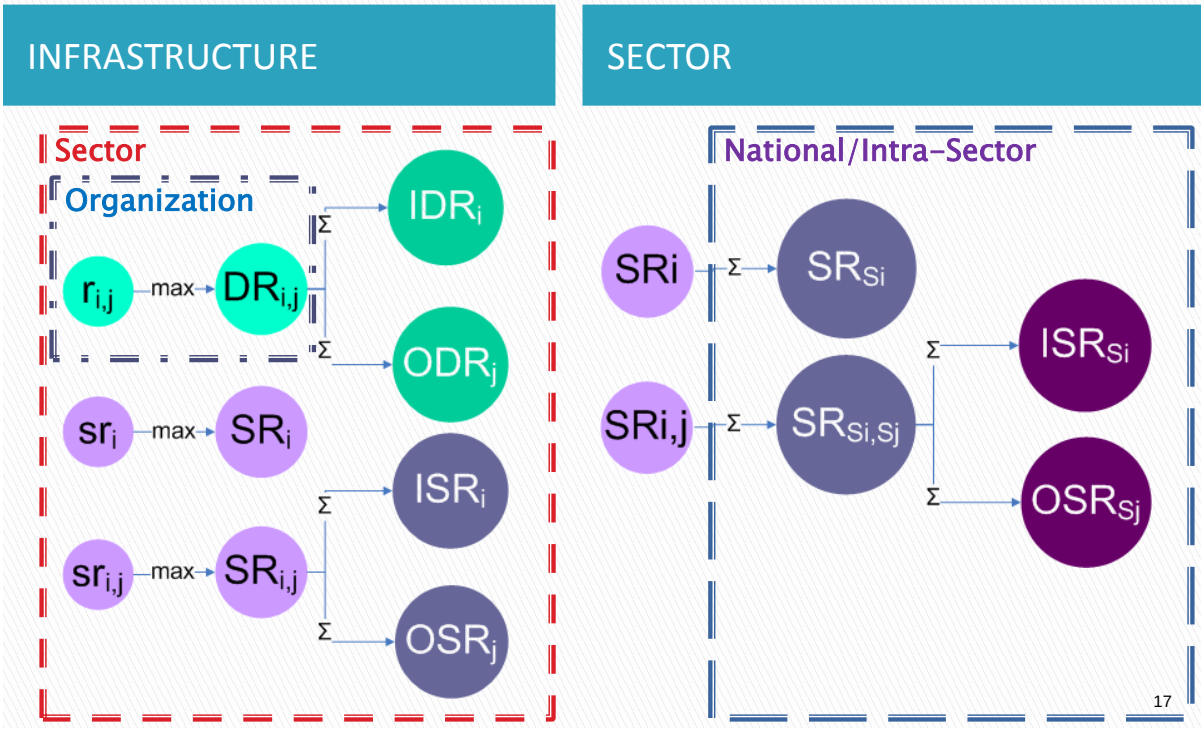
Intra-Sector Layer: Overall Sector Risk

- Sector Risk *Si*: $R_{Si} = f(OSR_{Si}, SR_{Si})$

$R_{s_i} = a\ OSR_{s_i} + \beta\ SR_{s_i}$, where $a+\beta = 1$ and $\alpha, \beta \in [0,1]$

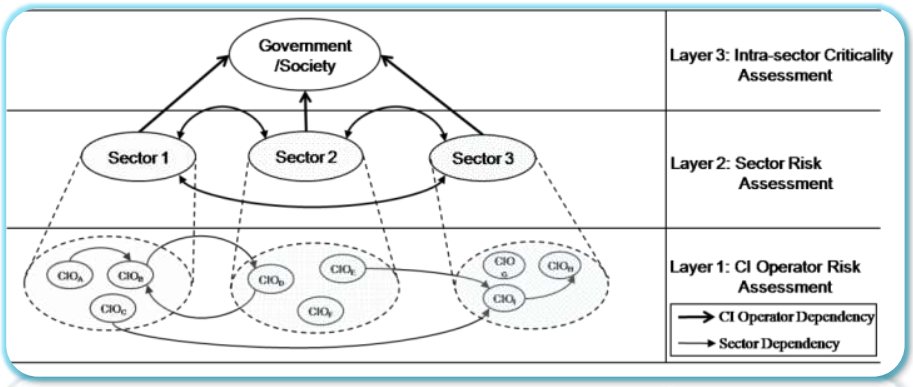
	Fin.	Ener.	ICT	Gov.
AVG (OSR_{s_i})	0,222	0,556	0,185	0,000
AVG (SR_{s_i})	0,333	0,777	0,630	0,611
R_{s_i}	**0,283**	**0,678**	0,430	0,336

Summary



17

Summary

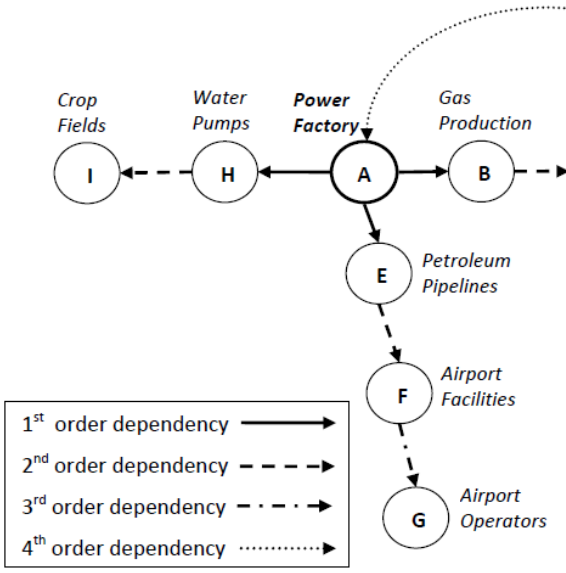


The **decision maker** is responsible for

a. selecting the infrastructures and sectors to be analyzed
b. assessing the risk parameters
c. selecting the scales
d. selecting the mathematical operators.

18

Multi-order Dependencies
Revisiting the California blackout



- *1-order dependencies:*

  $R = R_{A,B} + R_{A,E} + R_{A,H}$

- *n-order dependencies:*

  $R = R_{A,B} + R_{A,E} + R_{A,H} + R_{B,C} + R_{E,F} + R_{H,I} + R_{C,D} + R_{F,G} + R_{D,A}$

19

Risk Mitigation

- Select the most cost-effective strategy:
  - Controls to reduce the likelihood of an incident in the source of the examined dependency chain.
  - Controls that reduce the likelihood of cascading effects in any intermediate node within the chain.
  - Controls that reduce the impact of dependencies by creating alternative paths.
  - Controls that reduce the impact on individual nodes.

20

Conclusions

- Emphasis on the societal risk, which is usually out of scope or underestimated, during traditional organisational risk assessments.
- Allows the decision maker to assess the criticality of sectors as well, in a similar way as the various techniques of the IIM model but not on strictly economic terms.
- Our approach assumes that the examined CIs have conducted risk assessment analyses.
  - This may act prohibitory for the implementation of the method!
  - It also requires canonicalization of the scales of various RA methodologies with the scales of our approach.

Future work

- Consider cycles and reverse interdependencies
- Consider parallel paths in an automated way, as well as their potential effect to minimize risk.
- Adopt graph analysis algorithms, in order to identify the most critical paths of dependencies, and to provide ways to reduce risks by adopting alternative paths in a graph.
- Validate our method by applying the model in a real scenario.

Thanks for your attention
Questions?

Contact me at:
mtheohar@aueb.gr

Supporting PPP for CI resilience with proper modelling and assessment tools: from a regional experience to the European perspective

Prof. Paolo Trucco
School of Management, Politecnico di Milano, Italy

Summary

P. Trucco presented a modelling framework in which it accounts for failure in physical structures which provide a service (quantity), coupled with a number of activities that rely on those services with functional dependencies. The model is simulated and resilience is one of the properties of interest. At present, it is applied to regional level and regional interdependent infrastructures but the possibility to use this approach at EU level has been also presented. Feeding the necessary data to this modelling framework is a demanding task.

POLITECNICO DI MILANO

Supporting PPP for CI resilience with proper modelling and assessment tools

from a regional experience to the European perspective

Prof. Paolo Trucco
Department of Management, Economics and Industrial Engineering
POLITECNICO DI MILANO

Agenda

1. The PPP for CI Resilience in Lombardy Region - PReSIC
2. PReSIC - Main activities and the toolkit
3. Specific modelling needs for the resilience analysis of CI systems
4. A pilot study in the metropolitan area of Milan (Italy)
   - Vital Node Analysis
   - Dynamic Risk Analysis
5. Contribution towards an integrated European strategy on CI resilience

PReSIC - The PPP for CI Resilience in Lombardy Region (Italy)

Integrated Programme for CI Protection and Resilience of (PReSIC)

Developing a collaborative environment and shared supporting tools as a strategic resilience capability




- Scope:
  - collaborative management at the interfaces between actors (operators and institutions)
  - prevention, preparedness and emergency management
  - without any additional requirement beyond current regulations (European and national)
  - fully exploiting internal resources and capabilities of each actor
- Organisation: **network governance model**

Improving the resilience of the infrastructural system for the long term sustainable development of the region

PReSIC - The PPP for CI Resilience in Lombardy Region (Italy)

Integrated Programme for CI Protection and Resilience of (PReSIC)

Developing a collaborative environment and shared supporting tools as a strategic resilience capability



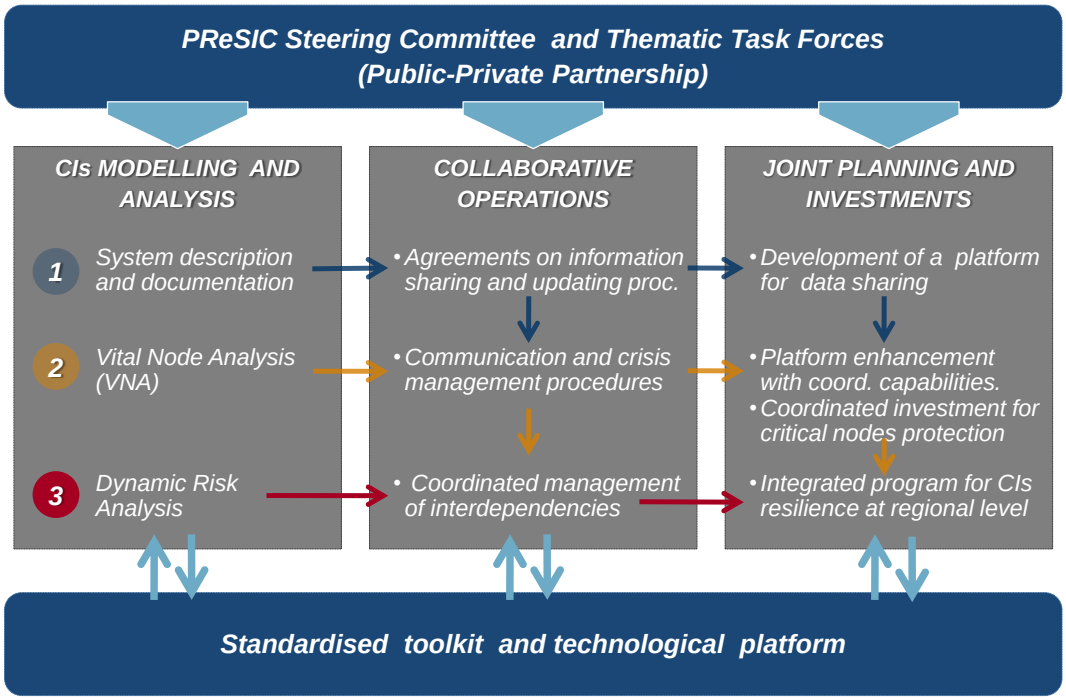

- **Inventory of CIs nodes and interdependency analysis**, due to potential accidents and service disruption events (all-hazard approach)
- Identification of criteria and protocols for enhanced **information sharing and operational coordination**
  - Scenario-based
  - Interdependency-based
- Large **exercises**
  - Snowfall event (2011)
  - Blackout (2012)
- Specification of requirements for a prototype **NEO platform** to support collaborative operations

PReSIC - The PPP for CI Resilience in Lombardy Region (Italy)

The PPP agreement involves **14** operators in the **Energy and Transportation** sectors and the Regional Civil Protection System

- Railways
- Metro lines
- Airports
- Highways
- National and regional road networks
- Power generation, transmission and distribution
- Gas

PReSIC - The PPP for CI Resilience in Lombardy Region



- **Definition of vulnerable node**:

Large functional part of a CI that assures the fulfillment of a considerable part of service demand at regional level (*e.g. part of a pipeline network, a large railway station, a portion of a highway or of a metro line*)

A vulnerable node has to be:

- homogeneous (i.e. uniform in structure and function with respect to service demand),
- service self-providing (i.e. a system able to supply a value-added service through own means),
- and vulnerable (i.e. susceptible to threats that could decrease its functional integrity).

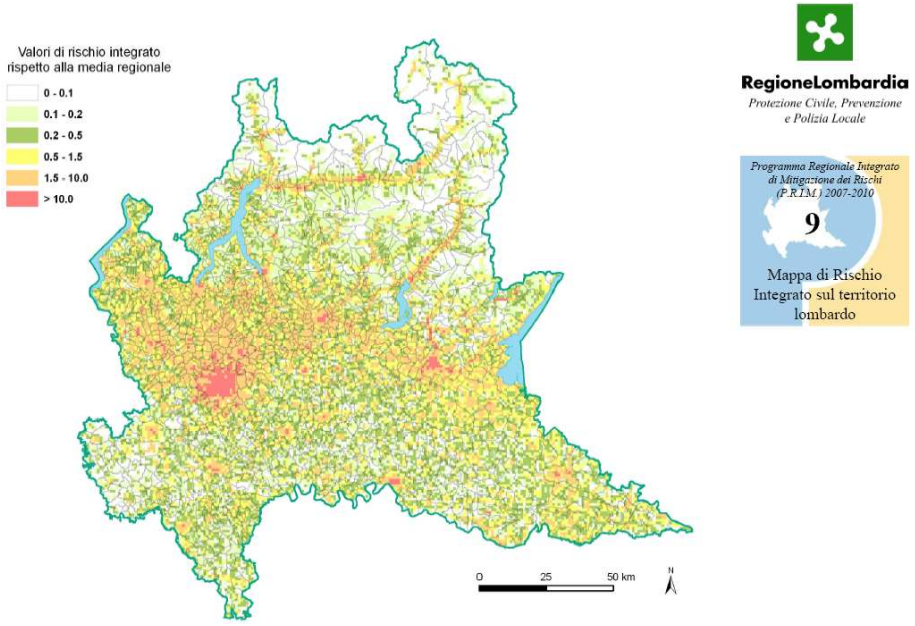
- **Inventory and Documentation of CI node vulnerabilities:**

Operational failures (internal threats)	Frequency	Loss of Functional integrity (%)	Recovery Time		Direct damages	Economic loss
			mean	max		

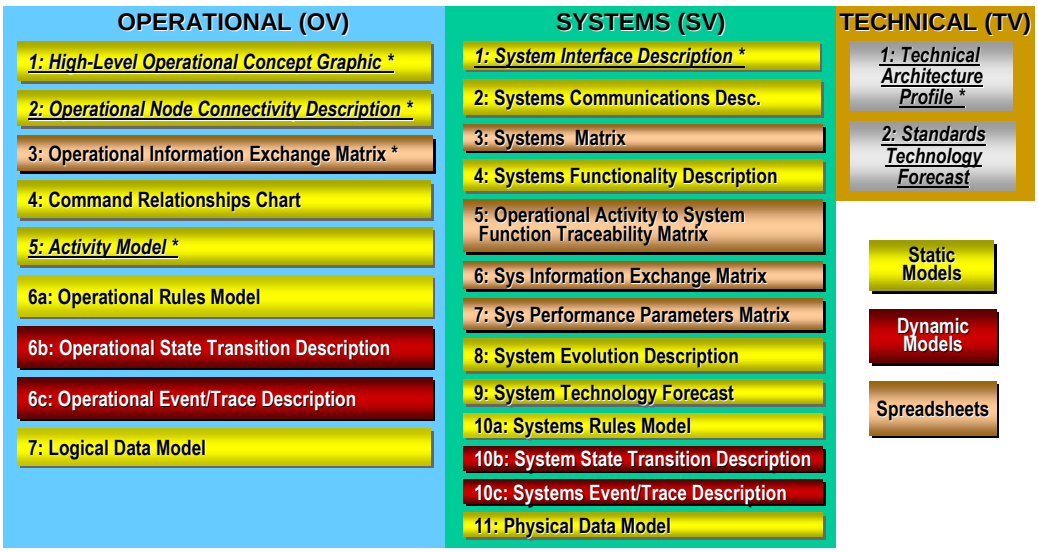
External threats	Degree of vulnerability			Loss of Functional integrity (%)	Recovery Time		Direct damages	Economic loss
	High	Average	Low		mean	max		
Floods								
Landslides/ Rockfalls								
Earthquake								
…								
Explosion								
Intentional attacks								

Interdependent nodes of other CI (father)	Type of service	Inoperability rate (%)	Max Transient Time (h)	Qualitative description of the interdependency

- **Inventory of external threats (natural and man-made):**
  PRIM - Integrated Regional Program for the mitigation of major risks (2007-2010)



- **Modelling operations and info sharing processes**
  NAF v.3 - NATO Architecture Framework.
  Architectures are used as analysis tools to develop new capabilities, structure organisations and to optimize processes in multi-agency contexts.



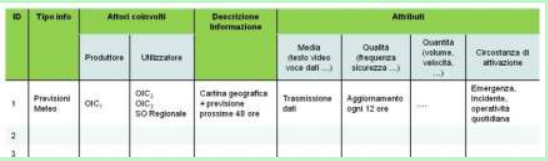
PReSIC - Main activities and the toolkit

- **NAF v.3 - NATO Architecture Framework**

NATO Operational View – NOV

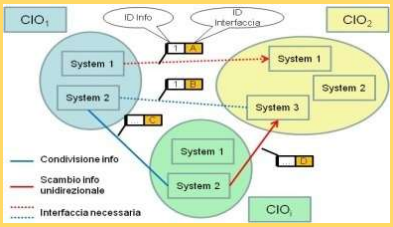
- NOV- 2 Operational Node Connectivity Description
  - Graphical description of existing information exchanges
  - Directory of contact points

- NOV- 3 Operational Information Requirements
  - Documentation of information flows



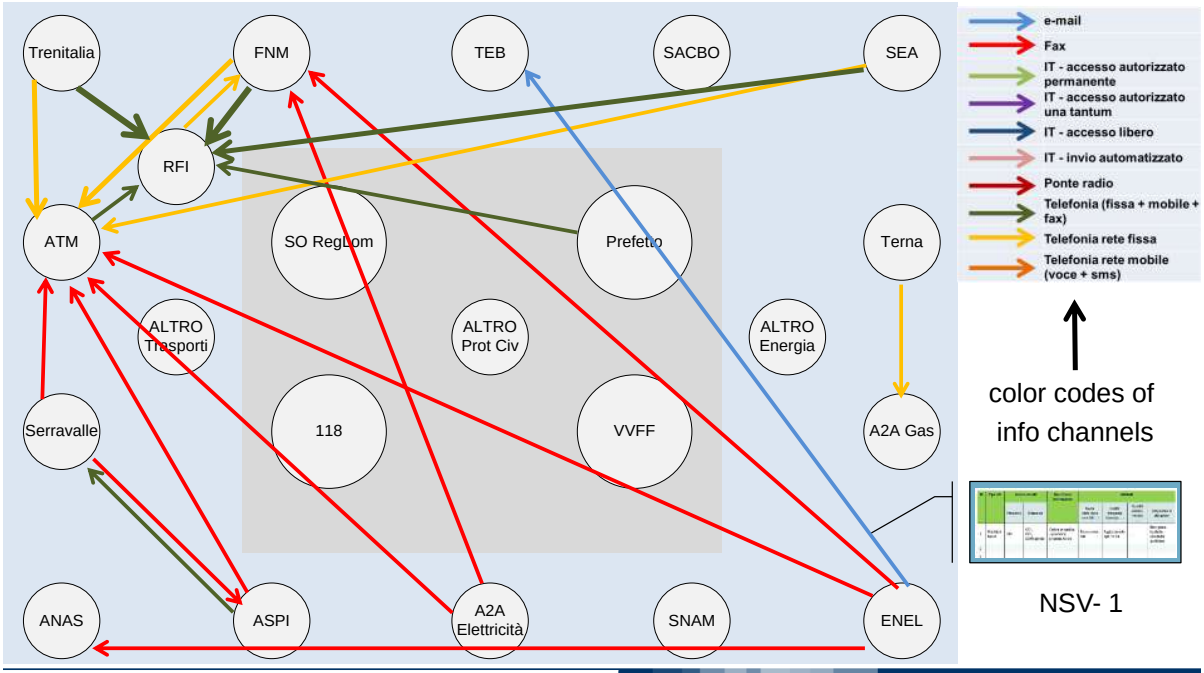
NATO Systems View – NSV

- NSV- 1 System Interface Description
  - Description of channels and interfaces supporting information flows (NOV – 3)



PReSIC - Main activities and the toolkit

- Example of NOV-2 for a specific disruption scenario



Specific modelling needs for the resilience analysis of CI systems

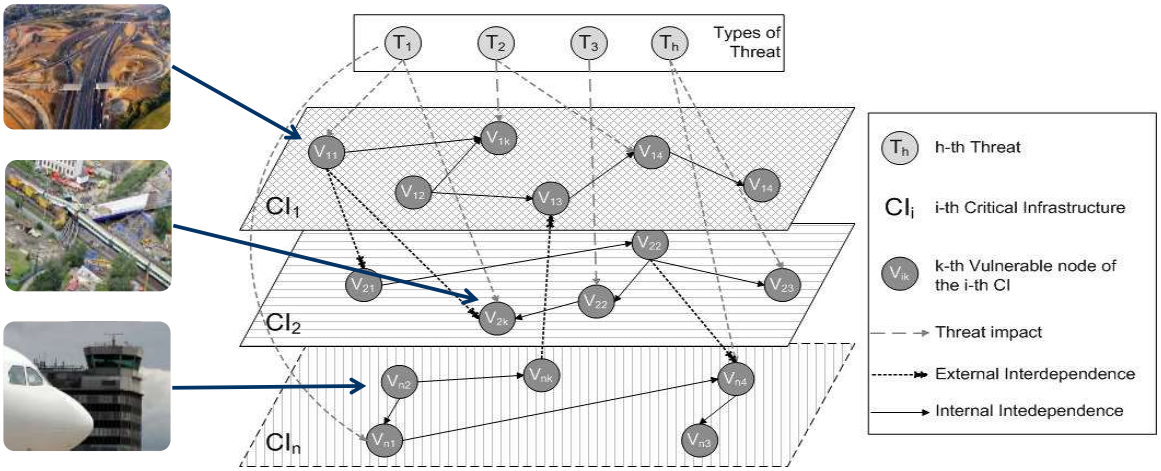
- To account for **different types of interdependencies**;
- To account for **different impacts** of interest;
- Dynamics of **service delivery** (inoperability) and **service demand** (e.g. behaviour of citizens) are relevant to recovery and crisis management;
- **Lack of detailed data** on physical assets and service operations (not disclosed by CI operators);
- The geographical reference (**GIS**) must be assured for vulnerable nodes, threats and impacts;



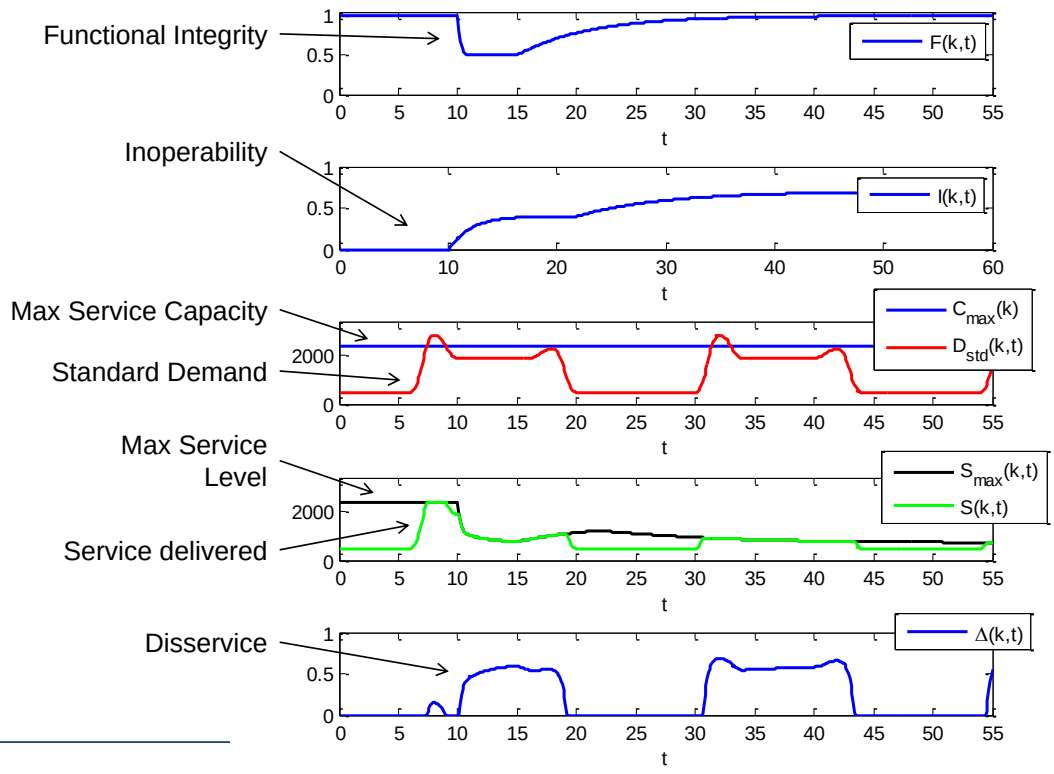

Functional and Dynamic Modelling of a Service Oriented Architecture (SOA)

Functional modelling of vulnerability and interoperability of CIs

- The proposed SOA modelling approach has some distinctive features:
  - Quantification of **functional and logic interdependencies** thanks to the use of service demand and service capacity parameters;
  - **Time dependent** specification of all the parameters of the model;
  - **Propagation of inoperability and demand variations** throughout the nodes of the same CI and between (inter)dependent CIs.

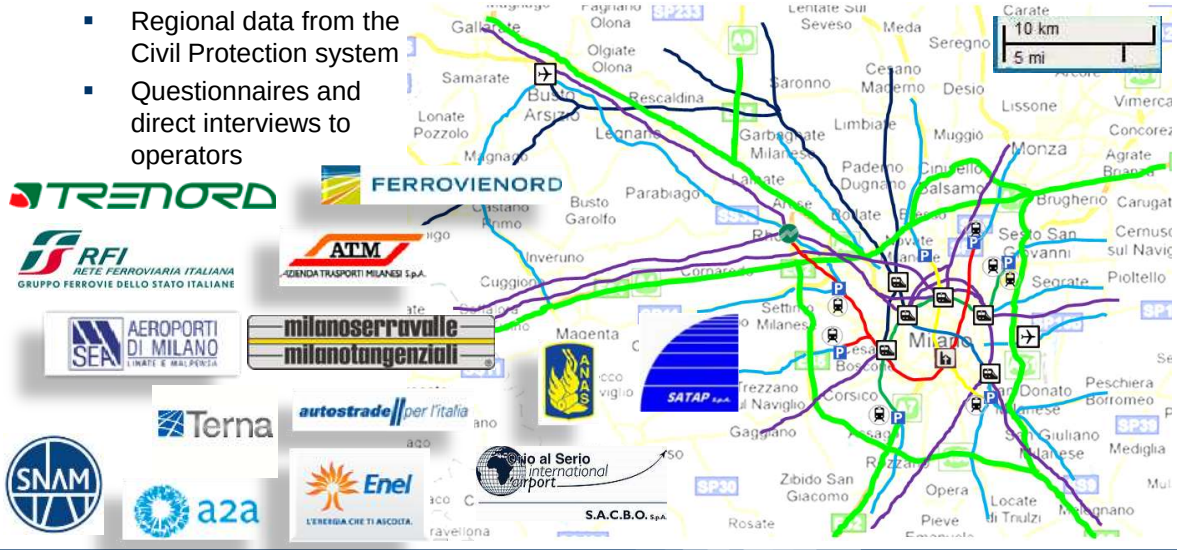


Functional modelling of vulnerability and interoperability of CIs



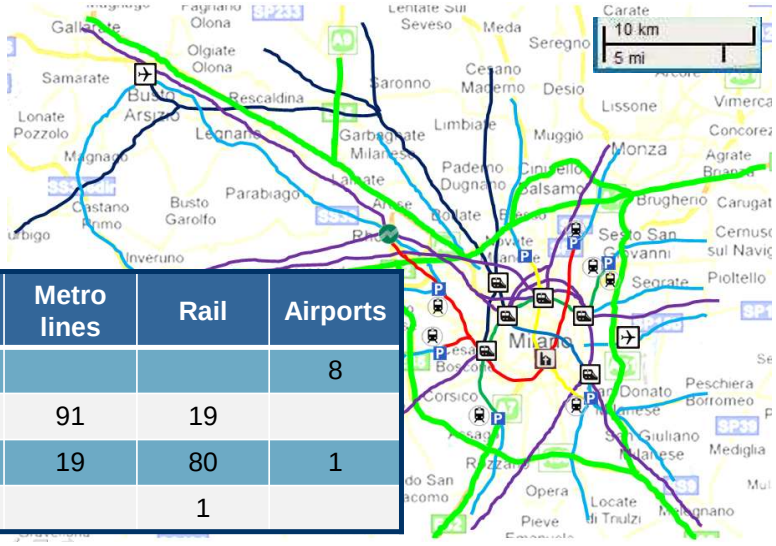
Vital Node Analysis (VNA): Pilot study in the metropolitan area of Milan

- Transport infrastructure systems modelled by **169 vulnerable nodes**
- **Electricity** and **Gas** networks were considered as sets of **threat** nodes
- Characterisation of vulnerable nodes and threats by means of:
  - Public data and theoretical models
  - Regional data from the Civil Protection system
  - Questionnaires and direct interviews to operators



Vital Node Analysis (VNA): Pilot study in the metropolitan area of Milan

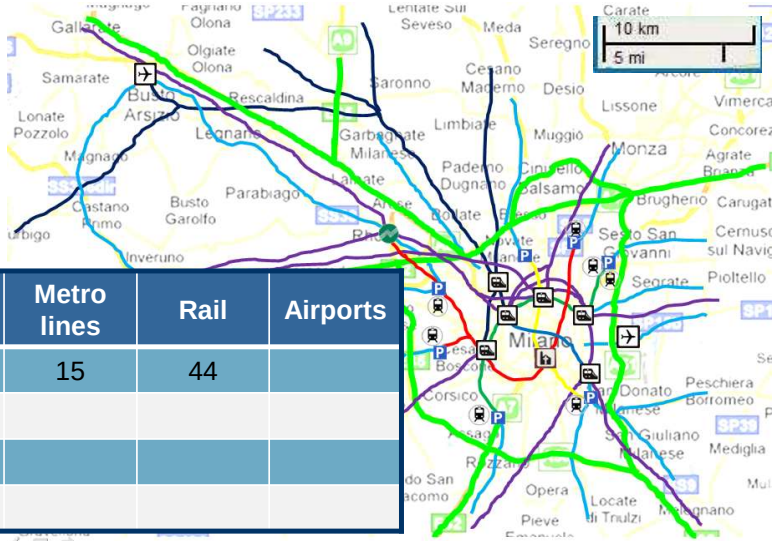
- Transport infrastructure systems modelled by **169 vulnerable nodes**
- **Electricity** and **Gas** networks were considered as sets of **threat** nodes
- Characterisation of vulnerable nodes and threats by means of:
  - Public data and theoretical models
  - Regional data from the Civil Protection system
  - Questionnaires and direct interviews to operators



Functional interdependencies	Road	Metro lines	Rail	Airports
Road	193			8
Metro lines		91	19	
Rail		19	80	1
Airports	8		1	

Vital Node Analysis (VNA): Pilot study in the metropolitan area of Milan

- Transport infrastructure systems modelled by **169 vulnerable nodes**
- **Electricity** and **Gas** networks were considered as sets of **threat** nodes
- Characterisation of vulnerable nodes and threats by means of:
  - Public data and theoretical models
  - Regional data from the Civil Protection system
  - Questionnaires and direct interviews to operators



Logic interdependencies	Road	Metro lines	Rail	Airports
Road	111	15	44	
Metro lines	15			
Rail	44			
Airports				

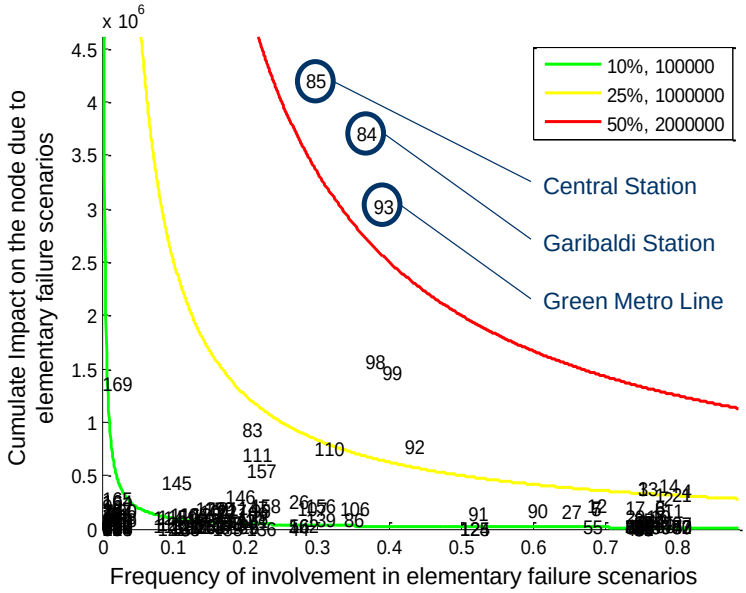
Vital Node Analysis (VNA): Pilot study in the metropolitan area of Milan

- **Elementary failure scenarios**: triggered by the activation of several threats or a single threat impacting on a single vulnerable node at a time and blocking it for the entire simulation time-window

Triggered node type	Total impact [persons* node]	% impact on the trigger node	Node affected by the highest impact	% impact on the node affected by the highest impact	Domino Index	Resilience Index
Central Station	4.2E06	7.5	Central Station	7.5	0.8	8.37
Garibaldi Station	3.7E06	2.0	Green Metro line	6.6	0.7	0.34
Green Metro line	3.0E06	7.7	Green Metro line	7.7	0.7	7.75

Vital Node Analysis (VNA): Pilot study in the metropolitan area of Milan

- **Elementary failure scenarios**: triggered by the activation of several threats or a single threat impacting on a single vulnerable node at a time and blocking it for the entire simulation time-window



Vital Node Analysis (VNA): Pilot study in the metropolitan area of Milan

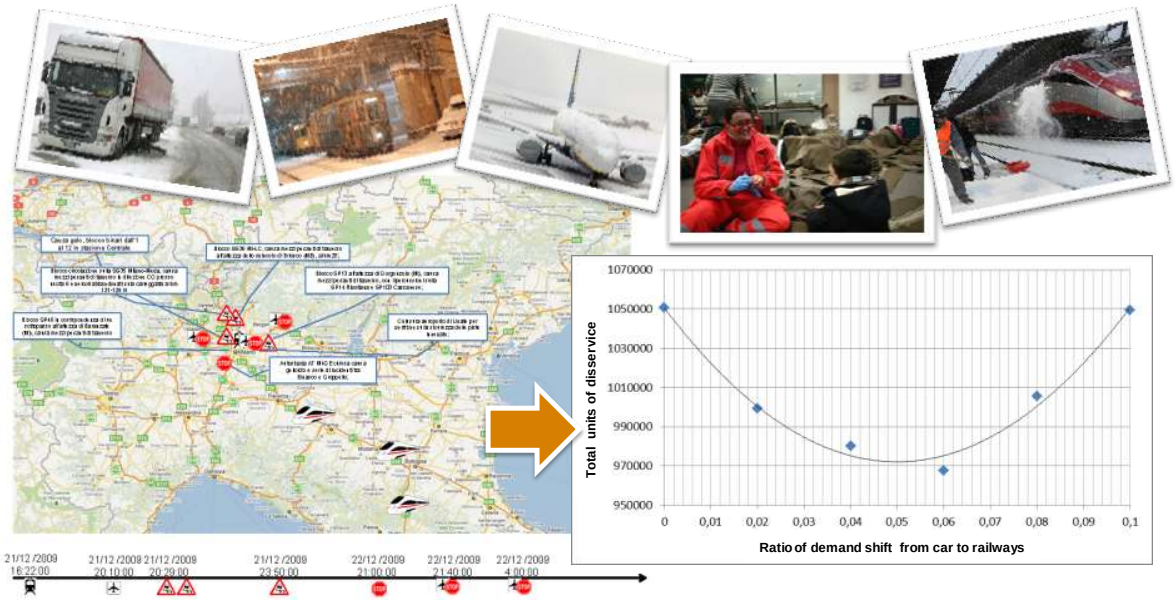
- **Complex failure scenarios**: several threats or a single threat able to disrupt several vulnerable nodes concurrently

Scenario	Total impact [persons* node]	Impact on the trigger node [%]	# node affected by the highest impact	Impact on the node affected by the highest impact [%]	Domino Index	Resilience Index
Highway (#1, 2) and Metro line (# 94, 95)	1.7E06	57.6	Green Metro line	15.0	0.4	76.7

Escalation factor =1.86

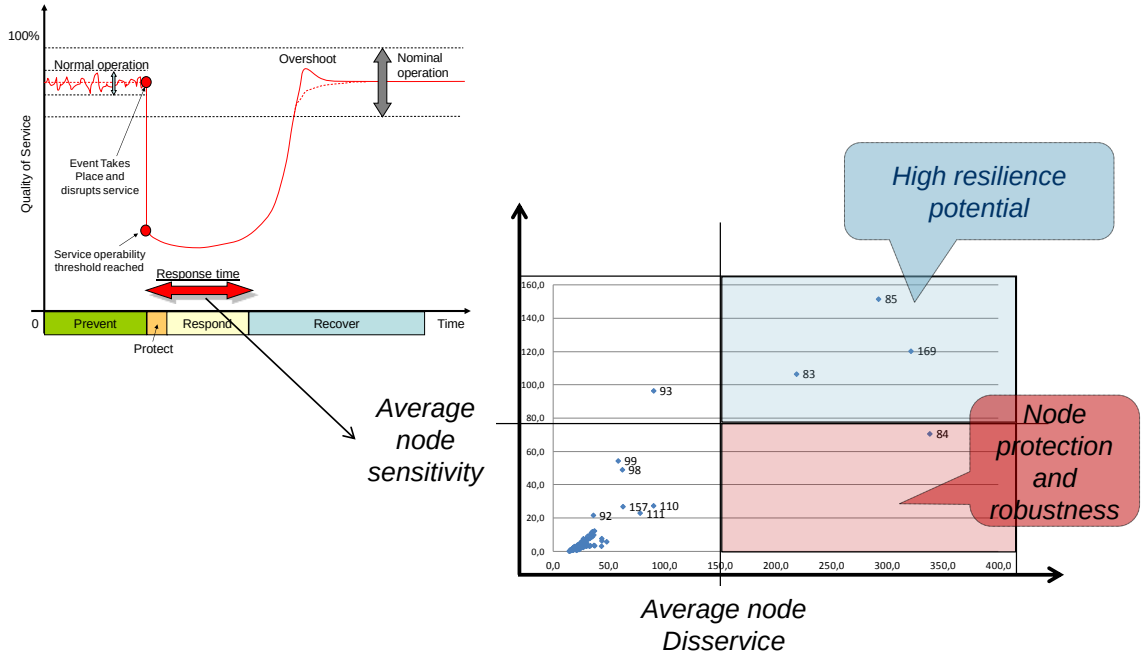
Dynamic Risk analysis: Scenario-based assessment of collaborative processes

- Large national snowfall event (21-23 December, 2009): improving info sharing processes by means of ex-post study of real disruptions



Dynamic Risk analysis: Impact assessment of reduced response times

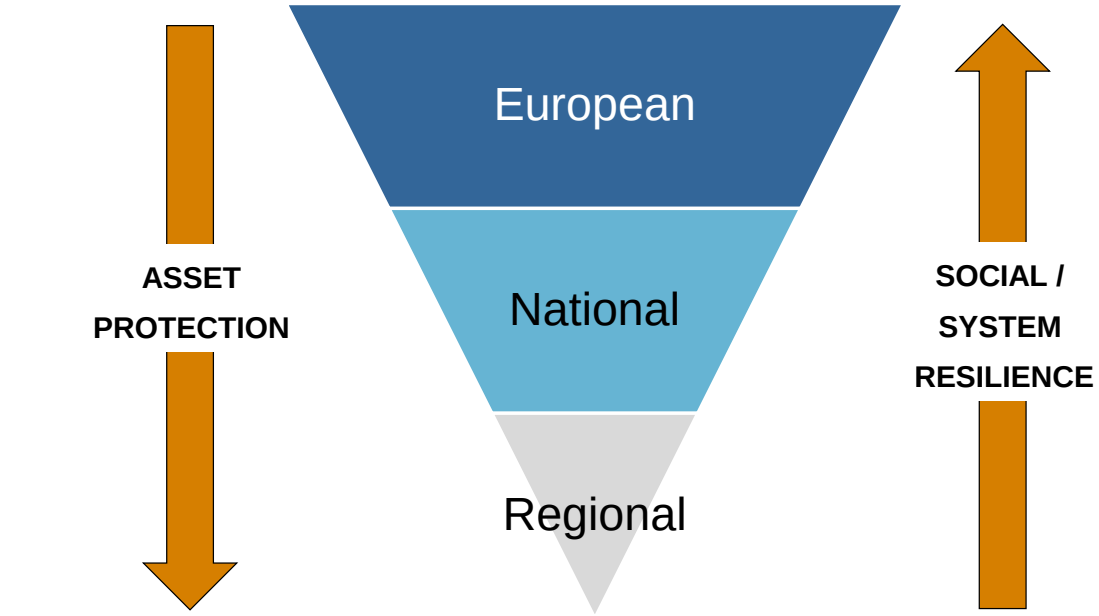
- **Node sensitivity analysis and system resilience characterisation**



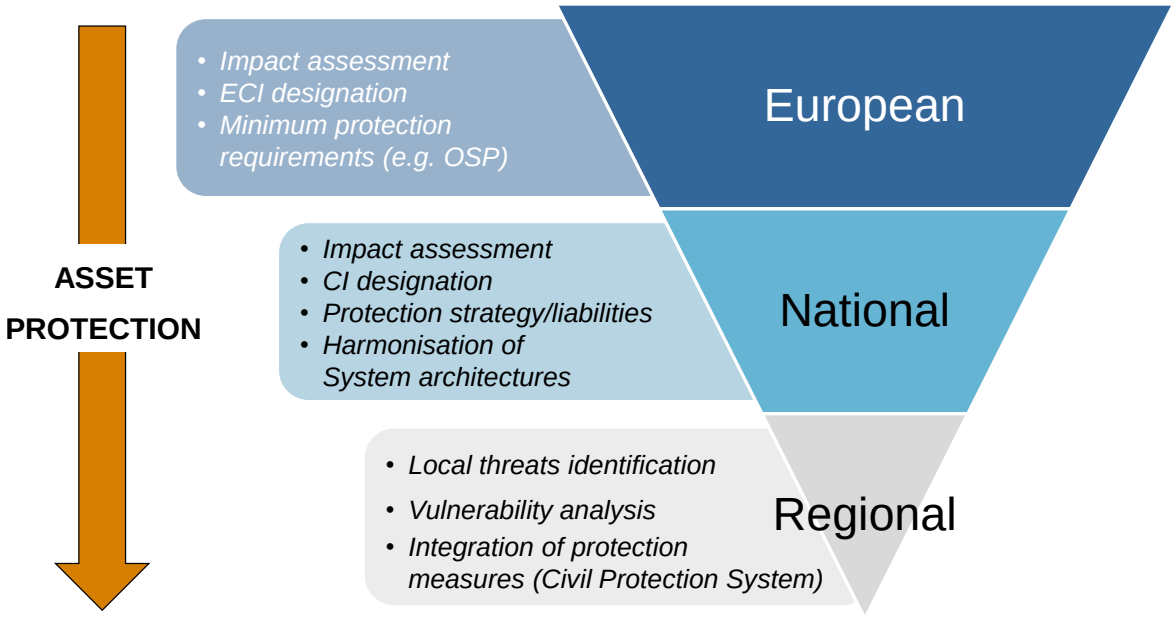
Open issues and limitations of current methodological approach

- The **completeness and quality of data** remain an issue …
  - The proposed data gathering method demonstrated to be sufficiently understood by managers and professionals
  - Collection and treatment of sensitive data currently acceptable. But …
- How to identify/assess detailed **organisational/technical inoperabilities** at a single infrastructure level or high level **interdependencies outside regional boundaries**?
  - Integrated approach by means of a federation of simulation models (Flammini et al., 2008)
  - Independent analyses carried out by CI operators + information sharing
  - …?
- How to **maintain** the model updated?
  It calls for methodological development and pilot experiences on:
  - Standardisation of data models and methods for data collection and pre-processing
  - Criteria for designing and executing review processes
  - Streamlining model updating procedures

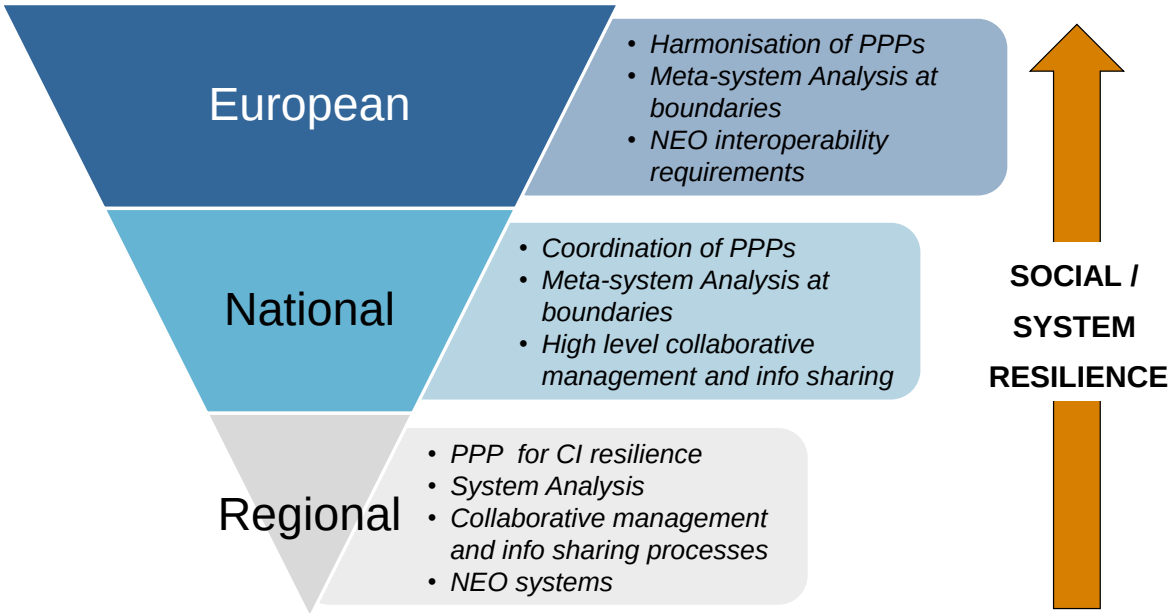
Contribution towards an integrated European strategy on CI resilience



Contribution towards an integrated European strategy on CI resilience



Contribution towards an integrated European strategy on CI resilience



POLITECNICO DI MILANO

Workshop on Risk Assessment and Resilience for Critical Infrastructures

Joint Research Centre
Ispra - 25-26 April 2012

Thank you!

Prof. Paolo Trucco
e-mail. paolo.trucco@polimi.it
URL. http://www.ssrm.polimi.it/

Preliminary Interdependency Analysis of Critical Infrastructures: Models, Tool Support and Data Analysis

Dr Peter Popov
Centre for Software Reliability, City University London, UK

Summary

Dr. Popov presented a study on critical infrastructure which is of probabilistic nature. The framework starts with the topology of the network, to which it associates a classic failure characterisation (TTF, TTR) of single systems and cluster of systems as well. The latter aspect takes into account the possibility that failure of a system may accelerate, by a stressing factor, if more systems have failed at the interface of it. The analysis returns the most critical nodes and it was tested on a Power grid (TELCO, UK).

CITY UNIVERSITY LONDON

Preliminary Interdependency Analysis of Critical Infrastructures: Models, Tool Support and Data Analysis

Dr Peter Popov
with Robin Bloomfield, Vladimir Stankovic, David Wright and Kizito Salako
Centre for Software Reliability
City University London

ptp@csr.city.ac.uk
College Building, City University London EC1V 0HB
Tel: +44 207 040 8963 (direct)
+44 207 040 8420 (sec. CSR)

CSR Building confidence in a computerised world
www.csr.city.ac.uk

CITY UNIVERSITY LONDON

Talk outline

- Interdependency analysis – why is needed
- Preliminary Interdependency Analysis
  - Method
  - Modelling dependencies
  - Parameterisation
- Tool support
  - PIA Designer
  - Execution Engine: Möbius-based Monte-Carlo simulator
    - Plug-ins
- Simulation results
- Interdependencies Data Analysis
- Current and Future work
- Conclusions

CITY UNIVERSITY LONDON

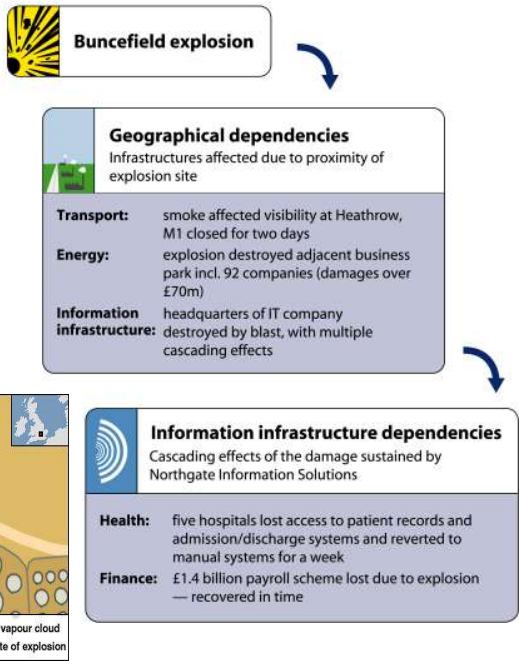
Sources of funding for the work

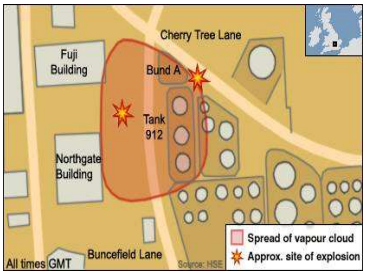
- Started in the IRRIIS project (EU FP6 – IP, 2006 - 2009),
- Followed by:
  - Cetifs (CPNI, EPSRC, TSB),
  - PIA-FARA (TSB, EPSRC)
  - City University Strategic Development Fund (CSR 2012)
- From September 2011 - AFTER (EU FP7 - STREP)
- May 2012 - SESSAMO (Artemis JU).
- This work is included in the report of the Expert Engineering Group on Interdependency between critical infrastructures commissioned by the Treasury of the UK.

CITY UNIVERSITY LONDON

Critical Infrastructure Interdependencies

- A key issue for achieving CI resilience and CI protection
  - risk of CI disturbances propagating across 'dependencies' links
- A complex phenomena, yet not well understood

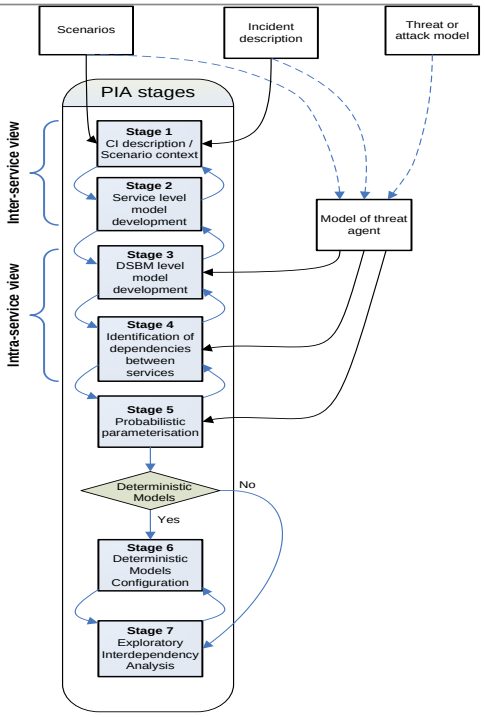




CITY UNIVERSITY LONDON

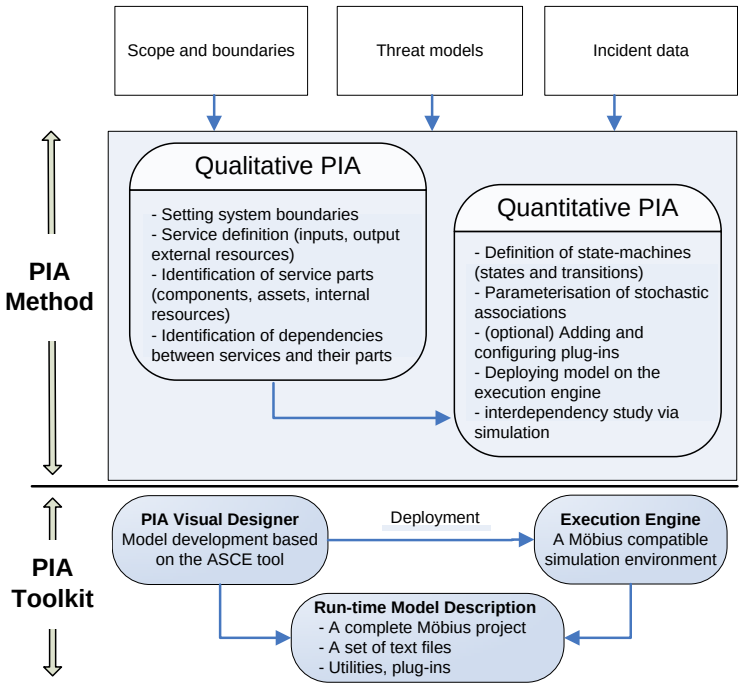
PIA - Interdependency Analysis

- PIA is an approach to interdependency analysis which consists of two steps
  - **Preliminary** Interdependency Analysis (Pre-IA) – HAZOP like analysis of interdependency ***discovery***
  - **Probabilistic** Interdependency Analysis (Pro-IA) – ***quantitative model*** of interacting CIs, each represented as a collection of services, which in turn encompass both:
    - Typically very large systems (***hardly amenable to analytic solutions***,
      - parameterization becomes problematic)
    - Probabilistic behaviour (rates/distributions of Time-To-Failure and Time-To-Repair)
    - Engineering (typically deterministic) models (e.g. various flows models)



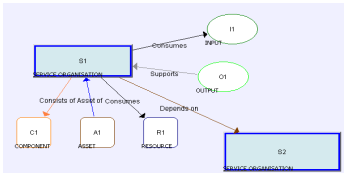
CITY UNIVERSITY LONDON

An overview of the PIA method



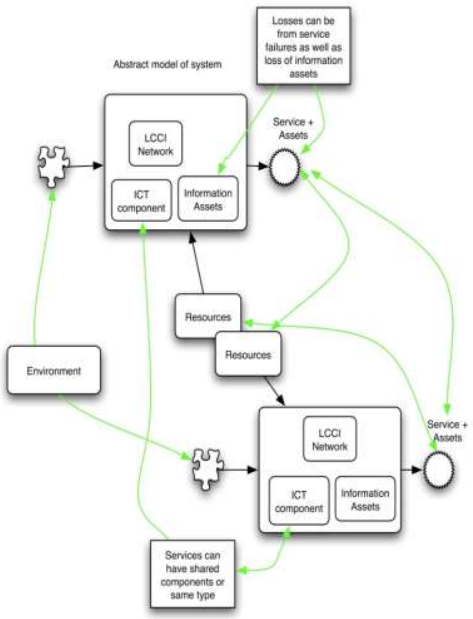
Preliminary Interdependency Analysis (Pre-IA)

- 'Preliminary' because one should start by establishing ***basic understanding***
- Service oriented, systematic elaboration of model components
  - "Quick and easy wins" rather than expensive and time-consuming detailed modelling and analysis
  - HAZOP style Identification of dependencies of assets/components/resources within and across organizations/departments
  - Basis for more detailed models
- Examples
  - Rome telecommunications incident (developed in IRRIIS)



Sources of dependencies in CIs

- shared services or functions
- shared resources
- similar policies
- similar assets attracting *correlated attacks*
- similar components (e.g. the same COTS software)
- traffic/load dependencies
- common environmental effects (flood, fire, disease, but also computer viruses)
- poisoning and spreading of failures, e.g.
  - by traffic on a telecommunications network,
  - denial of service by device failing on network and causing flooding of network
- human networks e.g. maintenance teams,
  - These can lead to a combination of unanticipated connectivity, greater impact of failure, and faster, cascade events.

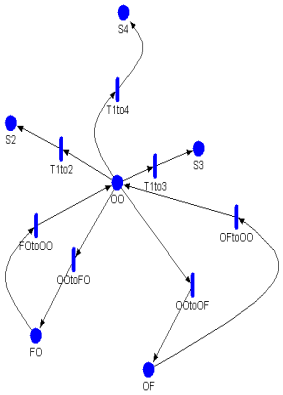


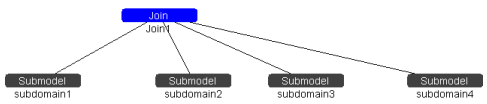
Probabilistic PIA (Pro-IA)

- uncertainty in the real world (aleatory) and in our knowledge of it (epistemic)
  - behaviours, structures (especially for Information Infrastructures)
- measures we want are probabilistic
  - overall aggregated ***risks*** (e.g. size of cascades vs. frequency)
  - probability of specific events (e.g. service loss, failure scenarios, "weakest link")
- allows for modelling approximations and efficiencies
  - consequence and environment models, infrastructure models
  - explore cascade mechanisms
  - can search for interesting cases, link to trials/demos
  - can explore many thousands situations
- important role to complement deterministic, qualitative, trails and analytic approaches

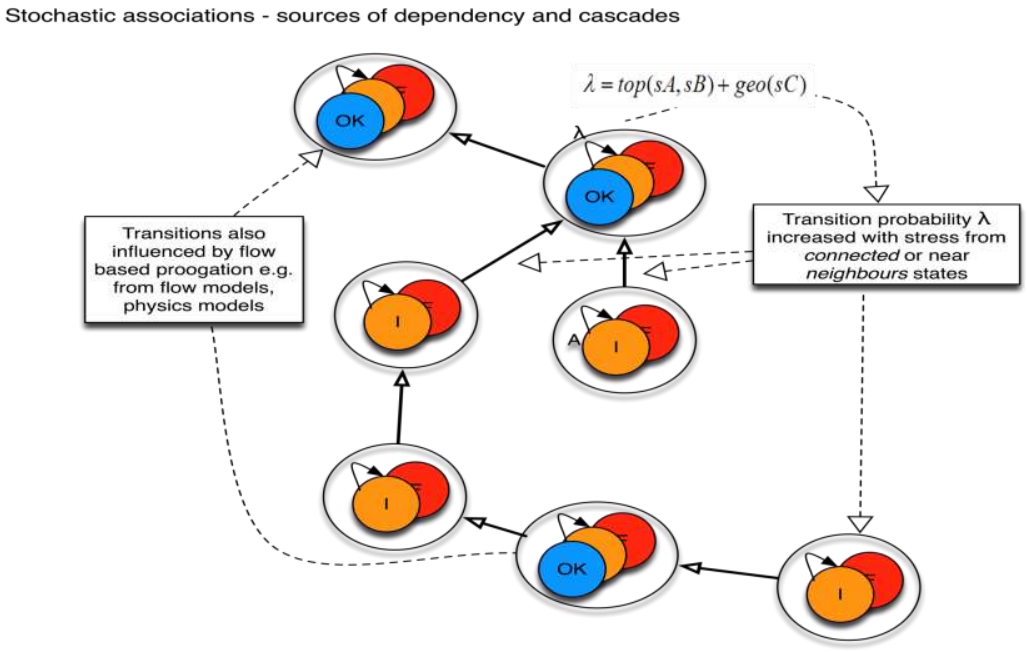
Pro-IA models

- Used SANs (stochastic activity networks) and Möbius Modelling Tool (by the performability group at the University of Illinois at Urbana Champaign, USA) to define parameterised continuous time semi-Markov models
- Finite state atomic components that mutually interact with each other to make ***impairment*** and failure "contagious":
  - Each component is modelled as a state-machine (a semi-Markov process)
  - rates (distributions) of transition between states are functions of the states of the 'neighbour' components ("model of stress").
- Embedded deterministic sub-models that can relate the "dynamics" of some subsets of the components in other specified ways
  - e.g. DC/AC approximate power flow model for power flow components
  - e.g. telecommunication service model.
- Components coupled via geographic location.
  - Spatial dependencies are important
  - ***BUT not the only ones worth studying! (design faults, viruses are not spatial)***



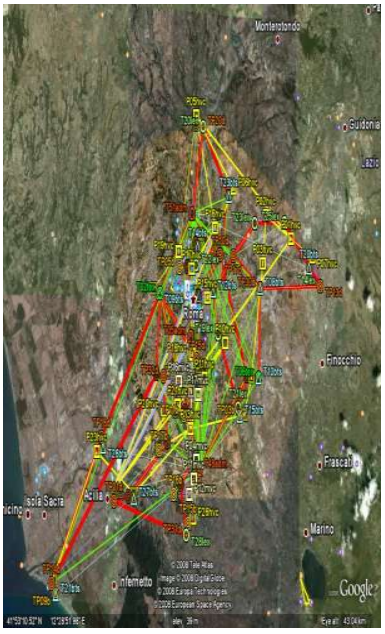


PIA approach to modelling (inter)dependencies



Rome Scenario Implementation

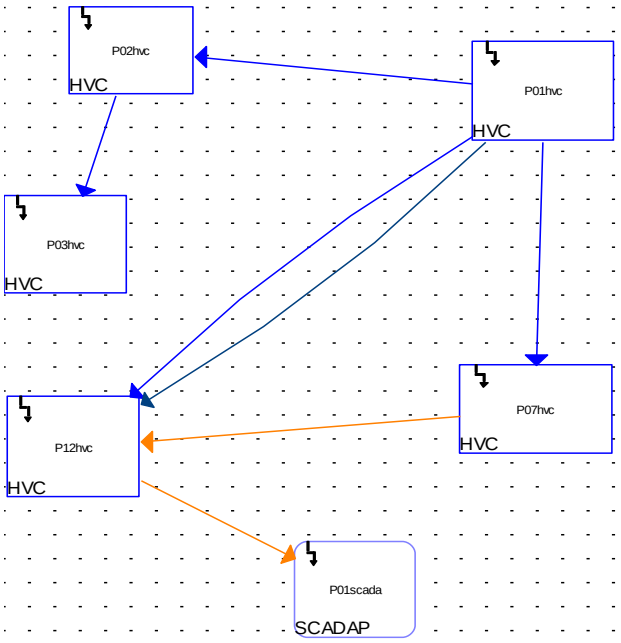
- Service layer – 5 services:
  - Power Grid: Power Transmission and Power Distribution
  - Telecommunications: Fibre-optics network, fixed lines telephony, GSM
- Physical layer;
  - **830 modelled physical elements** - nodes and links (high-voltage cabins, trunks, fibre cables, transmitters, gateways)
- Dependencies –
  - deterministic based on functional dependencies (telecommunications need power, power components controlled remotely via telecommunication channels)
  - stochastic associations – spatial proximity and cross-CI functional dependencies;
  - Non-probabilistic models (causality, flow models which may lead to overloading and tripping)
- Parameter values;
  - Probabilistic models: Failure rates, Repair rates,
  - Deterministic: flows, capacity (of lines, batteries), power load, voltage levels, line resistance (ETHZ);



PIA:FARA Toolkit Prototype

- The toolkit consists of:
  - PIA Designer – an interactive tool to allow a modeller to 'design' an interdependency study.
    - Supported by Adelard's ASCE visual editing tool (designed to support documenting safety-cases and customised for the needs of PIA)
  - PIA Run-time support – execution environment based on the Möbius tool (and in particular its SAN formalism) with very ***extensive customisation***
- PIA Designer - a 2-layer approach:
  - ***Intra***-services model - networks behind the individual services are explicitly modelled (as SANs with dependencies between the modelled elements)
  - ***Inter***-services model – explicitly models (inter)dependencies between the services that belong to different Intra-service models;
    - Coupling points – path for interdependencies to propagate between services;
  - Deterministic models added via ***plug-ins*** to the system at run-time (DLLs and initialisation files, e.g. XML)
  - Exporting the model for 'execution' on a run-time environment such as Möbius's SAN execution engine.
  - Visualisation of the probabilistic model simulation traces (using the Möbius built-in provisions or custom built utilities)

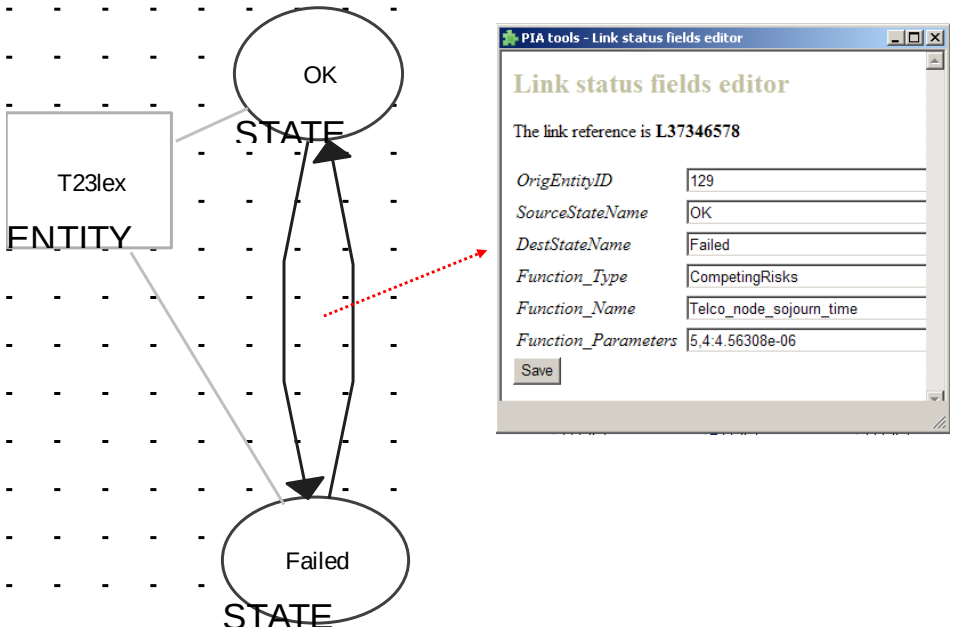
PIA:FARA Toolkit: ***Intra***-service view



Node status fields	
Reference	N26470700
Id	18
Title	P07hvc
Node type	HVC
State	True
Latitude	41.923
Longitude	12.6721
Functionality	Power
MemberOf	Power-Network
SubCl	Transmission
IsInterClCouplingPoint	True
IsSubClCouplingPoint	False

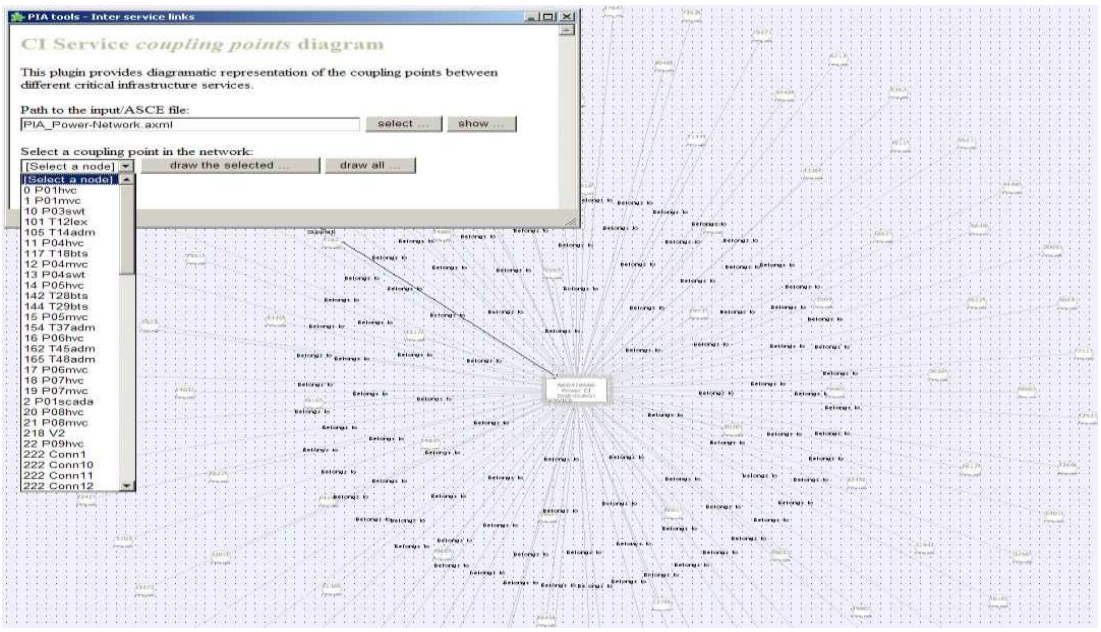
CITY UNIVERSITY LONDON

PIA:FARA Toolkit: State Machines



CITY UNIVERSITY LONDON

PIA:FARA Toolkit: Plug-ins



PIA:FARA Run-time engine

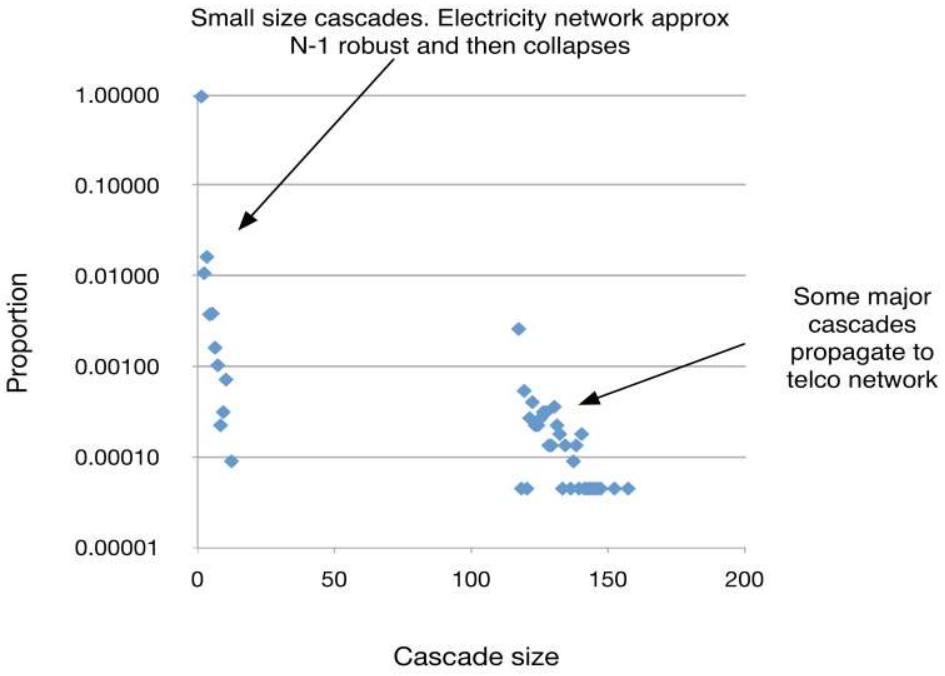
- Möbius project template
  - Every study is derived from the *same template*
  - Study specifics provided in a set of data files (created by the Designer), which define:
    - model structure
    - parameters (state-machines, transition activities , stochastic associations)
    - plug-ins with their executable (DLLs) and initialisation data files;
- Extensive bespoke code:
  - Integrated with the standard Möbius code base:
    - Möbius "thinks" that all modelled elements are the same (i.e. only replication used)
    - Initialisation establishes correspondence between the data structures maintained by Möbius and by the bespoke code;
    - "Reactivation" used to implement stochastic dependencies, i.e. restarting the activities affected by change of components state;
  - Maintains all meaningful data structures outside Möbius
    - Möbius sees the current and the next state of each element
    - All "activities" of state-machines are seen as deterministic (pseudo-random numbers generated by the bespoke code)
  - Plug-ins implement a well ***defined interfaces*** so that the engine can load and use the plug-ins ***uniformly*** (despite the differences in their functionality).
    - 3rd party code must be wrapped before integration

What can we do with these models

- Sensitivity analysis with respect to ***model parameters***
  - e.g. which parameters are the most critical (highest impact on likelihood of cascade failures), supports validation
- Does interdependency really matter? E.g. we can study a single CI:
  - as a ***part of a system*** of several interdependent CIs (including all known interdependencies)
  - on its own as a single infrastructure (i.e. ignoring many interdependencies with other CIs) as is typically done by the CI operators;
- Model the 'future'
  - Impact of climate change (a study for Network Rail in the UK is about to start)
  - Implications of various short- to mid- term trends
    - E.g. what would be the implications for the stability of the power supply if the proportion of renewable energy increases, say to 20-25% of the needs (a target set by the EC).
- Short term predictions (risk estimation)
  - E.g. given the current state of the network, what is the probability that a service will be disrupted at a particular point of consumption in the next ΔT.
- Test case and scenario generation:
  - ***training*** or demonstration purposes,
  - ***business continuity planning***;

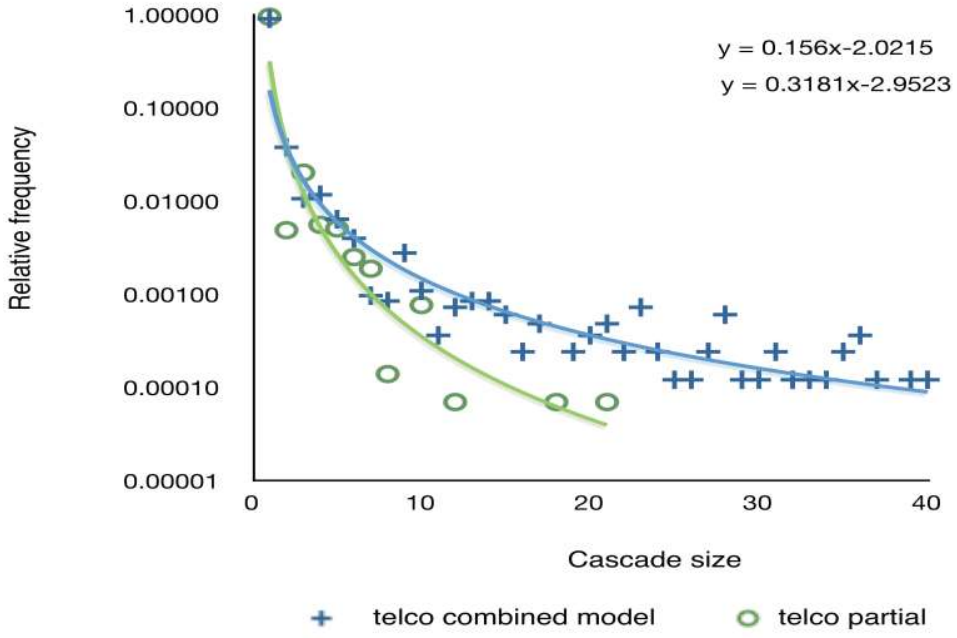
CITY UNIVERSITY LONDON

Results



CITY UNIVERSITY LONDON

Results (2)



CITY UNIVERSITY LONDON

TNO Data Analysis

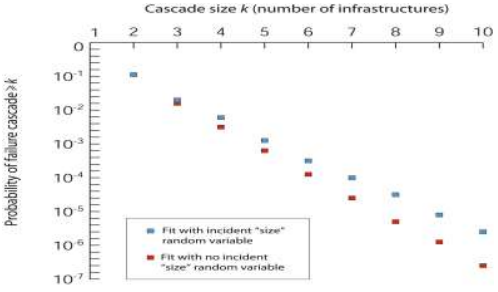
- Interdependency Analysis Models depend on many parameters
- TNO (The Netherlands) have collected data on 4000+ interdependency related incidents using public sources
  - incident frequency, and also frequency with which incidents in practice `cascade' between sectors.
- Statistical models fitted to the data. Models of:
  - chances of simple **cascade "size"** (e.g. cost, or number of sectors involved); or
  - including chances of which specific sectors are involved in the cascade;
  - Fitted parameters from these models inform numerical parameterization of conditional probabilities input to Mobius–based simulations.
- Using system wide emergent properties to give a reality check on the model

CITY UNIVERSITY LONDON

TNO Data Analysis (cont.)

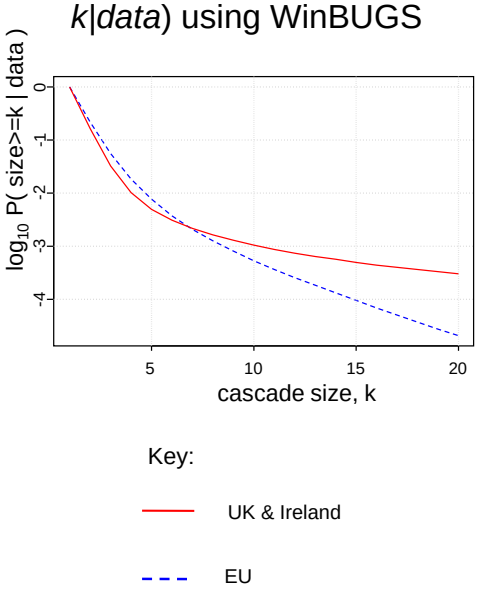
Incident data on cascade between infrastructures

- Analysis by CSR of dataset collected by TNO of UK and other European incidents
- Issues of completeness, representativeness etc.
- Estimated Cascade Size Probabilities



Bayesian Prediction

- E.g. Fitted P(Cascade size ≥ k|*data*) using WinBUGS



CITY UNIVERSITY LONDON

Conclusions

- We have built capability of undertaking complex interdependency studies
  - A methodology for interdependency analysis developed and tried
  - Tool support developed (continuous improvements)
- Results about modelling
  - impact of abstraction
    - how to represent coupling service-network-component
  - impact of sub-model fidelity, impact of scale
- Results about modelled system
  - loss vs. frequency, recovery wrt resource allocation
  - damage from geographical events (flooding scenario)
  - Impact of elements on system resilience
- Open issues related to methodology
  - how to do complex systems research, link with economic models
  - Issues of research methodology, testbeds, scaling, realism
    - realistic examples
    - lack of theories and generalisability

CITY UNIVERSITY LONDON

Questions

Thank you!

Impact Estimation: from questionnaires to interdependencies

Prof. Stefano Panzieri
Universita degli Studi, Roma Tre, Italy

Summary

S. Panzieri presented a mixed holistic/reductionistic approach to the analysis of critical infrastructure. The basis of this approach is the I/O inoperability model (IIM). It is claimed in the presentation that emergency is taken into a account by the holistic view of the system, which in its turn is based on the understanding of the behaviour of each sub-system. Similarly to the presentation from Prof. Zio, the failure process propagates throughout physical and geographical dependencies. The methodology is applied to a case study of interconnected infrastructures in the region of Rome.

Prof. Stefano Panzieri
Dept. Informatica e Automazione

SYSTEM METHODOLOGIES FOR CRITICAL INFRASTRUCTURES LABORATORY

Prof. Roberto Setola
University Campus Biomedico

Inpact estimation: from questionnaires to interdependencies

Prof. Stefano Panzieri

OUTLINE

The Holistic Approach

- Input Output Inoperability Model (Leontiev)
- Dynamics, Time Varying

Reductionistic Models

- CISIA
- Application: Regional Infrastructures

Mixed Holistic-Reductionistic modelling

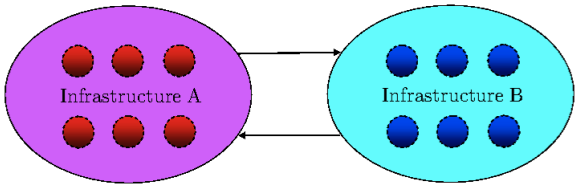
- MHR
- Applications: MICIE & CockpitCI

HOLISTIC VS. REDUCTIONISTIC APPROACHES

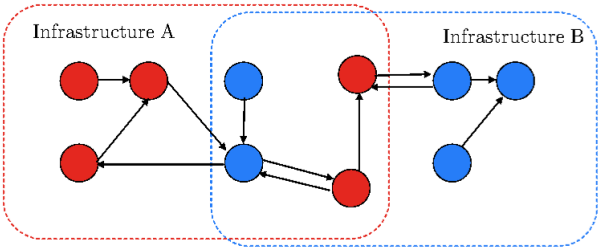
- **Holistic**: consider the CI as a whole (a single number as well as a vertical simulator)
- **Reductionistic**: decompose each CI in *accessible* components

Dependencies ***may*** be analysed:

- among systems
- among components



(a)



(b)

Reductionistic Simulation Vs. Federated Simulation

HOLISTIC APPROACH

(in the same simulation framework)

INPUT-OUTPUT INOPERATIVITY MODEL (LEONTIEF)

INPUT-OUTPUT INOPERABILITY MODEL

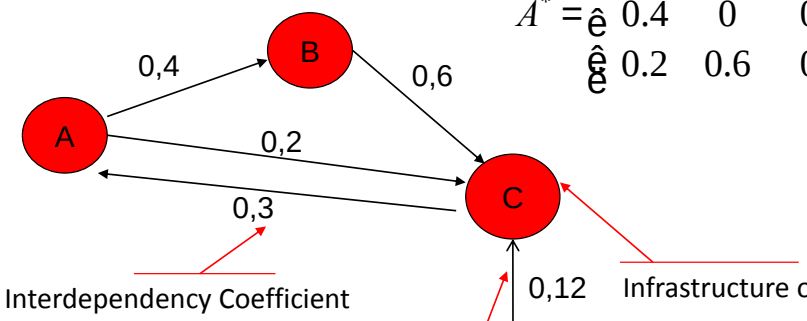
- Based on Leontief economics equilibrium theory (1966)
- Each infrastructure has an **inoperability** ***q***
  - Incapacity in % to correctly operate
- The model allows perturbations (e.g., terroristic attacks, faults) inducing inoperability, and evaluates their effects
- The model accounts for domino effects and loops
- It can be build using economic data or **questionnaires**

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.

AN EXAMPLE OF IIM

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



Interdependency Matrix. The coefficients represent the effect of the full inoperability of an infrastructure on another one.

Induced Perturbation. E.g., Terroristic attack, failure, earthquake, etc

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

DYNAMIC IIM MODEL

- A dynamic term is added to model the evolution until equilibrium is reached

$$q(t) = A^* q(t) + c^*(t) + B\frac{d[q(t)]}{dt}$$

- Set $B = -K^{-1}$ with K>0 diagonal:

$$\frac{d[q(t)]}{dt} = K(A^* - I)\ q(t) + Kc^*(t)$$

- Very often c*(t) is assumed to be constant.

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.

DISCRETE TIME IIM

- It is often useful to approximate in the discrete time

$$\frac{d[q(t)]}{dt} = K(A^* - I)\ q(t) + Kc^*(t) \qquad \dot{\mathbf{q}}(t) \simeq \frac{\mathbf{q}(t+T_s) - \mathbf{q}(t)}{T_s}$$

$$\mathbf{q}(k+1) = [T_s K A - T_s K + I]\mathbf{q}(k) + T_s K \mathbf{c}$$

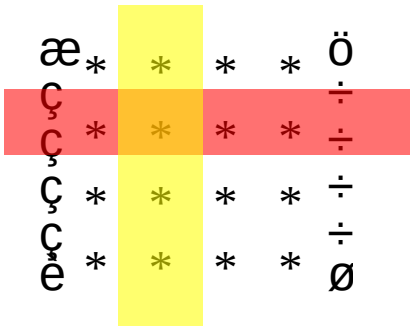
$$\mathbf{q}(k+1) = A^d \mathbf{q}(k) + \mathbf{c}^d$$

INTERDEPENDENCY INDICES

- How can we characterize the most vulnerable infrastructures? Those who may cause the greater damage if down?
- IIM model is suited for such kind of analysis:
  - **Inspecting A^d → direct** dependencies
  - **Inspecting $(I-A^d)^{-1}$ → indirect** dependencies

9

DIRECT DEPENDENCY INDICES



dependency index

$$d_i = \sum_{j=1}^{n} a_{ij}^d$$

Measures the robustness of an infrastructure with respect to the others

influence gain $r_i = \sum_{j=1}^{n} a_{ji}^d$

Measures the influence of an infrastructure with respect to the others

R. Setola, S. De Porcellinis and M. Sforna, Critical infrastructure dependency assessment using the input-output inoperability model, International Journal on Critical Infrastructure Protection, vol. 2(4), pp.170-178, 2009.

INDIRECT DEPENDENCY INDICES

$$(I - A^d)^{-1} = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix}$$

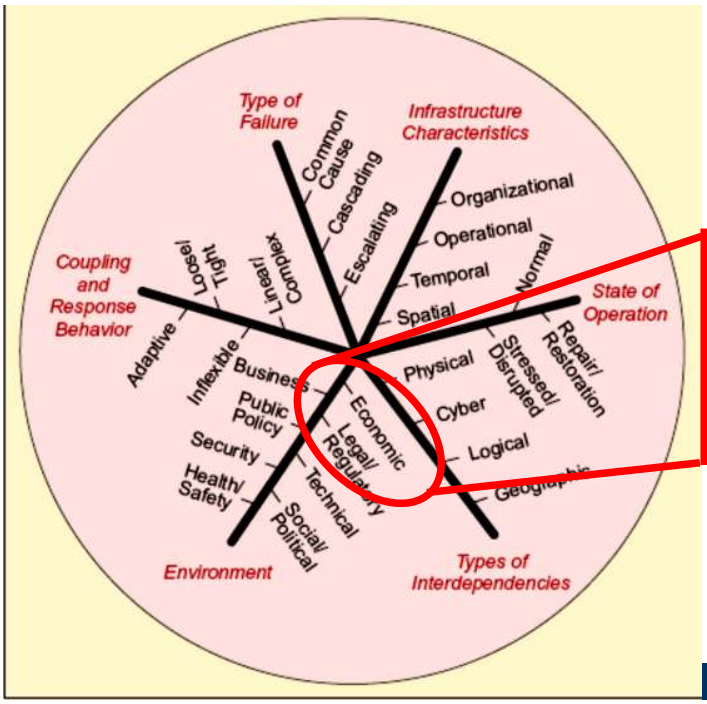
Overall dependency index $\bar{d}_i$

Overall influence gain $\bar{r}_i$

Vulnerability/influence is measured taking into account domino effects

R. Setola, S. De Porcellinis and M. Sforna, Critical infrastructure dependency assessment using the input-output inoperability model, International Journal on Critical Infrastructure Protection, vol. 2(4), pp.170-178, 2009.

INTERDEPENDENCY VS. ECONOMY

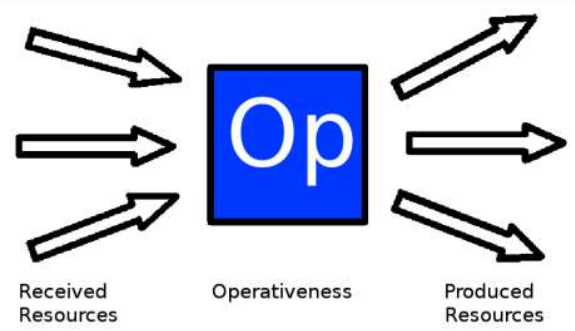


Economy is just an aspect

There is the need to consider other factors

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

AGENT-BASED IIM



Lower level entities (e.g., wire, power plant, etc.)

Each entity receives different resources

Resources influence **operativeness** (1-q) and operativeness influences produced resources

$$\begin{bmatrix}\dot{\mathbf{q}}(t)\\ \dot{\mathbf{r}}(t)\end{bmatrix} = \begin{bmatrix}-K & -K\Psi\Delta\\ -W\Phi & -W\end{bmatrix}\begin{bmatrix}\mathbf{q}(t)\\ \mathbf{r}(t)\end{bmatrix} + \begin{bmatrix}KA\\ W\Phi\end{bmatrix}\mathbf{1_n} + \begin{bmatrix}K\\ 0\end{bmatrix}\mathbf{c}^*(t)$$

G. Oliva, S. Panzieri and R. Setola, Agent Based Input-Output Interdependency Model, International Journal on Critical Infrastructure Protection, 2010

AGENT-BASED IIM

$$\begin{bmatrix}\dot{\mathbf{q}}(t)\\ \dot{\mathbf{r}}(t)\end{bmatrix} = \begin{bmatrix}-K & -K\Psi\Delta\\ -W\Phi & -W\end{bmatrix}\begin{bmatrix}\mathbf{q}(t)\\ \mathbf{r}(t)\end{bmatrix} + \begin{bmatrix}KA\\ W\Phi\end{bmatrix}\mathbf{1_n} + \begin{bmatrix}K\\ 0\end{bmatrix}\mathbf{c}^*(t)$$

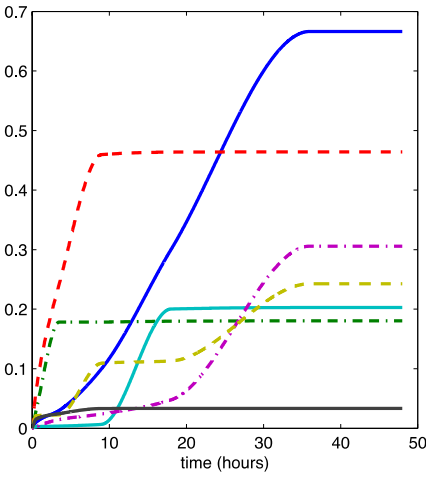
Φ : from in resources to inoperability
Δ : from in resources to out resources
Ψ: from operability to resources

It is possible to derive a standard IIM model by choosing

$$A^* = \Psi\Delta\Phi$$

Idea: ask the operators for quantities with a physical sense and combine them to assess the coefficients

TIME VARING IIM



$$\begin{bmatrix} q(k+1) \\ \tau(k+1) \end{bmatrix} = \begin{bmatrix} A^*(\tau) & 0 \\ T_s I & I \end{bmatrix} \begin{bmatrix} q(k) \\ \tau(k) \end{bmatrix} + \begin{bmatrix} I \\ 0 \end{bmatrix} c^d$$

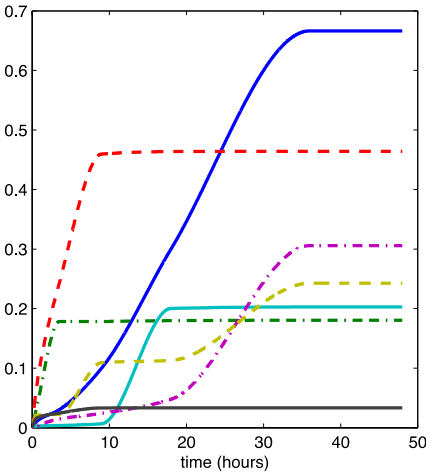
Time varying coefficients

Coefficients grow with time and duration of failures

$$t(k+1) = t(k) + T_s q(k)$$

F. Conte, G. Oliva and R. Setola, Time varying Input-Output inoperability model, International Journal on Infrastructure Systems, to appear.

COEFFICIENT BEHAVIOR



Linear + Constant

The coefficient grows up to a limit

Single Knee

Initially a buffer limits the impact. After the buffer is expired the dependency reaches its maximum value.

Double Knee

The buffer is used in different moments for instance some basic functions are granted (e.g., cooling for a nuclear power plant)

F. Conte, G. Oliva and R. Setola, Time varying Input-Output inoperability model, International Journal on Infrastructure Systems, to appear.

COEFFICIENT TUNING

- Experts were asked to provide the coefficients for 5 IIM models that represent scenarios where the duration on failures is about:
  - 1 hour
  - 6 hours
  - 12 hours
  - 24 hours
  - 48 hours
- The time dependency is transformed into a dependency on time and severity of failures scaling τ with the inoperability

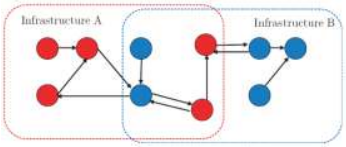
$$A(k) \rightarrow A(t(k))$$

REDUCTIONISTIC APPROACH

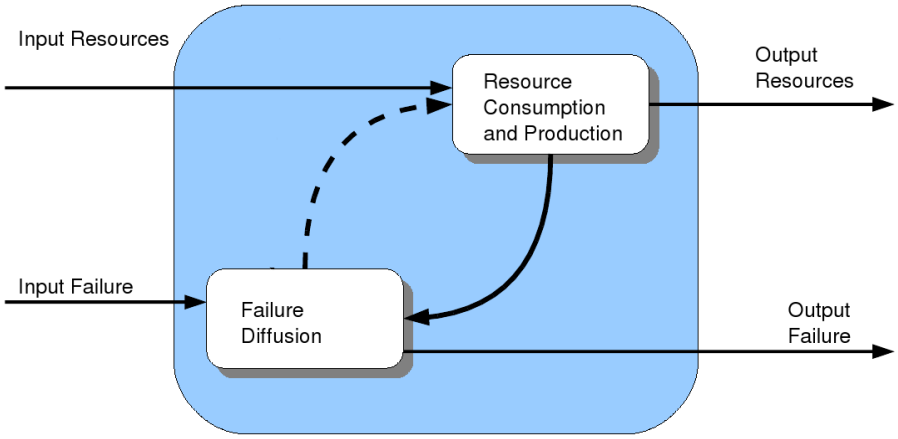
(in the same simulation framework)

CISIA

REDUCTIONISTIC MODEL: ENTITIES



1. Entities use and produce resources
2. Some of them can have faults
3. Resources and faults can propagate using different proximity concepts
4. The ability of producing resources is relate to their **Operative Level** that is function of input resources and failures



In a Reductionistic approach the simulation environment is one!

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 t	
Localization (geographic	
Subnets are inside MV po	

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

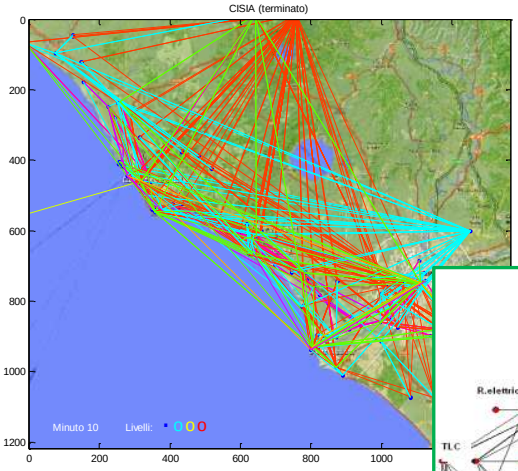
		Name	Nfl	Name	Nfl
Produces or provides resources ?		Current	**PR-1**		**PR-6**
Transports or forwards resources ?		Impedance	**PR-2**		**PR-7**
			PR-3		**PR-8**
No	**Yes** (use the pattern to the right to specify)		**PR-4**		**PR-9**
			PR-5		**PR-10**

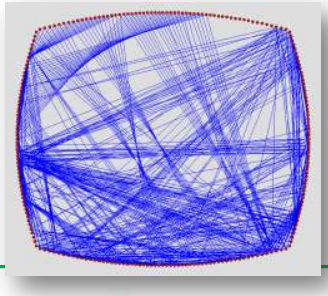
A CASE STUDY: INFRASTRUCTURES

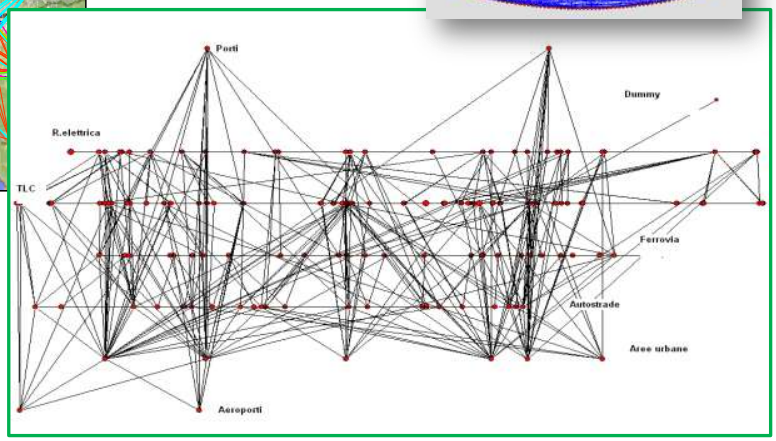
Infrastructure	Macro-components
Electric Grid	35
Urban areas	6
Airports	2

Ports	2
Railway	27
Highways	23
TLC	141

THE INTERDEPENDENCY NETWORKS







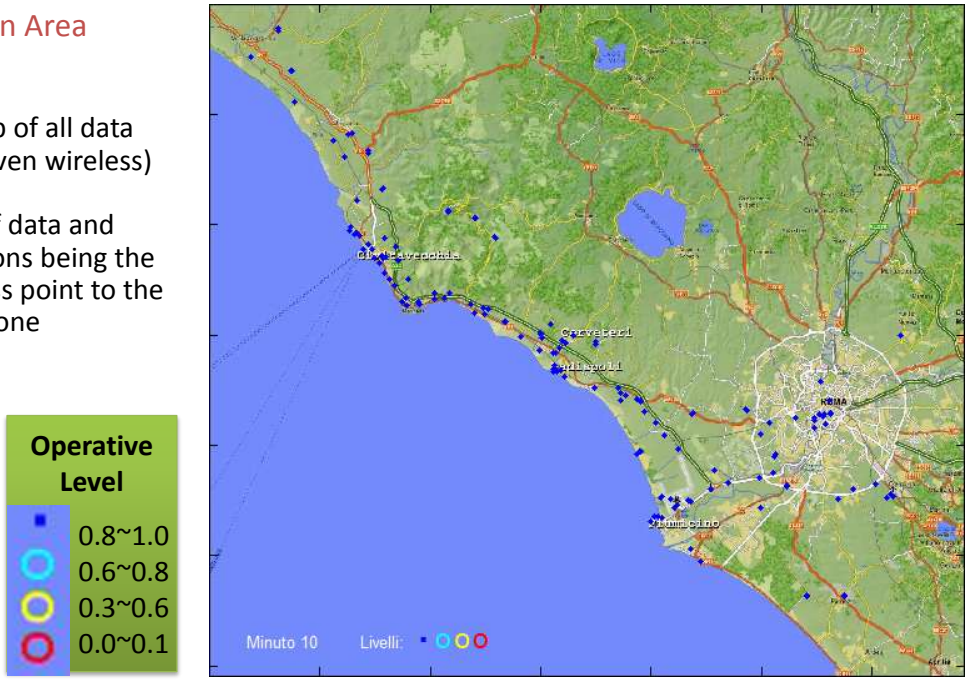
- 233 Entities
- 844 Link

THE WHOLE SMULATION

Sabotage of an Area Gateway

Immediate stop of all data connections (even wireless)

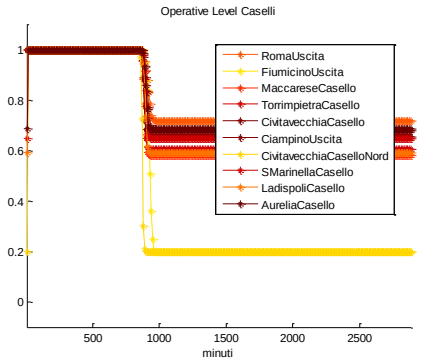
Inoperability of data and voice connections being the GTWA an access point to the national backbone

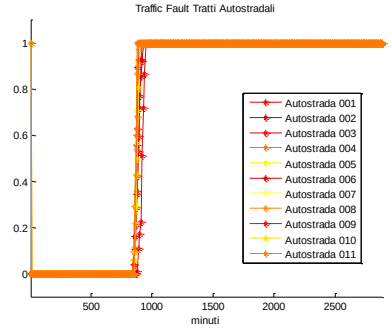


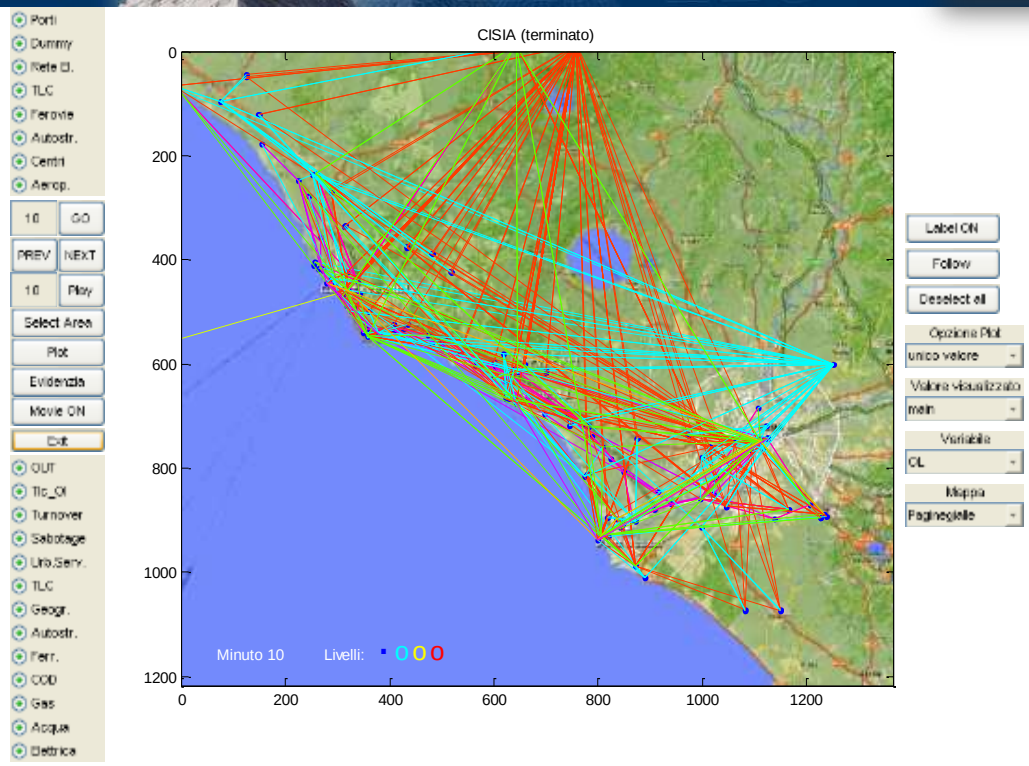
Operative Level

- 0.8~1.0
- 0.6~0.8
- 0.3~0.6
- 0.0~0.1

MOTORWAY FAULT

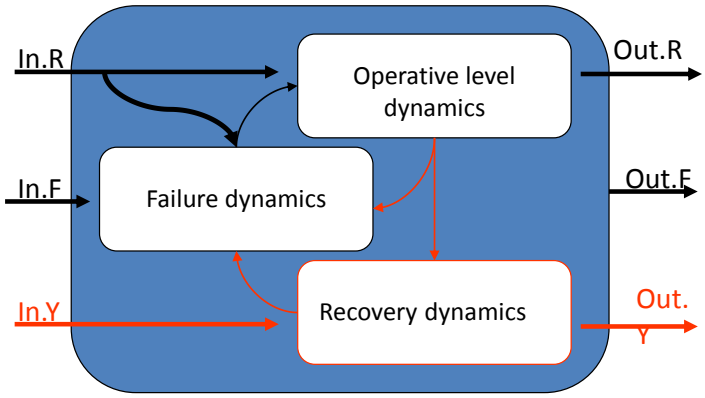






CISIA MODEL WITH RECOVERY DYNAMICS

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



Failure dynamics may be damped or inverted through the influence of recovery dynamcs.

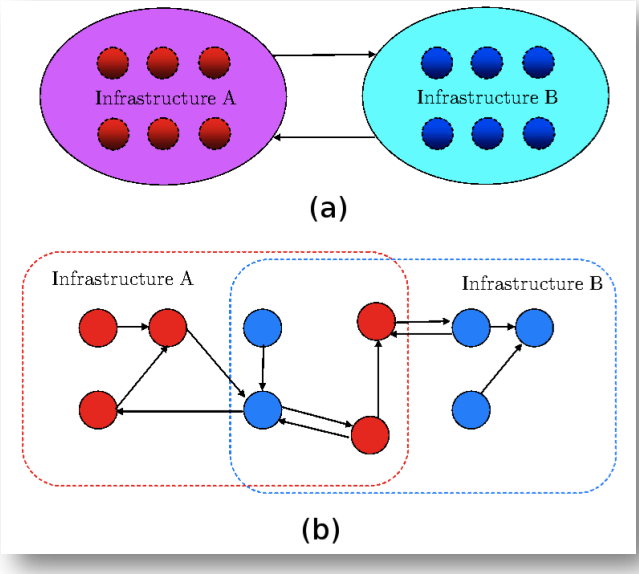
Recovery actions can have both endogenous or exogenous nature

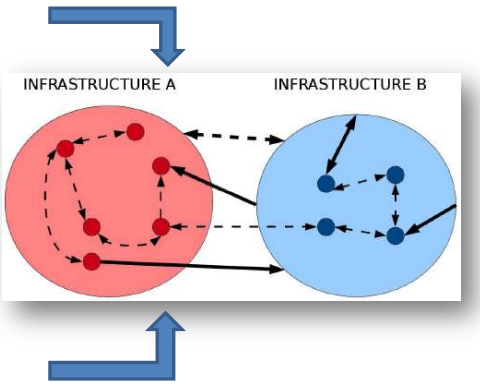
MIXED HOLISTIC REDUCTIONISTIC APPROACH

(maybe with different simulation frameworks)

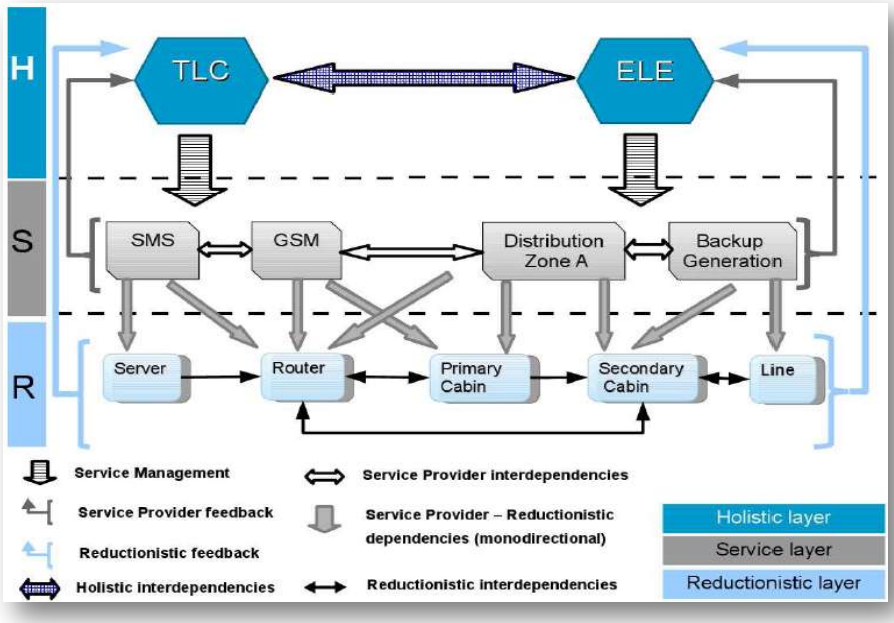
MHR

MOVING TO HOLISTIC-REDUCTIONISTIC





THE MIXED HOLISTIC-REDUCTIONISTIC MODELLING PERSPECTIVE

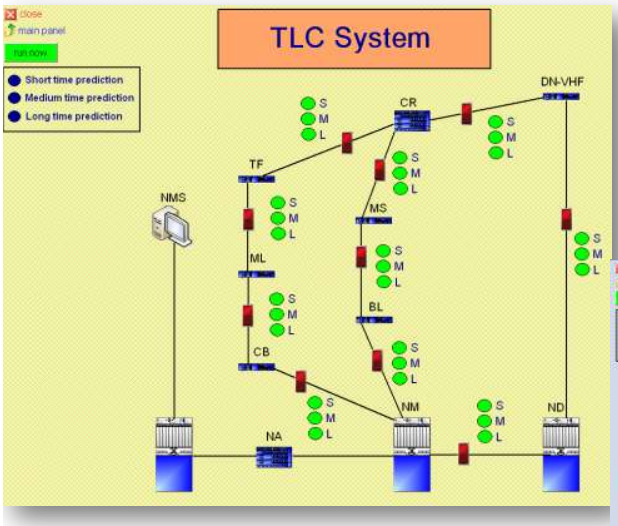


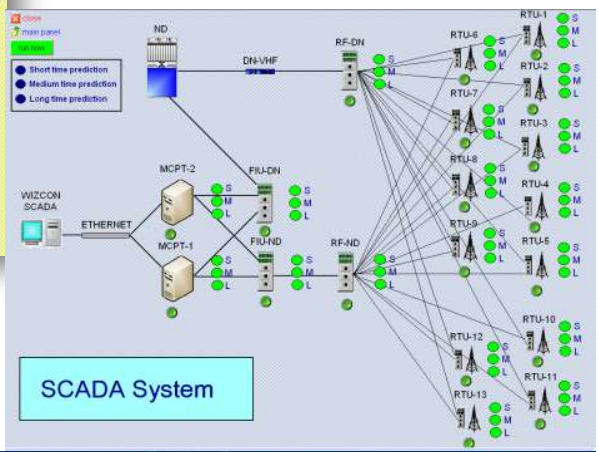
Behaviours (physical or logical or political) not emerging from R layer

Expressions of both Holistic and Reductionistic models

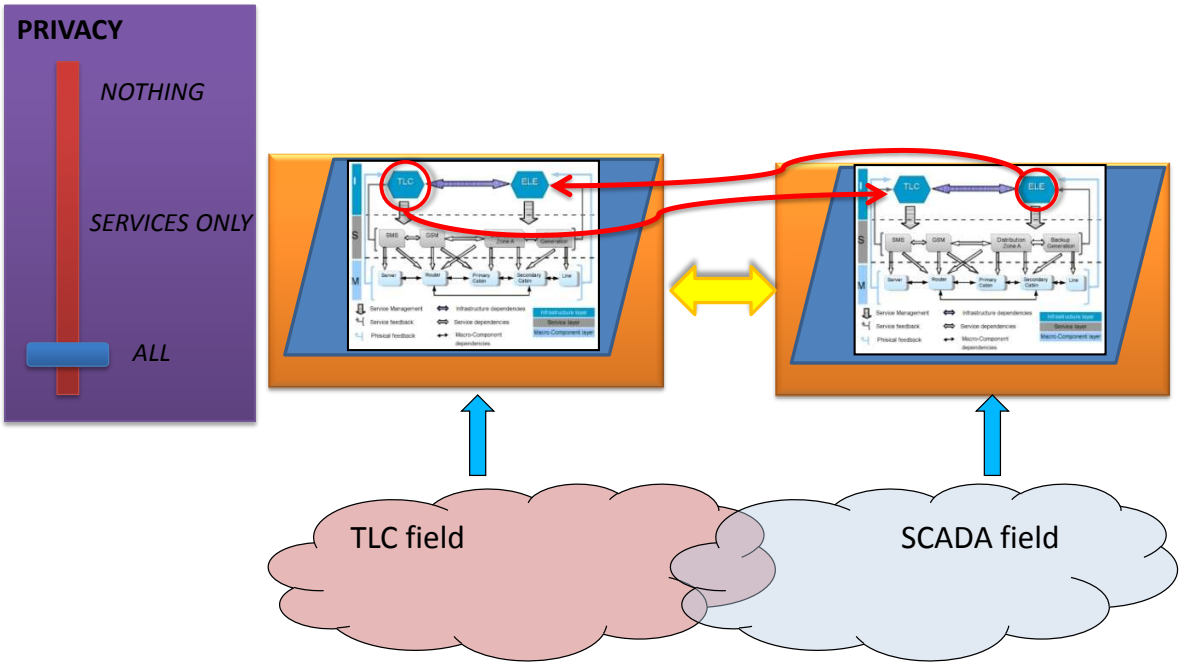
Intra-Inter-Infrastructure homogeneous layer capturing interdependencies

MICIE PROJECT: TLC + ELECTRIC SCADA SYSTEMS

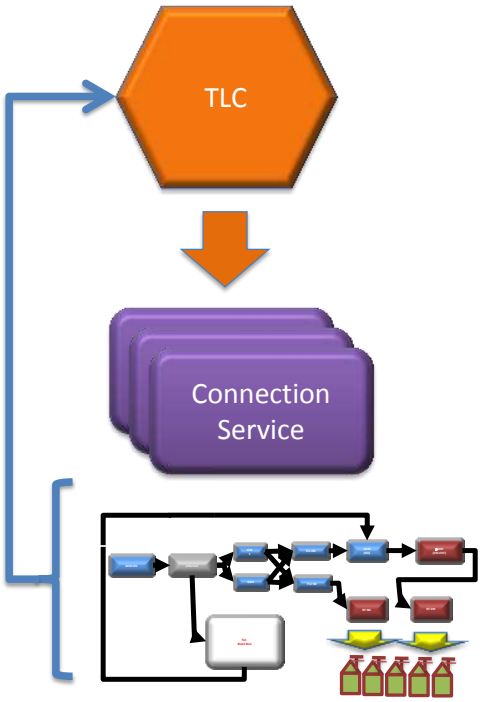




DISTRIBUTED SIMULATION



CONNECTION SERVICES MANAGEMENT

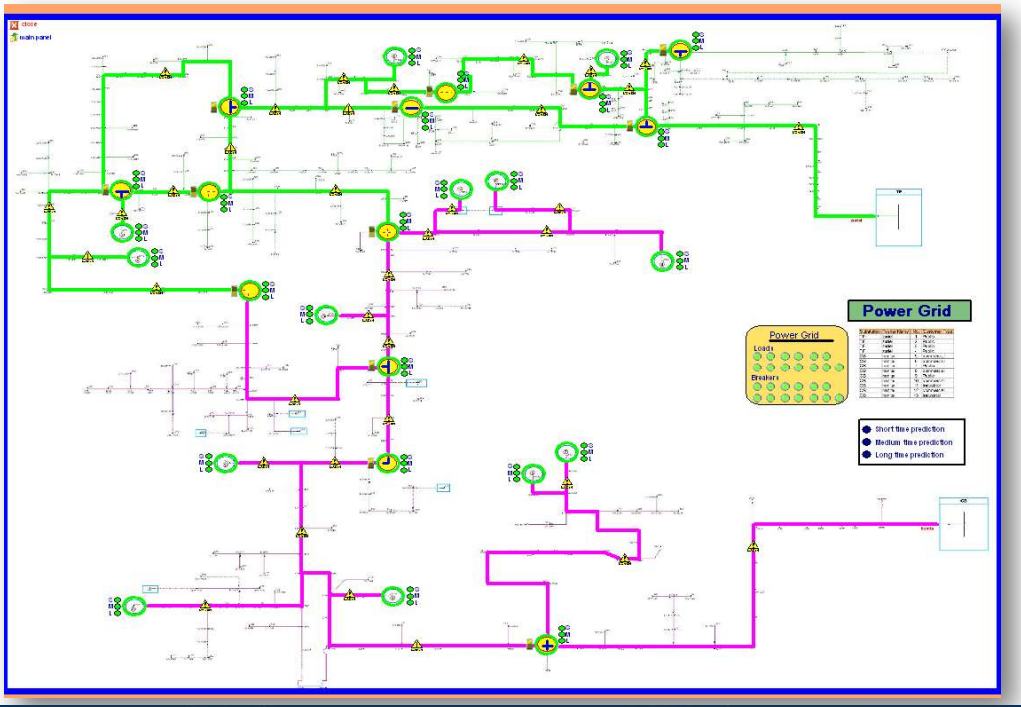


An approach for the Estimation of the QosS

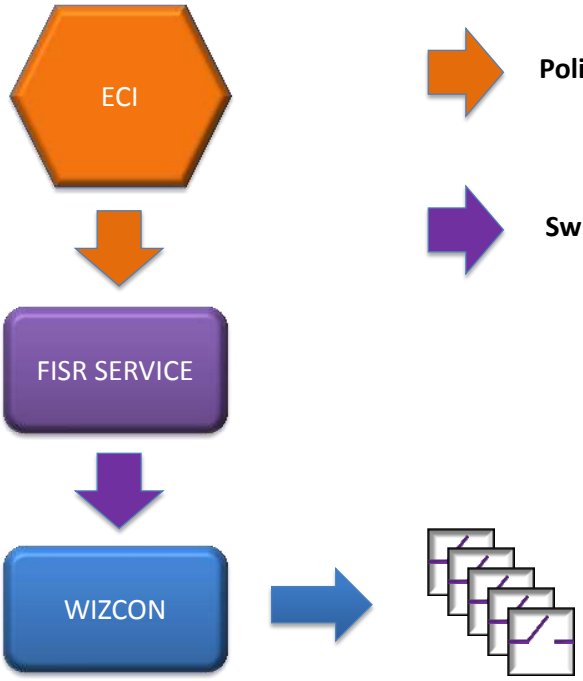
The logic has been implemented in the TLC holistic node

The TLC node uses the feedbacks from the reductionistic nodes

MICIE PROJECT: OPERATOR INTERFACE TO ELECTRIC GRID



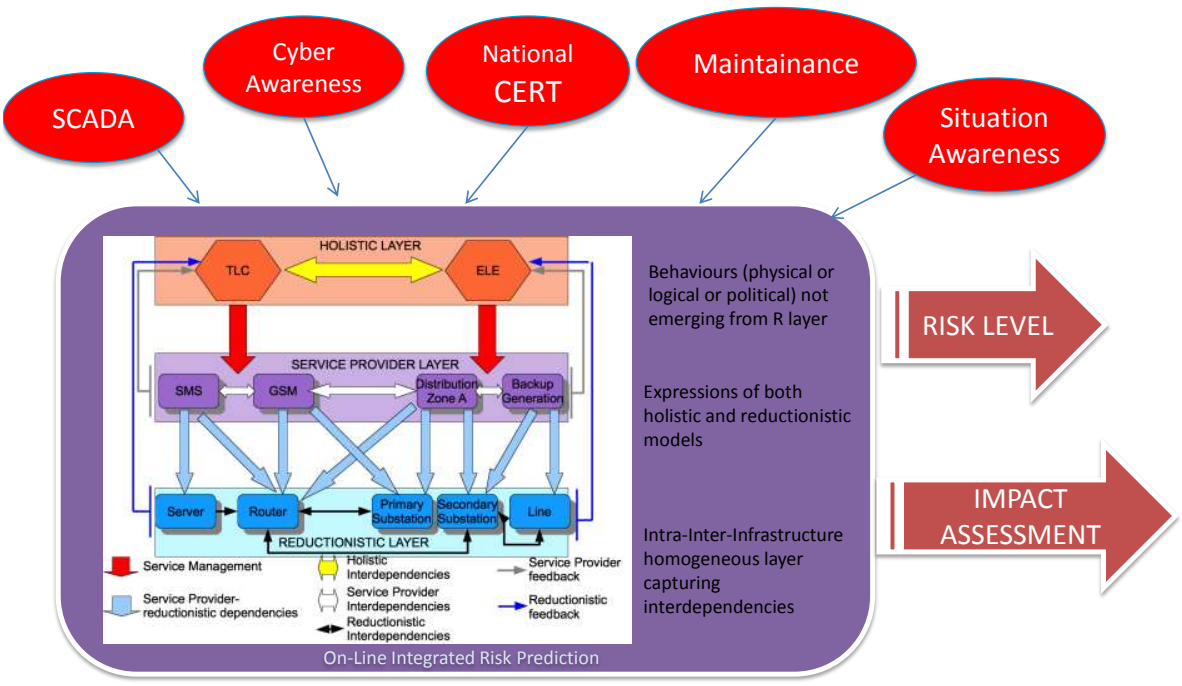
FISR SERVICE & SWITCHING LOGIC



Policy: Random/Incremental/Index Based

Switching logic: who and how

CYBERSECURITY ON SCADA: RISK PREDICTION, ANALYSIS AND REACTION TOOLS FOR CRITICAL INFRASTRUCTURES




Any question ?

Workshop wrap-up and conclusions

Roberto Filippini
EC, DG JRC
Unit G.6 Security Technology Assessment
email: roberto.filippini@jrc.ec.europa.eu

Summary

Concluding the workshop, a number of issues were outlined. The most important are the following three: 1) The importance of tailoring the system analysis to the user. The user maybe a designer, an operator, a policy maker etc. which means that diverse degree of details is required and diverse outcome. 2) The level of abstraction for managing complexity and heterogeneity and 3) The implementation of research goals to obtain resilience oriented design guidelines for next generation infrastructures.

Workshop wrap up and conclusions

Risk assessment and resilience

- Which representation
- Which analysis and quantities
- Which recommendations and to whom

Representation

- Sector-specific versus cross-sectors
- Abstraction level – functional vs. structural vs. physical
- Static or dynamic
- Deterministic versus probabilistic
- Nominal versus off-nominal behavior
- Threats – geographical, natural hazards, cyber…
- …

Analysis

- Structural
  - Topology-driven, interdependencies, criticalities, vulnerabilities
- Physical
  - dynamic models
- Cause-effect => risk
  - Failure mechanisms and data
  - Estimate costs
  - Protection/risk reduction measures
- Disturbance – misbehavior => resilience
  - Misbehavior is within the system variability
  - Control system response

Recommendations

- To whom?
  - Designer, operator, decision maker
- Structural recommendations
  - Reduce/remove criticalities
- Resilience informed design
  - Implement controls across dependencies
  - Harmonize local versus global assets
- Risk informed design

The way forward

- Which modeling and analysis framework
  - The JRC view
- ETH Risk centre as example of best practices
  - Envisage similar initiatives?

European Commission
EUR 25398 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: **Risk Assessment and Resilience for Critical Infrastructures**

Editors: Georgios Giannopoulos Roberto Filippini

Luxembourg: Publications Office of the European Union

2012 – 152 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424 (online), ISSN 1018-5593 (print)

ISBN 978-92-79-25589-2 (pdf)
ISBN 978-92-79-25590-8 (print)

doi:10.2788/35908

Abstract

Critical Infrastructures are essential for supporting everyday functions of modern societies. These functions depend on an extensive network of infrastructures that nowadays are highly connected, forming a complex mesh of interdependencies which facilitate exchange of services of various forms. The benefits from networking are accompanied by new threats and risks. Close cooperation of scientists and policy makers is paramount in order to establish the necessary methodologies and tools from threat identification for critical infrastructures to overall increase of their resilience.

LB-NA-25398-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new standards, methods and tools, and sharing and transferring its know-how to the Member States and international community.

Key policy areas include: environment and climate change; energy and transport; agriculture and food security; health and consumer protection; information society and digital agenda; safety and security including nuclear; all supported through a cross-cutting and multi-disciplinary approach.

Publications Office

ISBN 978-92-79-25589-2